SMART SECURITY SYSTEMS AND APPLICATIONS

ระบบรักษาความปลอดภัยอัจฉริยะและการประยุกต์ใช้

Prepared for:

สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์และระบบอัตโนมัติ
คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

Prepared by:

ชลดา ปานสง

คำนำ

ตำรา เรื่อง ระบบรักษาความปลอดภัยอัจฉริยะและการประยุกต์ใช้ (Smart Security Systems and Applications) เริ่มเรียบเรียงและนำมาใช้ประกอบการเรียนการสอนตั้งแต่ พ.ศ. 2567 สำหรับรายวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ ในหลักสูตรครุศาสตร์อุตสาหกรรมบัณฑิต สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์และระบบอัตโนมัติ โดยมีวัตถุประสงค์เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจ ประยุกต์ และมีทักษะด้านเทคโนโลยีระบบรักษาความปลอดภัยสมัยใหม่ เชื่อมโยงองค์ความรู้ทางทฤษฎีกับการปฏิบัติ และนำไปประยุกต์ใช้ในการออกแบบ พัฒนา ติดตั้ง และบำรุงรักษาระบบรักษาความปลอดภัยอัจฉริยะได้อย่างเหมาะสม โดยฉบับปรับปรุง พ.ศ. 2569 นี้ ผู้เรียบเรียงได้ทบทวน ปรับปรุง และเพิ่มเติมเนื้อหาจากฉบับเดิมให้มีความสมบูรณ์และสอดคล้องกับพัฒนาการของเทคโนโลยีในปัจจุบัน โดยจัดเนื้อหาเป็น 9 บท ได้แก่ ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยอัจฉริยะ อุปกรณ์เซนเซอร์สำหรับระบบรักษาความปลอดภัย ระบบกล้องโทรทัศน์วงจรปิด ระบบควบคุมการเข้าออก ระบบตรวจสอบอัตลักษณ์เพื่อความปลอดภัย ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัย อินเทอร์เน็ตของสรรพสิ่งสำหรับระบบรักษาความปลอดภัย ปัญญาประดิษฐ์สำหรับระบบรักษาความปลอดภัย และโครงงานระบบรักษาความปลอดภัยอัจฉริยะ เนื้อหาได้รับการเรียบเรียงจากพื้นฐานไปสู่การประยุกต์ใช้ โดยมุ่งเน้นการบูรณาการเซนเซอร์ ระบบเครือข่าย อินเทอร์เน็ตของสรรพสิ่ง ระบบคลาวด์ ปัญญาประดิษฐ์ และเทคโนโลยีที่เกี่ยวข้อง เพื่อให้ผู้เรียนสามารถนำองค์ความรู้ไปพัฒนาระบบรักษาความปลอดภัยอัจฉริยะที่สามารถประยุกต์ใช้ได้จริง

การจัดทำตำราฉบับนี้ ผู้เรียบเรียงได้ใช้เครื่องมือปัญญาประดิษฐ์เชิงกำเนิด (Generative AI) ได้แก่ ChatGPT และ Gemini เป็นเครื่องมือสนับสนุนในบางขั้นตอน โดยเฉพาะการออกแบบและปรับปรุงภาพประกอบ ตลอดจนการตรวจสอบและปรับการใช้ภาษาให้มีความถูกต้อง ชัดเจนและเหมาะสม ทั้งนี้ผู้เรียบเรียงได้ตรวจสอบและพิจารณาความถูกต้องของเนื้อหาทางวิชาการก่อนนำมาใช้ และขอขอบคุณเครื่องมือดังกล่าวที่มีส่วนสนับสนุนในการจัดทำให้มีความสมบูรณ์ยิ่งขึ้น ผู้เรียบเรียงขอกราบขอบพระคุณบิดา มารดา ครู อาจารย์ ตลอดจนขอขอบพระคุณครอบครัว ผู้ทรงคุณวุฒิ นักศึกษา และกัลยาณมิตรทุกท่าน ที่ได้ให้การสนับสนุน ให้คำแนะนำ และมีส่วนสำคัญในการจัดทำตำราฉบับนี้จนสำเร็จด้วยดี เหนือสิ่งอื่นใดผู้เรียบเรียงขอขอบคุณตนเอง ที่อดทนในวันที่เหนื่อยล้า พยายามในวันที่พบอุปสรรค และยังคงเลือกที่จะก้าวเดินต่อไป แม้ในวันที่ความสำเร็จยังมองเห็นไม่ชัดเจน หากปราศจากความมุ่งมั่นและความพยายามในวันวานเหล่านั้น ก็คงไม่มีตำราเล่มนี้ในวันนี้

ผู้เรียบเรียงหวังเป็นอย่างยิ่งว่าตำราเล่มนี้จะเป็นประโยชน์ต่อนักศึกษา อาจารย์ผู้สอน และผู้สนใจด้านระบบรักษาความปลอดภัยอัจฉริยะ สามารถใช้เป็นพื้นฐานในการพัฒนาความรู้ ทักษะทางวิชาชีพ การจัดทำโครงงาน และการต่อยอดองค์ความรู้ด้านวิศวกรรมอิเล็กทรอนิกส์ ระบบอัตโนมัติ และเทคโนโลยีดิจิทัล หากมีข้อบกพร่องหรือข้อเสนอแนะประการใด ผู้เรียบเรียงขอน้อมรับไว้ด้วยความขอบคุณ เพื่อนำไปใช้ในการปรับปรุงและพัฒนาตำราให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

ชลดา ปานสง

8 สิงหาคม 2569

สารบัญ

เรื่อง	หน้า
คำนำ	**ก**
สารบัญ	**ข**
บทที่ 1 ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยอัจฉริยะ	**1**
1.1 ความหมาย ความสำคัญ แนวคิดระบบรักษาความปลอดภัย	2
1.1.1 ความหมายของระบบรักษาความปลอดภัย	2
1.1.2 วิวัฒนาการของระบบรักษาความปลอดภัย	2
1.1.3 ความสำคัญของระบบรักษาความปลอดภัยอัจฉริยะ	3
1.1.4 หลักการทำงานของระบบรักษาความปลอดภัยอัจฉริยะ	4
1.2 องค์ประกอบของระบบรักษาความปลอดภัยอัจฉริยะ	5
1.2.1 อุปกรณ์ตรวจจับในระบบรักษาความปลอดภัย	5
1.2.2 อุปกรณ์ควบคุมในระบบรักษาความปลอดภัย	5
1.2.3 อุปกรณ์แจ้งเตือนในระบบรักษาความปลอดภัย	6
1.2.4 แหล่งพลังงานสารองในระบบรักษาความปลอดภัย	6
1.3 ประเภทของระบบรักษาความปลอดภัย	7
1.3.1 ระบบกล้องโทรทัศน์วงจรปิด	7
1.3.2 ระบบควบคุมการเข้า-ออก	8
1.3.3 ระบบเสียงประกาศ	11
1.3.4 ระบบแจ้งเตือนการบุกรุก	11
1.3.5 ระบบแจ้งเหตุเพลิงไหม้	12
1.4 มาตรฐานและกฎหมายที่เกี่ยวข้องกับระบบรักษาความปลอดภัย	13
1.4.1 ระดับที่ 1 พื้นที่รั้วและทางเข้าสถานที่	14
1.4.2 ระดับที่ 2 พื้นที่ระหว่างรั้วถึงอาคาร	15
1.4.3 ระดับที่ 3 พื้นที่ภายในห้องรับรอง	16
1.4.4 ระดับที่ 4 พื้นที่ภายในอาคารที่มีความสำคัญ	16
1.5 หลักความปลอดภัยในการปฏิบัติงานด้านไฟฟ้า	16
1.5.1 ข้อควรปฏิบัติเกี่ยวกับความปลอดภัยในการปฏิบัติงานไฟฟ้า	16
1.5.2 กฎ 5 ข้อความปลอดภัยในการปฏิบัติงานทางไฟฟ้า	21
1.5.3 ระดับการป้องกันของอุปกรณ์ไฟฟ้า	23
1.5.4 รหัสบ่งชี้ระดับความทนต่อสภาพแวดล้อมของอุปกรณ์ไฟฟ้า	24
1.5.5 อุปกรณ์ป้องกันอันตรายส่วนบุคคล	26
1.5.6 การปฐมพยาบาลเบื้องต้น	31

สารบัญ (ต่อ)

เรื่อง	หน้า
บรรณานุกรมบทที่ 1	35
สรุปสาระสำคัญของบทที่ 1	36
แบบฝึกหัดท้ายบทที่ 1	38
บทที่ 2 อุปกรณ์เซนเซอร์สำหรับระบบรักษาความปลอดภัย	**43**
2.1 หลักการทำงานของเซนเซอร์	45
2.1.1 ความหมายของเซนเซอร์	45
2.1.2 หลักการแปลงสัญญาณของเซนเซอร์	45
2.1.3 การจำแนกเซนเซอร์ตามแหล่งพลังงาน	46
2.1.4 สมรรถนะที่สำคัญของเซนเซอร์	46
2.2 เซนเซอร์ตรวจจับการเคลื่อนไหว	47
2.2.1 ลักษณะการใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหว	47
2.2.2 ส่วนประกอบของเซนเซอร์ตรวจจับการเคลื่อนไหว	48
2.2.3 หลักการทำงานของเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR	49
2.2.4 การต่อวงจรใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR	51
2.3 เซนเซอร์ตรวจจับประตูและหน้าต่าง	53
2.3.1 หลักการเบื้องต้นของเซนเซอร์ประตูและหน้าต่าง	53
2.3.2 ชนิดของเซนเซอร์ประตูและหน้าต่าง	53
2.3.3 หลักการทำงานของเซนเซอร์ประตูและหน้าต่าง	56
2.4 เซนเซอร์ตรวจจับควัน	61
2.4.1 ความหมายของเซนเซอร์ตรวจจับควัน	61
2.4.2 ประเภทของเซนเซอร์ตรวจจับควัน	61
2.4.3 โครงสร้างและหลักการทำงานของเซนเซอร์ตรวจจับควัน	63
2.4.4 การต่อวงจรใช้งานเซนเซอร์ตรวจจับควัน	66
2.5 เซนเซอร์ตรวจจับก๊าซ	70
2.5.1 ความหมายของเซนเซอร์ตรวจจับก๊าซ	70
2.5.2 ชนิดของเซนเซอร์ตรวจจับก๊าซ	70
2.5.3 โครงสร้างของเซนเซอร์ตรวจจับก๊าซ	73
2.5.4 วงจรการใช้งานเซนเซอร์ตรวจจับก๊าซ	77
2.6 เซนเซอร์ตรวจจับเปลวไฟ	81
2.6.1 คุณสมบัติของคลื่นแม่เหล็กไฟฟ้าที่ตรวจพบจากเปลวไฟ	82
2.6.2 ชนิดของเซนเซอร์ตรวจจับเปลวไฟ	83
2.6.3 โครงสร้างของเซนเซอร์ตรวจจับเปลวไฟ	85

สารบัญ (ต่อ)

เรื่อง	หน้า
2.6.4 หลักการทำงานของเซนเซอร์ตรวจจับเปลวไฟ	88
2.6.5 วงจรใช้งานเซนเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด	90
บรรณานุกรมบทที่ 2	93
สรุปสาระสำคัญของบทที่ 2	96
แบบฝึกหัดท้ายบทที่ 2	98
บทที่ 3 ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ	**102**
3.1 พื้นฐานของระบบกล้องวงจรปิด	104
3.1.1 ความหมายของกล้องโทรทัศน์วงจรปิด	104
3.1.2 ความเป็นมาของกล้องโทรทัศน์วงจรปิด	104
3.1.3 องค์ประกอบของระบบกล้องโทรทัศน์วงจรปิด	107
3.1.4 ระบบเครือข่ายคอมพิวเตอร์ในระบบกล้องวงจรปิด	107
3.1.5 มาตรฐาน Ingress Protection Rating	112
3.1.6 หน่วยวัดความละเอียดภาพ	112
3.2 ประเภทของกล้องโทรทัศน์วงจรปิด	114
3.2.1 กล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	114
3.2.2 กล้องโทรทัศน์วงจรปิดระบบดิจิทัล	116
3.3 อุปกรณ์ของระบบกล้องโทรทัศน์วงจรปิด	117
3.3.1 กล้องโทรทัศน์วงจรปิด	117
3.3.2 เซ็นเซอร์รับภาพ	119
3.3.3 เลนส์ของกล้องโทรทัศน์วงจรปิด	119
3.3.4 เครื่องบันทึกภาพ	125
3.3.5 ฮาร์ดดิสก์สำหรับงานระบบกล้องโทรทัศน์วงจรปิด	129
3.3.6 จอภาพ	135
3.3.7 สายนำสัญญาณ	135
3.3.8 เครื่องสลับภาพ	144
3.3.9 เครื่องแบ่งสัญญาณภาพ	145
3.3.10 อุปกรณ์แปลงสัญญาณภาพ	146
3.3.11 อุปกรณ์เชื่อมต่อระบบเครือข่าย	147
3.3.12 ขั้วต่อสายสัญญาณในงานกล้องโทรทัศน์วงจรปิด	148
3.3.13 อุปกรณ์เสริมในงานกล้องโทรทัศน์วงจรปิด	150
3.4 การออกแบบและติดตั้งระบบกล้องโทรทัศน์วงจรปิด	153
3.4.1 เครื่องมือพื้นฐานสำหรับงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด	153

สารบัญ (ต่อ)

เรื่อง **หน้า**

3.4.2 การสำรวจพื้นที่การติดตั้งระบบกล้องโทรทัศน์วงจรปิด 155
3.4.3 การเขียนแบบงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด 156
3.4.4 การคำนวณระยะเลนส์ของกล้องโทรทัศน์วงจรปิด 159
3.4.5 การคำนวณความกว้างของพื้นที่ที่กล้องมองเห็นได้ 161
3.4.6 การคำนวณความจุฮาร์ดดิสก์และแบนด์วิดท์ของระบบกล้องโทรทัศน์วงจรปิด 164
3.4.7 สรุปการเลือกอุปกรณ์สำหรับการติดระบบกล้องโทรทัศน์วงจรปิด 166
3.5 โปรแกรมบริหารจัดการระบบกล้องโทรทัศน์วงจรปิด 167
3.5.1 ความหมายของโปรแกรมบริหารจัดการ 167
3.5.2 ซอฟแวร์ Central Management System (CMS) 168
3.5.3 การติดตั้งโปรแกรมบริหารจัดการ 169
3.5.4 การทดสอบการใช้งานโปรแกรมบริหารจัดการ 172
3.5.5 เมนูหลักของโปรแกรม CMS 176
3.6 การแก้ไขปัญหาและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด 177
3.6.1 อาการภาพดับหรือไม่เกิดภาพ 177
3.6.2 อาการภาพเป็นคลื่น 178
3.6.3 อาการภาพเบลอ 179
3.6.4 การบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด 180
บรรณานุกรมบทที่ 3 182
สรุปสาระสำคัญของบทที่ 3 184
แบบฝึกหัดท้ายบทที่ 3 189

บทที่ 4 ระบบควบคุมการเข้าออก 197
4.1 ความรู้พื้นฐานของระบบควบคุมการเข้าออก 199
4.1.1 ความหมายของระบบควบคุมการเข้าออก 199
4.1.2 ความสำคัญของระบบควบคุมการเข้าออก 199
4.1.3 หลักการทำงานของระบบควบคุมการเข้าออก 198
4.1.4 องค์ประกอบพื้นฐานของระบบควบคุมการเข้าออก 200
4.1.5 ความแตกต่างระหว่าง Authentication, Authorization และ Access Control 201
4.1.6 คุณลักษณะของระบบควบคุมการเข้าออกสมัยใหม่ 202
4.2 ระบบอาร์เอฟไอดี 202
4.2.1 ความหมายของ RFID 202
4.2.2 องค์ประกอบของ RFID 203

สารบัญ (ต่อ)

เรื่อง	หน้า
4.2.3 ประเภทของระบบ RFID	207
4.2.4 มาตรฐาน RFID	211
4.2.5 หลักการทำงานของระบบ RFID	213
4.2.6 หลักการทำงานของ RFID มาตรฐาน ISO14443 Type A	226
4.2.7 โครงสร้างของโมดูล RFID รุ่น RC522	231
4.3 เทคโนโลยีการสื่อสารระยะใกล้	233
4.3.1 ความหมายของระบบ NFC	233
4.3.2 ความรู้พื้นฐานของเทคโนโลยี NFC	234
4.3.3 หลักการทำงานของ NFC	235
4.3.4 โครงสร้างระบบของ NFC	236
4.3.5 โหมดการทำงานของ NFC	236
4.3.6 ประเภทของอุปกรณ์ NFC และลักษณะการใช้งาน	237
4.4 ระบบล็อกประตูด้วยคิวอาร์โค้ด	240
4.4.1 หลักการพื้นฐานของ QR Code	240
4.4.2 สถาปัตยกรรมของระบบ QR Code Door Lock	241
4.4.3 หลักการทำงานของระบบ QR Code Door Lock	242
4.4.4 แบบจำลองการตรวจสอบสิทธิ์	243
4.4.5 กลไกการทำงานของระบบล็อกประตูไฟฟ้า	245
4.4.6 การบันทึกและติดตามการเข้าออก	246
4.4.7 ความมั่นคงปลอดภัยของระบบ QR Code Door Lock	246
บรรณานุกรมบทที่ 4	248
สรุปสาระสำคัญของบทที่ 4	251
แบบฝึกหัดท้ายบทที่ 4	255
บทที่ 5 ระบบตรวจสอบอัตลักษณ์เพื่อความปลอดภัย	**264**
5.1 ระบบรักษาความปลอดภัยด้วยการยืนยันตัวตนด้วยลายนิ้วมือ	265
5.1.1 พื้นฐานของระบบตรวจสอบลายนิ้วมือ	266
5.1.2 หลักการทำงานของเครื่องสแกนลายนิ้วมือ	266
5.1.3 ประเภทของเซนเซอร์ลายนิ้วมือ	267
5.1.4 หลักการตรวจสอบลายนิ้วมือด้วยจุดลักษณะเฉพาะ	271
5.1.5 กระบวนการสแกนและตรวจสอบลายนิ้วมือ	274
5.1.6 การแปลงลายนิ้วมือเป็นข้อมูลดิจิทัลสำหรับการตรวจสอบอัตลักษณ์	275
5.1.7 การใช้งานเซนเซอร์สแกนลายนิ้วมือ	276
5.1.8 การประยุกต์ใช้งานเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์	280

สารบัญ (ต่อ)

เรื่อง **หน้า**

5.2 ระบบรักษาความปลอดภัยด้วยการยืนยันตัวตนด้วยใบหน้า 281
5.2.1 หลักการตรวจสอบและจดจำใบหน้า 282
5.2.2 กระบวนการระบบจดจำใบหน้า 285
5.2.3 วิธีการตรวจจับใบหน้าด้วย OpenCV และ Haar Cascade 286
5.2.4 ความปลอดภัยของระบบตรวจสอบใบหน้า 290
5.2.5 ข้อดีและข้อจำกัดของระบบสแกนใบหน้า 290
5.3 ระบบจดจำเสียง 291
5.3.1 ความหมายของระบบจดจำเสียง 291
5.3.2 ประเภทของระบบจดจำเสียง 292
5.3.3 รูปแบบการรู้จำเสียง 292
5.3.4 หลักการทำงานของระบบจดจำเสียง 294
5.3.5 สถาปัตยกรรมของระบบรู้จำเสียงสมัยใหม่ 294
บรรณานุกรมบทที่ 5 296
สรุปสาระสำคัญของบทที่ 5 298
แบบฝึกหัดท้ายบทที่ 5 301

บทที่ 6 ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัย 307
6.1 ความรู้เบื้องต้นเกี่ยวกับเครือข่ายในระบบรักษาความปลอดภัย 310
6.1.1 ความหมายของเครือข่ายในระบบรักษาความปลอดภัย 310
6.1.2 ความสำคัญของระบบเครือข่ายในระบบรักษาความปลอดภัย 311
6.1.3 องค์ประกอบของเครือข่ายในระบบรักษาความปลอดภัย 311
6.2 โครงสร้างการเชื่อมต่อเครือข่าย 314
6.2.1 โทโพโลยีแบบบัส 314
6.2.2 โทโพโลยีแบบดาว 315
6.2.3 โทโพโลยีแบบวงแหวน 315
6.2.4 โทโพโลยีแบบตาข่าย 315
6.2.5 โทโพโลยีแบบผสม 316
6.3 ชุดโปรโตคอล Transmission Control Protocol/Internet Protocol (TCP/IP) 316
6.3.1 ความหมายของโปรโตคอล 316
6.3.2 แนวคิดของการแบ่งชั้นโปรโตคอล 316
6.3.3 หลักการสำคัญของ Protocol Layering 317
6.3.4 การเชื่อมต่อเชิงตรรกะระหว่างชั้น 318
6.3.5 สถาปัตยกรรมของชุดโปรโตคอล TCP/IP 318
6.3.6 บทบาทของ Host, Switch และ Router ใน TCP/IP 322

สารบัญ (ต่อ)

เรื่อง	หน้า
6.3.7 การสื่อสารแบบ End-to-End และ Hop-to-Hop	323
6.3.8 หน่วยข้อมูลในแต่ละชั้นการสื่อสาร	323
6.3.9 การห่อหุ้มข้อมูลและการถอดห่อหุ้มข้อมูล	323
6.4 IP Address และ Subnet	324
6.4.1 IP Address	324
6.4.2 การกำหนด IP Address	325
6.4.3 ส่วนประกอบของ IPv4 Address	326
6.5 เครือข่ายท้องถิ่น	329
6.5.1 องค์ประกอบของเครือข่าย LAN	329
6.5.2 คุณลักษณะของ LAN ในระบบรักษาความปลอดภัย	332
6.6 เครือข่ายบริเวณกว้าง	333
6.6.1 องค์ประกอบของเครือข่าย WAN	333
6.6.2 โครงข่ายแกนกลางของ WAN	334
6.6.3 สื่อส่งสัญญาณที่ใช้ในโครงข่าย WAN	335
6.6.4 โปรโตคอลกำหนดเส้นทาง	336
6.7 เทคโนโลยีเครือข่ายแบบใช้สาย	338
6.7.1 ความหมายและวิวัฒนาการของ Ethernet	338
6.7.2 สถาปัตยกรรมของ Ethernet	339
6.7.3 Ethernet Frame Format	341
6.7.4 หลักการทำงานของ CSMA/CD	342
6.7.5 Ethernet Switching	345
6.8 ไวไฟ (Wi-Fi)	348
6.8.1 Wi-Fi และ Wireless	348
6.8.2 สถาปัตยกรรม Wi-Fi	349
6.8.3 วิธีเข้าถึงสื่อของ Wi-Fi	350
6.8.4 การรักษาความมั่นคงปลอดภัยของ Wi-Fi	350
6.9 Zigbee	351
6.9.1 ย่านความถี่และอัตราการรับส่งข้อมูล	351
6.9.2 การออกแบบวงจรความถี่วิทยุสำหรับอุปกรณ์ Zigbee	353
6.9.3 หลักการทำงานของ Zigbee	353
6.9.4 คุณลักษณะของเครือข่าย Zigbee	354
6.9.5 รูปแบบโครงสร้างเครือข่ายของ Zigbee	354
6.9.7 ประเภทของอุปกรณ์ในเครือข่าย Zigbee	356

สารบัญ (ต่อ)

เรื่อง	หน้า
6.10 Z-Wave	357
6.10.1 คุณลักษณะของ Z-Wave	357
6.10.2 สถาปัตยกรรมเครือข่าย Z-Wave	357
6.10.3 โหนดในเครือข่าย Z-Wave	359
6.10.4 รูปแบบการทำงานของอุปกรณ์เครือข่าย Z-Wave	361
6.11 LoRaWAN	362
6.11.1 ความหมายของ LoRaWAN	362
6.11.2 หลักการทำงานของ LoRaWAN	362
6.11.3 คุณลักษณะของ LoRaWAN	363
6.11.4 คลาสของอุปกรณ์ LoRaWAN	363
6.11.5 สถาปัตยกรรมเครือข่าย LoRaWAN	364
6.11.6 โครงสร้างพื้นฐานของเครือข่าย LoRaWAN	364
6.11.7 ความปลอดภัยของ LoRaWAN	366
6.11.8 การประยุกต์ใช้ LoRaWAN ในระบบรักษาความปลอดภัยอัจฉริยะ	366
6.12 เครือข่ายท้องถิ่นเสมือน	367
6.12.1 หลักการทำงานของ VLAN	367
6.12.2 VLAN กับ Subnet	368
6.12.3 การกำหนดสมาชิกของ VLAN	369
6.12.4 Access Port และ Trunk Port	369
6.12.5 มาตรฐาน IEEE 802.1Q	370
6.12.6 การประยุกต์ใช้ VLAN ในระบบรักษาความปลอดภัยอัจฉริยะ	371
6.12.7 ประโยชน์ของ VLAN ต่อระบบรักษาความปลอดภัยอัจฉริยะ	373
6.12.8 ข้อจำกัดของ VLAN	373
6.12.9 แนวทางการออกแบบ VLAN อย่างปลอดภัย	373
6.13 Power over Ethernet (PoE)	374
6.13.1 ความหมายของ Power over Ethernet (PoE)	374
6.13.2 หลักการทำงานของ PoE	374
6.13.3 องค์ประกอบของระบบ PoE	375
6.13.4 มาตรฐานของ PoE	376
6.13.5 การประยุกต์ใช้ PoE ในระบบรักษาความปลอดภัยอัจฉริยะ	376
บรรณานุกรมบทที่ 6	378
สรุปสาระสำคัญของบทที่ 6	380
แบบฝึกหัดท้ายบทที่ 6	384

สารบัญ (ต่อ)

เรื่อง	หน้า
บทที่ 7 อินเทอร์เน็ตของสรรพสิ่งสำหรับระบบรักษาความปลอดภัย	**393**
7.1 พื้นฐานของ Internet of Things (IoT)	395
7.1.1 องค์ประกอบพื้นฐานของระบบ IoT	395
7.1.2 หลักการทำงานของระบบ IoT	397
7.1.3 ความสำคัญของ IoT ในระบบรักษาความปลอดภัยอัจฉริยะ	398
7.2 ไมโครคอนโทรลเลอร์ Arduino	398
7.2.1 แพลตฟอร์ม Arduino	398
7.2.2 สถาปัตยกรรมของ Arduino Uno R3	401
7.2.3 ซอฟต์แวร์ Arduino IDE	404
7.2.4 การเชื่อมต่อโมดูล RC522 RFID กับไมโครคอนโทรลเลอร์ Arduino	407
7.2.5 การติดตั้งไลบรารี MFRC522	408
7.2.6 การตรวจสอบการเชื่อมต่อและการอ่านข้อมูลของ MFRC522	410
7.2.7 การประยุกต์ใช้แท็ก RFID ควบคุมการเปิดปิดอุปกรณ์	411
7.3 NodeMCU ESP8266	412
7.3.1 ประเภทของโมดูลและบอร์ดพัฒนา ESP8266	412
7.3.2 โครงสร้างของ ESP8266	413
7.3.3 การเชื่อมต่อ ESP8266 กับโปรแกรม Arduino IDE	416
7.3.4 การเชื่อมต่อโมดูล RFID RC522 กับ ESP8266	418
7.3.5 การพัฒนาเว็บเซิร์ฟเวอร์ด้วย ESP8266	420
7.4 Raspberry Pi	427
7.4.1 ความหมายและวิวัฒนาการของ Raspberry Pi	427
7.4.2 สถาปัตยกรรมและองค์ประกอบของ Raspberry Pi	429
7.4.3 คุณสมบัติของ Raspberry Pi	431
7.4.3 GPIO ของ Raspberry Pi	433
7.5 แพลตฟอร์มคลาวด์เพื่อใช้ในระบบความปลอดภัยอัจฉริยะ	435
7.5.1 ความหมายของ Cloud Platform	435
7.5.2 องค์ประกอบของ Cloud Platform	435
7.5.3 รูปแบบการให้บริการของ Cloud Platform	436
7.5.4 บทบาทของ Cloud Platform ในระบบความปลอดภัยอัจฉริยะ	440
7.6 REST API	442
7.6.1 หลักการทำงานของ REST API	442
7.6.2 LINE Messaging API	444
7.6.3 การเชื่อมต่อ Google Cloud และ Google Sheets	450

สารบัญ (ต่อ)

เรื่อง	หน้า
บรรณานุกรมบทที่ 7	458
สรุปสาระสำคัญของบทที่ 7	460
แบบฝึกหัดท้ายบทที่ 7	464
บทที่ 8 ปัญญาประดิษฐ์สำหรับระบบรักษาความปลอดภัย	**470**
8.1 ความรู้พื้นฐานของปัญญาประดิษฐ์	472
8.1.1 ความหมายของปัญญาประดิษฐ์ในระบบรักษาความปลอดภัยอัจฉริยะ	472
8.1.2 บทบาทของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ	473
8.1.3 เทคโนโลยี AI ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ	473
8.1.4 การทำงานของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ	474
8.1.5 ข้อดีของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ	475
8.1.6 ข้อจำกัดและประเด็นด้านจริยธรรมของ AI	475
8.2 การเรียนรู้ของเครื่อง	476
8.2.1 ความหมายของการเรียนรู้ของเครื่อง	476
8.2.2 หลักการทำงานของ Machine Learning	476
8.2.3 ประเภทของ Machine Learning	477
8.2.4 การประยุกต์ใช้ Machine Learning ในระบบรักษาความปลอดภัยอัจฉริยะ	478
8.2.5 กระบวนการพัฒนา Machine Learning	478
8.2.6 การประเมินแบบจำลอง	483
8.2.7 การกำหนดเกณฑ์การตัดสินใจและการแจ้งเตือน	486
8.2.7 การรักษาความปลอดภัยของกระบวนการ Machine Learning	487
8.2.9 การติดตามแบบจำลองหลังนำไปใช้งาน	488
8.3 การตรวจจับใบหน้าจากกล้องด้วยแบบจำลองตระกูล YOLO	489
8.3.1 กระบวนการตรวจจับใบหน้าด้วย YOLO	489
8.3.2 การเตรียมสภาพแวดล้อม	490
8.3.3 การเตรียมชุดข้อมูลใบหน้า	491
8.3.4 รูปแบบการจัดชุดข้อมูล YOLO	491
8.3.5 การแบ่งชุดข้อมูล	493
8.3.6 การเลือกแบบจำลอง YOLO	493
8.3.7 การฝึกแบบจำลอง	493
8.3.8 การตรวจสอบผลการฝึก	496

สารบัญ (ต่อ)

เรื่อง **หน้า**

8.3.9 การตรวจสอบการทำงานของกล้องก่อนนำไปใช้กับ YOLO 497
8.3.10 การทำงานภายในโปรแกรม 499
8.3.11 การวาดกรอบด้วยตนเอง 500
8.3.12 การบันทึกภาพเมื่อพบใบหน้า 501
8.3.13 การเพิ่มการแจ้งเตือนของระบบตรวจจับใบหน้าด้วย YOLO 500
8.3.14 การปรับค่า Confidence และ IoU 403
8.3.15 การเพิ่มความเร็วของการประมวลผลข้อมูล 503
8.3.16 ข้อควรระวังด้านความเป็นส่วนตัว 504
บรรณานุกรมบทที่ 8 507
สรุปสาระสำคัญของบทที่ 8 509
แบบฝึกหัดท้ายบทที่ 8 511

บทที่ 9 โครงงานระบบรักษาความปลอดภัยอัจฉริยะ **518**

9.1 ระบบกล้องโทรทัศน์วงจรปิด 519
9.1.1 งานออกแบบติดตั้งกล้องโทรทัศน์วงจรปิด 519
9.1.2 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก 520
9.1.3 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบ IP/Network 522
9.1.4 งานติดตั้งและใช้งานกล้อง IP Camera 522
9.2 ระบบควบคุมประตูอัจฉริยะด้วยเทคโนโลยี RFID 523
9.2.1 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino 523
9.2.2 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID โดยใช้ NodeMCU ESP8266 526
9.2.3 งานประยุกต์ใช้ RFID ร่วมกับ IP Camera และ LINE Messaging API 528
9.3 ระบบประตูอัจฉริยะด้วยเทคโนโลยีตรวจสอบลายนิ้วมือ 529
9.3.1 งานควบคุมการเปิด–ปิดอุปกรณ์ด้วยเซนเซอร์ตรวจสอบลายนิ้วมือ 529
9.3.2 งานควบคุมการเข้า–ออกประตูด้วยลายนิ้วมือร่วมกับ RFID 530
9.3.3 งานติดตั้งเครื่องสแกนลายนิ้วมือสำหรับระบบควบคุมการเข้า–ออกประตู 531
9.4 ระบบประตูอัจฉริยะด้วยเทคโนโลยีจดจำใบหน้า 533
9.4.1 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า 533
9.4.2 งานประยุกต์ใช้ Google Cloud และ Google Sheets 535

สารบัญ (ต่อ)

เรื่อง **หน้า**

9.5 การประยุกต์ใช้เซนเซอร์ตรวจจับก๊าซ MQ-2 ในระบบความปลอดภัย 537

9.5.1 งานตรวจจับก๊าซและควบคุมวาล์วก๊าซอัตโนมัติด้วยเซนเซอร์ MQ-2 และ NodeMCU ESP8266 537

บรรณานุกรมบทที่ 9 539

ภาคผนวก ก ใบงาน **541**

ภาคผนวก ข โปรแกรมควบวบคุมการทำงาน **713**

ดัชนีค้นคำ **755**

สารบัญรูป

รูปที่		หน้า
1.1	ระบบระบบกล้องโทรทัศน์วงจรปิด	7
1.2	ระบบควบคุมการเข้า-ออก	9
1.3	หลักการทำงานของระบบควบคุมการเข้า-ออก	10
1.4	การแบ่งระดับพื้นที่ตามความปลอดภัยขององค์การรักษาความปลอดภัยฝ่ายพลเรือน	14
1.5	แสดงลักษณะของกระแสไฟฟ้าที่ไหลผ่านร่างกาย	18
1.6	กราฟความสัมพันธ์ระหว่างกระแสไฟฟ้าและเวลาที่มีผลต่อร่างกายสำหรับผู้ใหญ่	19
1.7	สัญลักษณ์ของการ Disconnect Mains	21
1.8	สัญลักษณ์และการ Lock-out and tag-out	22
1.9	เครื่องมือการตรวจสอบแรงดันไฟฟ้า	22
1.10	วิธีการเชื่อมต่อสายดินเข้าไปลัดวงจรกับสายไฟฟ้าหลัก	23
1.11	การป้องกันกระแสไฟฟ้าจากส่วนของอุปกรณ์ไฟฟ้าอื่นๆ ที่ยังมีกระแสไฟฟ้า	23
1.12	ตารางสรุปกฎ 5 ข้อของความปลอดภัยในระบบไฟฟ้า	24
1.13	แสดงระดับการป้องกันของอุปกรณ์ไฟฟ้า	24
1.14	รหัสบ่งชี้ระดับความทนต่อสภาพแวดล้อมของอุปกรณ์ไฟฟ้า	25
1.15	รหัสบ่งชี้อักษรเพิ่มเติม	26
1.16	หมวกป้องกันศีรษะ	26
1.17	อุปกรณ์ป้องกันหู	27
1.18	แว่นนิรภัย	27
1.19	เสื้อสะท้อนแสง	28
1.20	เข็มขัดนิรภัย	28
1.21	จุดยึดตัวกับฐานหรือโครงสร้างต่าง ๆ	29
1.22	เชือกสำหรับป้องกันการตก	29
1.23	เชือกในลักษณะรักษาตำแหน่ง	30
1.24	เชือกช่วยชีวิต	30
1.25	รองเท้านิรภัย	31
1.26	การล้วงสิ่งที่ขวางทางเดินลมหายใจออกมาจากช่องปาก	32
1.27	แสดงการเป่าปากผู้ป่วย	32
1.28	การวางตำแหน่งวางมือเพื่อนวดหัวใจ	33
1.29	แสดงการใช้นิ้วล็อกกันไว้เพื่อใช้แรงกดกระดูกสันอกถ่ายเทผ่านฝ่ามือล่าง	34
1.30	การนวดหัวใจและให้ลมหายใจทางปาก	34

สารบัญรูป (ต่อ)

รูปที่		หน้า
2.1	ส่วนประกอบของเซนเซอร์ PIR	49
2.2	หลักการทำงานของเซนเซอร์ PIR	50
2.3	หลักการตรวจจับความแตกต่างของพลังงานอินฟราเรด	50
2.4	วงจรใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR	51
2.5	วงจรใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR โดยใช้ Arduino UNO	52
2.6	โครงสร้างของสวิตช์แม่เหล็ก	54
2.7	บล็อกไดอะแกรมการทำงานของฮอลล์เซ็นเซอร์	55
2.8	หลักการทำงานของสวิตช์แม่เหล็ก	57
2.9	กลไกการทำงานของสวิตช์แม่เหล็ก	58
2.10	หลักการแพร่กระจายสนามไฟฟ้าบนแผ่นฮอลล์	59
2.11	ประเภทของเซนเซอร์ตรวจจับควัน	62
2.12	โครงสร้างของเซนเซอร์ตรวจจับควันแบบโฟโตอิเล็กทริก	63
2.13	โครงสร้างของอุปกรณ์ตรวจจับควันแบบไอออไนเซชัน	64
2.14	โครงสร้างของอุปกรณ์ตรวจจับควันแบบลำแสง	66
2.15	วงจรตรวจจับควันด้วยเซนเซอร์ MQ และแจ้งเตือนด้วย LED และบัซเซอร์	67
2.16	การต่อวงจรใช้งานตัวตรวจจับควันแบบ 4 สาย	69
2.17	วงจรตรวจจับก๊าซโดยใช้ เซนเซอร์ตรวจจับก๊าซ MQ-2 ร่วมกับ Arduino	69
2.18	เซนเซอร์ตรวจจับก๊าซชนิดต่าง ๆ	72
2.19	โครงสร้างของเซนเซอร์ตรวจจับก๊าซ	73
2.20	โครงสร้างและวงจรอ่านสัญญาณของเซนเซอร์ก๊าซแบบไฟฟ้าเคมี	76
2.21	วงจรตรวจจับแก๊สและคุณภาพอากาศด้วยเซนเซอร์ MQ-135	78
2.22	วงจรตรวจจับและแจ้งเตือนแก๊สด้วยเซนเซอร์ MQ-2 ร่วมกับ Arduino	80
2.23	คลื่นแม่เหล็กไฟฟ้าที่ตรวจพบจากเปลวไฟ	82
2.24	เซนเซอร์ตรวจจับเปลวไฟชนิดต่าง ๆ	85
2.25	โครงสร้างของเซนเซอร์ตรวจจับเปลวไฟแต่ละชนิด	88
2.26	หลักการทำงานของเซนเซอร์ตรวจจับเปลวไฟ	89
2.27	วงจรเซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด	90
2.28	วงจรเซนเซอร์ตรวจจับเปลวไฟร่วมกับ Arduino UNO เพื่อการแจ้งเตือน	91
3.1	กล้องโทรทัศน์วงจรปิดยุคที่ 1	105
3.2	กล้องโทรทัศน์วงจรปิดยุคที่ 2	106
3.3	กล้องโทรทัศน์วงจรปิดยุคที่ 3	106
3.4	กล้องโทรทัศน์วงจรปิดยุคที่ 4	107

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.5	องค์ประกอบระบบกล้องโทรทัศน์วงจรปิด	108
3.6	รูปแบบการเชื่อมต่อเครือข่ายแบบบัส	109
3.7	รูปแบบการเชื่อมต่อเครือข่ายแบบดาว	110
3.8	การเชื่อมต่อเครือข่ายแบบวงแหวน	111
3.9	โครงสร้างและหลักการทำงานของ WLAN	112
3.10	แผ่นทดสอบความละเอียดของภาพ (Resolution Test Chart)	114
3.11	การเปรียบเทียบความละเอียดของภาพระหว่าง 400 TVL และ 500 TVL	114
3.12	โครงสร้างของกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	116
3.13	โครงสร้างของกล้องโทรทัศน์วงจรปิดระบบดิจิทัล	117
3.14	กล้องโทรทัศน์วงจรปิดชนิดต่าง ๆ	120
3.15	ข้อต่อแบบ C-Mount และ CS-Mount	121
3.16	รูรับแสง	121
3.17	ตัวอย่างขาดของรูรับแสงขนาดต่าง ๆ	122
3.18	เลนส์ที่มีขนาดช่องรับแสงคงที่	123
3.19	ลักษณะของเลนส์ปรับช่องรับแสงได้	124
3.20	ลักษณะของเลนส์ปรับขนาดช่องรับแสงอัตโนมัติ	124
3.21	ขนาดของความยาวโฟกัสและมุมมองในการเห็นภาพ	125
3.22	ความสัมพันธ์ระหว่างระยะโฟกัส ระยะทาง และขนาดอุปกรณ์รับภาพ	126
3.23	ความสัมพันธ์ระหว่างความยาวโฟกัส ระยะห่างจากวัตถุ และพื้นที่การมองเห็น	127
3.24	โปรแกรมคิดขนาดของเลนส์ออนไลน์	129
3.25	เครื่องบันทึกภาพ NVR และ DVR	130
3.26	ฮาร์ดดิสก์สำหรับระบบกล้องโทรทัศน์วงจรปิด	132
3.27	โปรแกรมคำนวณความจุของฮาร์ดดิสก์ไดร์ฟ	135
3.28	จอภาพ	136
3.29	โครงสร้างของโคแอกเชียล	137
3.30	ลักษณะของสาย RG ชนิดต่าง ๆ	139
3.31	สายคู่เกลียวบิด	140
3.32	โครงสร้างของสายสายคู่เกลียวบิด	141
3.33	สายไฟฟ้าในงานระบบกล้องโทรทัศน์วงจรปิด	145
3.34	การใช้งานเครื่องสลับภาพ	146

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.35	เครื่องแบ่งสัญญาณภาพ	147
3.36	อุปกรณ์ขยายสัญญาณภาพบาลัน	148
3.37	การใช้งาน Router ในระบบ CCTV	149
3.38	ขั้วต่อสายสัญญาณในงานระบบกล้องโทรทัศน์วงจรปิด	150
3.39	ขายึดกล้องโทรทัศน์วงจรปิด	151
3.40	กล่องครอบกล้องโทรทัศน์วงจรปิด	152
3.41	อะแดปเตอร์ในระบบกล้องโทรทัศน์วงจรปิด	153
3.42	เบรกเกอร์	154
3.43	เครื่องมือพื้นฐานสำหรับงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด	155
3.44	ตัวอย่างการสำรวจพื้นที่และกำหนดตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดภายในอาคารสำนักงาน	156
3.45	ตัวอย่างการใช้แอพพลิเคชั่น AR Plan: Room & Floor Measure	157
3.46	ตัวอย่าง Video Surveillance Design Apps	158
3.47	ตัวอย่างการเขียนแบบติดตั้งระบบกล้องโทรทัศน์วงจรปิดภายในสำนักงาน	158
3.48	ตัวอย่างมุมมองภาพสามมิติของกล้องโทรทัศน์วงจรปิดแต่ละตำแหน่งติดตั้ง จาก Video Surveillance Design Apps	160
3.49	แสดงตัวอย่างงความสามารถมองเห็นพื้นที่ด้านกว้างของกล้อง CCTV 1	163
3.50	แสดงตัวอย่างงความสามารถมองเห็นพื้นที่ด้านกว้างของกล้อง CCTV 2	164
3.51	แสดงตัวอย่างงความสามารถมองเห็นพื้นที่ด้านกว้างของกล้อง CCTV 3	165
3.52	แผนผังระบบกล้องโทรทัศน์วงจรปิดภายในอาคาร	166
3.53	การ Download โปรแกรม CMS	171
3.54	ขั้นตอนการคลิก “Next” สำหรับการติดตั้งโปรแกรม CMS	171
3.55	การเลือกเส้นทางการติดตั้ง	172
3.56	ขั้นตอนการลงโปรแกรมสำเร็จ	172
3.57	ไอคอนโปรแกรม CMS	172
3.58	การเลือกภาษาสำหรับตัวโปรแกรมบริหารจัดการ	173
3.59	หน้าต่างล็อคอินโปรแกรมบริหารจัดการ	173
3.60	หน้าต่างแสดงตัวโปรแกรมแสดงการติดตั้งเสร็จสมบูรณ์	174
3.61	หน้าต่างแสดงตัวโปรแกรมแสดงช่วงเวลาที่ต้องการดูภาพ	174
3.62	หน้าต่างแสดงตัวโปรแกรมแสดงการเพิ่ม Zone List และ ADD Area	175
3.63	หน้าต่างแสดงการตั้งค่าอุปกรณ์	175

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.64	หน้าต่างแสดงการปรับเปลี่ยนการตั้งค่าอุปกรณ์	176
3.65	หน้าต่างแสดงการลบอุปกรณ์	176
3.66	เมนูหลักของโปรแกรม CMS	177
3.67	แสดงอาการภาพดับหรือไม่เกิดภาพในระบบกล้องโทรทัศน์วงจรปิด	178
3.68	อาการภาพเป็นคลื่น	190
3.69	อาการภาพเบลอ	181
4.1	องค์ประกอบพื้นฐานของระบบควบคุมการเข้าออก	201
4.2	องค์ประกอบของ RFID	203
4.3	โครงสร้างและหลักการทำงานของแท็ก RFID แบบ Passive และ Active	204
4.4	แสดงแท็ก RFID ชนิดต่าง ๆ	205
4.5	แสดงเครื่องอ่าน RFID ประเภทต่าง ๆ	206
4.6	การจำแนกประเภทของระบบ RFID	207
4.7	หลักการทำงานของ RFID ชนิด EAS	210
4.8	สรุปประเภทของระบบ RFID	211
4.9	หลักการเชื่อมต่อแบบเหนี่ยวนำแม่เหล็ก	215
4.10	หลักการเชื่อมต่อแบบสะท้อนกลับแม่เหล็กไฟฟ้า	218
4.11	สรุปเทคนิคการมอดูเลตในระบบ RFID	220
4.12	การเชื่อมต่อแบบสนามไฟฟ้า	224
4.13	โครงสร้างข้อมูลของบัตร MIFARE ขนาด 1 kB	227
4.14	โครงสร้างของ Sector 0 Block 0	228
4.15	โครงสร้างของ Block 0, 1, 2 ของทุก Sector	229
4.16	การอ่านและเขียนข้อมูลบนบัตร MIFARE	229
4.17	โมดูล RFID รุ่น RC522	232
4.18	อุปกรณ์ในการสื่อสารด้วยเทคโนโลยี NFC	234
4.19	หลักการทำงานของ NFC	235
4.20	การเปรียบเทียบลักษณะการใช้งานของแท็ก NFC แบบสแตติก แบบไดนามิก และอุปกรณ์ NFC Transceiver	237
4.21	หลักการทำงานของการแตะเพื่อใช้งาน (Tap & Pair)	238
4.22	การทำงานของระบบชำระเงินอิเล็กทรอนิกส์	239
4.23	องค์ประกอบของระบบ QR Code Door Lock	241
4.24	หลักการทำงานของระบบ QR Code Door Lock	243
4.25	วงจรขับและกลไกการทำงานของระบบล็อกประตูไฟฟ้า	246

สารบัญรูป (ต่อ)

รูปที่		หน้า
5.1	ประเภทของลายนิ้วมือ	266
5.2	ตัวอย่างเครื่องสแกนลายนิ้วมือ	266
5.3	หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบใช้แสง	267
5.4	หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบ Capacitive Fingerprint Sensor	268
5.5	หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบอัลตราโซนิก	269
5.6	หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบตรวจจับความร้อน	271
5.7	หลักการตรวจสอบลายนิ้วมือด้วยจุดลักษณะเฉพาะ	272
5.8	หลักการตรวจสอบลายนิ้วมือด้วยการวิเคราะห์จุดลักษณะเฉพาะและความสัมพันธ์ของจุด	273
5.9	กระบวนการสแกนและตรวจสอบลายนิ้วมือ	274
5.10	กระบวนการแปลงลายนิ้วมือเป็นข้อมูลดิจิทัล	276
5.11	โครงสร้าง หลักการทำงาน และส่วนประกอบของเซนเซอร์สแกนลายนิ้วมือ R307	277
5.12	วงจรเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือ R307 ร่วมกับไมโครคอนโทรล-เลอร์	279
5.13	แผนผังการเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์เบื้องต้น	280
5.14	เครื่องสแกนใบหน้าและวิธีการจดจำใบหน้า	281
5.15	กระบวนการจดจำใบหน้าด้วยเทคโนโลยีไบโอเมตริกซ์	285
5.16	กระบวนการตรวจจับใบหน้าด้วย OpenCV และ Haar Cascade	287
5.17	แนวคิดระบบระบุตัวผู้พูด	291
5.18	แผนภาพการทำงานของระบบยืนยันตัวตนผู้พูดแบบบูรณาการ	293
5.19	สถาปัตยกรรมของระบบแยกเสียงผู้พูดเป้าหมาย	295
6.1	องค์ประกอบสำคัญของเครือข่ายระบบรักษาความปลอดภัย	312
6.2	โทโพโลยีเครือข่ายในระบบรักษาความปลอดภัยอัจฉริยะ	314
6.3	เปรียบเทียบแนวคิดของการแบ่งชั้นโปรโตคอล	317
6.4	การเปรียบเทียบการสื่อสารข้อมูลระหว่างแบบจำลอง OSI กับ TCP/IP ระหว่างสถานีต้นทางและสถานีปลายทาง	319
6.5	การห่อหุ้มข้อมูลและการถอดห่อหุ้มข้อมูล	324
6.6	โครงสร้าง IP Address	325
6.7	องค์ประกอบของเครือข่าย LAN	330

สารบัญรูป (ต่อ)

รูปที่		หน้า
6.8	คุณลักษณะของ LAN ในระบบรักษาความปลอดภัยอัจฉริยะ	332
6.9	องค์ประกอบและการทำงานของเครือข่าย WAN สำหรับระบบรักษาความปลอดภัย	333
6.10	สื่อส่งสัญญาณที่ใช้ในโครงข่าย WAN	336
6.11	หลักการทำงานของโปรโตคอลกำหนดเส้นทาง	337
6.12	ความสัมพันธ์ระหว่างมาตรฐาน IEEE 802.3กับ OSI Model	340
6.13	กระบวนการทำงานของ CSMA/CD	344
6.14	สถาปัตยกรรมเครือข่าย Ethernet ระบบรักษาความปลอดภัยแบบรวมศูนย์	347
6.15	สถาปัตยกรรม Wi-Fi	349
6.16	อุปกรณ์รับส่งสัญญาณที่ทำงานในย่านความถี่ต่ำกว่า 1 GHz	353
6.17	โครงสร้างเครือข่ายของ Zigbee	355
6.18	สถาปัตยกรรมเครือข่ายและลำดับชั้นโปรโตคอลของ Z-Wave	358
6.19	รูปแบบทั่วไปของ Physical เฟรม	358
6.20	รูปแบบทั่วไปของ MAC เฟรม	359
6.21	โทโพโลยีของโหนดในเครือข่ายบ้านอัจฉริยะ Z-Wave	361
6.22	สถาปัตยกรรมเครือข่ายและการสื่อสารของ LoRaWAN สำหรับระบบ IoT	363
6.23	สถาปัตยกรรมของเครือข่าย LoRaWAN และการเชื่อมต่อกับระบบ Cloud	364
6.24	โครงสร้างพื้นฐานของเครือข่าย LoRaWAN	366
6.25	หลักการทำงานของ VLAN	368
6.26	หลักการแบ่งเครือข่าย และการเชื่อมต่อของ VLAN ตามมาตรฐาน IEEE 802.1Q	370
6.27	การประยุกต์ใช้ VLAN ในระบบรักษาความปลอดภัยอัจฉริยะ	372
6.28	สถาปัตยกรรมของระบบ PoE	375
7.1	องค์ประกอบพื้นฐานของระบบ IoT	397
7.2	ตัวอย่างบอร์ด Arduino รุ่นต่าง ๆ	400
7.3	สถาปัตยกรรมภายในโดยสังเขปของไมโครคอนโทรลเลอร์ AVR แบบ 8 bit	402
7.4	โครงสร้างของ Arduino Uno R3	404
7.5	การเชื่อมต่อสายโมดูล RFID RC522 กับ Arduino UNO	407
7.6	ดาวน์โหลดไลบรารี MFRC522	408
7.7	การติดตั้งไลบรารี MFRC522	408

สารบัญรูป (ต่อ)

รูปที่		หน้า
7.8	การตรวจสอบการอ่านแท็กของโมดูล RC522	409
7.9	การการกำหนดขา RST	409
7.10	ค่า UID และข้อมูลในแต่ละ data blocks	410
7.11	แสดงรูปแบบ Memory Layout แบบสามมิติ	411
7.12	วงจร RFID RC522 เพื่อควบคุมการติด ดับ LED	411
7.13	ขาต่อใช้งานของบอร์ด NodeMCU ESP8266	416
7.14	ขั้นตอนการเชื่อมต่อ ESP8266 กับ Arduino IDE	417
7.15	การต่อวงจรโมดูล RFID RC522 กับ NodeMCU ESP8266	418
7.16	การต่อวงจรโมดูล RFID ร่วมกับไฟ LED และไอซี MCP23017	420
7.17	การควบคุมเอาต์พุตของ ESP8266 ผ่านเว็บเซิร์ฟเวอร์บนอุปกรณ์เคลื่อนที่	421
7.18	การติดตั้งแพ็กเกจ ESP8266 ผ่าน Boards Manager	422
7.19	การอัปโหลดโปรแกรมเว็บเซิร์ฟเวอร์เข้าสู่บอร์ด ESP-12E NodeMCU	423
7.20	การเชื่อมต่อโมดูล ESP-01 กับอุปกรณ์ USB-to-UART สำหรับอัปโหลดโปรแกรม	424
7.21	การเชื่อมต่อ LED สองดวงกับ GPIO4 และ GPIO5 ของ ESP-12E NodeMCU	425
7.22	การเชื่อมต่อ LED สองดวงกับ GPIO0 และ GPIO2 ของโมดูล ESP-01	425
7.23	แสดง IP Address ของ ESP8266 ผ่าน Serial Monitor	426
7.24	หน้าเว็บสำหรับควบคุม GPIO4 และ GPIO5 ของ ESP8266	426
7.25	วิวัฒนาการของ Raspberry Pi	428
7.26	องค์ประกอบหลักของ Raspberry Pi และพอร์ตเชื่อมต่ออุปกรณ์ภายนอก	430
7.27	องค์ประกอบของ Cloud Platform	435
7.28	รูปแบบการให้บริการของ Cloud Platform	439
7.29	ช่องทางการสื่อสารที่ผู้พัฒนาสามารถใช้บริการต่าง ๆ ของ LINE Platform	446
7.30	การลงทะเบียน Business ID	446
7.31	การกรอกแบบฟอร์มสมัครใช้งาน	447
7.32	การตรวจสอบ LINE Official Account	447
7.33	การพิจารณาเลือก Provider	448
7.34	การเปิดใช้งาน Messaging API	449
7.35	การตรวจสอบ Channel	449
7.36	การเข้าสู่หน้าจัดการทรัพยากรเพื่อสร้างโปรเจกต์ใน Google Cloud	541

สารบัญรูป (ต่อ)

รูปที่		หน้า
7.37	การสร้างโปรเจกต์สำหรับระบบบันทึกข้อมูลลง Google Sheets	541
7.38	การกำหนดชื่อและรายละเอียดของโปรเจกต์	452
7.39	หน้าแดชบอร์ดสำหรับตรวจสอบ API ของโปรเจกต์	452
7.40	การค้นหาและเลือก Google Sheets API	452
7.41	การเปิดใช้งาน Google Sheets API	453
7.42	การตรวจสอบสถานะของ API ที่เปิดใช้งานแล้ว	453
7.43	การสร้างบัญชีบริการสำหรับแอปพลิเคชัน	454
7.44	ขั้นการ Create Service Account	454
7.45	การกำหนดชื่อและรหัสของบัญชีบริการ	455
7.46	เสร็จสิ้นการสร้างบัญชีบริการ	455
7.47	การเข้าสู่แท็บ Keys ของบัญชีบริการ	456
7.48	การสร้างกุญแจของบัญชีบริการในรูปแบบ JSON	456
7.49	การยืนยันการดาวน์โหลดกุญแจส่วนตัวของบัญชีบริการในรูปแบบ JSON	457
8.1	เทคโนโลยี AI ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ	474
8.2	ประเภทของ Machine Learning	477
8.3	กระบวนการพัฒนา Machine Learning	478
8.4	กระบวนการตรวจจับใบหน้าด้วยสถาปัตยกรรม YOLO	490
8.5	โครงสร้างโฟลเดอร์สำหรับเก็บข้อมูล	491
8.6	หลักการทำงานของระบบตรวจจับใบหน้าด้วย YOLO และการแจ้งเตือน	504
8.7	การตรวจจับใบหน้าด้วยสถาปัตยกรรม YOLO และการประเมินประสิทธิภาพ	506
9.1	แผนผังโรงจอดรถสำหรับออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด	519
9.2	แบบจำลองการติดตั้งและเดินสายระบบกล้องโทรทัศน์วงจรปิด	521
9.3	หลักการออกแบบระบบควบคุมการเข้า ออกประตูด้วย RFID และ Arduino	524
9.4	โครงสร้างแถวและคอลัมน์ของแป้นกดแบบเมทริกซ์ 4×4	525
9.5	หลักการควบคุมการเข้า–ออกประตูด้วย RFID, NodeMCU ESP8266 และจอ LCD	526
9.6	หลักการควบคุมกลอนประตูโซลินอยด์ด้วย RFID โดยใช้ NodeMCU ESP8266	527
9.7	การประยุกต์ใช้ RFID ร่วมกับ IP Camera และ LINE Messaging API	528
9.8	หลักการควบคุมอุปกรณ์ด้วยระบบตรวจสอบลายนิ้วมือ	530

สารบัญรูป (ต่อ)

รูปที่		หน้า
9.9	แผนผังการทำงานของระบบควบคุมการเข้า–ออกประตูด้วยลายนิ้วมือร่วมกับ RFID	531
9.10	ผังการเชื่อมต่อระบบควบคุมการเข้า–ออกด้วยเครื่องสแกนลายนิ้วมือรุ่น CMG 280	532
9.11	การออกแบบระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า	533
9.12	แนวคิดการทำงานของระบบจดจำใบหน้าสำหรับควบคุมการเข้า–ออกประตู	534
9.13	สถาปัตยกรรมการเชื่อมต่อระบบตรวจจับและรู้จำใบหน้ากับ Google Sheets API และ LINE Messaging API	535
9.14	แนวคิดการออกแบบระบบตรวจจับก๊าซและควบคุมวาล์วก๊าซอัตโนมัติด้วยเซนเซอร์ MQ-2 และ NodeMCU ESP8266	538

สารบัญตาราง

ตารางที่		หน้า
1.1	อันตรายต่อร่างกายจากกระแสไฟฟ้าจากการเพิ่มขึ้นของแรงดันไฟฟ้า	17
1.2	แสดงอาการที่ได้รับจากปริมาณกระแสไฟฟ้าที่ไหลผ่านร่างกาย	17
1.3	ความสัมพันธ์ระหว่างปริมาณกระแสไฟฟ้า ระยะเวลา และอาการที่ได้รับ	18
2.1	การเปรียบเทียบชนิดของเซนเซอร์ตรวจจับก๊าซ	73
2.2	สรุปคุณสมบัติของคลื่นแม่เหล็กไฟฟ้าที่ใช้ในการตรวจจับเปลวไฟ	83
2.3	การเปรียบเทียบชนิดของเซนเซอร์ตรวจจับเปลวไฟ	84
3.1	ค่าความละเอียดของภาพ	115
3.2	ความละเอียดของ TVL เมื่อเทียบเป็นพิคเซล	115
3.3	การเลือกขนาดเลนส์ให้เหมาะสมกับลักษณะการใช้งาน	125
3.4	ขนาดอุปกรณ์รับภาพของ CCD	127
3.5	แสดงแสงสว่างโดยประมาณของค่า Lux	130
3.6	อัตราการใช้งานพื้นที่บันทึกข้อมูล HDD	133
3.7	คุณลักษณะของสายโคแอกเชียลเบอร์ต่าง ๆ	138
3.8	สายคู่บิดเกลียว Category ต่าง ๆ	140
3.9	สรุปจำนวนกล้องโทรทัศน์วงจรปิดและมุมมองที่ชัดเจนและครอบคลุมพื้นที่ใช้งาน	167
3.10	ตารางประมาณการค่าใช้จ่ายในการติดตั้งระบบกล้องโทรทัศน์วงจรปิด	168
3.11	Software CMS ของ PEOPLE FU สำหรับการดูกล้องโทรทัศน์วงจรปิด	169
4.1	ความหมายแตกต่างระหว่าง Authentication, Authorization และ Access Control	201
4.2	สรุปเปรียบเทียบการใช้งาน RFID แต่ละประเภท	209
4.3	ตัวอย่างมาตรฐานที่ใช้ Inductive Coupling	216
4.4	เปรียบเทียบคุณลักษณะของ ASK, FSK, และ PSK	219
4.5	ความแตกต่างระหว่าง Close Coupling และ Inductive Coupling	222
4.6	สรุปความแตกต่างระหว่าง Capacitive Coupling และ Inductive Coupling	226
4.7	การกำหนด Access Bits	231
5.1	สายสัญญาณสำหรับเชื่อมต่อของเซนเซอร์ R307	278
5.2	การเชื่อมต่อขาเซนเซอร์กับไมโครคอนโทรลเลอร์ Arduino UNO	280
6.1	หน่วยข้อมูลในแต่ละชั้นของการสื่อสาร	323
6.2	รายละเอียดของแต่ละชั้นของหมายเลขของ IP	326
6.3	ตัวอย่างการแบ่งซับเน็ตแบบ /26 ของ เครือข่าย 192.168.10.0/24	327

สารบัญตาราง (ต่อ)

ตารางที่		หน้า
6.4	การแบ่งเลข IP 172.16.254.1 เป็น 4 Octet	327
6.5	ตัวอย่างมาตรฐาน ความเร็ว และสื่อในการสื่อสารสัญญาณ	341
6.6	ส่วนสำคัญของ Ethernet Frame	341
6.7	จำนวนช่วงเวลาที่สุ่ม	443
6.8	MAC Address กับหมายเลขพอร์ตของสวิตช์	346
6.9	สรุปเปรียบเทียบเครือข่าย LAN, WAN, Ethernet, และ Wi-Fi	350
6.10	คุณลักษณะของย่านความถี่และอัตราการรับส่งข้อมูลของ Zigbee ตามมาตรฐาน IEEE 802.15.4	352
6.11	ตัวอย่างการบริหารจัดการและการกำหนดเส้นทางของ VLAN	368
6.12	ตัวอย่างโครงสร้าง VLAN สำหรับ Smart Security	372
6.13	แสดงการเปรียบเทียบมาตรฐาน PoE ที่ใช้งานในปัจจุบัน	376
7.1	ตัวอย่างบอร์ด Arduino รุ่นต่าง ๆ	400
7.2	การเชื่อมต่อโมดูล RC522 RFID กับ Arduino	407
7.3	การเชื่อมต่อระหว่างโมดูล RFID RC522 กับ NodeMCU ESP8266	418
7.4	การต่อวงจรระหว่าง ESP-01 และ FTDI Programmer	423
7.5	ตัวอย่างการทดสอบปุ่มควบคุม	427
7.6	ความแตกต่างของรูปแบบบริการของ Cloud Platform	439
7.7	การใช้คำสั่ง HTTP เพื่อดำเนินการกับทรัพยากร	443
8.1	ลักษณะงานและผลลัพธ์ที่ต้องการในการเลือกแบบจำลอง	482
8.2	ตัวอย่างของแบบจำลองตรวจจับหลายคลาส	486
8.3	คำอธิบายพารามิเตอร์ในการเขียนโค้ดโปรแกรมสำหรับการฝึกแบบจำลอง	495
8.4	ปัญหาที่พบและแนวทางแก้ไขเมื่อไม่สามารถเปิดกล้องกล้องไม่ทำงาน	498

1 ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยอัจฉริยะ

11

ความหมาย ความสำคัญ แนวคิดระบบรักษาความปลอดภัย

1.1.1 ความหมายของระบบรักษาความปลอดภัย
1.1.2 วิวัฒนาการของระบบรักษาความปลอดภัย
1.1.3 ความสำคัญของระบบรักษาความปลอดภัยอัจฉริยะ
1.1.4 หลักการทำงานของระบบรักษาความปลอดภัยอัจฉริยะ

12

องค์ประกอบของระบบรักษาความปลอดภัย

1.2.1 อุปกรณ์ตรวจจับในระบบรักษาความปลอดภัย
1.2.2 อุปกรณ์ควบคุมในระบบรักษาความปลอดภัย
1.2.3 อุปกรณ์แจ้งเตือนในระบบรักษาความปลอดภัย
1.2.4 แหล่งพลังงานสำรองในระบบรักษาความปลอดภัย

13

ประเภทของระบบรักษาความปลอดภัย

1.3.1 ระบบกล้องโทรทัศน์วงจรปิด
1.3.2 ระบบควบคุมการเข้า-ออก
1.3.3 ระบบเสียงประกาศ
1.3.4 ระบบแจ้งเตือนการบุกรุก
1.3.5 ระบบแจ้งเหตุเพลิงไหม้

14

มาตรฐานและกฎหมายที่เกี่ยวข้องกับระบบรักษาความปลอดภัย

1.4.1 ระดับที่ 1 พื้นที่รั้วและทางเข้าสถานที่
1.4.2 ระดับที่ 2 พื้นที่ระหว่างรั้วถึงอาคาร
1.4.3 ระดับที่ 3 พื้นที่ภายในห้องรับรอง
1.4.4 ระดับที่ 4 พื้นที่ภายในอาคารที่มีความสำคัญ

15

หลักความปลอดภัยในการปฏิบัติงานด้านไฟฟ้า

1.5.1 ข้อควรปฏิบัติเกี่ยวกับความปลอดภัยในการปฏิบัติงานไฟฟ้า
1.5.2 กฎ 5 ข้อความปลอดภัยในการปฏิบัติงานทางไฟฟ้า
1.5.3 ระดับการป้องกันของอุปกรณ์ไฟฟ้า
1.5.4 รหัสบ่งชี้ระดับความทนต่อสภาพแวดล้อมของอุปกรณ์ไฟฟ้า
1.5.5 กฎหมายเกี่ยวกับความปลอดภัย
1.5.6 หลักความปลอดภัยในการปฏิบัติงานด้านไฟฟ้า
1.5.7 อุปกรณ์ป้องกันอันตรายส่วนบุคคล
1.5.8 การปฐมพยาบาลเบื้องต้น

บทที่ 1 ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยอัจฉริยะ

Introduction to Smart Security Systems

1.1 ความหมาย ความสำคัญ แนวคิดระบบรักษาความปลอดภัย

1.1.1 ความหมายของระบบรักษาความปลอดภัย (Definition of Security Systems)

ระบบรักษาความปลอดภัย (security system) หมายถึง ระบบหรือกระบวนการที่ถูกออกแบบและพัฒนาขึ้นเพื่อป้องกันอันตรายที่อาจเกิดขึ้นต่อชีวิต ร่างกาย และทรัพย์สินของบุคคลภายในพื้นที่ที่กำหนด โดยครอบคลุมตั้งแต่การป้องกันการบุกรุก การเฝ้าระวังเหตุการณ์ผิดปกติ การตรวจจับภัยคุกคาม ตลอดจนการแจ้งเตือนและตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ ระบบรักษาความปลอดภัยในปัจจุบันไม่ได้จำกัดอยู่เพียงการใช้กำลังคน เช่น เจ้าหน้าที่รักษาความปลอดภัยเท่านั้น แต่ยังรวมถึงการนำเทคโนโลยีสมัยใหม่เข้ามาประยุกต์ใช้ เช่น ระบบกล้องโทรทัศน์วงจรปิด ระบบควบคุมการเข้า-ออก และระบบแจ้งเตือนอัตโนมัติ เพื่อเพิ่มความแม่นยำ ความรวดเร็ว และลดความผิดพลาดจากมนุษย์ โดยสรุประบบรักษาความปลอดภัยมีวัตถุประสงค์หลัก 4 ประการ ได้แก่

1) การป้องกัน (prevention) เป็นการลดโอกาสการเกิดเหตุการณ์ไม่พึงประสงค์ เช่น การติดตั้งรั้ว กล้องโทรทัศน์วงจรปิด หรือป้ายเตือน เพื่อยับยั้งผู้กระทำผิด

2) การตรวจจับ (detection) เป็นการค้นหาหรือระบุเหตุการณ์ผิดปกติที่เกิดขึ้น เช่น การใช้เซ็นเซอร์ตรวจจับความเคลื่อนไหว หรือเครื่องตรวจจับควันไฟ

3) การแจ้งเตือน (alert) เป็นการส่งสัญญาณเตือนเมื่อเกิดเหตุการณ์ เช่น เสียงไซเรน การแจ้งเตือนผ่านโทรศัพท์มือถือ หรือระบบศูนย์ควบคุม

4) การตอบสนอง (response) เป็นการดำเนินการแก้ไขสถานการณ์ เช่น การแจ้งเจ้าหน้าที่ การล็อกพื้นที่ หรือการสั่งการระบบอัตโนมัติ

1.1.2 วิวัฒนาการของระบบรักษาความปลอดภัย (Evolution of Security Systems)

ระบบรักษาความปลอดภัยได้พัฒนาอย่างต่อเนื่องตามความก้าวหน้าของเทคโนโลยีและความซับซ้อนของภัยคุกคาม จากเดิมที่มุ่งเน้นการป้องกันทรัพย์สินและบุคคลด้วยมาตรการทางกายภาพ ได้ก้าวสู่การประยุกต์ใช้เทคโนโลยีอิเล็กทรอนิกส์ ระบบเครือข่าย และปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพในการเฝ้าระวัง การตรวจจับ และการตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและแม่นยำยิ่งขึ้น (Kruegle, 2006; Fischer et al., 2018; Norman, 2018; Ismail, 2019; Vardakis et al., 2024) จำแนกพัฒนาการของระบบรักษาความปลอดภัยเป็น 4 ระยะสำคัญ ดังนี้

1) ระยะการรักษาความปลอดภัยทางกายภาพ (Physical Security Era)

เป็นระยะเริ่มต้นที่อาศัยมาตรการป้องกันเชิงกายภาพ เช่น รั้ว กำแพง ประตู กุญแจ ลูกกรง ตู้เซฟ และการใช้พนักงานรักษาความปลอดภัยในการเฝ้าระวัง แม้ว่าวิธีการดังกล่าวจะมีความเรียบง่ายและมีต้นทุนไม่สูง แต่ยังต้องพึ่งพากำลังคนเป็นหลัก ทำให้ประสิทธิภาพในการตรวจจับและตอบสนองต่อเหตุการณ์มีข้อจำกัด

2) ระยะระบบรักษาความปลอดภัยอิเล็กทรอนิกส์ (Electronic Security Era)

เมื่อเทคโนโลยีอิเล็กทรอนิกส์เริ่มมีบทบาท ระบบรักษาความปลอดภัยได้รับการพัฒนาให้สามารถตรวจสอบและบันทึกเหตุการณ์ได้อย่างต่อเนื่อง โดยมีการนำกล้องโทรทัศน์วงจรปิด (Close Circuit Television: CCTV) ระบบสัญญาณเตือนภัย (alarm system) ระบบควบคุมการเข้าออกด้วยคีย์การ์ด และอุปกรณ์ตรวจจับชนิดต่าง ๆ มาใช้งาน ช่วยลดการพึ่งพาบุคลากรและเพิ่มความน่าเชื่อถือในการรักษาความปลอดภัย

3) ระยะระบบรักษาความปลอดภัยอัจฉริยะบนพื้นฐานอินเทอร์เน็ตของสรรพสิ่ง (IoT-Based Smart Security Era)

การพัฒนาเครือข่ายอินเทอร์เน็ตและอุปกรณ์ Internet of Things (IoT) ทำให้ระบบรักษาความปลอดภัยสามารถเชื่อมต่ออุปกรณ์ต่าง ๆ เข้าด้วยกันได้แบบเรียลไทม์ ผู้ใช้งานสามารถควบคุม ตรวจสอบ และรับการแจ้งเตือนผ่านสมาร์ตโฟนหรืออุปกรณ์เคลื่อนที่ได้จากทุกที่ ตัวอย่างเทคโนโลยีที่ได้รับความนิยม ได้แก่ กล้องโทรทัศน์วงจรปิดชนิด Internet Protocol (IP camera) สมาร์ทล็อก (smart lock) ระบบตรวจสอบลายนิ้วมือ (fingerprint scan) เซนเซอร์ตรวจจับการเคลื่อนไหว (motion sensor) และระบบแจ้งเตือนผ่านระบบคลาวด์ (cloud-based alert system)

4) ระยะระบบรักษาความปลอดภัยอัจฉริยะที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI-Driven Smart Security Era)

ปัจจุบันระบบรักษาความปลอดภัยได้ก้าวสู่การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) และการวิเคราะห์ข้อมูลขนาดใหญ่ (big data analytics) เพื่อเพิ่มความสามารถในการตัดสินใจและป้องกันเหตุการณ์เชิงรุก ระบบสามารถวิเคราะห์ภาพจากกล้องวงจรปิด ตรวจจับใบหน้า (facial recognition) จดจำป้ายทะเบียนรถ ตรวจจับวัตถุหรือบุคคล วิเคราะห์พฤติกรรมที่ผิดปกติ (behavior analysis) และแจ้งเตือนเหตุการณ์อัตโนมัติได้อย่างแม่นยำ นอกจากนี้ ยังผสานการทำงานร่วมกับระบบรักษาความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) เพื่อปกป้องข้อมูลและอุปกรณ์ที่เชื่อมต่อผ่านเครือข่าย ทำให้เกิดระบบรักษาความปลอดภัยแบบบูรณาการที่สามารถรองรับการใช้งานในบ้านอัจฉริยะ อาคารอัจฉริยะ โรงงานอัจฉริยะ และเมืองอัจฉริยะได้อย่างมีประสิทธิภาพ

1.1.3 ความสำคัญของระบบรักษาความปลอดภัยอัจฉริยะ (Importance of Smart Security Systems)

1) เพิ่มความสะดวกในการควบคุมและตรวจสอบ

ระบบระบบความปลอดภัยอัจฉริยะ ช่วยให้ผู้ใช้งานสามารถตรวจสอบสถานการณ์ภายในพื้นที่ได้แบบเรียลไทม์ผ่านอุปกรณ์สื่อสาร เช่น สมาร์ตโฟน แท็บเล็ต หรือคอมพิวเตอร์ โดยไม่จำเป็นต้องอยู่ในสถานที่จริง อีกทั้งยังสามารถสั่งงานอุปกรณ์ต่าง ๆ ได้จากระยะไกล เช่น การเปิดปิดระบบสัญญาณเตือน การดูภาพจากกล้องโทรทัศน์วงจรปิด หรือการควบคุมการเข้า-ออก ทำให้การบริหารจัดการความปลอดภัยมีความสะดวก รวดเร็ว และยืดหยุ่นมากยิ่งขึ้น

2) ลดภาระของเจ้าหน้าที่รักษาความปลอดภัย

การนำระบบอัตโนมัติเข้ามาใช้ช่วยลดความจำเป็นในการพึ่งพากำลังคนในบางส่วน เช่น การตรวจตราพื้นที่ การบันทึกข้อมูลผู้เข้า-ออก หรือการเฝ้าระวังเหตุการณ์ผิดปกติ ระบบสามารถทำงานแทนเจ้าหน้าที่ได้อย่างต่อเนื่องตลอด 24 ชั่วโมง ส่งผลให้เจ้าหน้าที่สามารถมุ่งเน้นไปที่งานที่ต้องใช้การตัดสินใจหรือการแก้ไขสถานการณ์ที่ซับซ้อนมากขึ้น

3) เพิ่มความรวดเร็วในการตอบสนองต่อเหตุการณ์

เมื่อเกิดเหตุการณ์ผิดปกติ เช่น การบุกรุกหรืออัคคีภัย ระบบจะสามารถตรวจจับและแจ้งเตือนได้ทันที พร้อมทั้งส่งข้อมูลไปยังผู้เกี่ยวข้องแบบอัตโนมัติ เช่น แจ้งเตือนไปยังเจ้าของสถานที่หรือศูนย์ควบคุม ซึ่งช่วยให้สามารถดำเนินการแก้ไขสถานการณ์ได้อย่างรวดเร็ว ลดความเสียหายที่อาจเกิดขึ้นจากการตอบสนองที่ล่าช้า

4) ลดความเสี่ยงต่อความเสียหายของชีวิตและทรัพย์สิน

ระบบความปลอดภัยอัจฉริยะช่วยป้องกันและลดความรุนแรงของเหตุการณ์ไม่พึงประสงค์ เช่น การโจรกรรม การบุกรุก หรืออุบัติเหตุภายในสถานที่ โดยอาศัยการทำงานร่วมกันของอุปกรณ์ตรวจจับ ระบบแจ้งเตือน และการควบคุมอัตโนมัติ ทำให้สามารถหยุดยั้งหรือจำกัดผลกระทบของเหตุการณ์ได้ตั้งแต่ระยะเริ่มต้น ส่งผลให้ลดความสูญเสียทั้งในด้านชีวิตและทรัพย์สินได้อย่างมีประสิทธิภาพ

1.1.4 หลักการทำงานของระบบรักษาความปลอดภัยอัจฉริยะ (Operating Principles of Smart Security Systems)

ระบบความปลอดภัยอัจฉริยะ (smart security system) เป็นรูปแบบของระบบรักษาความปลอดภัยสมัยใหม่ที่นำเทคโนโลยีดิจิทัลและระบบอัตโนมัติเข้ามาประยุกต์ใช้ เพื่อเพิ่มประสิทธิภาพในการดูแลความปลอดภัยให้มีความแม่นยำ รวดเร็ว และสามารถควบคุมได้จากระยะไกล ระบบนี้ทำงานโดยอาศัยอุปกรณ์ตรวจจับ (sensor) เช่น เซ็นเซอร์ตรวจจับความเคลื่อนไหว (motion sensor) เซ็นเซอร์ตรวจจับการเปิด ปิดประตู หน้าต่าง (magnetic sensor) และ เซ็นเซอร์ตรวจจับควันหรือความร้อน (smoke/heat sensor) โดยเมื่อเซ็นเซอร์ตรวจพบความผิดปกติ ระบบจะประมวลผลและดำเนินการตามที่ตั้งค่าไว้ เช่น ส่งการแจ้งเตือนไปยังสมาร์ตโฟนของผู้ใช้งาน สั่งให้ไซเรนหรือสัญญาณเตือนทำงาน บันทึกภาพผ่านกล้องโทรทัศน์วงจรปิด แจ้งไปยังศูนย์ควบคุมหรือเจ้าหน้าที่รักษาความปลอดภัย (Kruegle, 2006; Fischer et al., 2018; Norman, 2018; Ismail, 2019) ซึ่งคุณลักษณะสำคัญของระบบความปลอดภัยอัจฉริยะ ได้แก่

1) การควบคุมผ่านอินเทอร์เน็ต เป็นการควบคุมผ่านระบบ IoT ซึ่งผู้ใช้งานสามารถตรวจสอบและควบคุมระบบได้ทุกที่ผ่านแอปพลิเคชัน เช่น การเปิด-ปิดระบบ การเฝ้าสังเกตแบบเรียลไทม์

2) การทำงานแบบอัตโนมัติ (automation) ระบบสามารถตั้งค่าให้ทำงานอัตโนมัติ เช่น เปิดไฟเมื่อมีการเคลื่อนไหว หรือแจ้งเตือนเมื่อมีผู้บุกรุก

3) การเชื่อมต่อหลายอุปกรณ์ (system integration) สามารถทำงานร่วมกับอุปกรณ์อื่น เช่น ระบบไฟฟ้า ระบบล็อกประตู หรือระบบดับเพลิง

4) การบันทึกและวิเคราะห์ข้อมูล (data logging and analysis) ระบบสามารถเก็บข้อมูลเหตุการณ์ย้อนหลัง เพื่อนำมาวิเคราะห์และปรับปรุงมาตรการรักษาความปลอดภัย

1.2 องค์ประกอบของระบบรักษาความปลอดภัยอัจฉริยะ (Components of Smart Security Systems)

ระบบรักษาความปลอดภัยอัจริยะ เป็นระบบที่ประกอบด้วยอุปกรณ์และกระบวนการทำงานหลายส่วนที่เชื่อมโยงกัน เพื่อให้สามารถตรวจจับ ควบคุม และตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างมีประสิทธิภาพ โดยองค์ประกอบหลักของระบบสามารถแบ่งออกเป็น 4 ส่วนสำคัญ ได้แก่ อุปกรณ์ตรวจจับ เครื่องควบคุม อุปกรณ์แจ้งเตือน และแหล่งพลังงานสำรอง

1.2.1 อุปกรณ์ตรวจจับในระบบรักษาความปลอดภัย

อุปกรณ์ตรวจจับ หรือเซ็นเซอร์ เป็นส่วนสำคัญที่ทำหน้าที่เฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติที่อาจเกิดขึ้นภายในพื้นที่ เช่น การบุกรุก การเคลื่อนไหว หรือการทำลายทรัพย์สิน โดยเซ็นเซอร์จะส่งสัญญาณไปยังเครื่องควบคุมเพื่อประมวลผลและดำเนินการต่อไป (Kruegle, 2006; Fennelly, 2017; Fischer et al., 2018; Norman, 2018; Ismail, 2019) เซ็นเซอร์มีหลายประเภท ขึ้นอยู่กับลักษณะการใช้งาน เช่น

1) แมกเนติกคอนแทคเตอร์ (magnetic contactor) ใช้ติดตั้งที่ประตูหรือหน้าต่าง ทำหน้าที่ตรวจจับการเปิด-ปิด หากมีการงัดแงะเปิดโดยไม่ได้รับอนุญาต จะส่งสัญญาณเตือนทันที

2) อุปกรณ์เซ็นเซอร์ในระบบสัญญาณกันขโมยที่ออกแบบมาเพื่อตรวจจับเสียงกระจกแตก (glass break detector) ใช้ตรวจจับแรงสั่นสะเทือนหรือเสียงที่เกิดจากการแตกของกระจก เหมาะสำหรับติดตั้งในพื้นที่ที่มีหน้าต่างหรือกระจกจำนวนมาก

3) เครื่องตรวจจับอินฟราเรด (infrared detector หรือ passive infrared: PIR) ใช้ตรวจจับการเคลื่อนไหวของบุคคลหรือวัตถุ โดยอาศัยการเปลี่ยนแปลงของพลังงานความร้อนในพื้นที่ เหมาะสำหรับติดตั้งภายในอาคารหรือพื้นที่ที่ต้องการเฝ้าระวัง

นอกจากนี้ ยังมีเซ็นเซอร์ประเภทอื่น ๆ เช่น เซ็นเซอร์ตรวจจับควัน (smoke detector) และเซ็นเซอร์ตรวจจับความร้อน (heat detector) ซึ่งช่วยเพิ่มความปลอดภัยในกรณีเกิดอัคคีภัยโดยรวมแล้ว อุปกรณ์ตรวจจับเปรียบเสมือน “ด่านหน้า” ของระบบรักษาความปลอดภัย ที่ช่วยให้สามารถรับรู้เหตุการณ์ได้อย่างรวดเร็วและแม่นยำ

1.2.2 อุปกรณ์ควบคุมในระบบรักษาความปลอดภัย

เครื่องควบคุม หรือศูนย์ควบคุมระบบ เป็นส่วนที่ทำหน้าที่เป็น “สมอง” ของระบบรักษาความปลอดภัย โดยรับข้อมูลจากเซ็นเซอร์ต่าง ๆ แล้วนำมาวิเคราะห์และประมวลผล เพื่อสั่งการให้อุปกรณ์อื่นทำงานตามที่กำหนดไว้ หน้าที่หลักของเครื่องควบคุม ได้แก่

1) รับข้อมูลจากเซ็นเซอร์ เครื่องควบคุมจะรับสัญญาณจากอุปกรณ์ตรวจจับทุกจุดภายในระบบ ไม่ว่าจะเป็นการเคลื่อนไหว การเปิดประตู หรือเหตุการณ์ผิดปกติอื่น ๆ

2) ประมวลผลเหตุการณ์ เมื่อได้รับข้อมูล เครื่องควบคุมจะวิเคราะห์ว่าข้อมูลนั้นเป็นเหตุการณ์ปกติหรือผิดปกติ โดยอิงจากค่าที่ตั้งไว้ เช่น เวลาใช้งาน พื้นที่ที่อนุญาต/เงื่อนไขเฉพาะ

3) สั่งงานอุปกรณ์ต่าง ๆ หากตรวจพบเหตุผิดปกติ เครื่องควบคุมจะสั่งงานอุปกรณ์ เช่น เปิดสัญญาณเตือนหรือไซเรน (siren) ส่งแจ้งเตือนไปยังผู้ใช้งานหรือศูนย์ควบคุม บันทึกภาพจากกล้องโทรทัศน์วงจรปิด และควบคุมการล็อกหรือปลดล็อกประตู

เครื่องควบคุมในปัจจุบันมีความสามารถสูง สามารถเชื่อมต่อกับระบบอื่น ๆ เช่น เครือข่ายอินเทอร์เน็ต แอปพลิเคชันบนมือถือ และระบบอัตโนมัติ ทำให้สามารถควบคุมระบบจากระยะไกล

1.2.3 อุปกรณ์แจ้งเตือนในระบบรักษาความปลอดภัย

อุปกรณ์แจ้งเตือนหรือไซเรน เป็นส่วนประกอบที่ทำหน้าที่ส่งสัญญาณเตือนเมื่อระบบตรวจพบเหตุการณ์ผิดปกติ โดยมีวัตถุประสงค์เพื่อแจ้งให้ผู้ที่อยู่ในพื้นที่รับทราบ และเป็นการยับยั้งหรือป้องกันผู้บุกรุก รูปแบบของการแจ้งเตือนสามารถแบ่งออกได้เป็น

1) สัญญาณเสียง เช่น เสียงไซเรน เสียงเตือนภัย

2) สัญญาณแสง เช่น ไฟกระพริบ

3) การแจ้งเตือนผ่านระบบสื่อสาร เช่น การแจ้งเตือนผ่านโทรศัพท์มือถือ หรือระบบเครือข่าย

การทำงานของไซเรนจะเชื่อมโยงกับเครื่องควบคุม เมื่อเครื่องควบคุมตรวจพบความผิดปกติ เช่น การบุกรุกหรือการงัดแงะ ระบบจะสั่งให้ไซเรนทำงานทันที การติดตั้งไซเรนควรคำนึงถึงตำแหน่งที่สามารถกระจายเสียงได้ทั่วถึง และยากต่อการเข้าถึงจากผู้บุกรุก เพื่อลดโอกาสในการถูกทำลายหรือปิดการทำงาน

1.2.4 แหล่งพลังงานสำรองในระบบรักษาความปลอดภัย

แหล่งพลังงานสำรอง เป็นอุปกรณ์ที่มีความสำคัญในการทำให้ระบบรักษาความปลอดภัยสามารถทำงานได้อย่างต่อเนื่อง แม้ในกรณีที่เกิดไฟฟ้าดับหรือถูกตัดกระแสไฟโดยทั่วไป ระบบรักษาความปลอดภัยจะต้องใช้พลังงานไฟฟ้าในการทำงาน หากไม่มีแหล่งพลังงานสำรอง ระบบจะหยุดทำงานทันที ซึ่งอาจก่อให้เกิดความเสี่ยงด้านความปลอดภัยได้ แบตเตอรี่สำรองจึงถูกติดตั้งไว้เพื่อรองรับสถานการณ์ฉุกเฉิน โดยมีคุณสมบัติสำคัญดังนี้ (1) สามารถจ่ายพลังงานให้ระบบได้ทันทีเมื่อไฟฟ้าหลักขัดข้อง (2) มีระบบชาร์จไฟอัตโนมัติเมื่อไฟฟ้ากลับมาใช้งาน และ (3) รองรับการทำงานของอุปกรณ์สำคัญ เช่น เครื่องควบคุม เซ็นเซอร์ และระบบแจ้งเตือน ในบางระบบอาจมีการใช้แหล่งพลังงานสำรอง เช่น แบตเตอรี่ร่วมกับเครื่องสำรองไฟ (Uninterruptible Power Supply: UPS) เพื่อเพิ่มความมั่นคงของระบบ การเลือกใช้แบตเตอรี่ควรพิจารณาความจุ ระยะเวลาในการสำรองไฟ และความเหมาะสมกับขนาดของระบบ เพื่อให้สามารถรองรับการทำงานในสถานการณ์ฉุกเฉินได้อย่างเพียงพอ โดยสรุปองค์ประกอบของระบบรักษาความปลอดภัย เมื่อพิจารณาองค์ประกอบทั้งหมด จะเห็นได้ว่าระบบรักษาความปลอดภัยทำงานแบบเป็นลำดับขั้น ดังนี้

1) เซ็นเซอร์ (sensor) ใช้สำหรับตรวจจับเหตุการณ์

2) เครื่องควบคุม (control unit) ใช้สำหรับประมวลผลข้อมูล

3) อุปกรณ์แจ้งเตือน (siren) ใช้สำหรับแจ้งเหตุการณ์

4) แหล่งพลังงานสำรอง (backup battery) สนับสนุนการทำงานต่อเนื่อง

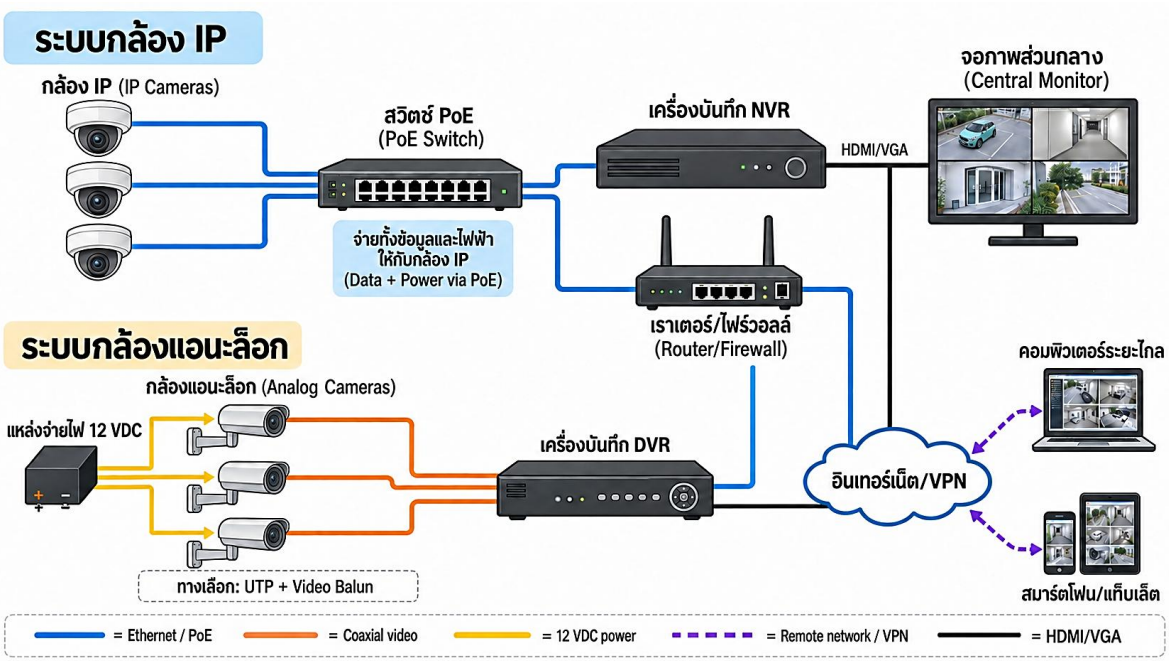
องค์ประกอบทั้ง 4 ส่วนนี้ทำงานร่วมกันอย่างเป็นระบบ เพื่อให้สามารถป้องกัน ตรวจจับ แจ้งเตือน และตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ

1.3 ประเภทของระบบรักษาความปลอดภัย (Types of Security Systems)

นอกจากระบบรักษาความปลอดภัยหลักแล้ว ยังมีระบบสนับสนุนอื่น ๆ ที่ทำงานร่วมกันเพื่อเพิ่มประสิทธิภาพในการป้องกัน เฝ้าระวัง และตอบสนองต่อเหตุการณ์ต่าง ๆ ระบบเหล่านี้มีบทบาทสำคัญในการเสริมความปลอดภัยให้ครอบคลุมมากยิ่งขึ้น ระบบที่เกี่ยวข้องกับงานรักษาความปลอดภัยที่สำคัญ

1.3.1 ระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV)

ระบบกล้องโทรทัศน์วงจรปิด เป็นระบบที่ใช้สำหรับตรวจสอบ เฝ้าระวัง และบันทึกภาพเหตุการณ์ภายในพื้นที่ที่ต้องการควบคุมหรือรักษาความปลอดภัย โดยภาพที่บันทึกได้สามารถนำมาใช้ในการเฝ้าระวังแบบเรียลไทม์ (real-time monitoring) และใช้เป็นหลักฐานสำหรับการตรวจสอบเหตุการณ์ย้อนหลังได้ องค์ประกอบหลัก ๆ ของระบบ CCTV ประกอบด้วย (1) กล้องโทรทัศน์วงจรปิด (camera) (2) เครื่องบันทึกภาพ (video recorder) ซึ่งแบ่งออกเป็น Digital Video Recorder (DVR) และ Network Video Recorder (NVR) (3) จอแสดงผล (monitor) และ (4) ระบบสายสัญญาณหรือระบบเครือข่ายสำหรับการรับส่งข้อมูล (Kruegle, 2006)



รูปที่ 1.1 ระบบระบบกล้องโทรทัศน์วงจรปิด

โครงสร้างและหลักการทำงานของระบบกล้องโทรทัศน์วงจรปิดแบบผสมผสาน (hybrid system) รูปที่ 1.1 เป็นการทำงานร่วมกันระหว่างกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก (analog camera) และกล้องโทรทัศน์วงจรปิดระบบดิจิทัล (IP camera) โดยกล้อง IP ส่งสัญญาณภาพผ่านสายเครือข่าย Cat 5e หรือ Cat 6 ไปยังสวิตช์เครือข่าย (network switch) ซึ่งทำหน้าที่รับส่งข้อมูลและจ่ายพลังงานผ่านเทคโนโลยี Power over Ethernet (PoE) ขณะที่กล้องแอนะล็อกส่งสัญญาณผ่านสายโคแอกเชียล เพื่อเชื่อมต่อเข้าสู่ระบบบันทึกภาพ ข้อมูลภาพจากกล้องทั้งสองประเภทจะถูกส่งไปยังเครื่องบันทึกภาพแบบผสม (DVR/NVR combo) บันทึกและจัดเก็บข้อมูลลงในฮาร์ดดิสก์ ผู้ใช้งานสามารถตรวจสอบภาพแบบเรียลไทม์ผ่านจอแสดงผลส่วนกลาง (central monitor) หรือเข้าถึงข้อมูลจากระยะไกลผ่านเครือข่ายอินเทอร์เน็ต โดยมีเราเตอร์ (router) ไฟร์วอลล์ (firewall) และโมเด็ม (modem) ทำหน้าที่เชื่อมต่อและรักษาความปลอดภัยของระบบ นอกจากนี้ยังสามารถเข้าถึงข้อมูลผ่านคอมพิวเตอร์ แท็บเล็ต หรือสมาร์ตโฟนได้ ทำให้ระบบสามารถเฝ้าระวัง บันทึก และตรวจสอบเหตุการณ์ได้อย่างมีประสิทธิภาพและต่อเนื่อง ประโยชน์ของระบบ CCTV ดังนี้ เฝ้าระวังและป้องกันเหตุการณ์ผิดปกติ ใช้ตรวจสอบเหตุการณ์ย้อนหลัง หรือเพิ่มความมั่นใจด้านความปลอดภัย

1.3.2 ระบบควบคุมการเข้า-ออก (Access Control System)

ระบบควบคุมการเข้า-ออก เป็นระบบที่ใช้ในการกำหนดสิทธิ์และควบคุมการเข้าถึงพื้นที่ของบุคคลหรือยานพาหนะ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และเพิ่มความปลอดภัยให้กับสถานที่ โดยระบบจะทำงานร่วมกับอุปกรณ์ต่าง ๆ เช่น แขนกั้นรถยนต์ (barrier gate) ระบบบัตร RFID และอุปกรณ์ตรวจสอบตัวตนอื่น ๆ

1) หลักการทำงานของระบบควบคุมการเข้า-ออก

ระบบควบคุมการเข้า-ออกจะเริ่มจากการตรวจสอบตัวตนของผู้ใช้งาน เมื่อบุคคลหรือยานพาหนะมาถึงจุดควบคุม เช่น ทางเข้าอาคารหรือประตูรั้ว ระบบจะทำการอ่านข้อมูลจากอุปกรณ์ยืนยันตัวตน เช่น บัตร RFID หรืออุปกรณ์สแกนอื่น ๆ หากข้อมูลตรงกับสิทธิ์ที่กำหนดไว้ ระบบจะส่งสัญญาณไปยังอุปกรณ์ควบคุม เช่น เปิดประตู ยกแขนกั้นรถยนต์ ในกรณีที่ไม่ผ่านการอนุญาต ระบบจะไม่เปิดทางเข้า และอาจมีการแจ้งเตือนเพื่อให้เจ้าหน้าที่ตรวจสอบเพิ่มเติม ตัวอย่างการใช้งาน เช่น การควบคุมรถเข้าออกในลานจอดรถ การเข้า-ออกหมู่บ้านหรืออาคารสำนักงาน หรือการควบคุมพื้นที่สำคัญ เช่น โรงงาน ธนาคาร หรือสถานที่ราชการ

2) องค์ประกอบของระบบควบคุมการเข้า-ออก

2.1) อุปกรณ์ระบุตัวตน (identification device) เช่น บัตร RFID หรือบัตรพนักงาน ใช้สำหรับระบุบุคคลหรือยานพาหนะ

2.2) เครื่องอ่านข้อมูล (reader) ทำหน้าที่อ่านข้อมูลจากบัตรหรืออุปกรณ์ระบุตัวตน

2.3) อุปกรณ์ควบคุม (controller) ทำหน้าที่ตรวจสอบสิทธิ์และสั่งงานอุปกรณ์อื่น เช่น ประตูหรือแขนกั้น

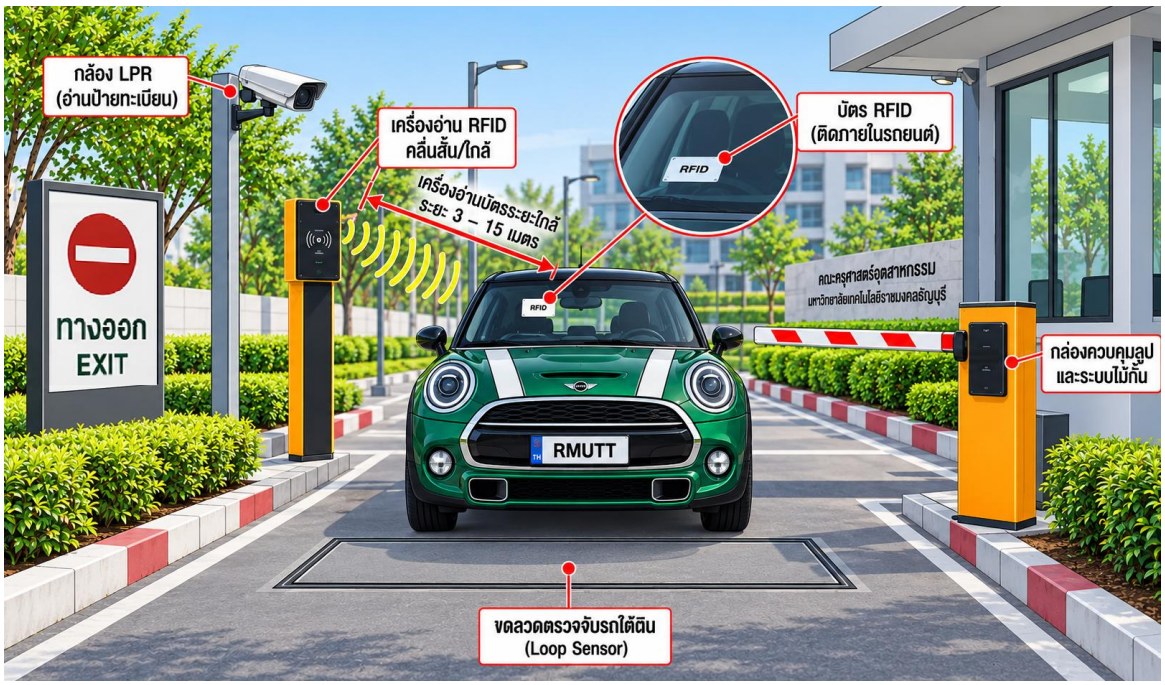
2.4) อุปกรณ์กั้นทาง (barrier/door control) เช่น แขนกั้นรถยนต์ ประตูไฟฟ้า

2.5) ระบบบันทึกข้อมูล (monitoring system) ใช้บันทึกข้อมูลการเข้า-ออก เพื่อการตรวจสอบย้อนหลัง

รูปที่ 1.2 ระบบควบคุมการเข้า-ออก

3) ปัจจัยในการเลือกใช้งานระบบควบคุมการเข้า-ออก

การเลือกใช้อุปกรณ์ เช่น แขนกั้นรถยนต์ ควรพิจารณา ความเร็วในการเปิด–ปิด (เช่น 1 วินาที (s), 3 s, 6 s) ปริมาณการจราจร ความยาวของไม้กั้น ลักษณะพื้นที่ใช้งาน โดยหากเป็นพื้นที่ที่มีรถจำนวนมาก เช่น ด่านเก็บเงินทางด่วน ควรเลือกแบบที่เปิด–ปิดเร็ว แต่ถ้าเป็นพื้นที่ทั่วไป เช่น หมู่บ้าน สามารถใช้ความเร็วปานกลางได้



(ก) อุปกรณ์ในระบบการควบคุมเข้า-ออก

(ข) หลักการทำงานของการตรวจสอบการเข้า-ออก

รูปที่ 1.3 หลักการทำงานของระบบควบคุมการเข้า-ออก

แขนกั้นรถอัตโนมัติ (boom barrier) เป็นอุปกรณ์ที่ใช้ควบคุมการเข้า-ออกของยานพาหนะ โดยมีให้เลือกใช้งานตามความเหมาะสมของพื้นที่ เช่น ความยาวไม้กั้น 3–6 เมตร (m) และสามารถติดตั้งอุปกรณ์เสริม เช่น แขนพับ 90 องศา สำหรับพื้นที่ที่มีข้อจำกัดด้านความสูง ตัวเครื่องออกแบบให้ทนทานต่อการใช้งานหนัก (heavy duty) เหมาะกับสภาพอากาศร้อน มีโครงสร้างทำจากวัสดุอลูมิเนียมเคลือบกันสนิม และใช้ระบบมอเตอร์เกียร์ที่ช่วยลดภาระการบำรุงรักษานอกจากนี้ ระบบยังรองรับการทำงานร่วมกับเทคโนโลยีระบุตัวตน เช่น บัตรหรือแท็ก RFID หลายความถี่ ได้แก่ 125 kHz, 13.56 MHz, 920–925 MHz และ 2.4 GHz โดยสามารถอ่านข้อมูลได้แบบไม่ต้องสัมผัส (contactless) ในระยะตั้งแต่ประมาณ 5 เซนติเมตร (cm) ถึง 5 m (ขึ้นอยู่กับชนิดของบัตรหรือแท็ก) ทำให้เหมาะสำหรับใช้งานในหมู่บ้าน อาคารสำนักงาน โรงงาน และลานจอดรถที่ต้องการความสะดวก รวดเร็ว และมีความปลอดภัยสูง

ความยาวของไม้แขนกั้นรถยนต์ โดยปกติจะมีให้หลายขนาด โดยส่วนมากความยาวของไม้แขนกั้นรถยนต์ (barrier gate) นั้นจะสัมพันธ์กับความเร็วของมอเตอร์ (บริษัท ซีเอ ออโตเมติก เกทส์ จำกัด, 2525) ดังนี้

- 1 s ความยาวไม้กั้น ยาวไม่เกิน 3 m
- 3 s ความยาวไม้กั้น ยาวไม่เกิน 4–4.5 m
- 6 s ความยาวไม้กั้น ยาวไม่เกิน 6 m

ระบบเสริมที่เกี่ยวข้องในการควบคุมการเข้า-ออกมักทำงานร่วมกับระบบอื่น เช่น ระบบกล้องโทรทัศน์วงจรปิด ระบบบันทึกเวลาเข้าออก (guard tour/time attendance) และระบบเครือข่ายและฐานข้อมูล

1.3.3 ระบบเสียงประกาศ (Public Address System: PA System)

ระบบเสียงประกาศ เป็นระบบที่ใช้สำหรับกระจายเสียงไปยังพื้นที่ต่าง ๆ ภายในอาคารหรือสถานที่ เพื่อสื่อสารข้อมูลข่าวสาร หรือแจ้งเตือนเหตุการณ์ต่าง ๆ ให้กับบุคคลจำนวนมากในเวลาเดียวกัน โดยมีบทบาทสำคัญทั้งในด้านการใช้งานทั่วไปและการแจ้งเตือนในภาวะฉุกเฉิน

1) หลักการทำงานของระบบ

ระบบเสียงประกาศทำงานโดยรับสัญญาณเสียงจากแหล่งกำเนิด เช่น ไมโครโฟน เครื่องเล่นเสียง หรือระบบควบคุมกลาง จากนั้นสัญญาณจะถูกส่งไปยังเครื่องขยายเสียง (amplifier) เพื่อเพิ่มกำลังเสียง ก่อนกระจายไปยังลำโพงที่ติดตั้งตามจุดต่าง ๆ ภายในพื้นที่ ทำให้ผู้ที่อยู่ในบริเวณนั้นสามารถได้ยินเสียงอย่างชัดเจนและทั่วถึง

2) องค์ประกอบของระบบ

2.1) แหล่งกำเนิดเสียง (audio source) เช่น ไมโครโฟน เครื่องเล่นสัญญาณเสียง

2.2) เครื่องขยายเสียง (amplifier) ทำหน้าที่เพิ่มกำลังของสัญญาณเสียง

2.3) ลำโพง (speaker) สำหรับกระจายเสียงไปยังพื้นที่ต่าง ๆ

2.4) อุปกรณ์ควบคุม (controller) ใช้ควบคุมการเลือกโซนหรือพื้นที่ที่ประกาศ

2.5) สายสัญญาณหรือระบบเครือข่าย สำหรับเชื่อมต่ออุปกรณ์ทั้งหมด

3) ประเภทของระบบเสียงประกาศ

3.1) ระบบประกาศทั่วไป (general PA system) ใช้สำหรับการประกาศข่าวสารหรือข้อมูลทั่วไป

3.2) ระบบประกาศฉุกเฉิน (emergency PA system) ใช้สำหรับการแจ้งเตือนในกรณีฉุกเฉิน เช่น ไฟไหม้ หรือการอพยพ

3.3) ระบบประกาศแบบแบ่งโซน (zoning system) สามารถเลือกประกาศเฉพาะพื้นที่ได้

4) ประโยชน์ของระบบ เช่น ช่วยสื่อสารกับบุคคลจำนวนมากได้อย่างรวดเร็ว ใช้แจ้งเตือนและควบคุมสถานการณ์ในกรณีฉุกเฉิน หรือเพิ่มประสิทธิภาพในการบริหารจัดการภายในองค์กร ระบบเสียงประกาศถูกนำไปใช้งานอย่างแพร่หลายในสถานที่ต่าง ๆ เช่น โรงเรียน โรงพยาบาล ห้างสรรพสินค้า โรงงาน อาคารสำนักงาน และสนามบิน

โดยสรุประบบเสียงประกาศเป็นองค์ประกอบสำคัญของระบบรักษาความปลอดภัยที่ช่วยในการสื่อสารและแจ้งเตือนอย่างมีประสิทธิภาพ โดยเฉพาะในสถานการณ์ฉุกเฉิน ซึ่งต้องการความรวดเร็วและความชัดเจนในการสื่อสารเพื่อความปลอดภัยของบุคคลในพื้นที่

1.3.4 ระบบแจ้งเตือนการบุกรุก (Intrusion Detection System)

ระบบแจ้งเตือนการบุกรุก (Intrusion Detection System: IDS) เป็นระบบที่ใช้สำหรับตรวจจับการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต และแจ้งเตือนเมื่อเกิดเหตุการณ์ผิดปกติ โดยมีบทบาทสำคัญในการป้องกันอาชญากรรมและลดความเสียหายต่อชีวิตและทรัพย์สิน

1) หลักการทำงานของระบบ

ระบบจะทำงานโดยอาศัยอุปกรณ์ตรวจจับที่ติดตั้งตามจุดต่าง ๆ เช่น ประตู หน้าต่าง หรือพื้นที่เสี่ยง เมื่อมีการเคลื่อนไหวหรือการกระทำที่ผิดปกติ เช่น การงัดแงะหรือการบุกรุก เซ็นเซอร์จะส่งสัญญาณไปยังเครื่องควบคุม (control panel) เพื่อประมวลผล หากพบว่าเป็นเหตุการณ์ผิดปกติ ระบบจะสั่งให้เกิดการแจ้งเตือน เช่น เสียงไซเรน ไฟกระพริบ หรือส่งสัญญาณไปยังผู้ดูแลผ่านโทรศัพท์หรือแอปพลิเคชัน

2) องค์ประกอบของระบบ

2.1) อุปกรณ์ตรวจจับ (sensor) ได้แก่ เซ็นเซอร์ตรวจจับการเคลื่อนไหว (motion sensor) เซ็นเซอร์ประตู/หน้าต่าง (magnetic contact) และเซ็นเซอร์ลำแสงอินฟราเรด (infrared beam)

2.2) เครื่องควบคุม (control panel) ทำหน้าที่รับสัญญาณ วิเคราะห์ สั่งการระบบ

2.3) อุปกรณ์แจ้งเตือน (alarm device) เช่น ไซเรน หรือไฟสัญญาณ

2.4) ระบบสื่อสาร (communication module) ใช้ส่งการแจ้งเตือนไปยังผู้ใช้งาน เช่น ผ่านเครือข่ายโทรศัพท์หรืออินเทอร์เน็ต

3) ประเภทของระบบ เช่น ระบบตรวจจับภายใน (indoor system) ใช้สำหรับตรวจจับภายในอาคาร ระบบตรวจจับภายนอก (outdoor system) ใช้สำหรับพื้นที่รอบนอก เช่น รั้วหรือกำแพง ระบบตรวจจับตามแนวเส้น (perimeter system) เช่น ระบบลำแสงอินฟราเรดตามแนวรั้ว

4) ประโยชน์ของระบบ เช่น ตรวจจับการบุกรุกได้อย่างรวดเร็ว ลดความเสี่ยงจากการโจรกรรมหรือความเสียหาย เพิ่มความปลอดภัยให้กับสถานที่ โดยสามารถทำงานร่วมกับระบบอื่น เช่น CCTV และ access control นิยมใช้ในสถานที่ที่ต้องการความปลอดภัย เช่น บ้านพักอาศัย อาคารสำนักงาน โรงงาน โกดังสินค้า ธนาคาร และสถานที่ราชการ

โดยสรุประบบแจ้งเตือนการบุกรุกเป็นระบบสำคัญที่ช่วยตรวจจับและแจ้งเตือนเหตุการณ์ผิดปกติได้อย่างทันท่วงที ทำให้สามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว และช่วยเพิ่มประสิทธิภาพของระบบรักษาความปลอดภัยโดยรวม

1.3.5 ระบบแจ้งเหตุเพลิงไหม้ (Fire Alarm System)

ระบบแจ้งเหตุเพลิงไหม้เป็นระบบสำคัญที่ใช้ในการตรวจจับและแจ้งเตือนเมื่อเกิดเหตุอัคคีภัย เพื่อให้สามารถอพยพผู้คนและควบคุมสถานการณ์ได้อย่างทันท่วงที ลดความสูญเสียต่อชีวิตและทรัพย์สิน ระบบทำงานอัตโนมัติร่วมกับอุปกรณ์ตรวจจับและอุปกรณ์แจ้งเตือนต่าง ๆ ภายในอาคาร

1) หลักการทำงานของระบบ

ระบบจะตรวจจับสัญญาณเริ่มต้นของเพลิงไหม้ เช่น ควัน ความร้อน หรือเปลวไฟ ผ่านอุปกรณ์ตรวจจับ (detector) เมื่อค่าที่ตรวจวัดได้เกินกว่าที่กำหนด ระบบจะส่งสัญญาณไปยังตู้ควบคุม (Fire Alarm Control Panel: FACP) เพื่อประมวลผล จากนั้นจะสั่งให้อุปกรณ์แจ้งเตือน เช่น เสียงไซเรน หรือไฟสัญญาณทำงาน พร้อมทั้งอาจเชื่อมต่อกับระบบอื่น เช่น ระบบสปริงเกลอร์ (sprinkler system) ระบบเสียงประกาศ (PA system) ระบบควบคุมลิฟต์และการอพยพ ระบบตัดไฟฟ้าอัตโนมัติ

2) องค์ประกอบของระบบ

2.1)อุปกรณ์ตรวจจับ (detector) ได้แก่ เครื่องตรวจจับควัน (smoke detector) เครื่องตรวจจับความร้อน (heat detector) เครื่องตรวจจับเปลวไฟ (flame detector)

2.2)อุปกรณ์แจ้งเหตุ (alarm device) ได้แก่ ไซเรน (siren) ไฟกระพริบ (strobe light)

2.2.1) อุปกรณ์แจ้งเหตุด้วยมือ (manual call point) ใช้สำหรับการกดแจ้งเหตุเมื่อพบเพลิงไหม้

2.2.2) ตู้ควบคุมระบบ (control panel) ซึ่งเป็นศูนย์กลางในการรับข้อมูล ประมวลผล และสั่งงานอุปกรณ์

2.3) ระบบสายสัญญาณและแหล่งพลังงานสำรอง เพื่อให้ระบบทำงานได้อย่างต่อเนื่องแม้ไฟฟ้าดับ

2.4) ประโยชน์ของระบบ เช่น ตรวจจับเหตุเพลิงไหม้ได้อย่างรวดเร็ว แจ้งเตือนให้สามารถอพยพได้ทันเวลา ลดความเสียหายต่อชีวิตและทรัพย์สิน เพิ่มความปลอดภัยให้กับอาคารและผู้ใช้งาน

โดยสรุประบบแจ้งเหตุเพลิงไหม้เป็นระบบที่มีบทบาทสำคัญในการป้องกันและลดความสูญเสียจากอัคคีภัย โดยอาศัยการทำงานร่วมกันของอุปกรณ์ตรวจจับ ระบบควบคุม และอุปกรณ์แจ้งเตือน ทำให้สามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ

1.4 มาตรฐานและกฎหมายที่เกี่ยวข้องกับระบบรักษาความปลอดภัย (Security Standards and Regulations)

อุปกรณ์และระบบรักษาความปลอดภัยระดับสากลสำหรับสถานที่และทรัพย์สิน (international security equipment and system for premises and properties) ตามมาตรฐานสากล เช่น แนวทางของสหรัฐอเมริกา (United States Sentencing Guidelines: USSG) มุ่งเน้นการควบคุมและบริหารจัดการพื้นที่อย่างเป็นระบบ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคาม โดยอาศัยทั้งบุคลากร เทคโนโลยี และกระบวนการทำงานร่วมกันอย่างมีประสิทธิภาพ องค์ประกอบสำคัญของระบบรักษาความปลอดภัยสามารถสรุปได้เป็น 3 ด้านหลัก ได้แก่

1) การควบคุมบุคคลและยานพาหนะ

การกำหนดมาตรการเข้า-ออกพื้นที่ เพื่อให้สามารถตรวจสอบและจำกัดสิทธิ์การเข้าถึงได้อย่างเหมาะสม

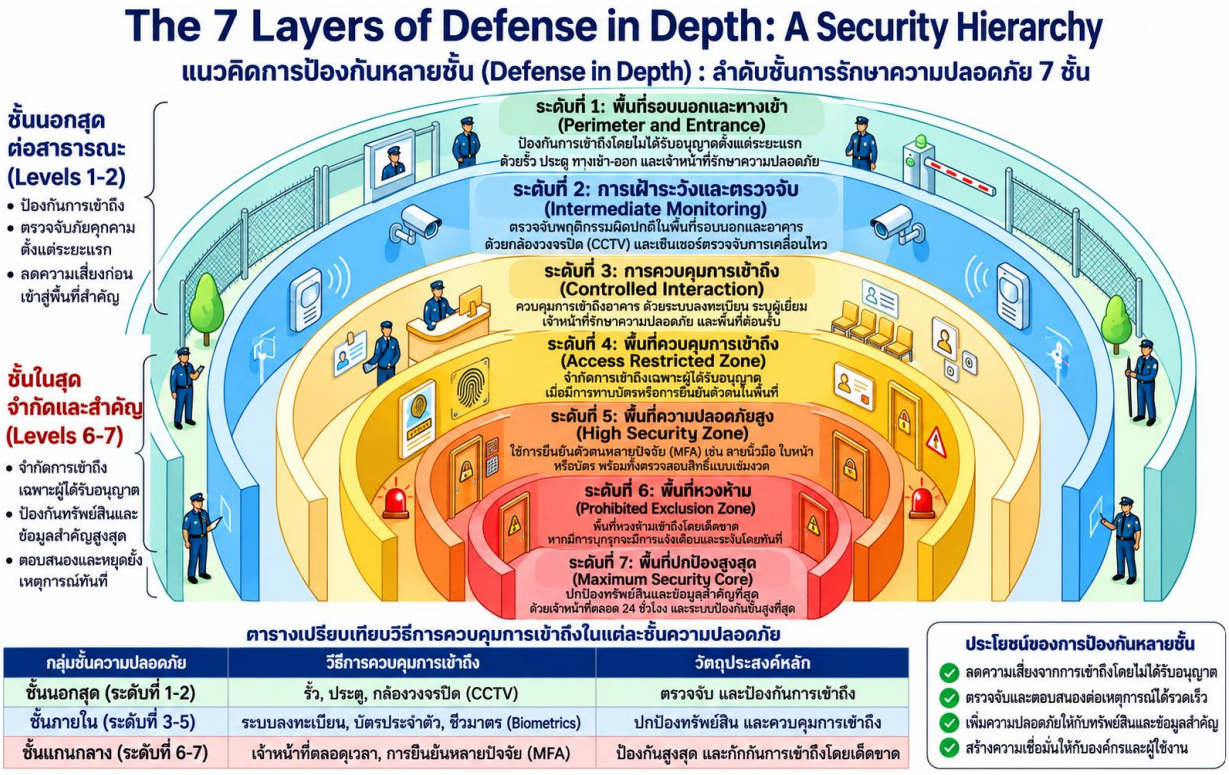
2) การใช้อุปกรณ์รักษาความปลอดภัย

การนำเครื่องมือและเทคโนโลยีมาใช้ในการตรวจสอบ ควบคุม และเฝ้าระวังพื้นที่ในแต่ละระดับความปลอดภัย

3) การตรวจตราและเฝ้าระวังอย่างต่อเนื่อง

การปฏิบัติงานของเจ้าหน้าที่รักษาความปลอดภัย เพื่อเฝ้าระวังเหตุการณ์และตรวจสอบความเรียบร้อยภายในพื้นที่ การแบ่งระดับพื้นที่ตามความปลอดภัย การจัดระบบรักษาความ

ปลอดภัยแบ่งพื้นที่ออกเป็นลำดับชั้นตามระดับความสำคัญและความเสี่ยง โดยทั่วไปสามารถแบ่งออกเป็น 7 ระดับ ดังนี้ (1) ระดับที่ 1 พื้นที่รั้วและทางเข้าสถานที่ (2) ระดับที่ 2 พื้นที่ระหว่างรั้วถึงตัวอาคารหรือห้องรับรอง (3) ระดับที่ 3 พื้นที่ภายในห้องรับรอง (4) ระดับที่ 4 พื้นที่ภายในอาคารที่เก็บทรัพย์สินหรือข้อมูลสำคัญ (restrict zone) 5) ระดับที่ 5 พื้นที่หวงห้าม (forbidding zone) (6) ระดับที่ 6 พื้นที่ห้ามเข้าโดยเด็ดขาด (exclusion zone) และ (7) ระดับที่ 7 พื้นที่ที่มีความสำคัญสูงสุดหรือมีความเสี่ยงสูงมาก (องค์การรักษาความปลอดภัยฝ่ายพลเรือน, 2015)



รูปที่ 1.4 การแบ่งระดับพื้นที่ตามความปลอดภัยขององค์การรักษาความปลอดภัยฝ่ายพลเรือน

การแบ่งระดับพื้นที่ตามความปลอดภัย ในบริบทของประเทศไทยนั้นพื้นที่ส่วนใหญ่ เช่น โรงงาน อาคารสำนักงาน ธนาคาร สถานทูต หรือเรือนจำ มักใช้มาตรการรักษาความปลอดภัยในช่วงระดับที่ 1 ถึงระดับที่ 4 เป็นหลัก เนื่องจากเป็นระดับที่ครอบคลุมการใช้งานทั่วไปและสามารถนำไปประยุกต์ใช้ได้จริงในสถานประกอบการส่วนใหญ่ ดังนั้น เนื้อหาในลำดับถัดไปจะมุ่งอธิบายรายละเอียดของระบบรักษาความปลอดภัยในระดับที่ 1 ถึงระดับที่ 4 จากรูปที่ 1.4 การแบ่งระดับพื้นที่ตามความปลอดภัย สามารถอธิบายได้ดังนี้

1.4.1 ระดับที่ 1 พื้นที่รั้วและทางเข้าสถานที่

พื้นที่ระดับนี้เป็นแนวป้องกันชั้นแรกของสถานที่ มีหน้าที่ควบคุมการเข้า-ออกของบุคคลและยานพาหนะ โดยเฉพาะในสถานที่ที่ต้องการความปลอดภัยสูง เช่น โรงงาน ธนาคาร หรือหน่วยงานสำคัญ ทั้งนี้สามารถปรับระดับความเข้มงวดได้ตามความสำคัญของพื้นที่

1) การควบคุมบุคคล

บริเวณทางเข้าควรจัดให้มีจุดคัดกรอง เช่น อาคารหรือจุดตรวจของเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) บุคคลภายในองค์กรสามารถผ่านเข้าออกได้โดยใช้ระบบยืนยันตัวตน เช่น บัตรพนักงาน เครื่องอ่านบัตร หรือระบบชีวมิติ เช่น เครื่องสแกนลายนิ้วมือ สำหรับผู้มาติดต่อจะต้องผ่านกระบวนการลงทะเบียน ตรวจสอบข้อมูล และบันทึกภาพ พร้อมออกบัตรผ่านก่อนเข้าสู่พื้นที่ภายใน โดยอาจมีเจ้าหน้าที่ควบคุมดูแลหรือพาเข้าไปยังจุดหมายตามความเหมาะสม

2) อุปกรณ์ที่ใช้ในทางเข้าบุคคล

2.1)กล้องโทรทัศน์วงจรปิด (CCTV)

2.2)บัตรประจำตัวพนักงานและบัตรผู้มาติดต่อ

2.3)กล้องถ่ายภาพสำหรับบันทึกข้อมูล

2.4)เครื่องกั้นทางเข้า เช่น turnstile หรือ barrier

2.5)เครื่องอ่านบัตร (card reader)

2.6)เครื่องสแกนลายนิ้วมือ (fingerprint scanner)

2.7)เครื่องสแกนใบหน้า (face scan/facial recognition)

3) การควบคุมยานพาหนะ

ทางเข้ารถควรติดตั้งอุปกรณ์ควบคุม เช่น แขนกั้นรถยนต์ และระบบตรวจสอบยานพาหนะ โดยใช้กล้องโทรทัศน์วงจรปิดและระบบอ่านบัตรอัตโนมัติ เช่น RFID หรือระบบอ่านระยะไกล

4) แนวทางป้องกันการบุกรุก

ในกรณีพื้นที่ที่มีความเสี่ยงสูง อาจกำหนดให้มีพื้นที่จอดรถภายนอก ใช้ระบบควบคุมเพิ่มเติม เช่น การอ่านบัตรผ่านรถ หรือการตรวจสอบโดยเจ้าหน้าที่ รวมถึงการติดตั้งรั้วเสริม หรือระบบตรวจจับการบุกรุก เช่น เซ็นเซอร์อินฟราเรด เพื่อแจ้งเตือนเมื่อมีการลักลอบเข้า-ออก

1.4.2 ระดับที่ 2 พื้นที่ระหว่างรั้วถึงอาคาร

พื้นที่ระดับนี้เป็นเขตเฝ้าระวังที่อยู่ระหว่างแนวรั้วกับตัวอาคาร มีบทบาทในการตรวจจับความผิดปกติก่อนเข้าสู่พื้นที่สำคัญ ควรติดตั้งระบบตรวจจับ เช่น เซ็นเซอร์แม่เหล็กที่ประตูหรือหน้าต่าง รวมถึงระบบสัญญาณเตือนภัย (alarm system) ที่สามารถแจ้งเตือนทันทีเมื่อมีเหตุการณ์ผิดปกติ งัดแงะ หรือบุกรุก นอกจากนี้ควรมีระบบกล้องโทรทัศน์วงจรปิดที่ครอบคลุมพื้นที่โดยรอบอาคาร โดยเฉพาะกล้องแบบหมุนได้ (speed dome หรือ PTZ camera) ซึ่งสามารถควบคุมทิศทางการมองเห็น และบางรุ่นสามารถติดตามวัตถุเคลื่อนไหวได้โดยอัตโนมัติ

1) อุปกรณ์ที่ใช้ในพื้นที่ระดับนี้

1.1) ระบบสัญญาณเตือนภัย (alarm system) เช่น เซ็นเซอร์แม่เหล็ก (magnetic sensor) ชุดควบคุม และสัญญาณเตือน

1.2) กล้องโทรทัศน์วงจรปิดภายนอกอาคาร เช่น กล้องมาตรฐาน กล้องแบบโดม หรือกล้องแบบติดตั้งภายนอก (box camera)

1.3) ระบบตรวจตรา (guard tour system)

1.4.3 ระดับที่ 3 พื้นที่ภายในห้องรับรอง

พื้นที่ระดับนี้เป็นจุดต้อนรับและควบคุมการเข้าถึงสำหรับบุคคลภายนอก โดยออกแบบให้มีความสะดวกควบคู่กับความปลอดภัย ระบบเข้าออกอาจใช้เทคโนโลยี เช่น เครื่องอ่านบัตร หรือระบบเปิดประตูแบบไม่สัมผัส (touchless sensor) เพื่อเพิ่มความสะดวกแก่ผู้ใช้งาน ผู้มาติดต่อจะต้องลงทะเบียนและรอในพื้นที่ที่กำหนด โดยเจ้าหน้าที่หรือพนักงานจะเป็นผู้ประสานงานภายในและควบคุมการเข้าถึงในขั้นตอนถัดไป อุปกรณ์ที่ใช้ในพื้นที่ระดับนี้

1) เครื่องอ่านบัตรหรือระบบควบคุมประตู
2) ระบบสวิตช์ไร้สัมผัส (touchless switch)
3) กล้องโทรทัศน์วงจรปิด

1.4.4 ระดับที่ 4 พื้นที่ภายในอาคารที่มีความสำคัญ

พื้นที่ระดับนี้เป็นเขตควบคุมพิเศษสำหรับเก็บทรัพย์สินหรือข้อมูลสำคัญ จึงต้องมีมาตรการรักษาความปลอดภัยที่เข้มงวด ควรกำหนดสิทธิ์การเข้าถึงอย่างชัดเจน เช่น บุคคลที่สามารถเข้าได้ บุคคลที่ต้องเข้าเป็นคู่ (two-person rule) และเงื่อนไขในการปฏิบัติงานภายในพื้นที่ การยืนยันตัวตนควรใช้ระบบชีวมิติ เช่น การสแกนลายนิ้วมือ ใบหน้า หรือม่านตา โดยอาจกำหนดให้ต้องยืนยันพร้อมกันมากกว่าหนึ่งคนในบางกรณี นอกจากนี้ ควรติดตั้งระบบกล้องโทรทัศน์วงจรปิดทั้งภายในและภายนอกห้อง รวมถึงระบบแจ้งเตือนเมื่อมีการเปิดประตูหรือหน้าต่างโดยไม่ได้รับอนุญาต อุปกรณ์ที่ใช้ในพื้นที่ระดับนี้

1) ระบบยืนยันตัวตนแบบชีวมิติ (biometric system) เช่น เครื่องสแกนม่านตา เครื่องสแกนใบหน้า และ เครื่องสแกนลายนิ้วมือ หรือแบบใช้งานร่วมกัน
2) ระบบสัญญาณเตือนการบุกรุก
3) กล้องโทรทัศน์วงจรปิดภายในและหน้าห้อง

1.5 หลักความปลอดภัยในการปฏิบัติงานด้านไฟฟ้า (Principles of Electrical Safety)

1.5.1 ข้อควรปฏิบัติเกี่ยวกับความปลอดภัยในการปฏิบัติงานไฟฟ้า

ปัจจุบันไฟฟ้ามีการจำเป็นต่อชีวิตประจำวันมาก ซึ่งไม่มีใครปฏิเสธถึงความสะดวกสบายที่ได้รับจากการใช้ไฟฟ้ารวมถึงงานอุตสาหกรรม และธุรกิจต้องใช้ไฟฟ้าเป็นปัจจัยสำคัญ ไฟฟ้ามีประโยชน์มากมายก็จริงแต่ในเวลาเดียวกันก็มีอันตรายอยู่ในตัวของมันเองถ้ารู้จักใช้ก็จะได้ประโยชน์มหาศาล ถ้าใช้ผิดวิธีก็อาจจะได้รับอันตรายถึงชีวิตจึงควรเข้าใจ และรู้พื้นฐานทางด้านความปลอดภัยในการใช้ เพราะความประมาทการสูญเสียต่างๆ ในชีวิตประจำวันของเรา ดังนั้นความปลอดภัยในการใช้ไฟฟ้าจึงเป็นเรื่องที่ควรได้รับความสนใจในการศึกษา ไฟฟ้าทำอันตรายให้แก่ร่างกายได้ผู้ที่จะได้รับอันตรายจากเครื่องใช้ไฟฟ้านั้น เนื่องจากส่วนหนึ่งส่วนใดของร่างกายสัมผัสหรือต่อเป็นส่วนหนึ่งในวงจรไฟฟ้า เมื่อมนุษย์ถูกไฟฟ้าดูดอันตรายหรืออาการบาดเจ็บที่ได้รับขึ้นอยู่กับปัจจัยสำคัญ 6 ประการ ดังต่อไปนี้

1) ความต้านทานภายในร่างกายมนุษย์คิดเป็นร้อยละของค่า แต่ถ้าผิวหนังเปียกความต้านทานจะลดลงเหลือเพียง 1,000 โอห์ม (Ω) เมื่อถูกกระแสไฟฟ้าดูดความต้านทานระหว่างมือถึงมือ กล่าวคือ ผิวหนังแห้งจะมีความต้านทานประมาณ 100,000 – 600,000 Ω เนื้อเยื่อกระดูก และระบบประสาททั้งหมดจะเกิดการนำไฟฟ้าทำให้ความต้านทานของผิวหนังลดลงและกระแสไฟฟ้า จะไหลผ่านร่างกายเพิ่มขึ้นอย่างรวดเร็วทำให้เกิดการบาดเจ็บอย่างรุนแรงถึงขั้นเสียชีวิตได้ โดยร่างกายของมนุษย์มีความต้านกระแสไฟฟ้าต่างกัน ขึ้นอยู่กับการพื้นที่ของร่างกายที่สัมผัสกับกระแสไฟฟ้า ดังนี้

- จากมือถึงมือ มีความต้านทานประมาณ 500 Ω
- จากมือถึงเท้า 1 ข้าง มีความต้านทานประมาณ 1,300 Ω
- จากมือถึงเท้า 2 ข้าง มีความต้านทานประมาณ 1,000 Ω
- จากมือ 2 ข้าง ถึงเท้า 2 ข้าง มีความต้านทานประมาณ 600 Ω

2) แรงดันไฟฟ้า อันตรายจากกระแสไฟฟ้าจะรุนแรงขึ้นเมื่อแรงดันไฟฟ้าเพิ่มสูงขึ้น รายละเอียดแสดงดังตารางที่ 1.1

ตารางที่ 1.1 อันตรายต่อรางกายจากกระแสไฟฟ้าจากการเพิ่มขึ้นของแรงดันไฟฟ้า

แรงดันไฟฟ้า (V)	อาการ
20 - 60	ช็อค ไม่สามารถสะบัดมือให้หลุดได้
40 - 100	หยุดหายใจ
80 - 100	กล้ามเนื้อหัวใจกระตุกหรือเต้นถี่รัว
มากกว่า 240	ผิวหนังฉีกขาด
มากกว่า 600	ผิวหนังไหม้

3) กระแสไฟฟ้าปริมาณกระแสไฟฟ้าที่ไหลผ่านร่างกาย รายละเอียดแสดงดังตารางที่ 1.2

ตารางที่ 1.2 แสดงอาการที่ได้รับจากปริมาณกระแสไฟฟ้าที่ไหลผ่านร่างกาย

ปริมาณ กระแสไฟฟ้า (mA)	อาการ
ต่ำกว่า 0.5	ยังไม่มีผลหรือยังไม่รู้สึก
0.5 – 2	รู้สึกว่าถูกไฟดูด
2 – 8	กระทบกระเทือนต่อระบบประสาท กล้ามเนื้อหดตัว เกิดอาการกระตุก
8 – 20	กระทบกระเทือนต่อระบบประสาท กล้ามเนื้อเกร็งหดตัวอย่างรุนแรงบางคนไม่สามารถปล่อยมือให้หลุดได้
20 – 25	กระทบกระเทือนต่อระบบประสาท กล้ามเนื้อหดตัวอย่างรุนแรงไม่สามารถ ปล่อยมือให้หลุดออกได้ ปอดทำงานผิดปกติมีโอกาสเสียชีวิตใน 2-3 นาที
สูงกว่า 100	หัวใจหยุดเต้น ผิวหนังไหม้ กล้ามเนื้อไม่ทำงาน

โดยสรุปปริมาณไฟฟ้าที่มีอันตรายถึงชีวิต คือ

- กระแสสูงกว่า 50 mA เป็นอันตรายถึงชีวิต
- แรงดันไฟฟ้ากระแสสลับ สูงกว่า 50 V เป็นอันตรายถึงชีวิต
- แรงดันไฟฟ้ากระแสตรง ที่สูงกว่า 120 V เป็นอันตรายถึงชีวิต
- สำหรับเด็กและสัตว์แรงดันไฟฟ้าเพียงครึ่งหนึ่ง เป็นอันตรายถึงชีวิต (25 VAC และ 60 VDC)

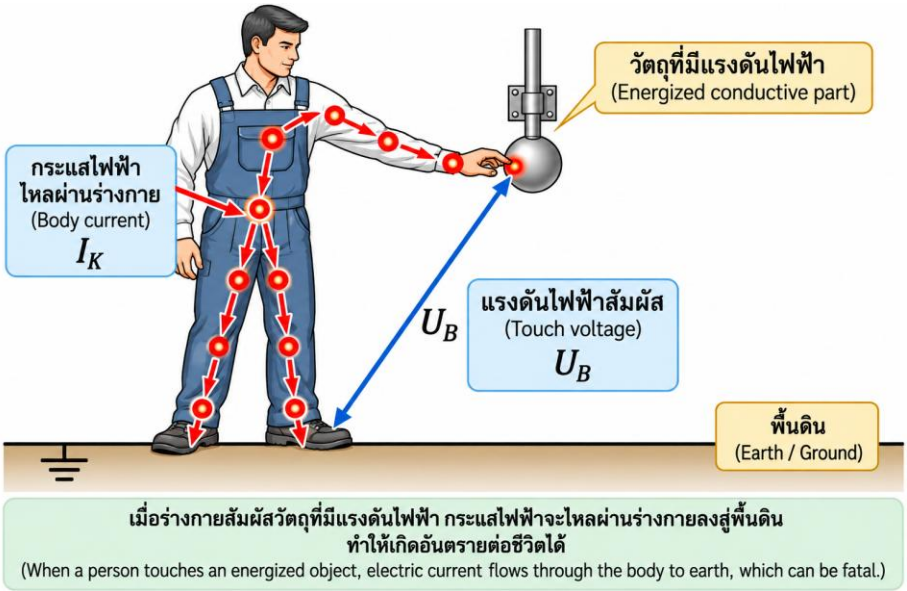
4) ระยะเวลาที่สัมผัสหรือระยะเวลาที่กระแสไฟฟ้าไหลผ่านหากร่างกายสัมผัสกับวงจรไฟฟ้าเป็นเวลานาน อันตรายที่ได้รับก็จะมีมากขึ้นและรุนแรง แสดงดังตารางที่ 1.3

ตารางที่ 1.3 ความสัมพันธ์ระหว่างปริมาณกระแสไฟฟ้า ระยะเวลา และอาการที่ได้รับ

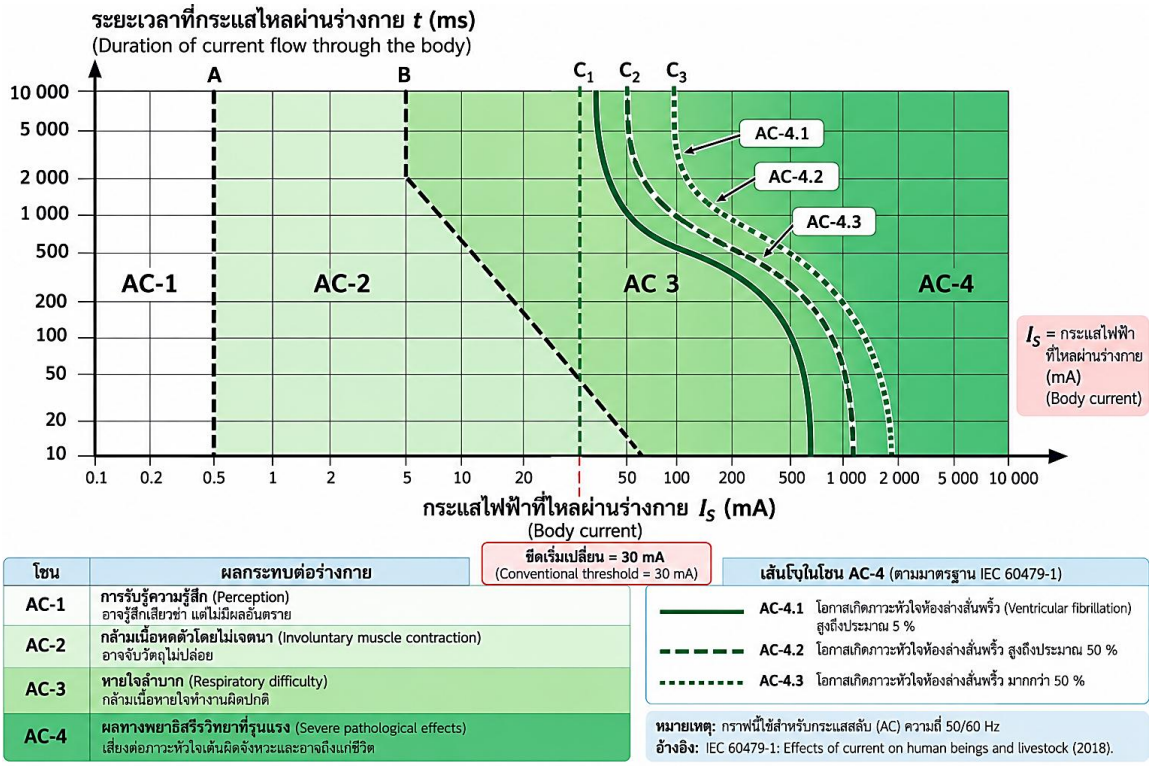
ปริมาณกระแสไฟฟ้า	ระยะเวลาที่ไหลผ่าน	อาการ
100 mA	นานกว่า 3 วินาที	เสียชีวิต
500 mA	นานกว่า 0.1 วินาที	เสียชีวิต
1,000 mA	นานกว่า 0.03 วินาที	เสียชีวิต

5) ความถี่ของระบบไฟฟ้า เมื่อความถี่เพิ่มขึ้นความต้านทานของร่างกายจะลดลง โดยความต้านทานของร่างกายจะมีค่าสูงสุดที่ความถี่ 50/60 Hz ทั้งนี้ระดับกระแสไฟฟ้าที่ทำให้กล้ามเนื้อควบคุมไม่ได้ จะแปรผันตรงกับความถี่ไฟฟ้าเช่นที่ความถี่ 60 Hz กระแสไฟฟ้าที่มากกว่า 10 mA จะทำให้กล้ามเนื้อควบคุมไม่ได้

6) ส่วนของร่างกายที่กระแสไฟฟ้าไหลผ่าน หากกระแสไฟฟ้าไหลผ่านศีรษะ หัวใจ และทรวงอก จะก่อให้เกิดอันตรายถึงชีวิตได้มากกว่าไหลผ่านส่วนอื่นๆ ของร่างกาย กราฟความสัมพันธ์ระหว่างกระแสไฟฟ้าและเวลาที่มีผลต่อร่างกาย ดังรูปที่ 1.5 และรูปที่ 1.6



รูปที่ 1.5 แสดงลักษณะของกระแสไฟฟ้าที่ไหลผ่านร่างกาย (ดัดแปลงจาก Thai Meister, 2017)



รูปที่ 1.6 กราฟความสัมพันธ์ระหว่างกระแสไฟฟ้าและเวลาที่มีผลต่อร่างกายสำหรับผู้ใหญ่ (ดัดแปลงจาก Häberle et al., 2015; Thai Meister, 2017; ชลดา ปานสง และคณะ, 2565)

7) สาเหตุของการเกิดอุบัติเหตุเกี่ยวกับงานไฟฟ้า

7.1) คนงานขาดความรู้และความเข้าใจเกี่ยวกับไฟฟ้า

7.2) คนงานขาดความระมัดระวัง ไม่เห็นถึงอันตรายของไฟฟ้า ทำอะไรด้วยความเคยชินจนกลายเป็นความประมาท อันเป็นสาเหตุสำคัญของการเกิดอันตราย

7.3) บางโรงงานก่อสร้างมานานหลายปี ไม่มีการปรับปรุงดูแลระบบไฟฟ้าเลย เป็นผลให้แปลนวงจรไฟฟ้าอาจชำรุดเสียหาย และก่อให้เกิดอันตรายได้ในวันใดวันหนึ่ง

7.4) มีการต่อเติมระบบไฟฟ้าขึ้นโดยไม่มีผู้เชี่ยวชาญในการแก้ไข

7.5) บางโรงงานเองขาดช่างเทคนิคด้านไฟฟ้า จึงใช้ช่างในส่วนอื่นๆ ที่อาจมีความรู้ด้านไฟฟ้าบ้าง ซึ่งอาจทำให้เกิดข้อบกพร่องในการตรวจสอบระบบไฟฟ้า

7.6) การขาดงบประมาณในการใช้อุปกรณ์ไฟฟ้าที่ได้มาตรฐาน ในบางโรงงานเองไม่เห็นความสำคัญของระบบไฟฟ้า จึงให้งบในการจัดซื้อวัสดุอุปกรณ์ในวงจำกัด ทำให้ไม่สามารถจัดหาอุปกรณ์ที่ได้คุณภาพเป็นผลให้อุปกรณ์ไฟฟ้าชำรุดเร็วหรือเสียหายได้

8) หลักความปลอดภัยในการปฏิบัติงานด้านไฟฟ้า

8.1) การป้องกันอันตรายจากงานไฟฟ้า

การใช้งานหรือทำงานเกี่ยวข้องกับไฟฟ้าอยู่ ทั้งในและนอกอาคารเพื่อความปลอดภัยต่อตนเองและผู้อื่น จึงควรเอาใจใส่ดูแลอุปกรณ์เครื่องใช้ไฟฟ้าและอุปกรณ์อิเล็กทรอนิกส์ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ (ไวพจน์ ศรีธัญ และวีรธรรม ไชยยงค์, 2558)

8.1.1) อย่าเข้าใกล้หรือแตะสายไฟฟ้าที่ห้อยลงมาหรือตกอยู่กับพื้น เพราะอาจมีกระแสไฟฟ้าอยู่ควรแจ้งการไฟฟ้าใกล้บ้านโดยเร็ว

8.1.2) การก่อสร้างใกล้แนวสายไฟฟ้า ควรติดต่อการไฟฟ้าเพื่อดำเนินการนำฉนวนมาครอบสายไฟฟ้าแรงสูงเพื่อป้องกันอันตรายจากไฟฟ้าดูด

8.1.3) พบกิ่งไม้ใกล้แนวสายไฟฟ้าแรงสูง ไม่ควรตัดเอง เพราะอาจถูกกระแสไฟฟ้าดูดได้ ควรแจ้งการไฟฟ้าใกล้บ้านทำการตัดออก

8.1.4) ไม่ควรยิงนกที่เกาะสายไฟฟ้า หรือใช้ไฟฟ้าจับปลา เพราะอาจได้รับอันตรายจากไฟฟ้าดูด

8.1.5) ติดตั้งเสาอากาศโทรทัศน์ ต้องห่างสายไฟฟ้าไม่น้อยกว่า 3 เมตร หรือระยะเสาล้มต้องไม่โดนสายไฟฟ้า

8.1.6) เมื่อไม่มีความรู้ทางไฟฟ้าอย่าแก้ไขอุปกรณ์ไฟฟ้าเอง หากเครื่องใช้ไฟฟ้าชำรุดหรือพบสิ่งผิดปกติเกี่ยวกับไฟฟ้าให้แจ้งช่างมาแก้ไข

8.1.7) ควรติดตั้งเต้ารับในระดับสูงพอเหมาะ เพื่อป้องกันน้ำท่วมถึงและเด็กเล็กอาจใช้นิ้วหรือวัสดุตัวนำแหย่เต้ารับเล่น ซึ่งทำให้ถูกกระแสไฟฟ้าดูดได้

8.1.8) เครื่องใช้ไฟฟ้าชำรุด ควรติดป้ายห้ามใช้ เพื่อนำส่งช่างซ่อมไฟฟ้าต่อไป

8.1.9) การถอดปลั๊กไฟฟ้า ควรจับดึงที่ตัวปลั๊ก อย่าดึงสายปลั๊กเพราะอาจทำให้สายไฟขาดเกิดอันตรายได้

8.1.10) ไม่ควรนำอุปกรณ์เครื่องใช้ไฟฟ้าหลายชนิดมาใช้กับเต้ารับเพียงอันเดียว เพราะอาจทำให้เกิดไฟลุกไหม้ได้

8.1.11) การตรวจสอบกระแสไฟฟ้าห้ามใช้มือสัมผัสโดยตรงควรกระทำโดยช่างผู้ชำนาญและใช้ไขควงทดสอบไฟฟ้า

8.1.12) สว่านไฟฟ้า กบไฟฟ้า เลื่อยไฟฟ้า ก่อนใช้ควรตรวจเช็คสภาพก่อนเสมอ เพราะเครื่องใช้ไฟฟ้าเหล่านี้ถ้าใช้งานมามากอาจมีการชำรุดเกิดขึ้นได้ง่าย และถ้าเป็นสว่านชนิดมีสายดิน ควรต่อสายดินให้เรียบร้อยก่อนใช้งาน

8.1.13) การปฏิบัติงานเกี่ยวกับไฟฟ้าทุกครั้ง ต้องสวมถุงมือยางหรือถุงมือหนังเพื่อป้องกันไฟฟ้าดูด

8.1.14) ตัดกระแสไฟฟ้าออกทุกครั้ง ก่อนที่จะทำการตรวจซ่อมเครื่องใช้ไฟฟ้า

8.2) ความปลอดภัยในการใช้เครื่องมือ

การใช้เครื่องมือให้ปลอดภัย ควรปฏิบัติ ดังนี้

8.2.1) ให้สวมแว่นนิรภัย เมื่อต้องใช้เครื่องมือ เช่น สกัด การเจียระไนด้วยมือต้องสวมแว่นตาเสมอเพื่อป้องกันเศษโลหะกระเด็นเข้าตา

8.2.2) ฝึกอบรมวิธีการใช้อย่างปลอดภัยก่อนให้ทำงาน

8.2.3) ใช้เครื่องมือคุณภาพดี ไม่ชำรุด

8.2.4) เลือกใช้อุปกรณ์เครื่องมือให้ถูกกับชนิดของงาน

8.2.5) หลีกเลี่ยงการใช้เครื่องมือที่ต้อง งอ ข้อมือทำงาน

8.2.6) บำรุงรักษาเครื่องมืออย่างสม่ำเสมอ เช็ค หรือชโลมน้ำมัน เก็บเข้าที่หลังเลิกใช้งาน

8.2.7) ตรวจสอบเครื่องมือทุกครั้งก่อนที่จะใช้งาน

8.2.8) จัดสภาพแวดล้อมในการทำงานให้สะอาดและเป็นระเบียบเพื่อหลีกเลี่ยงการเกิดอุบัติเหตุ

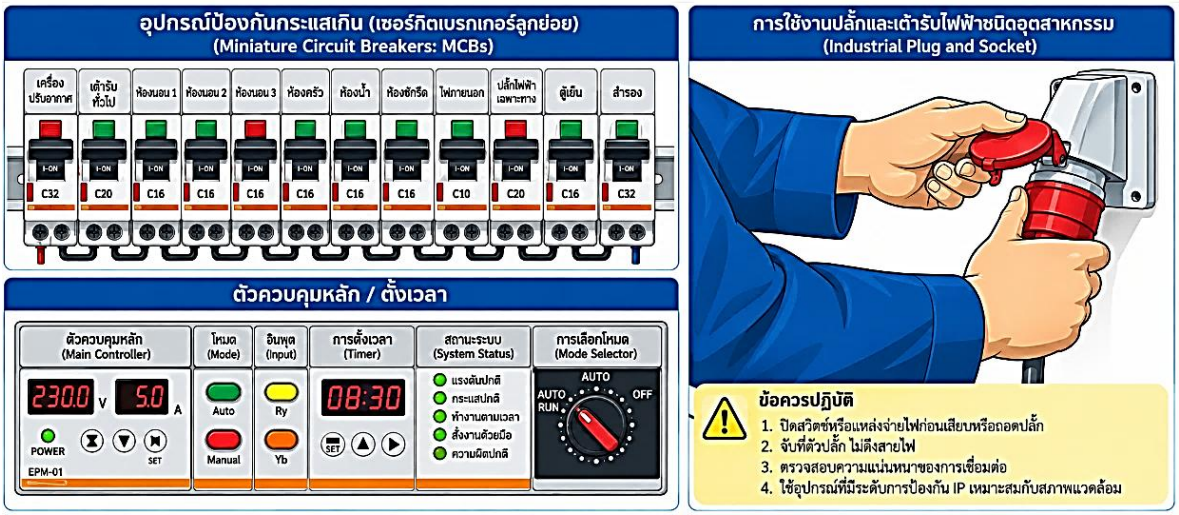
8.2.9) การใช้ประแจให้อยู่ในลักษณะดึงเข้าหาตัว

1.5.2 กฎ 5 ข้อความปลอดภัยในการปฏิบัติงานทางไฟฟ้า

กฎความปลอดภัยในการปฏิบัติงานทางไฟฟ้า หมายถึง ข้อบังคับในการปฏิบัติงานทางไฟฟ้าเพื่อป้องกันอันตรายที่เกิดจากไฟฟ้าต่อผู้ปฏิบัติงาน โดยมี 5 ข้อ (Häberle et al., 2015; Thai Meister, 2017; ชลดา ปานสง และคณะ, 2565) ดังนี้

1) ตัดการเชื่อมต่อแหล่งจ่ายไฟหลัก (Disconnect Mains)

Disconnect mains เป็นกฎที่มีความสำคัญอันดับแรกของการปฏิบัติงานทางไฟฟ้าทุกครั้ง ผู้ปฏิบัติงานจำเป็นต้องทำการปลดแหล่งจ่ายพลังงานไฟฟ้า (power off) หรือตัดวงจรเซอร์กิตเบรกเกอร์หลัก (off main circuit breaker) ออกจากวงจรที่ทำการปฏิบัติงาน ดังรูปที่ 1.7



รูปที่ 1.7 สัญลักษณ์ของการ Disconnect Mains

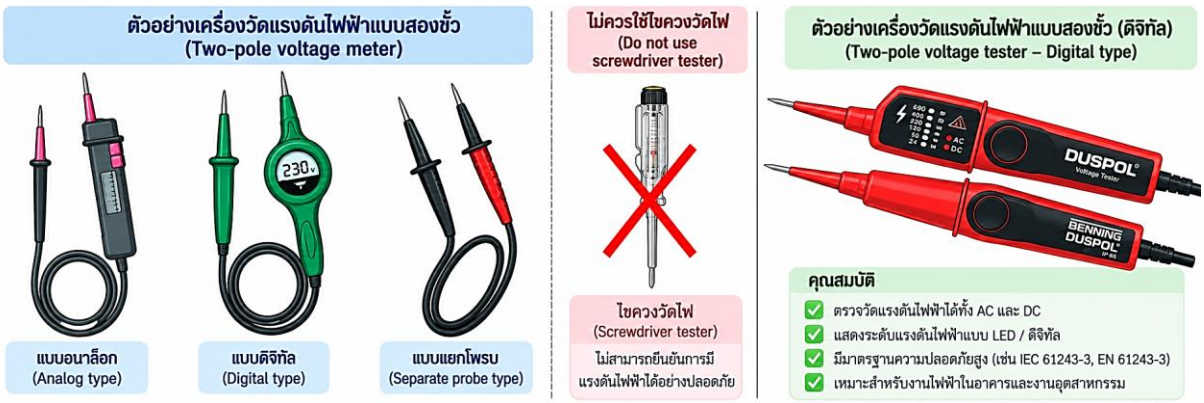
2) การล็อกและติดป้ายเตือน (Lock-Out and Tag-Out)

โดยหลังจากที่ทำการปลดพลังงานไฟฟ้าแล้ว ผู้ปฏิบัติจำเป็นต้องติดป้ายกำกับบริเวณปฏิบัติงาน เพื่อป้องกันผู้อื่นทำการต่อพลังงานไฟฟ้าเข้าสู่ระบบหรือวงจร ซึ่งจะเป็นอันตรายต่อผู้ปฏิบัติงานได้ แสดงสัญลักษณ์และการ lock-out and tag-out ดังรูปที่ 1.8

รูปที่ 1.8 สัญลักษณ์และการ Lock-Out and Tag-Out

3) การตรวจสอบแรงดันไฟฟ้า (Voltage Check)

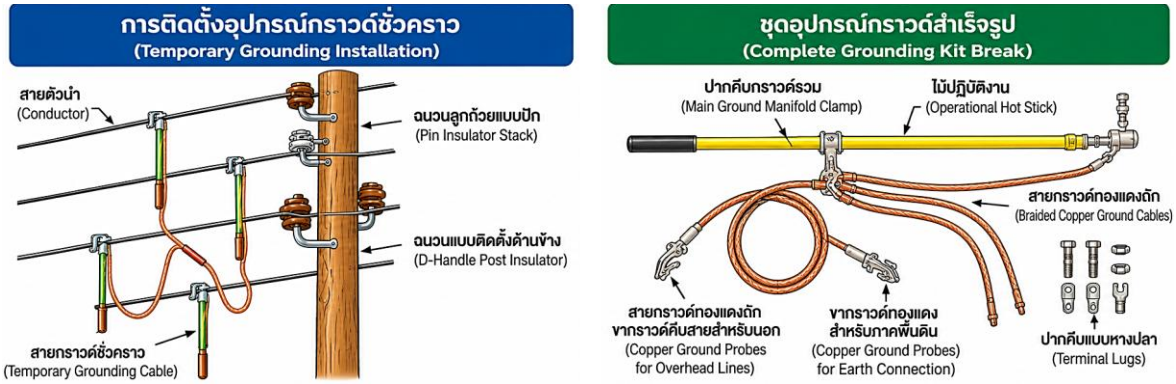
โดยหลังจากทำขั้นตอน 1 และ 2 เรียบร้อยแล้ว เพื่อความมั่นใจควรตรวจเช็คแรงดันไฟฟ้า ณ บริเวณที่ปฏิบัติงาน โดยใช้ two pole voltage meter ห้ามใช้ไขควงวัดไฟเด็ดขาด เนื่องจากถ้าในวงจรยังมีกระแสไฟฟ้า กระแสไฟฟ้าจะไหลผ่านตัวเราจากการสัมผัสไขควง ซึ่งจะเป็นอันตรายอย่างมาก ลักษณะของ two pole voltage meter ดังรูปที่ 1.9



รูปที่ 1.9 เครื่องมือการตรวจสอบแรงดันไฟฟ้า

4) การต่อสายดินและการลัดวงจร (Earth and Shorten)

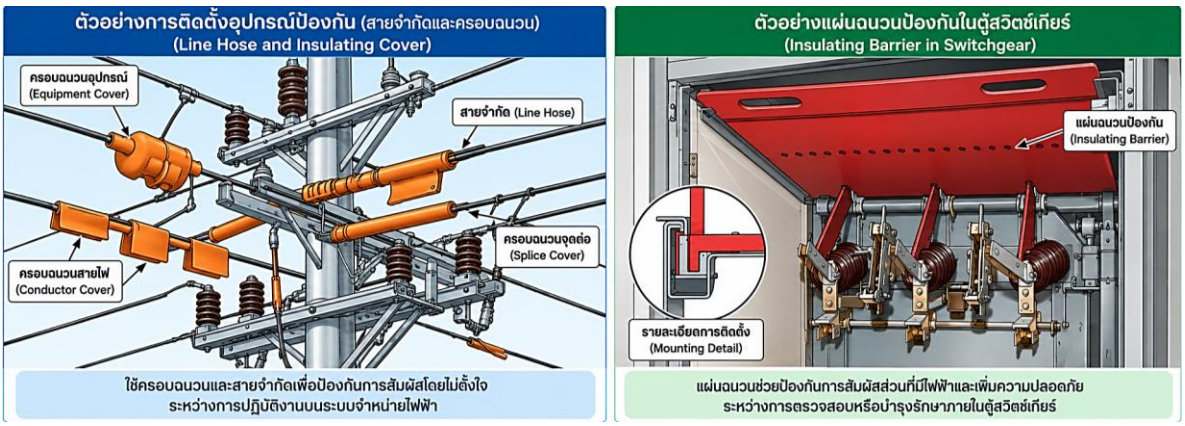
เพื่อความมั่นใจว่าระบบไฟฟ้าที่กำลังจะทำการปฏิบัติงานไม่มีกระแสไฟฟ้าอยู่ ผู้ปฏิบัติจะต้องทำการเชื่อมต่อสายดิน (ground) เข้าไปลัดวงจรกับสายไฟฟ้าหลัก (Line: L) ทั้งหมดของระบบที่จะปฏิบัติงาน เพื่อเป็นการป้องกันหากมีกระแสไฟฟ้าในระบบที่ต้องการ จะปฏิบัติงานวิ่งไปสู่สายดิน ทำให้ผู้ปฏิบัติงานเกิดความปลอดภัย ดังรูปที่ 1.10



รูปที่ 1.10 วิธีการเชื่อมต่อสายดินเข้าไปลัดวงจรกับสายไฟฟ้าหลัก

5) การปกคลุมส่วนประกอบข้างเคียงที่มีแรงดันไฟฟ้า (Cover Adjacent Components Under Voltage)

เป็นการป้องกันกระแสไฟฟ้าจากส่วนของอุปกรณ์ไฟฟ้าอื่นๆ ที่ยังมีกระแสไฟฟ้าและอยู่ในบริเวณใกล้เคียงกับสถานที่ปฏิบัติงาน เพื่อป้องกันการสัมผัสกับอุปกรณ์ไฟฟ้าดังกล่าว โดยการใช้ฉนวนไฟฟ้าปิดครอบอุปกรณ์หรือระบบที่มีกระแสไฟฟ้าที่อยู่ในบริเวณใกล้เคียง ดังรูปที่ 1.11



รูปที่ 1.11 การป้องกันกระแสไฟฟ้าจากส่วนของอุปกรณ์ไฟฟ้าอื่นๆ ที่ยังมีกระแสไฟฟ้า

การทำงานกับอุปกรณ์ไฟฟ้า		อ้างอิง: DIN VDE 0105
กฎความปลอดภัยทั่วไป		
กฎข้อที่	**คำอธิบาย**	**หมายเหตุ / คำแนะนำ**
1. ตัดแหล่งจ่ายไฟ (Disconnect Mains)	ปลดสวิตช์และตัดการเชื่อมต่อสายตัวนำที่มีไฟฟ้าทั้งหมดออกจากระบบ เพื่อให้แน่ใจว่าอุปกรณ์ไม่มีแรงดันไฟฟ้า	ต้องตัดตอนแหล่งจ่ายไฟ และใช้อุปกรณ์ตัดตอนที่เหมาะสม เช่น สวิตช์ตัดตอน เซอร์กิตเบรกเกอร์ หรืออุปกรณ์ตัดไฟรั่ว (RCDs) ตามมาตรฐาน
2. ล็อกและติดป้ายเตือน (Lock-Out and Tag-Out)	ป้องกันการจ่ายไฟกลับโดยล็อกอุปกรณ์ตัดตอนและติดป้ายเตือนที่ชัดเจน ห้ามผู้ที่ไม่เกี่ยวข้องสับสวิตช์หรือจ่ายไฟกลับ	ใช้กุญแจล็อกและป้ายเตือนที่ระบุข้อความ เช่น "กำลังปฏิบัติงาน ห้ามสับสวิตช์" และระบุชื่อผู้ปฏิบัติงาน วัน–เวลา อย่างชัดเจน
3. ตรวจสอบแรงดันไฟฟ้า (Voltage Check)	ตรวจสอบว่าไม่มีแรงดันไฟฟ้าที่จุดปฏิบัติงาน โดยใช้เครื่องวัดแรงดันไฟฟ้าที่เหมาะสม ตรวจสอบก่อน–หลังการวัด และทดสอบเครื่องวัดให้พร้อมใช้งาน	**อุปกรณ์ตรวจวัดแรงดันไฟฟ้า** การตรวจสอบด้วยมัลติมิเตอร์ การตรวจสอบวัดแรงดัน
4. ต่อสายดินและลัดวงจร (Earthing and Short-Circuiting)	สำหรับระบบที่มีแรงดันไฟฟ้าไม่เกิน 1,000 V กระแสสลับ (AC) และ/หรือ 1,500 V กระแสตรง (DC) เมื่อเป็นสายส่งหรือสายจ่ายในลักษณะอาจเกิดแรงดันเหนี่ยวนำสูง ต้องต่อลงดินก่อน (Earthing, E) แล้วจึงลัดวงจร (Short-Circuiting) เพื่อให้แน่ใจว่าไม่มีแรงดันตกค้าง	**อุปกรณ์ลัดวงจรและต่อลงดิน**
5. ปิดคลุมอุปกรณ์ที่อยู่ใกล้เคียงซึ่งมีไฟ (Cover Adjacent Components under Voltage)	ใช้แผงกั้น ฉนวนครอบ หรือฝาครอบป้องกันสำหรับอุปกรณ์ที่ยังคงมีแรงดันไฟฟ้าอยู่ใกล้กับจุดปฏิบัติงาน และไม่สามารถตัดไฟได้ เพื่อป้องกันการสัมผัสโดยไม่ตั้งใจ	หากอุปกรณ์ที่มีแรงดันไฟฟ้าอยู่ใกล้พื้นที่ทำงาน ให้ปิดคลุมด้วยฉนวน แผ่นกั้น หรือครอบป้องกันที่เหมาะสม เช่น แผ่นฉนวนยาง แผ่นพลาสติกครอบ หรือฉากกั้น เพื่อเพิ่มความปลอดภัยในการปฏิบัติงาน

รูปที่ 1.12 สรุปกฎ 5 ข้อความปลอดภัยในระบบไฟฟ้า (ดัดแปลงจาก Häberle et al., 2015)

1.5.3 ระดับการป้องกันของอุปกรณ์ไฟฟ้า (Protection Class of Electrical Equipment)

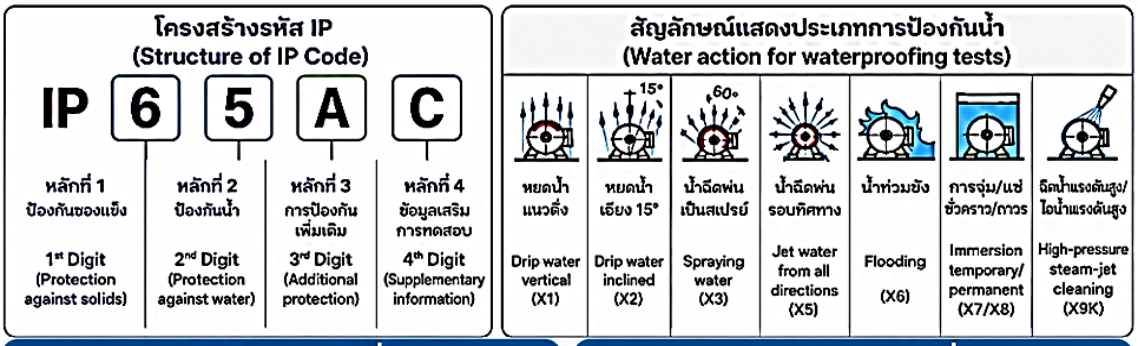
ระดับการป้องกันของอุปกรณ์ หมายถึง ความสามารถของตัวถัง (case) ของอุปกรณ์ไฟฟ้าต่อการไหลของกระแสไฟฟ้ารวมถึงรูปแบบของการนำไปใช้งาน แบ่งออกเป็น 3 ระดับ ดังรูปที่ 1.13

รายการ (Item)	Class I	Class II	Class III
สัญลักษณ์ (Marking)	**ไม่มีสัญลักษณ์** (No marking)	สัญลักษณ์ สี่เหลี่ยมซ้อนกัน 2 ชั้น (Double square)	III สัญลักษณ์เลขโรมัน III ในรูปสี่เหลี่ยมข้าวหลามตัด (Roman numeral III inside a diamond)
การต่อสายดินป้องกัน (Connection to PE conductor of installation)	**ต้องต่อ** กับตัวนำดิน (PE) ของระบบติดตั้ง (Yes, all accessible metal parts)	**ไม่ต้องต่อ** (No)	**ไม่ต้องต่อ** และไม่ต่อกับแหล่งจ่ายไฟหลัก (No connection to mains)
ฉนวนพื้นฐาน (Basic insulation)	**มี** (Performed)	**มี** (Performed)	**มี** แต่ไม่เข้มงวดเท่า Class I และ II (Performed / looser limits)
ฉนวนเสริม/ฉนวนสองชั้น (Supplementary or reinforced insulation)	**โดยทั่วไปไม่จำเป็น** (Not needed in general)	**มี** (Performed)	**โดยทั่วไปไม่จำเป็น** (Not needed)
สายไฟเลี้ยง (Supply cord)	**3 เส้น** (L, N, PE)	**2 เส้น** (L, N)	**2 เส้น** (SELV) (Separately supplied or SELV)
หมายเหตุ (Notes)	การติดตั้งต้องมีค่าความต้านทานดินเพียงพอ (Installation must have adequate earthing resistance)	**ไม่มี** (No)	ใช้แหล่งจ่ายแรงดันต่ำเพื่อความปลอดภัย เช่น 12 V, 24 V (Safety low voltage source, i.e. 12 V, 24 V)
ตัวอย่างอุปกรณ์ (Examples)	ปลั๊กอุตสาหกรรม 3 ขา, ปลั๊กไฟ 3 ขา (3-pin industrial plug, 3-pin plug)	ปลั๊กไฟ 2 ขา (ฉนวนสองชั้น) (2-pin plug, double insulated)	อะแดปเตอร์ 12 V DC, USB, อุปกรณ์ SELV (12 V DC adapter, USB, SELV devices)

รูปที่ 1.13 แสดงระดับการป้องกันของอุปกรณ์ไฟฟ้า (ดัดแปลงจาก Thai Meister, 2017)

1.5.4 รหัสบ่งชี้ระดับความทนต่อสภาพแวดล้อมของอุปกรณ์ไฟฟ้า (Ingress Protection Code หรือ Ingress Protection Ratings: IP code)

IP คือ มาตรฐานที่ใช้วัดความสามารถในการป้องกัน สิ่งที่อยู่ภายในจากสภาวะแวดล้อมภายนอก เช่นในกรณีของกล้องโทรทัศน์วงจรปิด รหัส IP คือ รหัสที่บ่งบอกถึงความสามารถของตัวถัง ของกล้องในการป้องกันวงจรที่อยู่ภายในจากสิ่งแวดล้อมภายนอก มาตรฐานนี้ถูกพัฒนาขึ้นมาโดยสมาคม European Committee for Electro Technical Standardization (CENELEC) (NEMA IEC 60529 Degrees of Protection Provided by Enclosures-IP Code) ซึ่งการจัดอันดับของการป้องกันจะแสดงด้วยตัวเลข 2 หลักโดยในหลักแรกแสดงถึงความสามารถในการป้องกันของแข็งและหลักที่สองแสดงถึงความสามารถในการป้องกันของเหลว เช่น IPXX เช่น IP45, IP66 เป็นต้น (Thai Meister, 2017)



รหัสตัวเลขหลักที่ 1
การป้องกันการสัมผัส (บุคคล) และของแข็ง

รหัส	คำอธิบาย
IP 0X	ไม่มีการป้องกันการสัมผัส และไม่มีการป้องกันของแข็ง
IP 1X	ป้องกันการสัมผัสด้วยหลังมือ และป้องกันของแข็งที่มีขนาดเส้นผ่านศูนย์กลาง ≥ 50 mm
IP 2X	ป้องกันการสัมผัสด้วยนิ้วมือ และป้องกันของแข็งที่มีขนาดเส้นผ่านศูนย์กลาง ≥ 12.5 mm
IP 3X	ป้องกันการสัมผัสด้วยเครื่องมือ และป้องกันของแข็งที่มีขนาดเส้นผ่านศูนย์กลาง ≥ 2.5 mm
IP 4X	ป้องกันการสัมผัสด้วยลวด และป้องกันของแข็งที่มีขนาดเส้นผ่านศูนย์กลาง ≥ 1.0 mm
IP 5X	ป้องกันฝุ่นละออง (ไม่เป็นอันตรายต่อการทำงาน) (ปริมาณฝุ่นที่เข้าได้ต้องไม่มากพอที่จะรบกวนการทำงาน)
IP 6X	ป้องกันฝุ่นละอองได้อย่างสมบูรณ์ (ไม่ให้ฝุ่นเข้าได้) (กันฝุ่นเต็มที่ / Dust-tight)

รหัสตัวเลขหลักที่ 2
การป้องกันการแทรกซึมของน้ำ

รหัส	คำอธิบาย
IP X0	ไม่มีการป้องกันการแทรกซึมของน้ำ
IP X1	ป้องกันหยดน้ำที่ตกลงมาในแนวดิ่ง
IP X2	ป้องกันหยดน้ำที่ตกลงมาในแนวเอียง เมื่ออุปกรณ์เอียงทำมุมไม่เกิน 15° จากแนวดิ่ง
IP X3	ป้องกันน้ำฉีดพ่นเป็นสเปรย์ เมื่ออุปกรณ์เอียงทำมุมสูงสุด 60° จากแนวดิ่ง
IP X4	ป้องกันน้ำกระเด็นจากทุกทิศทาง
IP X5	ป้องกันน้ำฉีดจากทุกทิศทาง
IP X6	ป้องกันน้ำฉีดที่มีแรงดันสูงจากทุกทิศทาง
IP X7	ป้องกันผลกระทบจากการจุ่มในน้ำที่ความลึกไม่เกิน 1 เมตร เป็นเวลาสูงสุด 30 นาที
IP X8	ป้องกันผลกระทบจากการจุ่มในน้ำอย่างต่อเนื่อง ตามที่ผู้ผลิตกำหนด
IP X9K	ป้องกันการฉีดล้างด้วยน้ำแรงดันสูงและอุณหภูมิสูง (ตามมาตรฐาน DIN 40050-9)

รูปที่ 1.14 รหัสบ่งชี้ระดับความทนต่อสภาพแวดล้อมของอุปกรณ์ไฟฟ้า (ดัดแปลงจาก Häberle et al., 2015)

รหัสตัวอักษรเพิ่มเติม (Additional & Supplementary Letters)					
ตัวอักษรหลักที่ 3 การป้องกันการสัมผัสส่วนอันตรายเพิ่มเติม (Additional protection against contact)			**ตัวอักษรหลักที่ 4** ข้อมูลเสริมสำหรับการทดสอบเฉพาะทาง (Supplementary letters for special testing)		
รหัส (Code)	คำอธิบาย (Description)		รหัส (Code)	คำอธิบาย (Description)	
A	ป้องกันการเข้าถึงด้วยหลังมือ (หัวโพรบทดสอบ Ø50 mm)	Access with the back of the hand (test probe Ø 50 mm)	H	อุปกรณ์ไฟฟ้าแรงดันสูง	High-voltage equipment.
B	ป้องกันการเข้าถึงด้วยนิ้วมือ (นิ้วทดสอบ Ø12 mm, ยาว 80 mm)	Access with the finger (test finger Ø12 mm, length 80 mm)	M	ทดสอบการป้องกันน้ำ ขณะที่อุปกรณ์กำลังเคลื่อนไหว/ทำงานอยู่	Tested when device was in motion.
C	ป้องกันการเข้าถึงด้วยเครื่องมือ (หัวโพรบทดสอบ Ø2.5 mm, ยาว 100 mm)	Access with tools (test probe Ø2.5 mm, length 100 mm)	S	ทดสอบการป้องกันน้ำ ขณะที่อุปกรณ์อยู่นิ่ง/หยุดนิ่ง	Tested when device was standing still.
D	ป้องกันการเข้าถึงด้วยลวด (หัวโพรบทดสอบ Ø1.0 mm, ยาว 100 mm)	Access with wire (test probe Ø1.0 mm, length 100 mm)	W	ทดสอบการได้เงื่อนไขสภาพอากาศที่กำหนดโดยเฉพาะ	Tested under defined weather conditions.

รูปที่ 1.15 รหัสบ่งชี้อักษรเพิ่มเติม (ดัดแปลงจาก Häberle et al., 2015)

1.5.5 อุปกรณ์ป้องกันอันตรายส่วนบุคคล

1) ความหมายของอุปกรณ์ป้องกันอันตรายส่วนบุคคล

อุปกรณ์ป้องกันอันตรายส่วนบุคคล (Personal Protection Equipment: PPE) หรือเรียกสั้น ๆ ว่า พีพีอี หมายถึง อุปกรณ์ที่สวมใส่ปกคลุมส่วนใดส่วนหนึ่งของร่างกาย เพื่อป้องกันอันตรายที่อาจเกิดขึ้นเนื่องจากสภาพและสิ่งแวดล้อมในขณะปฏิบัติงาน โดยทั่วไปในการทำงานจะมีการป้องกันและควบคุมสภาพแวดล้อมของการทำงานก่อน โดยการแก้ไขปรับปรุงทางวิศวกรรม เช่น การปรับเปลี่ยนเครื่องจักร เปลี่ยนวิธีการทำงาน เป็นต้น แต่ในกรณีที่ไม่สามารถดำเนินการดังกล่าวได้ จะต้องใช้อุปกรณ์ป้องกันอันตรายส่วนบุคคลมาใช้เพื่อช่วยป้องกันอวัยวะของร่างกายไม่ให้เกิดอันตรายที่อาจเกิดขึ้นในขณะปฏิบัติงาน

2) วิธีการใช้อุปกรณ์ป้องกันอันตรายส่วนบุคคล

2.1) หมวกป้องกันศีรษะ (Head Protection Devices)

หมวกป้องกันศีรษะใช้สำหรับป้องกันศีรษะจากการถูกกระแทกชนหรือวัตถุตกจากที่สูงมากระทบศีรษะมีลักษณะแข็งแรงและทำด้วยวัสดุที่แตกต่างกันออกไปคือใช้ในงานอุสาหกรรมทุกประเภทเป็นต้น ดังรูปที่ 1.16

รูปที่ 1.16 หมวกป้องกันศีรษะ

2.2) อุปกรณ์ป้องกันหู (Ear Protection)

อุปกรณ์ป้องกันหูใช้สำหรับการทำงานในอุตสาหกรรมต่าง ๆ เช่น อุตสาหกรรมยานยนต์ อุตสาหกรรมก่อสร้าง อุตสาหกรรมการผลิต รวมทั้งการทำงานกับเครื่องจักรกล เช่น เครื่องถลุงเหล็ก เครื่องเจาะปูน เครื่องปาดคอนกรีต เครื่องจักรกลอัตโนมัติ ขนาดใหญ่ที่มีเสียงเกินดังที่หูจะรับได้หรือไม่ก็ในพื้นที่ ๆ ควรระมัดระวังเรื่องเสียงเป็นพิเศษ ดังรูปที่ 1.17

รูปที่ 1.17 อุปกรณ์ป้องกันหู

2.3) แว่นนิรภัย (Eye Protection)

แว่นนิรภัยอุปกรณ์ป้องกันดวงจากสารเคมีหรือวัสดุอื่นขณะปฏิบัติงานซึ่งอาจกระเด็นเข้าตาทำให้ตาบอดได้โดยปกติแว่นตานิรภัยใช้ในวงการอุตสาหกรรมเคมีอุตสาหกรรมงานไม้ อุตสาหกรรมงานเครื่องมือ เครื่องจักรกล งานเชื่อมไฟฟ้า และงานเชื่อมแก๊สโดยแว่นตานิรภัยทำจากพลาสติกหรือกระจกนิรภัยไม่แตกกระเด็นเข้าตาผู้ปฏิบัติงาน ดังรูปที่ 1.18

รูปที่ 1.18 แว่นนิรภัย

2.4) เสื้อสะท้อนแสง (Reflective Clothing)

เสื้อสะท้อนแสงเป็นเสื้อเพื่อความปลอดภัยในการจราจร และเพิ่มสวัสดิภาพให้แก่ผู้สวมใส่ในกรณีที่มีการปฏิบัติงานตามถนน หรืออาคารสถานที่ต่าง ๆ เช่น ซ่อมบำรุง

ก่อสร้างทาง กรมทางหลวง ตำรวจ รปภ. ตามลานจอดรถ ฯลฯ โดยเสื้อสะท้อนแสงสามารถสะท้อนให้เห็นเด่นชัด ทั้งในเวลากลางวัน และกลางคืน ดังรูปที่ 1.19

รูปที่ 1.19 เสื้อสะท้อนแสง

2.5) เข็มขัดนิรภัย (Safety Harness)

เข็มขัดนิรภัยเป็นอุปกรณ์ช่วยป้องกันอันตรายจากการทางานในที่สูงจะมีสายรัดลำตัวคาดตั้งแต่หัวไหล่หน้าอกเอวและขาเกี่ยวติดกับสายช่วยชีวิตเพิ่มความปลอดภัยได้มาก เนื่องจากจะเฉลี่ยแรงกระตุกหรือกระชากไปที่ลำตัวด้วยและมักทำจากวัสดุที่มีความอ่อนนุ่มเพื่อช่วยลดแรงกระแทกของลาตัวอีกชั้นหนึ่งด้วย ดังรูปที่ 1.20

รูปที่ 1.20 เข็มขัดนิรภัย

2.6) จุดยึด Anchor Point (Tie-off Point)

จุดยึดคือจุดที่เอาไว้สำหรับยึดตัวกับฐานหรือโครงสร้างต่างๆ โดยตามมาตรฐาน ANSI ของอเมริกา อุปกรณ์ต้องสามารถรับแรงได้อย่างน้อย 22 kN (5000lb) การใช้งานควรอยู่ในตำแหน่งเหนือหัวขึ้นไปและอยู่ในแนวเดียวกับผู้ใช้ เพื่อป้องกันการลดระยะการตกและลดการเหวี่ยงตัวเพื่อป้องกันอันตรายจากการกระแทกกับโครงสร้าง ดังรูปที่ 1.21

รูปที่ 1.21 จุดยึดตัวกับฐานหรือโครงสร้างต่าง ๆ

2.7) เชือกสำหรับป้องกันการตก (Fall Absorbing Lanyard)

เชือกสำหรับป้องกันการตกจะทำจากเหล็กไนล่อน (โพลีเอไมด์) หรือเส้นใย dacron โดยอาจจะมีเสริมอุปกรณ์ดูดซับแรงเพื่อลดแรงกระแทกเวลาตก ซึ่งให้จำไว้ว่าเชือกจะต้องช่วยไม่ทำให้เกิดแรงสูงสุดที่เข็มขัดรัดลำตัว (full-body harness) เกิน 1800 ปอนด์เวลาตก และความยาวเชือกสูงสุดจะต้องไม่ทำให้ผู้ใช้งานตกลงมาเกิน 6 ฟุต ดังรูปที่ 1.22

รูปที่ 1.22 เชือกสำหรับป้องกันการตก

2.8) เชือกในลักษณะรักษาตำแหน่ง (Restrain Lanyard)

เชือกในลักษณะรักษาตำแหน่งความยาวเชือกควรมีระยะสั้นที่สุดเพื่อไม่ให้ผู้ใช้พลัดตกไปเกิน 2 ฟุต ซึ่งเชือกสามารถทำจากวัสดุได้หลายชนิดทั้ง ลวดสลิง โซ่ เชือกไนล่อน โพลีเอไมด์ ดังรูปที่ 1.23

รูปที่ 1.23 เชือกในลักษณะรักษาตำแหน่ง

2.9) เชือกช่วยชีวิต (Lifelines)

เชือกช่วยชีวิตเพื่อเพิ่มความหลากหลายในการใช้งานให้กับระบบการป้องกันการตก โดยจะใช้ร่วมกับอุปกรณ์ยึดจับเชือก เชือกช่วยชีวิตทำให้ผู้ใช้งานเคลื่อนไหวได้ไปตามความยาวของเชือกที่ขึงอยู่ แทนที่จะต้องปลดและหาจุดยึดใหม่ตลอดเวลา โดยอุปกรณ์ยึดจับเชือก (rope grap) จะทำหน้าที่ยัดจับเชือกโดยอัตโนมัติที่เกิดการตกขึ้น นอกจากนี้ยังมีเชือกช่วยชีวิตแบบที่หดกลับอัตโนมัติ (retractable lifelines) ซึ่งเชือกแบบนี้ไม่ต้องใช้อุปกรณ์ยึดจับเชือก เนื่องจากมันจะหดกลับเองอัติโนมัติเมื่อมีการตกขึ้น ดังรูปที่ 1.24

รูปที่ 1.24 เชือกช่วยชีวิต

2.10) รองเท้านิรภัย (Foot Protection)

รองเท้านิรภัย เป็นอุปกรณ์ที่ถูกออกแบบมาเพื่อต้านทานแรงกระแทกและแรงบีบบริเวณหัวประกอบด้วยโครงเหล็กใช้สำหรับวัตถุหล่นใส่ป้องกันกระดูกส่วนบนป้องกันอันตรายจากกระแสไฟฟ้าป้องกันแรงกระแทกผ่านการทดสอบแรงบีบ พื้นรองเท้าป้องกันน้ำมันและน้ำกรด ส่วนบนป้องกันน้ำซึมเข้ารองเท้า ดังรูปที่ 1.25

รูปที่ 1.25 รองเท้านิรภัย

1.5.6 การปฐมพยาบาลเบื้องต้น

1) ความหมายของการปฐมพยาบาล

การปฐมพยาบาล หมายถึง การให้ความช่วยเหลือแก่ผู้ป่วยหรือผู้ที่ได้รับบาดเจ็บ ณ สถานที่เกิดเหตุ โดยใช้อุปกรณ์เท่าที่จะหาได้ในขณะนั้น นำมาใช้ในการรักษาเบื้องต้น ควรทำการปฐมพยาบาลให้เร็วที่สุดหลังเกิดเหตุโดยอาจทำได้ในทันที หรือระหว่างการนำผู้ป่วยหรือผู้บาดเจ็บไปยังโรงพยาบาลหรือสถานที่รักษาพยาบาลอื่น ๆ เพื่อช่วยบรรเทาอาการเจ็บป่วย หรืออาการบาดเจ็บนั้น ๆ ก่อนที่ผู้ป่วยหรือผู้ที่ได้รับบาดเจ็บจะได้รับการดูแลรักษาจากบุคลากรทางการแพทย์ หรือถูกนำส่งไปยังโรงพยาบาล (สภากาชาดไทย, 2559)

2) การปฐมพยาบาลผู้ที่ได้รับอันตรายจากไฟฟ้า ให้เลือกใช้วิธีใดวิธีหนึ่ง ดังนี้

2.1) ตัดกระแสไฟฟ้าโดยปลดสวิตช์หรือคัทเอาท์ หรือเต้าเสียบออก

2.2) หากตัดกระแสไฟฟ้าไม่ได้ ให้ใช้ไม้แห้ง หรือวัสดุที่เป็นฉนวนไฟฟ้าเขี่ยสิ่งที่มีกระแสไฟฟ้าออกไปให้พ้น

2.3) ให้ใช้ผ้าหรือเชือกแห้งคล้องแขน ขา หรือลำตัว ผู้ถูกไฟฟ้าดูดชักลากออกไปให้พ้นสิ่งที่มีกระแสไฟฟ้า หากผู้ถูกไฟดูดสลบหมดสติให้ทำการปฐมพยาบาลให้ฟื้นต่อไป

3) การช่วยเหลือด้วยวิธีปฐมพยาบาล

เมื่อช่วยเหลือผู้บาดเจ็บออกจากกระแสไฟฟ้าได้แล้วเพื่อช่วยชีวิตผู้บาดเจ็บ การปฐมพยาบาลก่อนนำส่งโรงพยาบาล จึงเป็นสิ่งสำคัญและจำเป็นที่สุด ซึ่งการปฐมพยาบาลผู้บาดเจ็บจากกระแสไฟฟ้ามีข้อสังเกตและหลักปฏิบัติ ดังนี้

3.1) กรณีผู้บาดเจ็บหมดสติ

3.1.1) พยายามหงายศีรษะผู้บาดเจ็บไปข้างหลังเท่าที่จะหงายได้ เพื่อเปิดทางอากาศเข้าสู่ปอดได้สะดวก

3.1.2) ใช้ผ้าหนาๆ ม้วนแล้วสอดเข้าใต้ช่วงไหล่ เพื่อหนุนหงายศีรษะไว้

3.1.3) ล้วงสิ่งที่อาจค้างอยู่ในปากซึ่งจะขัดขวางทางลม เช่น หมากฝรั่ง ของขบเคี้ยว ฟันปลอม โดยอาจใช้ผ้าพันนิ้วมือก่อน เพราะหากผู้ป่วยไม่หมดสติเสียทีเดียว อาจงับนิ้วมือได้ ดังรูปที่ 1.26

รูปที่ 1.26 การล้วงสิ่งที่ขวางทางเดินลมหายใจออกมาจากช่องปาก (ดัดแปลงจาก สสส., 2560)

3.2) กรณีผู้บาดเจ็บไม่หายใจ

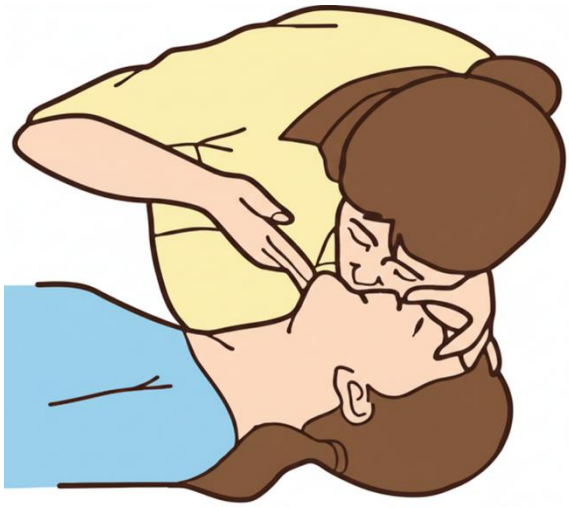
หากพบว่าผู้บาดเจ็บไม่หายใจต้องช่วยหายใจ หรือเรียกว่า การผายปอดเพื่อให้ปอดได้รับออกซิเจนเพียงพอ และป้องกันไม่ให้เกิดความพิการแก่สมองและอวัยวะอื่น ๆ ซึ่งอาจใช้วิธีให้ลมหายใจทางปาก (mouth to mouth breathing) ซึ่งมีขั้นตอน ดังนี้

3.2.1) หงายศีรษะผู้บาดเจ็บไปด้านหลัง เพื่อเปิดทางอากาศเข้าสู่ปอด

3.2.2) สอดนิ้วหัวแม่มือเข้าไปในปาก จับขากรรไกรล่างยกขึ้นจนปากอ้า

3.2.3) ใช้นิ้วควานล้วงสิ่งที่อาจค้างอยู่ในปาก เช่น ของขบเคี้ยว ออกให้หมด

3.2.4) เริ่มเป่าอากาศเข้าสู่ปอดของผู้บาดเจ็บ ถ้าผู้บาดเจ็บมีลมรั่วออกทางจมูกอาจใช้มือบีบจมูกไว้ แสดงดังรูปที่ 1.27



รูปที่ 1.27 การเป่าปากผู้ป่วย (ดัดแปลงจาก สสส., 2560)

3.2.5) ถอนปากออกจากผู้บาดเจ็บ สูดลมหายใจเต็มที่ แล้วเริ่มเป่าอากาศเข้าทางปากผู้บาดเจ็บอีกในอัตรา 12–15 ครั้ง/นาที

3.2.6) สังเกตว่าผู้บาดเจ็บหายใจได้เองหรือยังโดยคลำดูชีพจร ถ้าผู้บาดเจ็บยังไม่หายใจเอก็เป่าต่อไปอีก ถ้ายังไม่พบชีพจรแสดงว่าผู้บาดเจ็บหัวใจหยุดเต้นต้องช่วยกระตุ้นหัวใจ พร้อม ๆ กับการช่วยหายใจ

3.3) กรณีผู้บาดเจ็บหัวใจหยุดเต้น

หากหัวใจของผู้บาดเจ็บหยุดเต้นเป็นครั้งคราว การนวดหัวใจโดยทันท่วงทีสามารถช่วยให้ฟื้นขึ้นมาได้ โดยใช้น้ำหนักคนโถมกดเป็นจังหวะๆ ให้หน้าอกยุบลงไป ซึ่งอาจทำให้เลือดไหลออกจากหัวใจไปเลี้ยงร่างกาย ซึ่งมีขั้นตอนการนวดหัวใจดังนี้ (ไวพจน์ ศรีธัญ และ วีรธรรม ไชยยงค์, 2558)

3.3.1) นำผู้บาดเจ็บเข้าที่ร่ม แล้วนอนหงายบนพื้นราบแข็งพอสมควร

3.3.2) หงายศีรษะผู้บาดเจ็บไปข้างหลัง เพื่อเปิดทางอากาศเข้าสู่ปอด

3.3.3) ใช้นิ้วล้วงสิ่งที่อาจค้างอยู่ในปากหรือลำคอ ซึ่งอาจขัดขวางทางอากาศเข้าสู่ปอด

3.3.4) คุกเข่าด้านขวาของผู้บาดเจ็บ วางฝ่ามือขวาบนทรวงอกบริเวณหัวใจ ใช้ฝ่ามือซ้ายวางซ้อนฝ่ามือขวา หรือตามที่ถนัด แสดงดังรูปที่ 1.28

รูปที่ 1.28 การวางตำแหน่งวางมือเพื่อนวดหัวใจ (ดัดแปลงจาก สสส., 2560)

3.3.5) กดให้กระดูกสันอกยุบเข้าหาแนวสันหลังประมาณ 3 - 4 เซนติเมตร อย่ากดแรงเกินไป เพราะกระดูกซี่โครงอาจหักได้ แสดงดังรูปที่ 1.29

รูปที่ 1.29 การใช้นิ้วล็อกกันไว้เพื่อใช้แรงกดกระดูกสันอกถ่ายเทผ่านฝ่ามือล่าง (ดัดแปลงจาก สสส., 2560)

3.3.6) ทำการนวดหัวใจเป็นจังหวะซ้ำกัน ครั้งละ 1 วินาที ทำเนิบๆ ไม่ควรลุกลี้ลุกลน

3.3.7) การนวดหัวใจต้องกระทำจนกว่าหัวใจจะเต้น หรือจนถึงมือแพทย์

3.3.8) หากพบว่าผู้บาดเจ็บหยุดหายใจ จะต้องช่วยให้ลมหายใจทางปากพร้อมกับการนวดหัวใจตลอดเวลา โดยเป่าปาก 1 ครั้ง นวดหัวใจ 3–4 ครั้ง หรือเป่าปาก 2 ครั้ง แสดงดังรูปที่ 1.30

รูปที่ 1.30 การนวดหัวใจและให้ลมหายใจทางปาก (ดัดแปลงจาก สสส., 2560)

บรรณานุกรมบทที่ 1

ชลดา ปานสง, ศราวุธ พลรักษา, ชาญณรงค์ บุตรทา, อุดมศักดิ์ จันทรทาโพ, และ บัญชา แสนโสดา. (2565). การพัฒนาชุดฝึกอบรมฐานสมรรถนะ เรื่อง การติดตั้งและเขียนโปรแกรมควบคุมอัตโนมัติในงานอุตสาหกรรม ตามมาตรฐานของ Thai-Meister. *วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น, 19*(2). 1-14.

บริษัท ซีเอ ออโตเมติก เกทส์ จำกัด. (2525). *แขนกั้นรถ ไม้กั้นรถยนต์ แขนกั้นรถอัตโนมัติ.* https://caautomatic.com/แขนกั้นรถ/.

ไวพจน์ ศรีธัญ และวีรธรรม ไชยยงค์. (2558). *งานไฟฟ้าและอิเล็กทรอนิกส์.* กรุงเทพฯ: วังอักษร.

สภากาชาดไทย. (2559). *คู่มือปฐมพยาบาล (First aids manual).* https://thaircy.redcross.or.th/2016/2016/06/23/คู่มือปฐมพยาบาล-first-aid-manual/.

สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.). (2560). *การปฐมพยาบาลเบื้องต้น.* https://www.lgblogger.com/การปฐมพยาบาลเบื้องต้นท/.

องค์การรักษาความปลอดภัยฝ่ายพลเรือน, สำนักข่าวกรองแห่งชาติ. (2015). *ระบบรักษาความปลอดภัย และอุปกรณ์รักษาความปลอดภัยสำหรับสถานที่ทรัพย์สิน.* https://www.secnia.go.th/2018/07/ระบบรักษาและอุปกรณ์รัก/.

Thai Meister. (2017). *คู่มือฝึกอบรม Thai Meister สาขา Mechatronics.* มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Al-Qutayri, M. (Ed.). (2010). Smart Home Systems. InTech. https://doi.org/10.5772/182.

Fennelly, L. J. (Ed.). (2017). *Effective physical security* (5th ed.). Butterworth-Heinemann.

Fischer, R. J., Halibozek, E. P., & Walters, D. C. (2018). *Introduction to security* (10th ed.). Butterworth-Heinemann.

Häberle, G. D., Häberle, H. O., Heinzelmann, R., Jöckel, H. W., Krall, R., Lücke, T., Rieger, K., Schiemann, B., Schmitt, S., & Tkotz, K. (2015). *Electrical engineering: Tables, standards, formulas* (2nd English ed.). Verlag Europa-Lehrmittel Nourney, Vollmer.

Ismail, Y. (Ed.). (2019). *Internet of Things (IoT) for automated and smart applications.* IntechOpen. https://doi.org/10.5772/intechopen.90022.

Kruegle, H. (2006). *CCTV surveillance: Video practices and technology* (2nd ed.). Butterworth-Heinemann.

Norman, T. L. (2018). *Electronic access control* (2nd ed.). Butterworth-Heinemann.

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. *Electronics, 13*(16), 3343. https://doi.org/10.3390/electronics13163343.

สรุปสาระสำคัญของบทที่ 1
ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยอัจฉริยะ

ความรู้เบื้องต้นเกี่ยวกับระบบรักษาความปลอดภัย

ระบบรักษาความปลอดภัยเป็นระบบที่ถูกออกแบบมาเพื่อป้องกันชีวิตและทรัพย์สิน โดยมีวัตถุประสงค์หลัก ได้แก่ การป้องกัน (prevention) การตรวจจับ (detection) การแจ้งเตือน (alert) และการตอบสนอง (response) ซึ่งเป็นกระบวนการสำคัญในการลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น ในปัจจุบันได้มีการพัฒนาไปสู่ ระบบ smart security ที่นำเทคโนโลยีเข้ามาประยุกต์ใช้ เช่น เซ็นเซอร์ตรวจจับ ระบบแจ้งเตือนผ่านแอปพลิเคชัน และการควบคุมจากระยะไกล ทำให้สามารถบริหารจัดการความปลอดภัยได้อย่างมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้ ระบบรักษาความปลอดภัยยังมีการจัดระดับพื้นที่ (security level) เพื่อควบคุมการเข้าถึงตามความสำคัญของพื้นที่ ตั้งแต่บริเวณภายนอกจนถึงพื้นที่ที่มีความปลอดภัยสูง โดยใช้เทคโนโลยีและอุปกรณ์ที่แตกต่างกันในแต่ละระดับ

โดยรวมแล้ว ระบบรักษาความปลอดภัยสมัยใหม่เป็นการทำงานแบบบูรณาการร่วมกันของอุปกรณ์และระบบต่าง ๆ เช่น ระบบตรวจจับ ระบบควบคุม และระบบเฝ้าระวัง เพื่อให้เกิดความปลอดภัยสูงสุดอย่างมีประสิทธิภาพ

องค์ประกอบของระบบรักษาความปลอดภัย

ระบบรักษาความปลอดภัยประกอบด้วยองค์ประกอบหลัก 4 ส่วนที่ทำงานร่วมกันอย่างเป็นลำดับ ได้แก่ อุปกรณ์ตรวจจับ (sensor) ทำหน้าที่ตรวจจับเหตุการณ์ผิดปกติ, เครื่องควบคุม (control unit) ทำหน้าที่รับและประมวลผลข้อมูล, อุปกรณ์แจ้งเตือน (siren) ทำหน้าที่แจ้งเหตุ และ แหล่งพลังงานสำรอง (backup battery/UPS) ที่ช่วยให้ระบบสามารถทำงานได้อย่างต่อเนื่องแม้ไฟฟ้าขัดข้อง

อุปกรณ์ตรวจจับเปรียบเสมือนด่านหน้าในการเฝ้าระวัง เช่น magnetic contact, PIR sensor และ glass break detector ซึ่งช่วยตรวจจับการบุกรุกหรือความผิดปกติได้อย่างรวดเร็ว ข้อมูลจากเซ็นเซอร์จะถูกส่งไปยังเครื่องควบคุมเพื่อวิเคราะห์และตัดสินใจสั่งการ

เมื่อระบบตรวจพบเหตุผิดปกติ อุปกรณ์แจ้งเตือนจะทำงานทันทีในรูปแบบเสียง แสง หรือการแจ้งเตือนผ่านเครือข่าย เพื่อให้ผู้เกี่ยวข้องสามารถตอบสนองต่อสถานการณ์ได้อย่างทันท่วงที ขณะที่แหล่งพลังงานสำรองมีบทบาทสำคัญในการรักษาความต่อเนื่องของระบบในกรณีฉุกเฉิน

โดยรวม ระบบรักษาความปลอดภัยเป็นการทำงานแบบบูรณาการของทั้ง 4 องค์ประกอบ เพื่อให้เกิดกระบวนการ ตรวจจับ > ประมวลผล > แจ้งเตือน > ตอบสนอง ได้อย่างมีประสิทธิภาพและครบวงจร

ระบบที่เกี่ยวข้องกับงานรักษาความปลอดภัย

ระบบที่เกี่ยวข้องกับงานรักษาความปลอดภัยเป็นระบบสนับสนุนที่ทำงานร่วมกันเพื่อเพิ่มประสิทธิภาพในการเฝ้าระวัง ป้องกัน และตอบสนองต่อเหตุการณ์ โดยประกอบด้วยระบบสำคัญ ได้แก่ ระบบกล้องโทรทัศน์วงจรปิด (CCTV) ระบบควบคุมการเข้า-ออก (access control) ระบบเสียงประกาศ (PA system) ระบบแจ้งเตือนการบุกรุก (intrusion detection system) และระบบแจ้งเหตุเพลิงไหม้ (fire alarm system)

ระบบกล้องโทรทัศน์วงจรปิดทำหน้าที่เฝ้าระวังและบันทึกเหตุการณ์แบบเรียลไทม์และย้อนหลัง ขณะที่ระบบควบคุมการเข้า-ออกช่วยกำหนดสิทธิ์และควบคุมการเข้าถึงพื้นที่ โดยใช้เทคโนโลยี เช่น บัตร RFID และแขนกั้นรถยนต์ ระบบเสียงประกาศมีบทบาทในการสื่อสารและแจ้งเตือนบุคคลจำนวนมาก โดยเฉพาะในสถานการณ์ฉุกเฉิน

นอกจากนี้ ระบบแจ้งเตือนการบุกรุกทำหน้าที่ตรวจจับและแจ้งเตือนเมื่อมีการเข้าถึงโดยไม่ได้รับอนุญาต ส่วนระบบแจ้งเหตุเพลิงไหม้ช่วยตรวจจับควัน ความร้อน และแจ้งเตือนเพื่อให้อพยพได้อย่างปลอดภัย

โดยรวม ระบบทั้งหมดทำงานร่วมกันแบบบูรณาการ เพื่อให้เกิดกระบวนการ เฝ้าระวัง > ควบคุม > ตรวจจับ > แจ้งเตือน > ตอบสนอง ซึ่งช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยและลดความเสี่ยงต่อชีวิตและทรัพย์สินอย่างมีประสิทธิภาพ

หลักความปลอดภัยในการปฏิบัติงานด้านไฟฟ้า

ไฟฟ้าเป็นสิ่งจำเป็นในชีวิตประจำวัน แต่มีความเสี่ยงอันตรายสูงหากใช้งานไม่ถูกวิธี โดยอันตรายจากไฟฟ้าขึ้นอยู่กับหลายปัจจัย เช่น ความต้านทานของร่างกาย แรงดันไฟฟ้า ปริมาณกระแสไฟฟ้า ระยะเวลาที่สัมผัส ความถี่ และเส้นทางที่กระแสไฟฟ้าไหลผ่านร่างกาย ซึ่งอาจก่อให้เกิดอาการตั้งแต่ช็อกจนถึงเสียชีวิต

การป้องกันอันตรายจากไฟฟ้าจำเป็นต้องปฏิบัติตามหลักความปลอดภัยอย่างเคร่งครัด โดยเฉพาะ “กฎ 5 ข้อ” ได้แก่ การตัดแหล่งจ่ายไฟ (disconnect mains) การล็อกและติดป้าย (lock-out/tag-out) การตรวจสอบแรงดันไฟฟ้า (voltage check) การต่อสายดินและลัดวงจร (earth and shorten) และการป้องกันอุปกรณ์ที่มีกระแสไฟฟ้าใกล้เคียง

นอกจากนี้ อุปกรณ์ไฟฟ้ายังมีการกำหนดระดับการป้องกัน (protection class) และมาตรฐาน IP code เพื่อบ่งชี้ความสามารถในการป้องกันฝุ่นและน้ำ รวมถึงต้องปฏิบัติตามกฎหมายที่เกี่ยวข้องกับความปลอดภัยอย่างเคร่งครัด

การทำงานด้านไฟฟ้าควรใช้อุปกรณ์ป้องกันส่วนบุคคล (PPE) เช่น หมวกนิรภัย แว่นตา ถุงมือ และรองเท้านิรภัย เพื่อลดความเสี่ยงในการเกิดอุบัติเหตุ และควรมีความรู้ด้านการปฐมพยาบาลเบื้องต้น เช่น การช่วยเหลือผู้ถูกไฟฟ้าดูด การช่วยหายใจ และการนวดหัวใจ เพื่อเพิ่มโอกาสในการช่วยชีวิตผู้ประสบเหตุ

โดยสรุป ความปลอดภัยในการปฏิบัติงานด้านไฟฟ้าเป็นสิ่งสำคัญที่ต้องอาศัยทั้งความรู้ ความระมัดระวัง การใช้อุปกรณ์ที่เหมาะสม และการปฏิบัติตามมาตรฐาน เพื่อป้องกันอุบัติเหตุและลดความสูญเสียต่อชีวิตและทรัพย์สิน

แบบฝึกหัดท้ายบทที่ 1
ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยอัจฉริยะ

ตอนที่ 1 เติมคำ

คำสั่ง: จงเติมคำให้ถูกต้อง

1. ระบบรักษาความปลอดภัยมีวัตถุประสงค์หลัก 4 ประการ ได้แก่ _____, _____, _____ และ _____
2. อุปกรณ์ตรวจจับเปรียบเสมือน _____ของระบบ
3. เครื่องควบคุมทำหน้าที่เป็น _____ของระบบ
4. UPS ย่อมาจาก _____
5. Siren เป็นอุปกรณ์ที่ใช้สำหรับ _____

ตอนที่ 2 จับคู่

คำสั่ง: จงจับคู่ให้ถูกต้อง

1. Sensor	ก. แจ้งเตือน
2. Control Unit	ข. ตรวจจับ
3. Siren	ค. ประมวลผล
4. Backup Battery	ง. สำรองไฟ

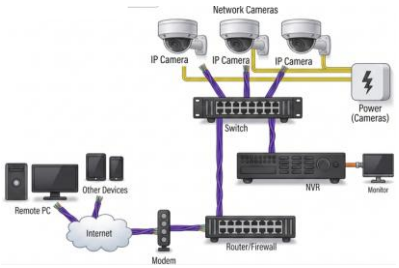
ตอนที่ 3 เลือกตอบ

คำสั่ง: จงเลือกคำตอบที่ถูกต้องที่สุด

1. ข้อใด “ไม่ใช่” วัตถุประสงค์หลักของระบบรักษาความปลอดภัย
   ก. Prevention
   ข. Detection
   ค. Decoration
   ง. Response
2. อุปกรณ์ใดทำหน้าที่ตรวจจับการเคลื่อนไหว
   ก. Magnetic Contact
   ข. PIR Sensor
   ค. Siren
   ง. UPS
3. เครื่องควบคุม (Control Unit) ทำหน้าที่ใด
   ก. ส่งเสียงแจ้งเตือน
   ข. จ่ายไฟฟ้า
   ค. ประมวลผลข้อมูลจากเซ็นเซอร์
   ง. บันทึกภาพ
4. อุปกรณ์ใดเป็น “แหล่งพลังงานสำรอง”
   ก. CCTV
   ข. UPS
   ค. Sensor
   ง. Card Reader

5. ระบบ Smart Security มีลักษณะเด่นอย่างไร
   ก. ใช้แรงงานคนเป็นหลัก
   ข. ไม่ต้องใช้ไฟฟ้า
   ค. ควบคุมและแจ้งเตือนผ่านเทคโนโลยีอัจฉริยะ
   ง. ใช้เฉพาะในโรงงาน
6. ระบบในภาพจัดอยู่ในระบบใด

   ก. CCTV
   ข. Access Control
   ค. Fire Alarm
   ง. Intrusion System
7. จากภาพในข้อที่ 6. อุปกรณ์ที่ใช้เปิดไม้กั้นอัตโนมัติคือข้อใด
   ก. PIR Sensor
   ข. RFID Card Reader
   ค. Smoke Detector
   ง. Siren
8. อุปกรณ์ใดทำหน้าที่ตรวจจับ
   ก. Siren
   ข. Sensor
   ค. UPS
   ง. Monitor
9. Control Unit เปรียบเสมือนอะไร
   ก. หู
   ข. สมอง
   ค. มือ
   ง. แบตเตอรี่
10. Siren มีหน้าที่อะไร
   ก. เก็บข้อมูล
   ข. ตรวจจับ
   ค. แจ้งเตือน
   ง. จ่ายไฟ
11. CCTV ใช้เพื่ออะไร
   ก. เปิดประตู
   ข. บันทึกภาพ
   ค. ส่งเสียง
   ง. ตรวจจับไฟ
12. ระบบ Intrusion Detection ทำหน้าที่
   ก. ตรวจจับการบุกรุก
   ข. เปิดไฟ
   ค. บันทึกเสียง
   ง. ควบคุมลิฟต์
13. ระบบ Fire Alarm ตรวจจับอะไร
   ก. การเคลื่อนไหว
   ข. ควันและความร้อน
   ค. บัตร RFID
   ง. เสียง
14. ข้อใดเป็นกฎความปลอดภัยไฟฟ้า
   ก. ทำงานโดยไม่ตัดไฟ
   ข. ตรวจสอบแรงดันก่อนทำงาน
   ค. ไม่ใช้ PPE
   ง. ใช้น้ำดับไฟ
15. IP Code ใช้บอกอะไร
   ก. ความเร็ว
   ข. ความทนฝุ่นและน้ำ
   ค. แรงดันไฟ
   ง. อุณหภูมิ
16. ระบบในภาพมีหน้าที่หลักคืออะไร



   ก. ควบคุมประตู
   ข. บันทึกและเฝ้าระวัง

ค. ตรวจจับไฟไหม้

ง. ส่งเสียงแจ้งเตือน

17. จากข้อ 16. อุปกรณ์ใดทำหน้าที่บันทึกข้อมูล

ก. Camera

ข. NVR/DVR

ค. Sensor

ง. UPS

18. อุปกรณ์ในภาพทำหน้าที่อะไร

ก. แจ้งเตือน

ข. ตรวจจับ

ค. ควบคุม

ง. จ่ายไฟ

19. ระบบแจ้งเหตุเพลิงไหม้ อุปกรณ์ใดทำหน้าที่ตรวจจับ

ก. อุปกรณ์ตรวจจับการเคลื่อนไหว

ข. อุปกรณ์ตรวจจับควัน

ค. อุปกรณ์ตรวจจับเสียง

ง. บัตร

20. ระบบรักษาความปลอดภัยหมายถึงข้อใด

ก. ระบบตกแต่ง

ข. ระบบป้องกัน ตรวจจับ แจ้งเตือน และตอบสนอง

ค. ระบบไฟฟ้า

ง. ระบบอินเทอร์เน็ต

21. เมื่อร่างกายโดนแรงดันไฟฟ้ามากกว่า 240 โวลต์ อาการที่จะเกิดขึ้นจะเป็นอย่างไร

ก. หยุดหายใจ

ข. กล้ามเนื้อหัวใจกระตุก หรือเต้นถี่รัว

ค. ผิวหนังฉีกขาด

ง. ผิวหนังไหม้

22. ปริมาณกระแสไฟฟ้าที่ไหลผ่านร่างกาย 0.5 – 2 mA

ก. ยังไม่มีผลหรือยังไม่รู้สึก

ข. รู้สึกว่าถูกไฟดูด

ค. กระทบกระเทือนต่อระบบประสาท

ง. หัวใจหยุดเต้น ผิวหนังไหม้

23. ข้อใด ไม่ใช่ สาเหตุของการเกิดอุบัติเหตุเกี่ยวกับงานไฟฟ้า

ก. คนงานขาดความระมัดระวัง

ข. ขาดความชำนาญ

ค. ขาดคนงานในการปฏิบัติงาน

ง. การขาดงบประมาณในการใช้อุปกรณ์ไฟฟ้าที่ได้มาตรฐาน

24. กฎหมายที่เกี่ยวข้องกับเรื่องของความปลอดภัยและอาชีวอนามัยฉบับล่าสุดประกาศ พ.ศ. ใด

ก. พ.ศ. 2560

ข. พ.ศ. 2554

ค. พ.ศ. 2542

ง. พ.ศ. 2535

25. ข้อใดไม่ใช่การป้องกันอันตรายจากงานไฟฟ้า

ก. เครื่องใช้ไฟฟ้าชำรุด ควรติดป้ายห้ามใช้ เพื่อรอนำส่งช่างซ่อมไฟฟ้าต่อไป

ข. การปฏิบัติงานเกี่ยวกับไฟฟ้าทุกครั้งไม่ควรสวมถุงมือยางเพื่อป้องกันไฟฟ้าดูด

ค. อย่าเข้าใกล้หรือแตะสายไฟฟ้าที่ห้อยลงมาหรือตกอยู่กับพื้น

ง. ควรตัดกระแสไฟฟ้าออกทุกครั้งก่อนที่จะทำการตรวจซ่อมเครื่องใช้ไฟฟ้า

26. เมื่อพบสายไฟฟ้าแรงสูงห้อยลงมาหรือตกอยู่กับพื้น ข้อใดเป็นวิธีการปฏิบัติที่ถูกต้องที่สุด
ก. หาไม้เขี่ยสายออกให้เร็วที่สุด
ข. ร้องขอความช่วยเหลือ
ค. อย่าเข้าใกล้และโทรแจ้งการไฟฟ้าใกล้บ้านโดยเร็ว
ง. ไม่สนใจกับสิ่งที่เกิดขึ้น

27. ในการติดตั้งเสาอากาศโทรทัศน์ ต้องติดตั้งเสาอากาศโทรทัศน์ ให้ห่างจากสายไฟฟ้ากี่เมตร ข้อใดถูกต้องที่สุด
ก. 2 เมตร
ข. 3 เมตร
ค. ไม่น้อยกว่า 3 เมตร หรือระยะเสาล้มต้องไม่โดนสายไฟฟ้า
ง. 4 เมตร

28. ข้อใด ไม่ใช่ ความปลอดภัยในการใช้เครื่องมือ
ก. การใช้ประแจให้อยู่ในลักษณะดึงเข้าหาตัว
ข. ใช้เครื่องมือที่ต้อง งอ ข้อมือทำงาน
ค. ใช้เครื่องมือคุณภาพดี ไม่ชำรุด
ง. ตรวจสอบเครื่องมือทุกครั้งก่อนที่จะใช้งาน

29. ในการใช้งานเครื่องมือควรปฏิบัติตนอย่างไร ข้อใดถูกต้องที่สุด
ก. ตรวจสอบเครื่องมือทุกครั้งก่อนที่จะใช้งาน
ข. ศึกษาวิธีการใช้ให้ดีก่อน
ค. บำรุงรักษาเครื่องมืออย่างสม่ำเสมอ
ง. ถูกทุกข้อ

30. ความหมายของอุปกรณ์ป้องกันอันตรายส่วนบุคคลคือข้อใด
ก. อุปกรณ์ที่สวมใส่ส่วนใดส่วนหนึ่งของร่างกาย เพื่อป้องกันอันตรายที่อาจเกิดขึ้นได้
ข. อุปกรณ์ที่สวมใส่แค่เพียงเสื้อ เพื่อป้องกันอันตรายที่อาจเกิดขึ้นได้
ค. อุปกรณ์ที่สวมใส่เพียงศีรษะ เพื่อป้องกันอันตรายที่อาจเกิดขึ้นได้
ง. อุปกรณ์ที่ใช้ในการติดตั้งกล้องโทรทัศน์วงจรปิด

31. ข้อใดเป็นการใช้งานอุปกรณ์ป้องกันศีรษะในการปฏิบัติงานที่ถูกต้อง
ก. การใช้งานหมวกนิรภัยจะใช้งานต่อเมื่อมีการปฏิบัติงานเกี่ยวกับเครื่องจักรในโรงงาน
ข. พนักงานรับเหมาและผู้มาเยือนจะต้องสวมหมวกป้องกันศีรษะตลอดเวลาในพื้นที่ที่มีการก่อสร้าง
ค. ผู้มาเยือนสถานที่ปฏิบัติงานจะต้องใส่หมวกนิรภัยสีขาว
ง. หมวกนิรภัยสีเหลือง เป็นหมวกสำหรับพนักงานประจำด้านงานอุตสาหกรรม

32. หน้ากากกรองฝุ่นละออง เป็นอุปกรณ์ที่มีวิธีการใช้งานอย่างไรในการปฏิบัติงาน
ก. เป็นอุปกรณ์ป้องกันการเต้นของหัวใจเมื่อปฏิบัติงานเกี่ยวกับงานที่เป็นอันตรายต่อสุขภาพ
ข. เป็นอุปกรณ์ป้องกันการมองเห็นเมื่อปฏิบัติงานเกี่ยวกับงานที่เป็นอันตรายต่อสายตา
ค. เป็นอุปกรณ์ป้องกันการหายใจเมื่อปฏิบัติงานเกี่ยวกับงานที่เป็นอันตรายต่อสุขภาพ
ง. ไม่มีข้อใดกล่าวถูก

33. ถุงมือนิรภัย เป็นอุปกรณ์ที่มีวิธีการใช้งานอย่างไรในการปฏิบัติงาน
ก. ใช้เพื่อป้องกันมือจากการถูกความเย็น
ข. ใช้เพื่อป้องกันมือจากการถูกความชื้น

ค. ใช้เพื่อป้องกันมือจากการเปียก

ง. ใช้เพื่อป้องกันมือจากการถูกความร้อน ความสกปรก การกระแทก สะเก็ดไฟ การเสียดสี

34. เชือกในลักษณะรักษาตำแหน่ง ควรมีระยะเท่าไหร่

ก. ควรมีระยะสั้น

ข. ควรมีระยะยาว 1 เมตร

ค. ควรมีระยะยาว 2 เมตร

ง. ควรมีระยะยาว 3 เมตร

35. การปฐมพยาบาลข้อใดกล่าวถูกต้องที่สุด

ก. การให้ความช่วยเหลือแก่ผู้ป่วยหรือผู้ที่ได้รับบาดเจ็บ โดยใช้อุปกรณ์เท่าที่หาได้ในขณะนั้นนำมาใช้ในการรักษาเบื้องต้น

ข. การให้ความช่วยเหลือแก่ผู้ป่วย

ค. การให้ความช่วยเหลือแก่ผู้ป่วยหรือผู้ที่ได้รับบาดเจ็บ

ง. ผิดทุกข้อ

36. เมื่อพบผู้ป่วยที่ถูกกระแสไฟฟ้าดูดและหัวใจหยุดเต้น ควรปฐมพยาบาลอย่างไร

ก. ผายปอด

ข. จับผู้ป่วยพาดบ่าแล้ววิ่งไปรอบ ๆ

ค. นวดแขนและขาของผู้ป่วยจนกว่าผู้ป่วยจะฟื้น

ง. ใช้สองมือซ้อนกันออกแรงกดบริเวณทรวงอกของผู้ป่วย

37. ในกรณีผู้บาดเจ็บหมดสติ ข้อใด ไม่ใช่วิธีในการปฐมพยาบาล

ก. พยายามหงายศีรษะผู้บาดเจ็บไปข้างหลังเท่าที่จะหงายได้ เพื่อเปิดทางอากาศเข้าสู่ปอดได้สะดวก

ข. ใช้ผ้าหนาๆ ม้วนแล้วสอดเข้าใต้ช่วงไหล่ เพื่อหนุนหงายศีรษะไว้

ค. ล้วงสิ่งที่อาจค้างอยู่ในปากซึ่งจะขัดขวางทางลม เช่น หมากฝรั่ง ของขบเคี้ยว

ง. นวดแขนและขาของผู้ป่วยจนกว่าผู้ป่วยจะฟื้น

38. การผายปอดเพื่อให้ปอดได้รับออกซิเจนเพียงพอ อยู่ในกรณีใด

ก. กรณีผู้บาดเจ็บหมดสติ

ข. กรณีผู้บาดเจ็บไม่หายใจ

ค. กรณีผู้บาดเจ็บหัวใจหยุดเต้น

ง. ไม่มีกรณีที่กล่าว

39. การนวดหัวใจเป็นจังหวะซ้ำกัน ครั้งละ 1 วินาที ทำเนิบๆ ไม่ควรลุกลี้ลุกลน อยู่ในกรณีใด

ก. กรณีผู้บาดเจ็บหมดสติ

ข. กรณีผู้บาดเจ็บไม่หายใจ

ค. กรณีผู้บาดเจ็บหัวใจหยุดเต้น

ง. ไม่มีกรณีที่กล่าว

40. ข้อใดเป็นกฎความปลอดภัยไฟฟ้า

ก. ทำงานโดยไม่ตัดไฟ

ข. ตรวจสอบแรงดันก่อนทำงาน

ค. ไม่ใช้ PPE

ง. ใช้น้ำดับไฟ

2 อุปกรณ์เซนเซอร์สำหรับระบบรักษาความปลอดภัย

21

หลักการทำงานของเซนเซอร์

2.1.1 ความหมายของเซนเซอร์
2.1.2 หลักการแปลงสัญญาณของเซนเซอร์
2.1.3 การจำแนกเซนเซอร์ตามแหล่งพลังงาน
2.1.4 สมรรถนะที่สำคัญของเซนเซอร์

22

เซนเซอร์ตรวจจับการเคลื่อนไหว

2.2.1 ลักษณะการใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหว
2.2.2 ส่วนประกอบของเซนเซอร์ตรวจจับการเคลื่อนไหว
2.2.3 หลักการทำงานของเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR
2.2.4 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR

23

เซนเซอร์ตรวจจับประตูและหน้าต่าง

2.3.1 หลักการเบื้องต้นของเซนเซอร์ประตูและหน้าต่าง
2.3.2 ชนิดของเซนเซอร์ประตูและหน้าต่าง
2.3.3 หลักการทำงานของเซนเซอร์ประตูและหน้าต่าง

24

เซนเซอร์ตรวจจับควัน

2.4.1 ความหมายของเซนเซอร์ตรวจจับควัน
2.4.2 ประเภทของเซนเซอร์ตรวจจับควัน
2.4.3 โครงสร้างและหลักการทำงานของเซนเซอร์ตรวจจับควัน
2.4.4 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับควัน

25

เซนเซอร์ตรวจจับก๊าซ

2.5.1 ความหมายของเซนเซอร์ตรวจจับก๊าซ
2.5.2 ชนิดของเซนเซอร์ตรวจจับก๊าซ
2.5.3 โครงสร้างของเซนเซอร์ตรวจจับก๊าซ
2.5.4 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับก๊าซ

26

เซนเซอร์ตรวจจับเปลวไฟ

2.6.1 คุณสมบัติของคลื่นแม่เหล็กไฟฟ้าที่ตรวจพบจากเปลวไฟ

2.6.2 ชนิดของเซนเซอร์ตรวจจับเปลวไฟ

2.6.3 โครงสร้างของเซนเซอร์ตรวจจับเปลวไฟ

2.6.4 หลักการทำงานของเซนเซอร์ตรวจจับเปลวไฟ

2.6.5 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับเปลวไฟ

บทที่ 2 อุปกรณ์เซนเซอร์สำหรับระบบรักษาความปลอดภัย

Sensor Devices for Security Systems

2.1 หลักการทำงานของเซนเซอร์ (Principles of Sensors)

2.1.1 ความหมายของเซนเซอร์ (Sensor)

เซนเซอร์ คือ อุปกรณ์ที่ทำหน้าที่ตรวจจับการเปลี่ยนแปลงของปริมาณทางกายภาพ (physical quantity) ทางเคมี (chemical quantity) หรือทางชีวภาพ (biological quantity) แล้วแปลงข้อมูลที่ตรวจวัดได้ให้อยู่ในรูปของสัญญาณไฟฟ้าที่สามารถนำไปประมวลผล แสดงผล หรือควบคุมการทำงานของระบบอัตโนมัติได้ เซนเซอร์จึงเป็นองค์ประกอบสำคัญของระบบอิเล็กทรอนิกส์ ระบบควบคุมอัตโนมัติ และระบบรักษาความปลอดภัยอัจฉริยะ (Bentley, 2005; Al-Qutayri, 2010; Ismail, 2019; Selvolini & Marrazza, 2023)

การทำงานของเซนเซอร์ประกอบด้วยกระบวนการหลัก 3 ขั้นตอน ได้แก่ การตรวจจับ (detection) การแปลงสัญญาณ (transduction) และการปรับสภาพสัญญาณ (signal conditioning) รายละเอียด ดังต่อไปนี้

1) การตรวจจับ (Detection)

เป็นขั้นตอนที่ส่วนตรวจจับของเซนเซอร์ (sensing element) สัมผัสหรือรับรู้การเปลี่ยนแปลงของสิ่งแวดล้อม เช่น อุณหภูมิ ความดัน ความเข้มของแสง ความชื้น การเคลื่อนไหว หรือการสั่นสะเทือน แล้วเปลี่ยนแปลงคุณสมบัติทางกายภาพของวัสดุที่ใช้เป็นตัวตรวจจับ

2) การแปลงสัญญาณ (Transduction)

เมื่อเซนเซอร์ตรวจจับปริมาณที่ต้องการวัดแล้ว พลังงานหรือการเปลี่ยนแปลงทางกายภาพจะถูกแปลงเป็นสัญญาณไฟฟ้า เช่น แรงดันไฟฟ้า (voltage) กระแสไฟฟ้า (current) ความต้านทานไฟฟ้า (resistance) หรือค่าความจุไฟฟ้า (capacitance) เพื่อให้สามารถนำไปประมวลผลต่อได้

3) การปรับสภาพสัญญาณ (Signal Conditioning)

สัญญาณไฟฟ้าที่ได้จากเซนเซอร์มักมีขนาดเล็กและอาจมีสัญญาณรบกวน (noise) ปะปนอยู่ จึงต้องผ่านวงจรปรับสภาพสัญญาณ เช่น การขยายสัญญาณ (amplification) การกรองสัญญาณ (filtering) และการแปลงสัญญาณแอนะล็อกเป็นดิจิทัล (Analog-to-Digital Conversion: ADC) ก่อนส่งไปยังไมโครคอนโทรลเลอร์หรือหน่วยประมวลผลของระบบ

2.1.2 หลักการแปลงสัญญาณของเซนเซอร์ (Sensor Transduction Principles)

เซนเซอร์สามารถจำแนกตามหลักการแปลงพลังงานหรือหลักการทางฟิสิกส์ที่ใช้ในการสร้างสัญญาณไฟฟ้าได้หลายประเภท (Bentley, 2005; Selvolini & Marrazza, 2023) ดังนี้

1) เซนเซอร์แบบความต้านทาน (Resistive Sensors)

การเปลี่ยนแปลงค่าความต้านทานไฟฟ้าตามปริมาณที่ต้องการวัด เช่น เทอร์มิสเตอร์ (thermistor) วัดอุณหภูมิ และสเตรนเกจ (strain gauge) สำหรับวัดแรงหรือความเครียด

2) เซนเซอร์แบบความจุไฟฟ้า (Capacitive Sensors)

ทำงานโดยตรวจวัดการเปลี่ยนแปลงของค่าความจุไฟฟ้า ซึ่งเกิดจากการเปลี่ยนแปลงระยะห่างระหว่างแผ่นตัวนำ พื้นที่ของแผ่นตัวนำ หรือค่าคงที่ไดอิเล็กทริกของวัสดุ เหมาะสำหรับการตรวจจับตำแหน่ง ระดับของเหลว และการสัมผัส

3) เซนเซอร์แบบเพียโซอิเล็กทริก (Piezoelectric Sensors)

อาศัยคุณสมบัติของวัสดุเพียโซอิเล็กทริกที่สามารถสร้างแรงดันไฟฟ้าเมื่อได้รับแรงกด แรงกระแทก หรือการสั่นสะเทือน จึงนิยมใช้ในการวัดแรง ความดัน และการสั่นสะเทือน

4) เซนเซอร์แบบออปติคัล (Optical Sensors)

ทำงานโดยใช้แหล่งกำเนิดแสงร่วมกับตัวรับแสง เพื่อตรวจวัดการเปลี่ยนแปลงของความเข้มแสง การสะท้อน การหักเห หรือการบดบังของแสง ซึ่งประยุกต์ใช้ในระบบตรวจจับวัตถุ ระบบนับชิ้นงาน และระบบจดจำภาพ

2.1.3 การจำแนกเซนเซอร์ตามแหล่งพลังงาน (Classification Based on Energy Source)

เซนเซอร์สามารถแบ่งออกเป็น 2 ประเภท ดังนี้

1) แอคทีฟ เซ็นเซอร์ (Active Sensors)

เป็นเซนเซอร์ที่สามารถสร้างสัญญาณไฟฟ้าได้เองจากพลังงานของปริมาณที่ต้องการวัด โดยไม่ต้องอาศัยแหล่งจ่ายไฟภายนอก เช่น เทอร์โมคัปเปิลและเซนเซอร์เพียโซอิเล็กทริก

2) แพสซีฟ เซ็นเซอร์ (Passive Sensors)

เป็นเซนเซอร์ที่ต้องอาศัยแหล่งจ่ายไฟภายนอกในการทำงาน โดยค่าทางไฟฟ้าของเซนเซอร์ เช่น ความต้านทาน ความจุไฟฟ้า หรือความเหนี่ยวนำ จะเปลี่ยนแปลงตามปริมาณที่ตรวจวัด ตัวอย่าง ได้แก่ เทอร์มิสเตอร์ สเตรนเกจ และเซนเซอร์แบบคาปาซิทีฟ

2.1.4 สมรรถนะที่สำคัญของเซนเซอร์ (Key Performance Characteristics)

การเลือกใช้งานเซนเซอร์จำเป็นต้องพิจารณาคุณลักษณะด้านสมรรถนะ เพื่อให้เหมาะสมกับลักษณะงาน (Selvolini & Marrazza, 2023) ดังนี้

1) ความไว (Sensitivity)

อัตราส่วนของการเปลี่ยนแปลงของสัญญาณเอาต์พุตต่อการเปลี่ยนแปลงของปริมาณที่วัด หากเซนเซอร์มีความไวสูง จะสามารถตรวจจับการเปลี่ยนแปลงเพียงเล็กน้อยได้

2) ความละเอียด (Resolution)

ค่าการเปลี่ยนแปลงที่น้อยที่สุดของปริมาณที่วัด ซึ่งเซนเซอร์สามารถตรวจจับและแสดงผลได้อย่างน่าเชื่อถือ

3) ความถูกต้อง (Accuracy)

ความใกล้เคียงระหว่างค่าที่เซนเซอร์วัดได้กับค่าจริงของปริมาณที่วัด โดยค่าความคลาดเคลื่อนยิ่งน้อย แสดงว่าเซนเซอร์มีความถูกต้องสูง

4) ช่วงการวัด (Dynamic Range)

ช่วงของค่าตั้งแต่ค่าต่ำสุดจนถึงค่าสูงสุดที่เซนเซอร์สามารถวัดได้อย่างถูกต้อง โดยไม่เกิดความผิดเพี้ยนของสัญญาณ (distortion)

2.2 เซนเซอร์ตรวจจับการเคลื่อนไหว (Motion Sensors)

เซนเซอร์ตรวจจับการเคลื่อนไหว เป็นอุปกรณ์ที่ได้รับความสนใจอย่างต่อเนื่องในงานวิจัยด้านวิศวกรรมและเทคโนโลยี เนื่องจากสามารถประยุกต์ใช้งานได้อย่างกว้างขวาง ทั้งในระบบรักษาความปลอดภัยอัจฉริยะ (smart security systems) ระบบบ้านอัจฉริยะ (smart home) ระบบอาคารอัจฉริยะ (smart building) อินเทอร์เน็ตของสรรพสิ่ง (IoT) วิศวกรรมชีวการแพทย์ (biomedical engineering) และระบบปัญญาประดิษฐ์ (AI) งานวิจัยส่วนใหญ่มุ่งเน้นการพัฒนาเซนเซอร์ให้มีความแม่นยำสูง ใช้พลังงานต่ำ และสามารถวิเคราะห์ข้อมูลได้อย่างชาญฉลาด

2.2.1 ลักษณะการใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหว

1) การใช้งานในด้านการแพทย์และชีวกลศาสตร์ (Healthcare and Biomechanics)

งานวิจัยด้านการแพทย์ให้ความสำคัญกับการใช้เซนเซอร์ตรวจจับการเคลื่อนไหวแบบสวมใส่ (wearable motion sensors) เช่น เซนเซอร์วัดความเร่ง (accelerometer) และไจโรสโคป (gyroscope) เพื่อเฝ้าติดตามการเคลื่อนไหวของผู้ป่วยแบบต่อเนื่องนอกสถานพยาบาล เทคโนโลยีดังกล่าวช่วยประเมินสมรรถภาพการเคลื่อนไหว ติดตามผลการฟื้นฟูสมรรถภาพ และสนับสนุนการวินิจฉัยความผิดปกติของการทรงตัวและการเดินได้อย่างมีประสิทธิภาพ นอกจากนี้ ยังมีการนำอัลกอริทึมการรู้จำกิจกรรมของมนุษย์ (Human Activity Recognition: HAR) มาประมวลผลข้อมูลจากเซนเซอร์ เพื่อจำแนกกิจกรรมต่าง ๆ ในชีวิตประจำวัน เช่น การเดิน การนั่ง การลุกขึ้น การรับประทานอาหาร และการรับประทานยา ซึ่งเป็นข้อมูลสำคัญสำหรับการดูแลสุขภาพและผู้สูงอายุ

2) การพัฒนาแบบจำลองการตรวจจับการเคลื่อนไหว (Motion Sensor Modeling)

งานวิจัยสมัยใหม่ได้ประยุกต์แนวคิดจากระบบประสาทชีวภาพ (biologically inspired computing) ในการพัฒนาแบบจำลองการตรวจจับการเคลื่อนไหว โดยใช้หลักการประมวลผลของเดนไดรต์ (dendritic computation) เพื่อเพิ่มประสิทธิภาพในการตรวจจับและจำแนกการเคลื่อนไหว วิธีการดังกล่าวสามารถลดข้อจำกัดของเซนเซอร์แบบดั้งเดิม และช่วยให้แบบจำลองสามารถทำนายการตอบสนองของเซลล์ประสาทเดี่ยว (single-neuron response) ได้ใกล้เคียงกับระบบประสาทของสิ่งมีชีวิตมากยิ่งขึ้น

3) การประยุกต์ใช้ในระบบรักษาความปลอดภัย (Energy Efficiency and Security Applications)

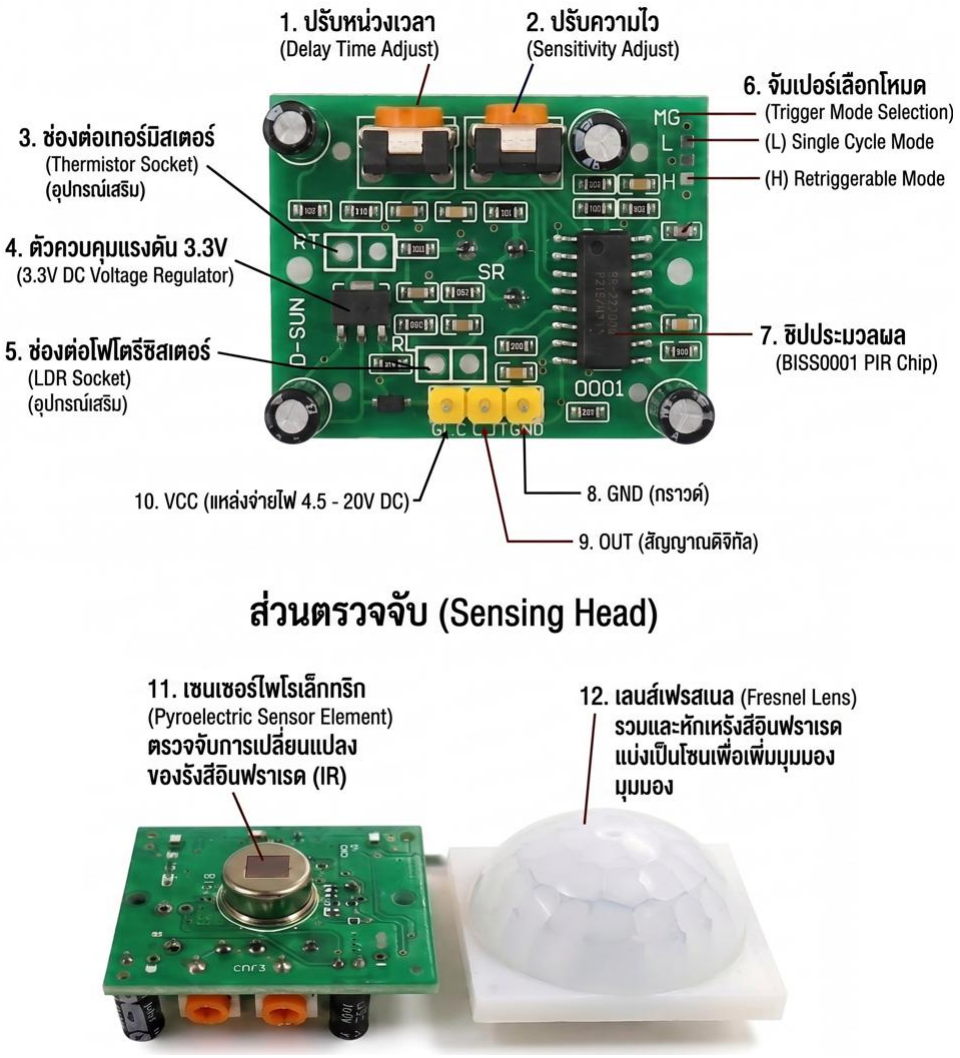
การขยายตัวของระบบบ้านอัจฉริยะและอาคารอัจฉริยะ ส่งผลให้การออกแบบเซนเซอร์ตรวจจับการเคลื่อนไหวมุ่งเน้นการลดการใช้พลังงาน เพื่อยืดอายุการใช้งานของแบตเตอรี่และลดต้นทุนในการบำรุงรักษา งานวิจัยหลายฉบับได้เปรียบเทียบประสิทธิภาพของเซนเซอร์ตรวจจับการเคลื่อนไหวประเภทต่าง ๆ ทั้งเซนเซอร์อินฟราเรดแบบพาสซีฟ (Passive Infrared Sensor: PIR) เซนเซอร์ไมโครเวฟ (microwave sensor) และเซนเซอร์อัลตราโซนิก (ultrasonic sensor) เพื่อเลือกใช้ให้เหมาะสมกับสภาพแวดล้อมและรูปแบบการใช้งาน นอกจากนี้ ยังมีการบูรณาการเซนเซอร์เข้ากับระบบอินเทอร์เน็ตของสรรพสิ่ง และระบบปัญญาประดิษฐ์ เพื่อเพิ่มความสามารถในการตรวจจับ วิเคราะห์ และแจ้งเตือนเหตุการณ์ผิดปกติแบบเรียลไทม์ ส่งผลให้ระบบรักษาความปลอดภัยมีความแม่นยำ ลดอัตราการแจ้งเตือนผิดพลาด (false alarm) และสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว (Pawar et al., 2018; Thu et al., 2020; Sahasika et al., 2023; Gagote et al., 2026)

จากการศึกษางานวิจัยที่ผ่านมา พบว่าแนวโน้มการพัฒนาเซนเซอร์ตรวจจับการเคลื่อนไหวมุ่งเน้นในสามประเด็นหลัก ได้แก่ (1) การเพิ่มความแม่นยำในการตรวจจับและจำแนกการเคลื่อนไหว (2) การลดการใช้พลังงานเพื่อรองรับการทำงานในระบบ IoT และอุปกรณ์แบบสวมใส่ และ (3) การประยุกต์ใช้ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (Machine Learning: ML) เพื่อเพิ่มประสิทธิภาพในการวิเคราะห์ข้อมูลและการตัดสินใจอัตโนมัติ ซึ่งเป็นพื้นฐานสำคัญของระบบรักษาความปลอดภัยอัจฉริยะในปัจจุบัน

2.2.2 ส่วนประกอบของเซนเซอร์ตรวจจับการเคลื่อนไหว (Passive Infrared Sensor: PIR)

ภายในเซนเซอร์ PIR ประกอบด้วย องค์ประกอบตรวจจับ (sensing elements) 2 ส่วน ซึ่งไวต่อรังสีอินฟราเรด เมื่อไม่มีวัตถุเคลื่อนที่ผ่าน พลังงานอินฟราเรดที่ตกกระทบทั้งสองส่วนจะมีค่าใกล้เคียงกัน ทำให้ผลต่างของสัญญาณไฟฟ้ามีค่าเป็นศูนย์หรือใกล้ศูนย์ อย่างไรก็ตาม เมื่อบุคคลหรือสัตว์เคลื่อนที่ผ่านบริเวณตรวจจับ รังสีอินฟราเรดจากร่างกายจะตกกระทบ

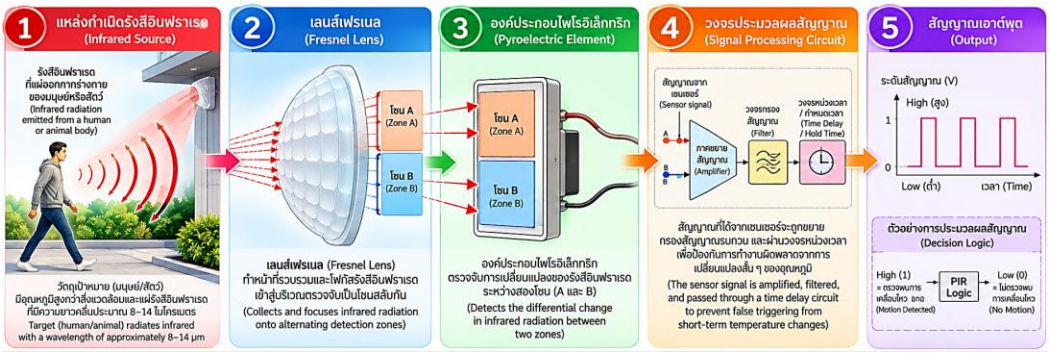
องค์ประกอบตรวจจับทีละส่วน ส่งผลให้เกิดความแตกต่างของพลังงานอินฟราเรดระหว่างองค์ประกอบทั้งสอง และเซนเซอร์จะสร้างสัญญาณไฟฟ้าแบบผลต่าง (differential output) เพื่อบ่งชี้ว่ามีการเคลื่อนไหวเกิดขึ้น หากวัตถุเคลื่อนที่ออกจากพื้นที่ตรวจจับ สัญญาณจะเปลี่ยนแปลงในทิศทางตรงกันข้ามเพื่อเพิ่มประสิทธิภาพในการตรวจจับ เซนเซอร์ PIR จะติดตั้งเลนส์เฟรสเนล (Fresnel lens) ไว้ด้านหน้าเซนเซอร์ ทำหน้าที่รวมและกระจายรังสีอินฟราเรดจากพื้นที่กว้างให้ตกกระทบองค์ประกอบตรวจจับได้อย่างมีประสิทธิภาพ ประสิทธิภาพของเซนเซอร์ PIR ขึ้นอยู่กับหลายปัจจัย ได้แก่ การตั้งค่าความไวของเซนเซอร์ ขนาดและคุณสมบัติทางความร้อนของวัตถุ ระยะห่างระหว่างวัตถุกับเซนเซอร์ รวมถึงสภาพแวดล้อม เช่น อุณหภูมิภายนอกและแหล่งกำเนิดความร้อน จากผลการศึกษาพบว่า เมื่ออุณหภูมิแวดล้อมสูงขึ้นหรือระยะห่างระหว่างวัตถุกับเซนเซอร์เพิ่มขึ้น ความไวและระยะการตรวจจับของเซนเซอร์จะลดลงอย่างชัดเจน (Pawar et al., 2018; Thu et al., 2020)



รูปที่ 2.1 ส่วนประกอบของเซนเซอร์ PIR

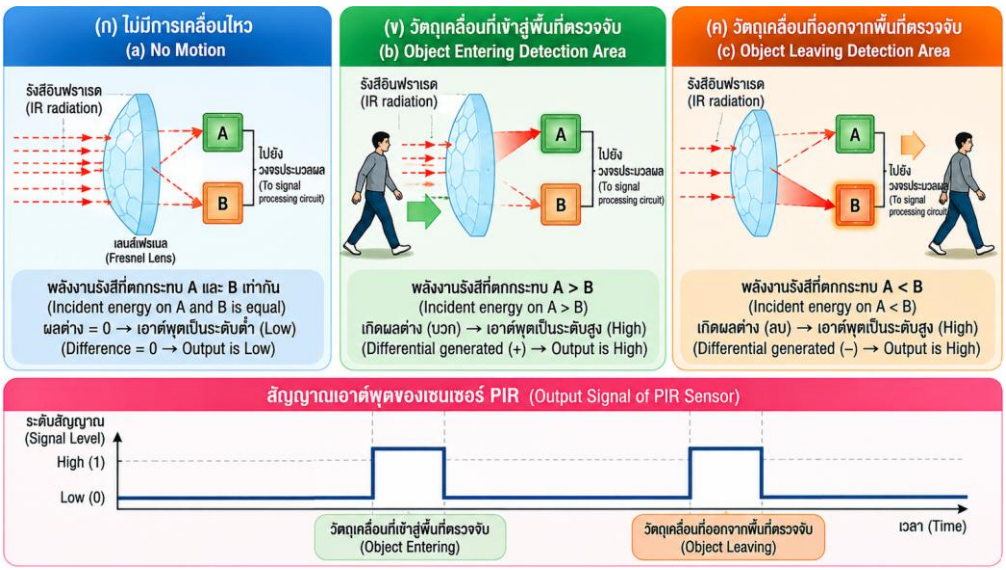
2.2.3 หลักการทำงานของเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR

เซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIRเป็นเซนเซอร์ที่ใช้ตรวจจับการเปลี่ยนแปลงของรังสีอินฟราเรด (infrared radiation) ที่แผ่ออกมาจากวัตถุหรือสิ่งมีชีวิต ซึ่งมีอุณหภูมิสูงกว่าศูนย์สัมบูรณ์ (absolute zero) โดยเซนเซอร์ชนิดนี้ไม่ปล่อยพลังงานหรือคลื่นใด ๆ ออกไปเพื่อการตรวจจับ จึงเรียกว่า passive sensor แต่ทำหน้าที่รับรังสีอินฟราเรดจากสงแวดลอมเพยงอย่างเดียว หลักการทำงานของเซ็นเซอร์ PIR อาศัยคุณสมบัติของวัสดุไพโรอิเล็กทริก (pyroelectric material) ซึ่งสามารถสร้างสัญญาณไฟฟ้าเมื่อได้รับการเปลี่ยนแปลงของพลังงานความร้อน เซนเซอร์ตอบสนองต่อรังสีอินฟราเรดในช่วงความยาวคลื่นประมาณ 10 ไมโครเมตร (10 μm) ซึ่งเป็นช่วงความยาวคลื่นที่สอดคล้องกับรังสีความร้อนที่แผ่ออกมาจากร่างกายมนุษย์และสัตว์ จึงเหมาะสำหรับการตรวจจับการเคลื่อนไหวของสิ่งมีชีวิต



รูปที่ 2.2 หลักการทำงานของเซนเซอร์ PIR

ภายในเซนเซอร์ PIR ประกอบด้วย องค์ประกอบตรวจจับ 2 ส่วน ซึ่งไวต่อรังสีอินฟราเรด เมื่อไม่มีวัตถุเคลื่อนที่ผ่าน พลังงานอินฟราเรดที่ตกกระทบทั้งสองส่วนจะมีค่าใกล้เคียงกัน ทำให้ผลต่างของสัญญาณไฟฟ้ามีค่าเป็นศูนย์หรือใกล้ศูนย์ เมื่อบุคคลหรือสัตว์เคลื่อนที่ผ่านบริเวณตรวจจับ รังสีอินฟราเรดจากร่างกายจะตกกระทบองค์ประกอบตรวจจับทีละส่วน ส่งผลให้เกิดความแตกต่างของพลังงานอินฟราเรดระหว่างทั้งสอง องค์ประกอบ จากนั้นเซนเซอร์จะสร้างสัญญาณไฟฟ้าแบบผลต่าง (differential output) เพื่อบ่งชี้ว่ามีการเคลื่อนไหวเกิดขึ้น หากวัตถุเคลื่อนที่ออกจากพื้นที่ตรวจจับ สัญญาณจะเปลี่ยนแปลงในทิศทางตรงกันข้าม เพื่อเพิ่มประสิทธิภาพในการตรวจจับ เซนเซอร์ PIR ส่วนใหญ่ติดตั้ง เลนส์เฟรสเนลไว้ด้านหน้าเซนเซอร์ ทำหน้าที่รวมและกระจายรังสีอินฟราเรดจากพื้นที่กว้างให้ตกกระทบองค์ประกอบตรวจจับได้อย่างมีประสิทธิภาพ ส่งผลให้ระยะตรวจจับและความไวของเซนเซอร์เพิ่มขึ้น โดยทั่วไปเซนเซอร์ PIR สามารถตรวจจับการเคลื่อนไหวได้ในระยะประมาณ 10 m และมีมุมตรวจจับน้อยกว่า 180 องศา ขณะที่บางรุ่นที่ออกแบบสำหรับติดตั้งบนเพดานสามารถตรวจจับได้รอบทิศทาง 360 องศา (Pawar et al., 2018) ซึ่ง PIR Sensor ตรวจจับการเปลี่ยนแปลงของรังสีอินฟราเรด ไม่ได้วัดอุณหภูมิของวัตถุโดยตรงจึงตอบสนองเมื่อมีวัตถุเคลื่อนที่ผ่านเท่านั้น

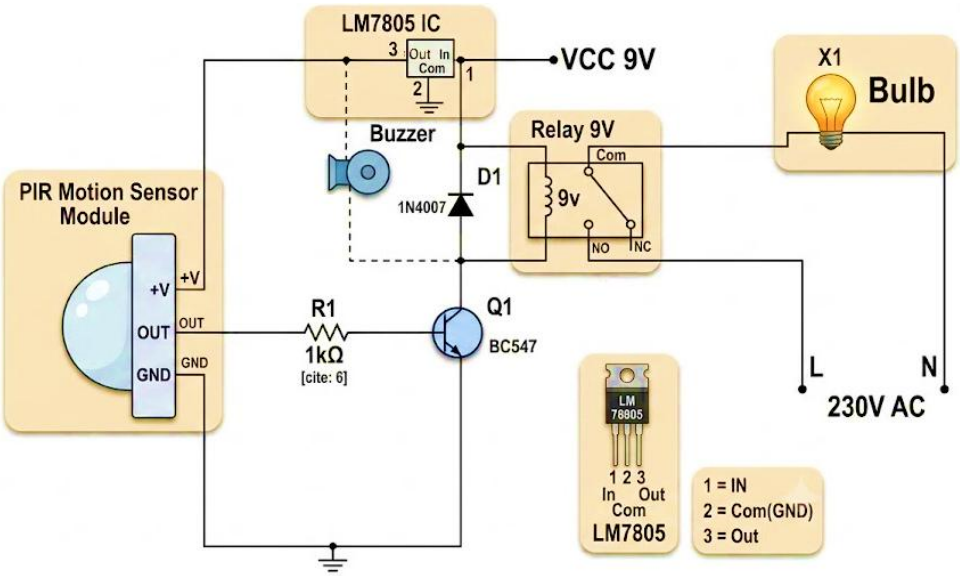


รูปที่ 2.3 หลักการตรวจจับความแตกต่างของพลังงานอินฟราเรด

ประสิทธิภาพของเซนเซอร์ PIR ขึ้นอยู่กับหลายปัจจัย ได้แก่ การตั้งค่าความไวของเซนเซอร์ (sensitivity setting) ขนาดและคุณสมบัติทางความร้อนของวัตถุ ระยะห่างระหว่างวัตถุกับเซนเซอร์ รวมถึงสภาพแวดล้อม เช่น อุณหภูมิภายนอกและแหล่งกำเนิดความร้อน จากผลการศึกษาพบว่า เมื่ออุณหภูมิแวดล้อมสูงขึ้นหรือระยะห่างระหว่างวัตถุกับเซนเซอร์เพิ่มขึ้น ความไวและระยะการตรวจจับของเซนเซอร์จะลดลงอย่างชัดเจน ด้วยคุณสมบัติที่มีขนาดเล็ก ใช้พลังงานต่ำ ราคาประหยัด และติดตั้งได้ง่าย เซนเซอร์ PIR จึงถูกนำไปประยุกต์ใช้อย่างแพร่หลายในระบบรักษาความปลอดภัย ระบบสัญญาณกันขโมย ระบบไฟส่องสว่างอัตโนมัติ ประตูอัตโนมัติ ระบบบ้านอัจฉริยะ และระบบอินเทอร์เน็ตของสรรพสิ่ง เพื่อเพิ่มประสิทธิภาพในการตรวจจับและตอบสนองต่อการเคลื่อนไหวของบุคคลหรือวัตถุโดยอัตโนมัติ

2.2.4 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR

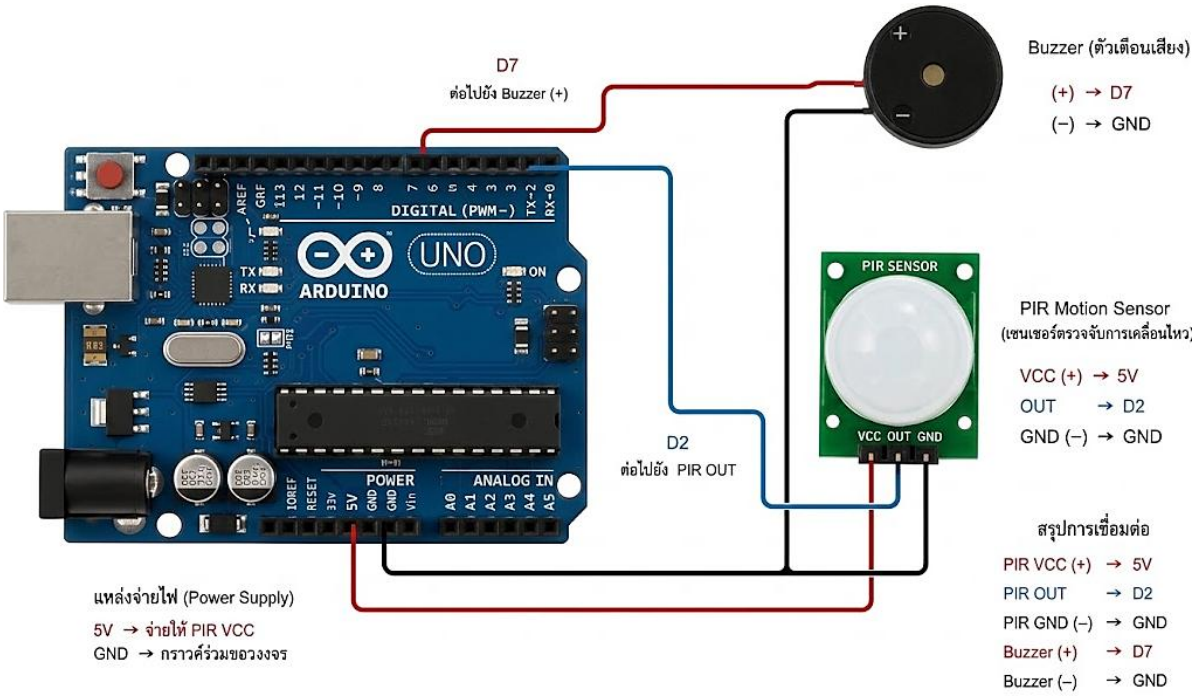
การนำเซนเซอร์ PIR มาใช้งานจำเป็นต้องออกแบบและต่อวงจรอิเล็กทรอนิกส์ให้เหมาะสม เพื่อให้สามารถรับสัญญาณเอาต์พุตจากเซนเซอร์และนำไปควบคุมอุปกรณ์ไฟฟ้าหรืออุปกรณ์อิเล็กทรอนิกส์ ดังรูปที่ 2.4



รูปที่ 2.4 วงจรใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR

วงจรตรวจจับการเคลื่อนไหวด้วยเซนเซอร์ PIR ทำงานโดยอาศัยการตรวจจับการเปลี่ยนแปลงของรังสีอินฟราเรดที่แผ่ออกมาจากร่างกายมนุษย์หรือวัตถุที่มีอุณหภูมิสูงกว่าสภาพแวดล้อม เมื่อมีบุคคลเคลื่อนที่ผ่านบริเวณตรวจจับ โมดูล PIR จะสร้างสัญญาณเอาต์พุตลอจิกระดับ HIGH (3.3 V) ที่ขา OUT จากนั้นสัญญาณดังกล่าวจะถูกส่งผ่านตัวต้านทาน R1 ไปยังขาเบส (Base: B) ทรานซิสเตอร์ Q1(BC547) ทำให้ทรานซิสเตอร์ทำงานในสภาวะอิ่มตัว (saturation) และยอมให้กระแสไฟฟ้าไหลผ่านจากคอลเลกเตอร์ (Collector: C) ไปยังอีมิตเตอร์ (Emitter: E) ส่งผลให้ขดลวดของรีเลย์ K1 ได้รับกระแสไฟฟ้าและเกิดสนามแม่เหล็กไฟฟ้า ทำให้หน้าสัมผัสของ

รีเลย์เปลี่ยนจากขั้ว Normally Open (NO) ไปเชื่อมต่อกับขั้ว Common (COM) วงจรไฟฟ้ากระแสสลับขนาด 230 VAC จึงถูกปิดวงจรและจ่ายพลังงานไปยังหลอดไฟ X1 ทำให้หลอดไฟสว่างขึ้นพร้อมทั้งบัซเซอร์ส่งเสียงแจ้งเตือน เมื่อไม่มีการเคลื่อนไหวในพื้นที่ตรวจจับ เซนเซอร์ PIR จะเปลี่ยนเอาต์พุตกลับเป็นระดับลอจิก LOW (0V) หลังครบระยะเวลาหน่วง (delay time) ที่กำหนด ทรานซิสเตอร์ Q1 จะหยุดการนำกระแส ทำให้ขดลวดรีเลย์ไม่มีสนามแม่เหล็ก หน้าสัมผัสรีเลย์จึงกลับสู่ตำแหน่งปกติ ส่งผลให้วงจรไฟฟ้ากระแสสลับถูกตัดออกและหลอดไฟดับลง ขณะเดียวกันไดโอด D1 (1N4007) ซึ่งต่อคร่อมขดลวดรีเลย์ทำหน้าที่ป้องกันแรงดันไฟฟ้าย้อนกลับ (Back Electromotive Force: Back EMF) ที่เกิดขึ้นในขณะรีเลย์หยุดทำงาน เพื่อป้องกันความเสียหายที่อาจเกิดกับทรานซิสเตอร์ ส่วน LM7805 ทำหน้าที่ควบคุมแรงดันไฟฟ้าให้คงที่ที่ 5 VDC สำหรับจ่ายให้กับโมดูล PIR และวงจรควบคุม ส่งผลให้ระบบสามารถทำงานได้อย่างมีเสถียรภาพและมีความน่าเชื่อถือในการตรวจจับการเคลื่อนไหว



รูปที่ 2.5 วงจรใช้งานเซนเซอร์ตรวจจับการเคลื่อนไหวแบบ PIR โดยใช้ Arduino UNO

รูปที่ 2.5 วงจรตรวจจับการเคลื่อนไหวด้วย PIR ทำงานโดยใช้ Arduino UNO ในการรับสัญญาณจากเซนเซอร์ และควบคุมการทำงานของบัซเซอร์ (buzzer) โดยโมดูล PIR HC-SR501 ได้รับแหล่งจ่ายไฟ 5 VDC จากบอร์ด Arduino ผ่านขา VCC และ GND ขณะที่ขา OUT ของเซนเซอร์เชื่อมต่อกับขาดิจิทัลของ Arduino เพื่อส่งสัญญาณตรวจจับการเคลื่อนไหวเข้าสู่ไมโครคอนโทรลเลอร์ ในสภาวะปกติ เมื่อไม่มีบุคคลหรือวัตถุเคลื่อนที่ผ่านพื้นที่ตรวจจับ เซนเซอร์ PIR จะส่งสัญญาณเอาต์พุตเป็นระดับลอจิก LOW (0V) ไปยัง Arduino ทำให้โปรแกรมกำหนดให้บัซเซอร์อยู่ในสถานะปิด (off) และไม่มีการส่งเสียงเตือน อย่างไรก็ตาม เมื่อมีบุคคลหรือวัตถุที่มีอุณหภูมิแตกต่างจาก

สภาพแวดล้อมเคลื่อนที่ผ่านบริเวณตรวจจับ เซนเซอร์จะตรวจจับการเปลี่ยนแปลงของรังสีอินฟราเรดและเปลี่ยนเอาต์พุตเป็นระดับลอจิก HIGH (3.3 V) จากนั้น Arduino จะอ่านค่าสัญญาณดังกล่าวผ่านขาดิจิทัลและประมวลผลตามโปรแกรมที่กำหนดไว้ เมื่อ Arduino ตรวจพบสัญญาณระดับ HIGH จะสั่งให้ขาดิจิทัลที่เชื่อมต่อกับบัซเซอร์จ่ายแรงดันไฟฟ้า ส่งผลให้บัซเซอร์ทำงานและส่งเสียงเตือน เพื่อแจ้งว่ามีการเคลื่อนไหวเกิดขึ้นภายในพื้นที่ตรวจจับ หลังจากบุคคลหรือวัตถุออกจากบริเวณตรวจจับ และเซนเซอร์ PIR ส่งสัญญาณกลับเป็นระดับลอจิก LOW ซึ่ง Arduino จะหยุดการจ่ายสัญญาณไปยังบัซเซอร์ ทำให้บัซเซอร์หยุดส่งเสียง และระบบกลับเข้าสู่สถานะพร้อมตรวจจับการเคลื่อนไหวครั้งถัดไป

2.3 เซนเซอร์ตรวจจับประตูและหน้าต่าง (Door and Window Sensors)

2.3.1 หลักการเบื้องต้นของเซนเซอร์ประตูและหน้าต่าง

หลักการทำงานของเซนเซอร์ประตูและหน้าต่างอาศัยการตรวจจับการเคลื่อนที่ของประตูหรือหน้าต่างผ่านสนามแม่เหล็กหรือหน้าสัมผัสทางไฟฟ้า (Kadum et al., 2018; Vega-Luna et al., 2019; Dempsey, 2022; Leslie, 2024) โดยแบ่งการทำงานออกเป็นลำดับดังนี้

1) สถานะปกติ (Normal State)

เมื่อประตูหรือหน้าต่างอยู่ในตำแหน่งปิด แม่เหล็กที่ติดตั้งบนบานประตูหรือบานหน้าต่างจะอยู่ใกล้กับเซนเซอร์ ทำให้เซนเซอร์ตรวจพบสนามแม่เหล็กและส่งสัญญาณแสดงว่าประตูปิด (door closed) หรือหน้าต่างปิด (window closed) สถานะดังกล่าวจะถูกส่งไปยังระบบควบคุมและบันทึกไว้ในฐานข้อมูลของระบบรักษาความปลอดภัย

2) การเปิดประตูหรือหน้าต่าง

เมื่อประตูหรือหน้าต่างถูกเปิด ระยะห่างระหว่างแม่เหล็กกับเซนเซอร์เพิ่มขึ้นจนเกินค่าที่กำหนด สนามแม่เหล็กที่เซนเซอร์ตรวจจับได้จะหายไป ส่งผลให้เอาต์พุตของเซนเซอร์เปลี่ยนสถานะทันที และส่งสัญญาณแจ้งเตือนไปยังไมโครคอนโทรลเลอร์หรือแผงควบคุม

3) การประมวลผลของระบบ

หลังจากได้รับสัญญาณ ระบบจะดำเนินการตามโปรแกรมที่กำหนด เช่น บันทึกวันและเวลาที่เกิดเหตุการณ์ แสดงสถานะบนหน้าจอ ส่งข้อมูลเข้าสู่ฐานข้อมูล และส่งข้อมูลผ่านเครือข่าย Wi-Fi ไปยัง cloud server แจ้งเตือนผ่าน SMS แจ้งเตือนผ่าน WhatsApp หรือแอปพลิเคชันบนสมาร์ตโฟน หรือสั่งงานไซเรนหรืออุปกรณ์แจ้งเตือนอื่น ๆ หากเปิดค้างเกินเวลาที่กำหนด (Vega-Luna et al., 2019; Dempsey, 2022)

2.3.2 ชนิดของเซนเซอร์ประตูและหน้าต่าง

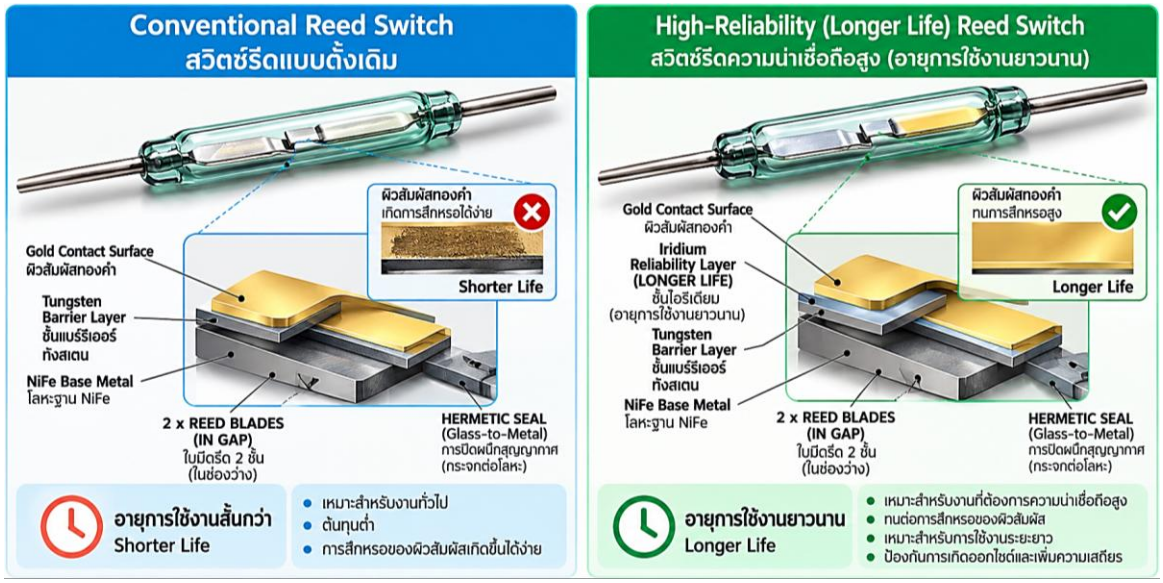
เซนเซอร์ประตูและหน้าต่างที่นิยมใช้มี 2 ประเภทหลัก ได้แก่

1) สวิตช์แม่เหล็ก (Reed Switch Sensor)

Reed switch เป็นสวิตช์แม่เหล็กแบบหน้าสัมผัส ประกอบด้วย หลอดแก้วสุญญากาศ แผ่นโลหะเฟอร์โรแมกเนติก 2 แผ่น และแม่เหล็กถาวร โดยเมื่อแม่เหล็กเข้าใกล้ แผ่นโลหะจะสัมผัส

กัน ทำให้วงจรปิด (closed circuit) และเมื่อแม่เหล็กออกห่าง วงจรจะเปิด (open circuit) สวิตช์ชนิดนี้มักนำมาใช้เป็นเซนเซอร์ตรวจจับการเปิด–ปิดประตูและหน้าต่าง (door and window sensor) รวมถึงการตรวจจับตำแหน่งของวัตถุและการตรวจวัดระดับของเหลวในภาชนะ โครงสร้างของสวิตช์แม่เหล็ก ประกอบด้วยแผ่นหน้าสัมผัสโลหะแม่เหล็ก (ferromagnetic contacts) จำนวน 2 แผ่น ซึ่งทำจากวัสดุที่สามารถถูกเหนี่ยวนำให้เกิดสนามแม่เหล็กได้ เช่น โลหะผสมนิกเกิล–เหล็ก หน้าสัมผัสทั้งสองถูกบรรจุอยู่ภายในหลอดแก้วปิดผนึก (glass capsule) ที่เติมก๊าซเฉื่อย เช่น ไนโตรเจน หรือสูญญากาศ เพื่อป้องกันการเกิดออกซิเดชันและลดการสึกหรอของหน้าสัมผัส ส่งผลให้อุปกรณ์มีอายุการใช้งานยาวนานและมีความเสถียรในการทำงาน

โดยทั่วไปค่าความเข้มของสนามแม่เหล็กที่ทำให้สวิตช์แม่เหล็ก เปลี่ยนสถานะจะเรียกว่า ค่าการทำงาน (operate point) ซึ่งมักระบุเป็นหน่วย Ampere-Turns (AT) หรือแอมแปร์-รอบ โดยมีค่าประมาณ 8–80 AT ขึ้นอยู่กับชนิดและขนาดของอุปกรณ์ ส่วนค่าที่ทำให้สวิตช์กลับสู่สถานะเดิมเรียกว่า Release Point ซึ่งมักมีค่าต่ำกว่าค่าการทำงานประมาณ 20–60 เปอร์เซ็น ความแตกต่างระหว่างค่าการทำงานและค่าการปลดปล่อยนี้เรียกว่า ฮิสเทอรีซิส (hysteresis) ซึ่งช่วยลดการสั่นของหน้าสัมผัส (contact chattering) เมื่อสนามแม่เหล็กมีการเปลี่ยนแปลงเล็กน้อย ค่าฮิสเทอรีซิสของสวิตช์แม่เหล็ก ขึ้นอยู่กับคุณสมบัติของวัสดุแม่เหล็กและโครงสร้างของหน้าสัมผัส หากใช้วัสดุที่มีค่าความเหนี่ยวนำตกค้าง (coercivity) ต่ำ และออกแบบให้ระยะห่างระหว่างหน้าสัมผัสมีขนาดเล็ก จะช่วยลดค่าฮิสเทอรีซิส ทำให้เซนเซอร์ตอบสนองต่อการเปลี่ยนแปลงของสนามแม่เหล็กได้รวดเร็วและมีความแม่นยำมากขึ้น



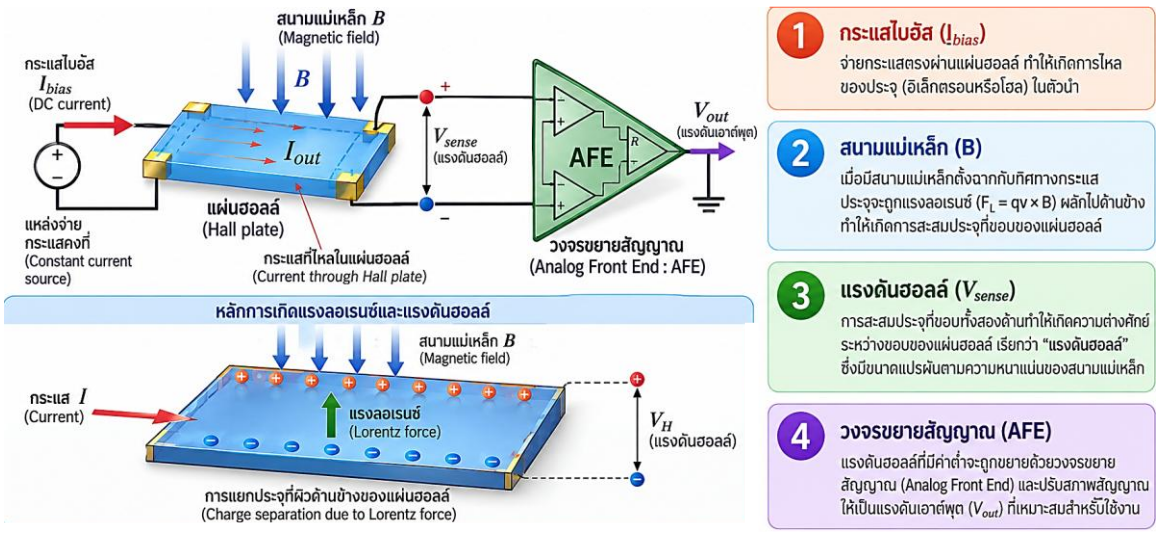
รูปที่ 2.6 โครงสร้างของสวิตช์แม่เหล็ก

จากรูปที่ 2.6 เป็นการเปรียบเทียบโลหะวิทยาของหน้าสัมผัส ข้อสังเกตคือมีการเพิ่มชั้นอิริเดียม (iridium layer) ในรุ่นที่มีความน่าเชื่อถือสูง เพื่อเพิ่มความทนทานและความเสถียรของ

ค่าความต้านทานหน้าสัมผัส (contact resistance) ตลอดอายุการใช้งาน โดยภาพซ้ายโดยผิวสัมผัสทองคำ (gold contact surface) ช่วยในการนำไฟฟ้าที่ดีและป้องกันการออกซิเดชัน ถัดไปชั้นกั้นทังสเตน (tungsten barrier layer) ช่วยป้องกันการแพร่กระจายของโลหะระหว่างชั้น ส่วนโลหะฐานนิกเกิล-เหล็ก (NiFe base metal) เป็นโลหะผสมที่มีคุณสมบัติสารแม่เหล็กชั่วคราวและมีสัมประสิทธิ์การขยายตัวทางความร้อนใกล้เคียงกับแก้ว หน้าสัมผัสรีดสวิตช์ 2 ชิ้น (two reed blades) เป็นบริเวณช่องว่างสัมผัส (gap) (glass-to-metal) การซีลปิดผนึกแน่นกันอากาศเข้า (hermetic seal) เป็นการรอยต่อระหว่างแก้วกับโลหะ อายุการใช้งานสั้น ส่วนภาพขวาเป็นสวิตช์แม่เหล็กความน่าเชื่อถือสูง ชั้นอิริเดียม (iridium reliability layer) เพิ่มความน่าเชื่อถือช่วยให้อายุการใช้งานยาวนานขึ้น เนื่องจากทนทานต่อการสึกหรอและการอาร์กไฟฟ้าได้ดีเยี่ยม

2) เซ็นเซอร์ฮอลล์เอฟเฟกต์ (Hall Effect Sensor)

เซ็นเซอร์ฮอลล์เอฟเฟกต์เป็นอุปกรณ์อิเล็กทรอนิกส์ที่ตรวจจับสนามแม่เหล็กโดยอาศัยปรากฏการณ์ Hall effect กล่าวคือ เมื่อมีกระแสไฟฟ้าไหลผ่านสารกึ่งตัวนำและมีสนามแม่เหล็กตั้งฉากกับทิศทางกระแส จะเกิดแรงดันไฟฟ้า Hall voltage ซึ่งสามารถนำมาใช้ตรวจจับการมีหรือไม่มีของสนามแม่เหล็กได้ โดยคุณสมบัติ คือ ไม่มีชิ้นส่วนเคลื่อนที่ ไม่เกิด contact bounce ทนต่อแรงสั่นสะเทือน ใช้พลังงานต่ำมาก อายุการใช้งานยาวนาน ตอบสนองรวดเร็ว และรองรับการทำงานแบบ sleep mode (Dempsey, 2022; Crescentini et al., 2022) จากงานวิจัยของ Vega-Luna et al. (2019) เลือกใช้โมดูล TIDA-01066 ซึ่งประกอบด้วย Hall effect sensor แบบดิจิทัลจำนวน 2 ตัว ใช้พลังงานเฉลี่ยเพียง 0.57 μA ใช้แบตเตอรี่ CR2032 ที่มีอายุการใช้งานประมาณ 10 ปี และสามารถตรวจจับขั้วเหนือหรือขั้วใต้ของแม่เหล็กได้ (omni-polar Hall sensor)



รูปที่ 2.7 บล็อกไดอะแกรมการทำงานของฮอลล์เซ็นเซอร์

จากรูปที่ 2.7 ลักการทำงานของเซนเซอร์วัดกระแสไฟฟ้าด้วยปรากฏการณ์ฮอลล์ (Hall-effect current sensor) โดยมีคำอธิบายส่วนประกอบและขั้นตอนการทำงานดังนี้

➲ ตัวนำที่มีกระแสไหล (current carrying conductor) เป็นสายไฟหรือตัวนำที่มีกระแสไฟฟ้า (I) ที่เราต้องการวัดไหลผ่าน

➲ B (magnetic Field) เป็นสนามแม่เหล็กที่เกิดขึ้นรอบตัวนำตามกฎมือขวา เมื่อมีกระแส I ไหลผ่าน สัญลักษณ์ $\otimes$ หมายถึง ทิศทางของสนามแม่เหล็กพุ่งตั้งฉากทะลุเข้าไปในแผ่นฮอลล์

➲ แผ่นฮอลล์ (Hall plate) เป็นสารกึ่งตัวนำที่ใช้ตรวจจับสนามแม่เหล็ก

➲ กระแสไบแอส (I_{bias} / I_{out}) กระแสไฟฟ้าคงที่ที่ป้อนให้ไหลผ่านแผ่นฮอลล์ในแนวระนาบ

➲ แรงดันฮอลล์ (V_{sense}/ V_H) เป็นความต่างศักย์ไฟฟ้าที่เกิดขึ้นในทิศตั้งฉากกับทิศทางการไหลของ I_{bias} และสนามแม่เหล็ก B

➲ AFE (Analog Front-End) คือวงจรขยายและประมวลผลสัญญาณแอนะล็อกแบบเครื่องมือวัด (Instrumentation Amplifier)

➲ แรงดันเอาต์พุต (V_{out}) สัญญาณแรงดันไฟฟ้าที่ผ่านการขยายและปรับสภาพแล้ว เพื่อส่งต่อไปยังไมโครคอนโทรลเลอร์หรือระบบประมวลผล

โดยมีลำดับการทำงาน ดังนี้

2.1)การกำเนิดสนามแม่เหล็ก โดยเมื่อมีกระแสไฟฟ้า (I) ไหลผ่านตัวนำ จะสร้างสนามแม่เหล็ก (B) ขึ้นรอบตัวนำโดยมีขนาดแปรผันตรงกับปริมาณกระแสไฟฟ้า

2.2)การเหนี่ยวนำแรงดันฮอลล์ เมื่อสนามแม่เหล็ก (B) จะพุ่งตั้งฉากเข้าสู่แผ่นฮอลล์ (Hall plate) ที่มีกระแสไบแอส (I_{bias}) ไหลอยู่ ส่งผลให้เกิดแรงลอเรนซ์ (Lorentz force) เบี่ยงเบนประจุไฟฟ้าจนเกิดเป็นความต่างศักย์ขนาดเล็กขึ้น เรียกว่า V_{sense}

2.3)การปรับสภาพและขยายสัญญาณ ซึ่งเนื่องจาก V_{sense} มีขนาดเล็กมาก (ระดับ μV ถึง mV) จึงต้องส่งเข้าวงจร AFE เพื่อขยายสัญญาณและลดสัญญาณรบกวน (noise filtering)

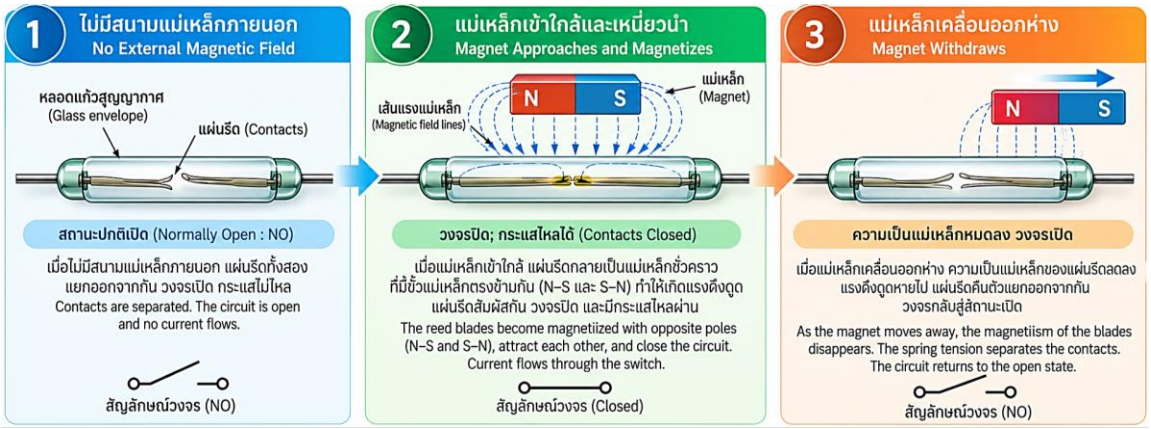
2.4)การส่งออกผลการวัด โดยวงจรส่งสัญญาณออกเป็น V_{out} ซึ่งเป็นแรงดันไฟฟ้าแบบเส้นตรง (linear output) ที่ได้สัดส่วนโดยตรงกับกระแสไฟฟ้า I ที่ต้องการวัด

2.3.3 หลักการทำงานของเซนเซอร์ประตูและหน้าต่าง

1) หลักการทำงานของสวิตช์แม่เหล็ก

สวิตช์แม่เหล็กถูกนำไปประยุกต์ใช้อย่างแพร่หลายในระบบตรวจจับการเปิด–ปิดประตูและหน้าต่าง โดยติดตั้งตัวสวิตช์ไว้ที่กรอบประตูหรือหน้าต่าง และติดตั้งแม่เหล็กไว้ที่บานประตูหรือบานหน้าต่าง เมื่อประตูอยู่ในตำแหน่งปิด แม่เหล็กจะอยู่ใกล้สวิตช์แม่เหล็ก ทำให้หน้าสัมผัสปิดและระบบรายงานสถานะว่า “ปิด” แต่เมื่อประตูหรือหน้าต่างถูกเปิด ระยะห่างระหว่างแม่เหล็กกับสวิตช์แม่เหล็ก จะเพิ่มขึ้นจนสนามแม่เหล็กลดต่ำกว่าค่าการทำงาน หน้าสัมผัสจะเปิดและส่งสัญญาณไปยังแผงควบคุมเพื่อแจ้งเตือนการเปิดประตูหรือหน้าต่าง นอกจากงานระบบรักษาความปลอดภัยแล้วสวิตช์แม่เหล็ก ยังถูกนำมาใช้ในระบบตรวจวัดระดับของเหลว (liquid level

monitoring) โดยติดตั้งสวิตช์แม่เหล็กภายในท่อหรือโพรบตรวจวัด และใช้ลูกลอยที่บรรจุแม่เหล็กถาวรลอยอยู่บนผิวของเหลว เมื่อระดับของเหลวเปลี่ยนแปลง ลูกลอยจะเคลื่อนที่ตามระดับของเหลว ทำให้แม่เหล็กเคลื่อนผ่านตำแหน่งของสวิตช์แม่เหล็ก และเปลี่ยนสถานะของหน้าสัมผัส ส่งผลให้วงจรไฟฟ้าส่งสัญญาณแสดงระดับของเหลวถึงค่าที่กำหนด โดยสามารถนำไปใช้ควบคุมการเติมน้ำ การป้องกันน้ำล้น และการตรวจสอบระดับของเหลวในถังเก็บได้อย่างมีประสิทธิภาพ



รูปที่ 2.8 หลักการทำงานของสวิตช์แม่เหล็ก

จากรูปที่ 2.8 กลไกการทำงานของสวิตช์แม่เหล็ก (reed switch operational mechanism) เมื่อมีการกระตุ้นด้วยสนามแม่เหล็กภายนอก โดยแบ่งออกเป็น 2 สถานะหลักเพื่อเปรียบเทียบให้เห็นกระบวนการทำงานทางวิศวกรรมไฟฟ้าอย่างชัดเจน ดังนี้ครับ

1.2.1) สถานะไม่ทำงาน (unactivated/normal state) เป็นสถานะปกติเมื่อไม่มีสนามแม่เหล็กภายนอกมากระทำ ทำให้เกิดสภาวะปกติเปิด (NO) โดย

1.2.1.1) หลอดแก้ว (glass capsule) หลอดแก้วสุญญากาศหรือบรรจุก๊าซเฉื่อยที่ทำหน้าที่ปกป้องหน้าสัมผัสภายในจากสิ่งปนเปื้อน

1.2.1.2) หน้าสัมผัสแผ่นเรียบ (reed blades) แผ่นโลหะผสมนิกเกิล-เหล็ก (NiFe) ที่มีคุณสมบัติสารแม่เหล็กชั่วคราว วางตัวเหลื่อมกันภายในหลอดแก้ว

1.2.1.3) หน้าสัมผัสแยก (contacts open) แผ่นรีดทั้งสองแยกออกจากกันด้วยแรงสปริงในตัว

1.2.1.4) ขยายมุมมองช่องว่าง (enlarged view of gap) แสดงให้เห็นระยะห่างระหว่างหน้าสัมผัส ทำให้กระแสไฟฟ้าไม่สามารถไหลผ่านได้

1.2.1.5) ไม่มีกระแสไหลในวงจร (no circuit flow) วงจรอยู่ในสถานะวงจรเปิด (open circuit)

1.2.2) สถานะทำงาน (activated/magnet approach) เป็นสถานะเมื่อมีแม่เหล็กเคลื่อนที่เข้าใกล้รีดสวิตช์ ทำให้เกิดสภาวะปกติปิด (NC)

1.2.2.1) แม่เหล็ก/ทิศทางการเคลื่อนที่ (magnet/motion vector) แม่เหล็กถาวรเคลื่อนที่เข้ามาใกล้ในระยะที่เส้นแรงแม่เหล็กส่งผลถึง

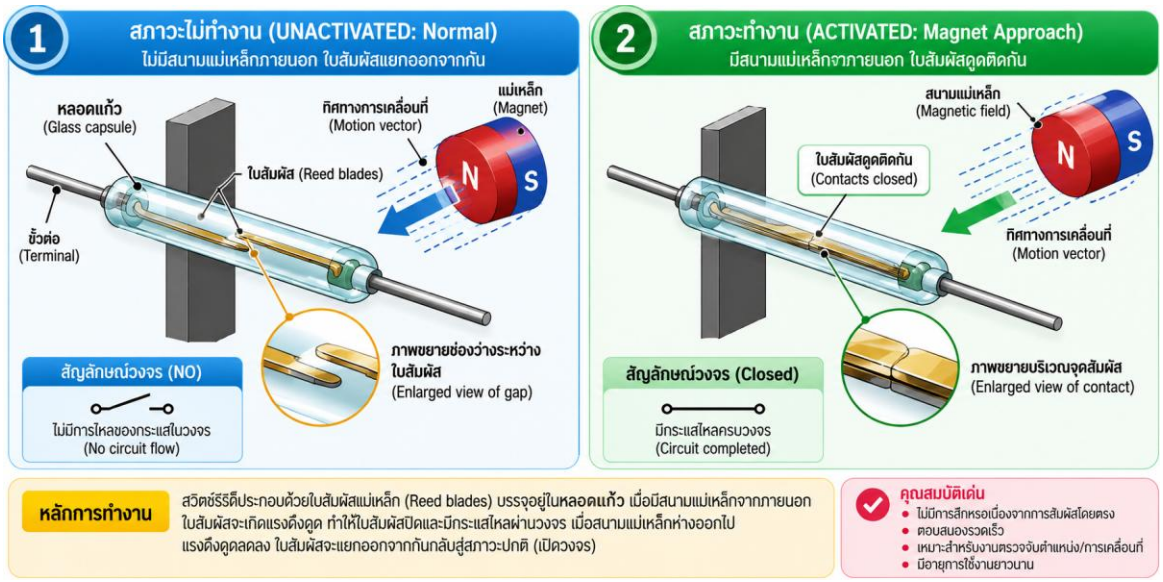
1.2.2.2) หน้าสัมผัสต่อ (contacts closed) เมื่อเส้นแรงแม่เหล็กวิ่งผ่านแผ่นรีด จะเกิดการเหนี่ยวนำให้ปลายแผ่นรีดทั้งสองฝั่งกลายเป็นขั่วแม่เหล็กที่ตรงกันข้ามกัน (N และ S) จึงเกิดแรงดึงดูดทางแม่เหล็ก

1.2.2.3) ขยายมุมมองจุดสัมผัส (enlarged view of contact) แรงดึงดูดแม่เหล็กที่เกิดขึ้นมีค่ามากกว่าแรงสปริงของแผ่นโลหะ ทำให้ปลายแผ่นรีดเคลื่อนที่เข้ามสัมผัสกันแนบสนิท

1.2.2.4) วงจรครบสมบูรณ์ (circuit completed) เมื่อหน้าสัมผัสแตะกัน กระแสไฟฟ้าจึงสามารถไหลผ่านสวิตช์ได้ วงจรเปลี่ยนเป็นสถานะ วงจรปิด (closed circuit)

1.2) ข้อดีของสวิตช์แม่เหล็ก

แม้ว่าสวิตช์แม่เหล็กจะมีข้อดีหลายประการ เช่น โครงสร้างเรียบง่าย ราคาประหยัด ใช้พลังงานต่ำ และมีการแยกวงจรไฟฟ้าออกจากสนามแม่เหล็กโดยสมบูรณ์ แต่เนื่องจากเป็นอุปกรณ์ที่มีหน้าสัมผัสเชิงกล จึงอาจเกิดการสึกหรอ การเด้งของหน้าสัมผัส (contact bounce) และมีข้อจำกัดด้านความเร็วในการสวิตช์เมื่อเทียบกับเซนเซอร์แบบสารกึ่งตัวนำ เช่น Hall effect Sensor อย่างไรก็ตาม สวิตช์แม่เหล็กยังคงเป็นอุปกรณ์ที่ได้รับความนิยมในงานตรวจจับสถานะที่ต้องการความเรียบง่าย ความน่าเชื่อถือ และต้นทุนต่ำ ข้อดี คือ ราคาถูก วงจรง่าย และใช้พลังงานต่ำ ส่วนข้อจำกัด คือมีหน้าสัมผัสเชิงกล ทำให้อายุการใช้งานจำกัด เกิดการเด้งของหน้าสัมผัส (contact bounce) ไวต่อแรงสั่นสะเทือน หลอดแก้วแตกได้ง่าย และต้องติดตั้งอย่างระมัดระวัง (Vega-Luna et al., 2019; Dempsey, 2022)

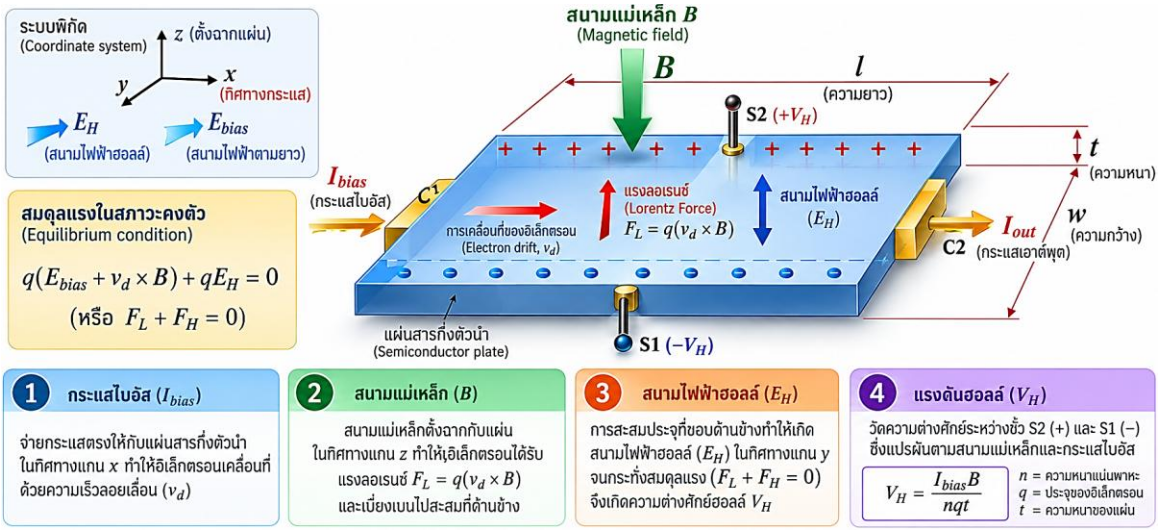


รูปที่ 2.9 กลไกการทำงานของสวิตช์แม่เหล็ก

2) หลักการทำงานของเซ็นเซอร์ฮอลล์เอฟเฟกต์

ปรากฏการณ์กัลวาโนแมกเนติก (galvanomagnetic effects) เป็นปรากฏการณ์ทางฟิสิกส์ที่เกิดขึ้นเมื่อกระแสไฟฟ้าไหลผ่านตัวนำหรือสารกึ่งตัวนำภายใต้สนามแม่เหล็กภายนอก

ส่งผลให้เกิดการเปลี่ยนแปลงของการกระจายตัวของพาหะนำไฟฟ้าและคุณสมบัติทางไฟฟ้าของวัสดุ ปรากฏการณ์ Hall effect เป็นหนึ่งในปรากฏการณ์กัลวาโนแมกเนติกที่สำคัญ และเป็นพื้นฐานของการพัฒนาเซนเซอร์ฮอลล์เอฟเฟกต์ ซึ่งใช้ตรวจวัดสนามแม่เหล็ก ตำแหน่ง ความเร็ว และการเคลื่อนที่ในระบบอัตโนมัติและระบบรักษาความปลอดภัย (Crescentini et al., 2022)



รูปที่ 2.10 หลักการแพร่กระจายสนามไฟฟ้าบนแผ่นฮอลล์ (ดัดแปลงจาก Crescentini et al., 2022)

จากรูปที่ 2.10 พิจารณาแผ่นสารกึ่งตัวนำชนิดเอ็นไทป์ (n-type semiconductor) รูปทรงสี่เหลี่ยมผืนผ้า มีความยาว (l) ความกว้าง (w) และความหนา (t) โดยมีกระแสไบอัส (I_{bias}) ไหลผ่านระหว่างขั้วสัมผัสของ C1 และ C2 ภายใต้สนามไฟฟ้าไบอัส (E_{bias}) ซึ่งทำให้พาหะนำไฟฟ้าอิเล็กตรอนเคลื่อนที่ไปตามแนวแกน x เมื่อมีสนามแม่เหล็กแนวแกน B กระทำในทิศตั้งฉากกับทิศทางการไหลของกระแสตามแนวแกน z พาหะนำไฟฟ้าจะได้รับแรงลอเรนซ์ (Lorentz force) ซึ่ง $F_L + F_H = 0$ จะสามารถคำนวณค่า F (Crescentini et al., 2022) ดังนี้

$$F = -qE_{bias} - q(v \times B) \qquad (2.1)$$

โดยที่ F คือ แรงลอเรนซ์ (N), q คือ 1.602×10^{-19} (C), E_{bias} คือ สนามไฟฟ้าไบอัส (V/m), v คือ ความเร็วของพาหะนำไฟฟ้า (m/s), และ B คือ ความหนาแน่นฟลักซ์แม่เหล็ก (T)

สมการเป็นแรงที่เกิดจากสนามไฟฟ้า ซึ่งทำให้อิเล็กตรอนเคลื่อนที่ไปตามแนวแกน (x) ส่วนพจน์ที่สองเป็นแรงแม่เหล็กที่เกิดจากผลคูณเชิงเวกเตอร์ระหว่างความเร็วของพาหะนำไฟฟ้ากับสนามแม่เหล็ก ส่งผลให้อิเล็กตรอน (E_H) เบี่ยงเบนไปตามแนวแกน (y) และเกิดการสะสมของประจุลบบริเวณขอบด้านหนึ่งของแผ่นสารกึ่งตัวนำ ในขณะที่อีกด้านหนึ่งเกิดการขาดอิเล็กตรอน จึงมีประจุบวกสะสม ส่งผลให้เกิดสนามไฟฟ้าตามแนวขวาง เรียกว่า สนามไฟฟ้าฮอลล์ (Hall electric field: F_H) แรงที่เกิดจากสนามไฟฟ้าฮอลล์สามารถเขียนได้เป็น

$$F_H = -qE_H \quad (2.2)$$

$$F_L = -q(v \times B) \quad (2.3)$$

เมื่อระบบเข้าสู่สภาวะคงตัว (steady state) แรงจากสนามไฟฟ้าฮอลล์จะมีค่าเท่ากับแรงแม่เหล็ก ทำให้พาหะนำไฟฟ้าไม่เคลื่อนที่ในแนวแกน (y) อีกต่อไป ดังนั้น สนามไฟฟ้าฮอลล์สามารถประมาณได้เป็น

$$E_H \approx \mu_n (E_{bias} \text{ x } B), \quad (2.4)$$

โดยที่ μn คือ ความคล่องตัวของอิเล็กตรอน (electron mobility)

สนามไฟฟ้ารวมภายในแผ่นสารกึ่งตัวนำจึงเป็นผลรวมของสนามไฟฟ้าไบอัสและสนามไฟฟ้าฮอลล์

$$E_{tot} = E_{bias} + E_H, \quad (2.5)$$

เนื่องจากสนามไฟฟ้ารวมไม่อยู่ในแนวเดียวกับเวกเตอร์ความหนาแน่นกระแสไฟฟ้า J จึงเกิดมุมเบี่ยงเบนระหว่างเวกเตอร์ทั้งสอง ซึ่งเรียกว่า มุมฮอลล์ (Hall angle) โดยมีความสัมพันธ์ดังนี้

$$\tan \theta_H = \mu_n B_z, \quad (2.6)$$

เมื่อ Bz คือองค์ประกอบของสนามแม่เหล็กในแนวแกน (z)

มุมฮอลล์เป็นพารามิเตอร์สำคัญที่ใช้บ่งชี้ความไวของ Hall effect เนื่องจากยิ่งค่าความคล่องตัวของพาหะนำไฟฟ้า (μ_n) สูง เซนเซอร์จะยิ่งตอบสนองต่อสนามแม่เหล็กได้ดี ทำให้แรงดันฮอลล์ที่เกิดขึ้นมีค่ามากขึ้น แรงดันฮอลล์ (V_H) ที่เกิดขึ้นระหว่างขั้ว S1 และ S2 สามารถเขียนได้เป็น

$$V_H = \int_{S1}^{S2} E_H \, dy \quad (2.7)$$

$$= \frac{\mu_n}{\sigma t} I_{bias} B_Z \quad (2.8)$$

$$= \frac{1}{nqt} I_{bias} B_Z, \quad (2.9)$$

โดยที่ โดยที่ V_H คือ แรงดันฮอลล์ (Hall voltage) มีหน่วยเป็นโวลต์ (V), I_{bias} คือ กระแสไบอัส (bias current) มีหน่วยเป็นแอมแปร์ (A), B_z คือ ความหนาแน่นฟลักซ์แม่เหล็กในทิศทางแกน z (magnetic flux density) มีหน่วยเป็นเทสลา (T), n คือ ความหนาแน่นของพาหะนำไฟฟ้า (carrier concentration) มีหน่วยเป็น m^{-3}, q คือ ประจุของอิเล็กตรอน (electron charge) มีค่า 1.602×10^{-19} คูลอมบ์ (C) และ t คือ ความหนาของแผ่นฮอลล์ (Hall plate thickness) มีหน่วยเป็นเมตร (m)

จากสมการจะเห็นว่าแรงดันฮอลล์แปรผันตรงกับกระแสไบอัสและความเข้มของสนามแม่เหล็ก แต่แปรผกผันกับความหนาของแผ่นสารกึ่งตัวนำและความหนาแน่นของพาหะนำไฟฟ้า ดังนั้น การเพิ่มความไวของ Hall sensor สามารถทำได้โดยใช้วัสดุที่มีความหนาแน่นของพาหะต่ำ และการออกแบบ Hall element ให้มีความบาง อย่างไรก็ตาม สมการข้างต้นเป็นสมการอุดมคติ ซึ่งยังไม่ได้พิจารณาปัจจัยต่าง ๆ เช่น การเคลื่อนที่เชิงความร้อนของพาหะนำไฟฟ้า (thermal motion) และการกระจายความเร็วของพาหะนำไฟฟ้า (velocity distribution) ดังนั้น ในทางปฏิบัติจึงใช้ ค่าความคล่องตัวฮอลล์ (Hall mobility)

$$V_H = \frac{r_H}{nqt} I_{bias} B_Z \tag{2.10}$$

$$= R_H \frac{I_{bias}}{t} B_Z \tag{2.11}$$

โดยที่ (r_H) คือ Hall factor ซึ่งมีค่าประมาณ 1 สำหรับสารกึ่งตัวนำส่วนใหญ่ เมื่อรวม Hall factor เข้าในสมการ จะได้แรงดันฮอลล์เป็น

$$R_H = \frac{r_H}{nq}, \tag{2.12}$$

R_H เมื่อ คือ สัมประสิทธิ์ฮอลล์ (Hall coefficient)

สมการเหล่านี้เป็นพื้นฐานที่ใช้อธิบายการทำงานของเซนเซอร์ Hall effect ในการตรวจวัดสนามแม่เหล็ก และเป็นพื้นฐานของการออกแบบ Hall effect sensor ที่ใช้ในระบบตรวจจับตำแหน่ง ความเร็ว การหมุน และระบบรักษาความปลอดภัย เช่น เซนเซอร์ตรวจจับการเปิด–ปิดประตูและหน้าต่าง (door and window sensors) ที่ใช้กันอย่างแพร่หลายในปัจจุบัน

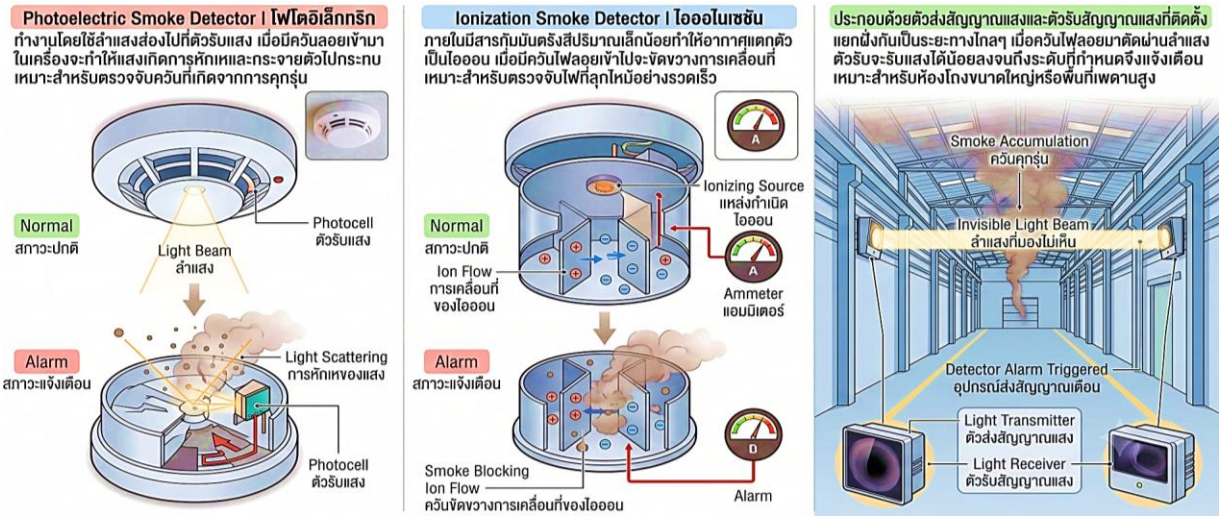
2.4 เซนเซอร์ตรวจจับควัน (Smoke Sensors)

2.4.1 ความหมายของเซนเซอร์ตรวจจับควัน

เซนเซอร์ตรวจจับควัน (smoke sensor หรือ smoke detector) เป็นอุปกรณ์ที่ใช้ตรวจจับอนุภาคควันที่เกิดขึ้นในระยะเริ่มต้นของการเกิดเพลิงไหม้ โดยอาศัยหลักการตรวจจับการเปลี่ยนแปลงของสภาพแวดล้อมภายในห้องตรวจจับ (detection chamber) เพื่อส่งสัญญาณแจ้งเตือนก่อนที่เปลวไฟจะลุกลามอย่างรุนแรง

2.4.2 ประเภทของเซนเซอร์ตรวจจับควัน

อุปกรณ์ตรวจจับควันแบ่งตามหลักการทำงานออกเป็น 3 ประเภทหลัก ซึ่งแต่ละประเภทถูกออกแบบมาให้มีระดับความไว (sensitivity) ต่อลักษณะของควันและพฤติกรรมการเผาไหม้ที่แตกต่างกัน (Hwang et al., 2024; Carletti et al., 2024; Elhanashi et al., 2025; Wang et al., 2025) ดังรูปที่ 2.11 และมีรายละเอียด ดังนี้



รูปที่ 2.11 ประเภทของเซนเซอร์ตรวจจับควัน

1) อุปกรณ์ตรวจจับควันแบบโฟโตอิเล็กทริก (Photoelectric Smoke Detector)

ทำงานโดยอาศัยการหักเหของแสง (light scattering) ภายในตัวตรวจจับจะมีแหล่งกำเนิดแสง (LED) ส่องผ่านช่องรับควันในแนวตรง ซึ่งในสภาวะปกติแสงจะไม่กระทบกับตัวรับแสง (photocell) แต่เมื่อมีอนุภาคของควันลอยเข้ามา แสงจะเกิดการหักเหและกระจายตัวไปตกกระทบที่ตัวรับแสง ส่งผลให้อุปกรณ์ส่งสัญญาณแจ้งเตือน โดยมีความไวสูงในการตรวจจับ “ไฟประเภทคุไหม้” (smoldering fire) หรือไฟที่ลุกไหม้ช้า ๆ แต่อมควันและมีอนุภาคควันขนาดใหญ่ เช่น ควันจากการไหม้ของวัสดุสิ่งทอ โฟม หรือที่นอน

2) อุปกรณ์ตรวจจับควันแบบไอออไนเซชัน (Ionization Smoke Detector)

ทำงานโดยอาศัยการเปลี่ยนแปลงกระแสไฟฟ้า (current change) ภายในห้องตรวจจับจะมีสารกัมมันตรังสีปริมาณต่ำ (มักใช้ americium-241) ทำหน้าที่แตกตัวอากาศให้กลายเป็นไอออนเพื่อนำกระแสไฟฟ้า เมื่ออนุภาคควันลอยเข้าไปในตัวตรวจจับ ควันจะเข้าไปเกาะและขัดขวางการเคลื่อนที่ของไอออน ทำให้กระแสไฟฟ้าในวงจรลดลงจนถึงจุดที่ระบบตั้งค่าไว้และเปิดสัญญาณเตือน มีความไวสูงในการตรวจจับ “ไฟที่ลุกไหม้อย่างรวดเร็ว” (fast-flaming fire) ซึ่งเป็นไฟที่มีเปลวแรงและมีอนุภาคควันขนาดเล็กมากจนมองไม่เห็นด้วยตาเปล่า เช่น ไฟที่เกิดจากเศษกระดาษ ไม้ หรือของเหลวไวไฟ

3) อุปกรณ์ตรวจจับควันแบบลำแสง (Beam Smoke Detector)

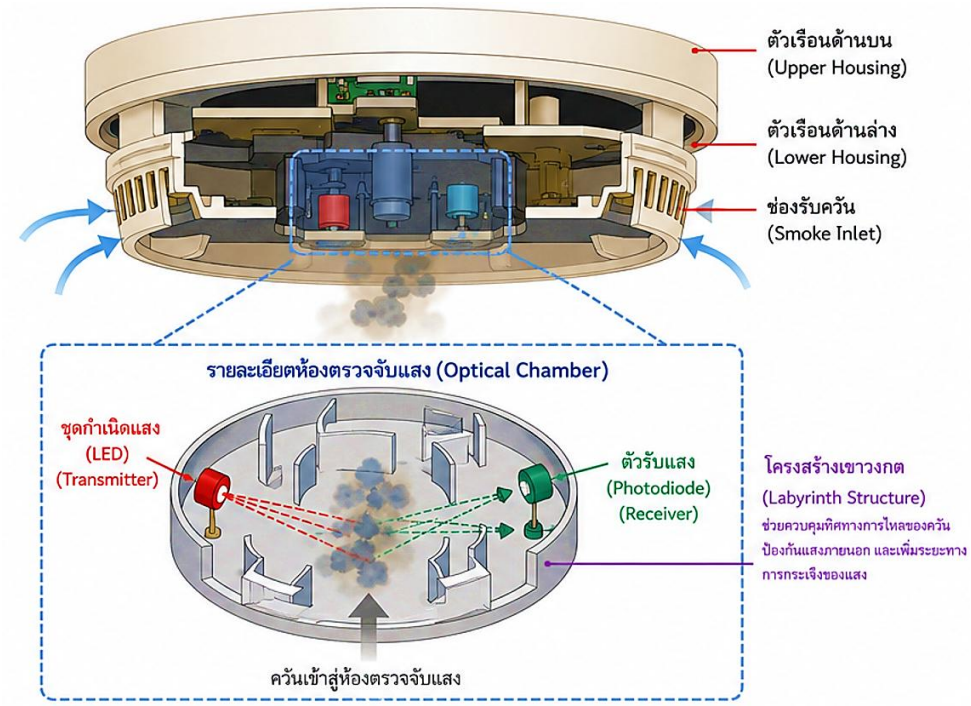
ทำงานโดยอาศัยหลักการลดทอนของแสง (light obscuration) ประกอบด้วยตัวส่ง (transmitter) และตัวรับ (receiver) ลำแสงอินฟราเรดติดตั้งแยกฝั่งหันหน้าเข้าหากันในระยะไกล ในสภาวะปกติตัวรับจะได้รับแสงเต็ม 100 เปอร์เซ็น แต่เมื่อมีกลุ่มควันลอยขึ้นมาบดบังหรือตัดผ่านลำแสง ปริมาณแสงที่ส่งถึงตัวรับจะลดน้อยลง (ถูกลดทอน) เมื่อความเข้มแสงลดลงถึงระดับที่กำหนด ระบบจะแจ้งเตือนทันที เหมาะสำหรับพื้นที่เปิดโล่งขนาดใหญ่ที่มี “เพดานสูง” (high ceiling) ซึ่งอุปกรณ์ตรวจจับควันแบบจุดทั่วไป (spot type) ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ เช่น โกดังเก็บสินค้า หอประชุม ศูนย์การค้า หรืออาคารผู้โดยสารในสนามบิน

2.4.3 โครงสร้างและหลักการทำงานของเซนเซอร์ตรวจจับควัน

1) เซนเซอร์ตรวจจับควันแบบโฟโตอิเล็กทริก

1.1) โครงสร้างของเซนเซอร์ตรวจจับควันแบบโฟโตอิเล็กทริก

โครงสร้างของเซนเซอร์ตรวจจับควันแบบโฟโตอิเล็กทริก ประกอบด้วยองค์ประกอบสำคัญหลายส่วนที่ทำงานร่วมกัน ได้แก่ ตัวเรือนด้านล่าง (lower housing) ตัวเรือนด้านบน (upper housing) ช่องรับควัน (smoke inlet) ห้องตรวจจับแสง (optical chamber) ชุดกำเนิดแสง (light transmitter หรือ LED) และตัวรับแสง (photodetector หรือ receiver) ซึ่งทั้งหมดถูกออกแบบให้สามารถรับควันเข้าสู่ห้องตรวจจับได้อย่างเหมาะสม พร้อมทั้งป้องกันแสงภายนอก ฝุ่น และแมลงไม่ให้รบกวนการตรวจจับ



รูปที่ 2.12 โครงสร้างของเซนเซอร์ตรวจจับควันแบบโฟโตอิเล็กทริก

1.2) หลักการทำงานของเซนเซอร์ตรวจจับควันแบบโฟโตอิเล็กทริก

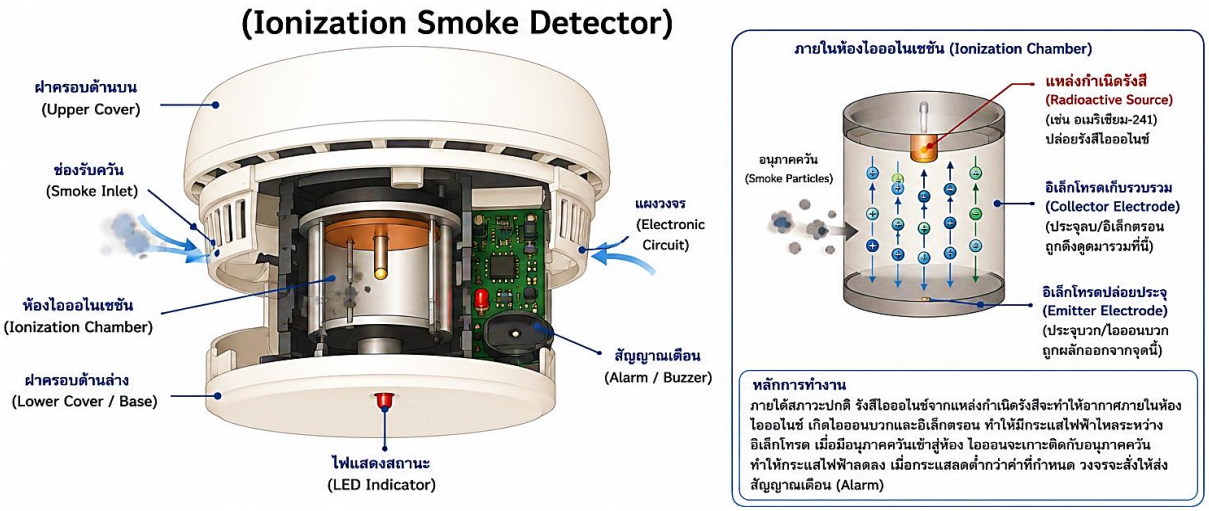
จากการศึกษาของ Hwang et al. (2024) พบว่าตัวเรือนของเซนเซอร์มีลักษณะเป็นทรงสามเหลี่ยม ภายในแบ่งออกเป็นตัวเรือนส่วนบนและส่วนล่าง โดยห้องตรวจจับแสง (optical chamber) ถูกติดตั้งอยู่บริเวณกึ่งกลางของตัวเรือน ภายในห้องตรวจจับประกอบด้วยโครงสร้างเขาวงกต (labyrinth structure) ซึ่งทำหน้าที่ควบคุมทิศทางการไหลของควัน ลดการรบกวนจากแสงภายนอก และช่วยเพิ่มประสิทธิภาพในการกระเจิงของแสงจากอนุภาคควันก่อนเข้าสู่ตัวรับแสง โดยห้องตรวจจับแสงประกอบด้วยแหล่งกำเนิดแสง LED จำนวนหนึ่งตัว และตัวรับแสง (receiver) จำนวนสองตัว ซึ่งติดตั้งในตำแหน่งที่ไม่รับแสงจาก LED โดยตรง ภายใต้สภาวะปกติแสงจาก LED จะไม่ตกกระทบตัวรับแสง เนื่องจากถูกกั้นด้วยโครงสร้างภายในห้องตรวจจับ แต่เมื่อมี

อนุภาคควันเข้าสู่ห้องตรวจจับ อนุภาคดังกล่าวจะทำให้เกิดการกระเจิงของแสง (light scattering) ส่งผลให้แสงบางส่วนตกกระทบตัวรับแสงและเปลี่ยนเป็นสัญญาณไฟฟ้า ก่อนส่งต่อไปยังวงจรประมวลผลเพื่อพิจารณาการแจ้งเตือนเหตุเพลิงไหม้ อีกองค์ประกอบสำคัญคือ ช่องรับควัน (smoke inlet) ซึ่งออกแบบเป็นช่องเปิดหลายตำแหน่งรอบตัวเรือน เพื่อให้ควันสามารถไหลเข้าสู่ห้องตรวจจับได้อย่างรวดเร็ว งานวิจัยของ Hwang et al. (2024) แสดงให้เห็นว่าขนาดของช่องรับควัน จำนวนช่องรับควัน และทิศทางการไหลของอากาศมีผลโดยตรงต่อเวลาการตอบสนอง (activation time) ของเซนเซอร์ หากการไหลของควันเข้าสู่ห้องตรวจจับถูกกีดขวางโดยโครงสร้างภายใน จะทำให้ควันเข้าสู่ห้องตรวจจับช้าลง ส่งผลให้การแจ้งเตือนล่าช้า ดังนั้นการออกแบบช่องรับควันและโครงสร้างเขาวงกตจึงเป็นปัจจัยสำคัญที่ส่งผลต่อความไวของเซนเซอร์ตรวจจับควัน

2) เซนเซอร์ตรวจจับควันแบบไอออไนเซชัน

2.1) โครงสร้างของเซนเซอร์ตรวจจับควันแบบไอออไนเซชัน

อุปกรณ์ตรวจจับควันแบบไอออไนเซชัน ประกอบด้วยส่วนประกอบหลัก ได้แก่ ฝาครอบด้านบน (upper cover) ช่องรับควัน (smoke inlet) ห้องไอออไนเซชัน (ionization chamber) แผงวงจรอิเล็กทรอนิกส์ (electronic circuit) สัญญาณเตือน (alarm/buzzer) และ ไฟแสดงสถานะ (LED indicator) ดังแสดงในรูปที่ 2.13 โดยโครงสร้างทั้งหมดถูกออกแบบให้สามารถรับควันจากภายนอกเข้าสู่ห้องไอออไนเซชันได้อย่างรวดเร็ว พร้อมทั้งป้องกันฝุ่นละออง แมลง และสิ่งแปลกปลอมที่อาจส่งผลกระทบต่อประสิทธิภาพของการตรวจจับ



รูปที่ 2.13 โครงสร้างของอุปกรณ์ตรวจจับควันแบบไอออไนเซชัน

2.2) หลักการทำงานของเซนเซอร์ตรวจจับควันแบบไอออไนเซชัน

หัวใจสำคัญของอุปกรณ์คือ ห้องไอออไนเซชัน (ionization chamber) ซึ่งภายในประกอบด้วย แหล่งกำเนิดรังสี (radioactive source) โดยทั่วไปใช้สารกัมมันตรังสี อเมริเซียม-241(americium-241, Am-241) ในปริมาณน้อยมาก ร่วมกับอิเล็กโทรดปล่อยประจุ (emitter electrode) และ อิเล็กโทรดเก็บรวบรวมประจุ (collector electrode) เมื่อแหล่งกำเนิดรังสีปล่อย

อนุภาคแอลฟา (alpha particles) ออกมา จะทำให้อากาศภายในห้องไอออไนเซชันเกิดการแตกตัวเป็นไอออนบวกและอิเล็กตรอนอิสระ ส่งผลให้เกิดกระแสไฟฟ้าขนาดเล็กไหลอย่างต่อเนื่องระหว่างอิเล็กโทรดทั้งสอง ภายใต้สภาวะปกติ กระแสไฟฟ้าภายในห้องไอออไนเซชันจะมีค่าค่อนข้างคงที่ อย่างไรก็ตาม เมื่อมีอนุภาคควันเข้าสู่ห้องตรวจจับ อนุภาคควันจะจับกับไอออนที่เกิดขึ้น ทำให้ความสามารถในการเคลื่อนที่ของไอออนลดลง ส่งผลให้กระแสไฟฟ้าระหว่างอิเล็กโทรดลดลงอย่างชัดเจน วงจรอิเล็กทรอนิกส์จะตรวจวัดการเปลี่ยนแปลงของกระแสดังกล่าว และเมื่อค่ากระแสต่ำกว่าค่าที่กำหนดไว้ (threshold) ระบบจะสั่งให้วงจรแจ้งเตือนทำงาน โดยส่งสัญญาณเสียงผ่าน alarm/buzzer พร้อมทั้งแสดงสถานะผ่าน LED indicator เพื่อแจ้งเตือนผู้ใช้งานถึงเหตุการณ์ที่อาจเกิดเพลิงไหม้ อุปกรณ์ตรวจจับควันแบบไอออไนเซชันมีความไวสูงต่ออนุภาคควันที่มีขนาดเล็ก ซึ่งมักเกิดจากการเผาไหม้ที่มีเปลวไฟ (flaming fire) เช่น การลุกไหม้ของกระดาษ น้ำมัน หรือของเหลวไวไฟ จึงสามารถตรวจพบเหตุเพลิงไหม้ได้อย่างรวดเร็วในระยะเริ่มต้น อย่างไรก็ตาม เซนเซอร์ชนิดนี้อาจเกิดการแจ้งเตือนผิดพลาดจากไอน้ำหรือฝุ่นละอองได้ง่ายกว่าระบบตรวจจับควันแบบโฟโตอิเล็กทริก ดังนั้นในอาคารสมัยใหม่จึงนิยมใช้เซนเซอร์หลายชนิดร่วมกัน (multi-sensor fire detection system) เพื่อเพิ่มความแม่นยำและลดการแจ้งเตือนผิดพลาด (Kuznetsov et al., 2022; Kumar, 2024)

3) เซนเซอร์ตรวจจับควันแบบลำแสง

3.1) โครงสร้างของเซนเซอร์ตรวจจับควันแบบลำแสง

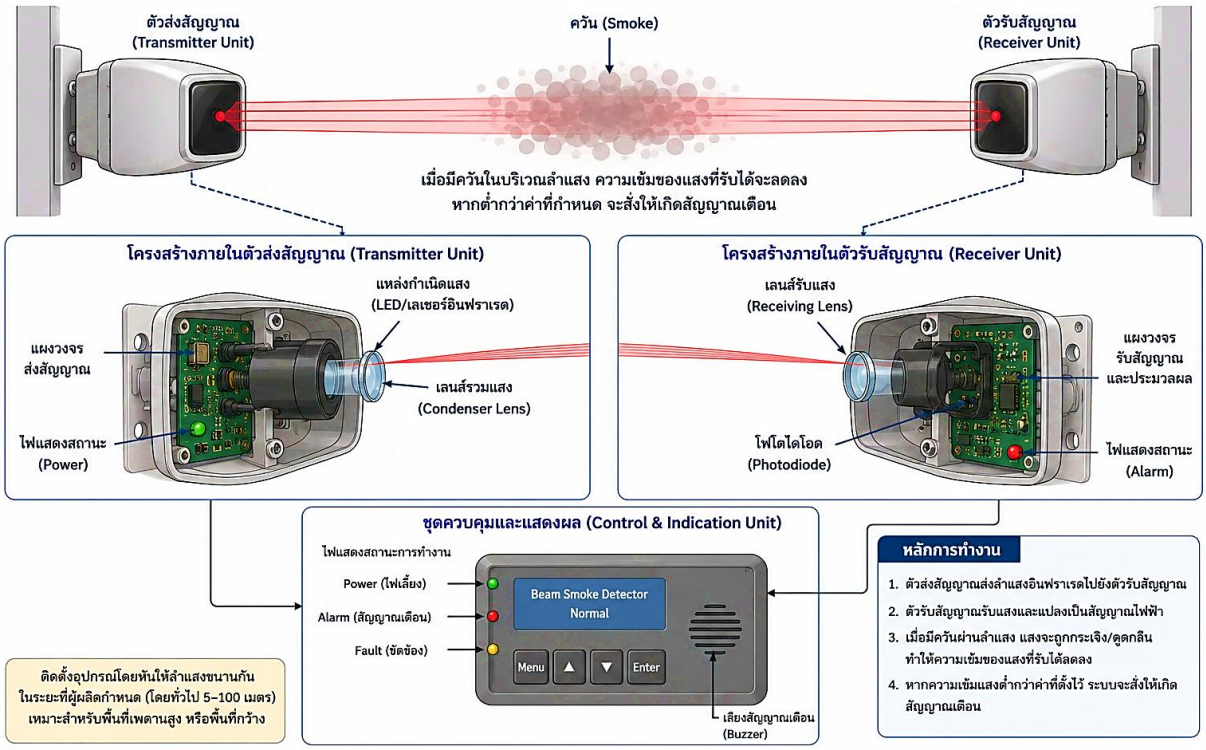
โครงสร้างและองค์ประกอบหลักของอุปกรณ์ตรวจจับควันแบบลำแสง (beam smoke detector) ซึ่งเป็นอุปกรณ์ตรวจจับควันที่อาศัยหลักการวัดการลดลงของความเข้มแสง (light obscuration principle) เมื่อมีควันผ่านแนวลำแสงระหว่างตัวส่งสัญญาณและตัวรับสัญญาณ เซนเซอร์ชนิดนี้เหมาะสำหรับการติดตั้งในพื้นที่ขนาดใหญ่หรือพื้นที่ที่มีเพดานสูง เช่น โกดังสินค้า โรงงานอุตสาหกรรม ศูนย์ประชุม อาคารผู้โดยสาร และโถงอาคาร เนื่องจากสามารถตรวจจับควันได้ในระยะไกล โดยทั่วไปมีระยะตรวจจับประมาณ 5–100 m ขึ้นอยู่กับรุ่นของอุปกรณ์และข้อกำหนดของผู้ผลิต (System Sensor Europe, 2011; Wang et al., 2025)

3.2) หลักการทำงานของเซนเซอร์ตรวจจับควันแบบลำแสง

จากรูปที่ 2.14 อุปกรณ์ประกอบด้วยตัวส่งสัญญาณ (transmitter unit) และ ตัวรับสัญญาณ (receiver unit) ติดตั้งหันหน้าเข้าหากันบนผนังหรือโครงสร้างของอาคาร ตัวส่งสัญญาณทำหน้าที่สร้างลำแสงอินฟราเรด (infrared beam) หรือแสงเลเซอร์กำลังต่ำผ่านเลนส์รวมแสง (condenser lens) ไปยังตัวรับสัญญาณอย่างต่อเนื่อง ภายในตัวส่งสัญญาณประกอบด้วยแหล่งกำเนิดแสง (LED หรือ infrared laser diode) วงจรควบคุมการส่งสัญญาณ และไฟแสดงสถานะการทำงาน (power indicator) เพื่อควบคุมความเข้มและความเสถียรของลำแสง ส่วน ตัวรับสัญญาณ (receiver unit) ประกอบด้วยเลนส์รับแสง (receiving lens) โฟโตไดโอด (photodiode) หรือโฟโตทรานซิสเตอร์ (phototransistor) สำหรับตรวจจับความเข้มของลำแสงที่ได้รับ รวมถึงวงจรขยายสัญญาณ (signal amplifier) และวงจรประมวลผล (signal processing circuit) ซึ่งทำหน้าที่เปรียบเทียบค่าความเข้มของแสงกับค่ามาตรฐานที่กำหนดไว้ หากพบว่าความเข้มของแสง

ลดลงเกินค่าร้อยละที่ตั้งไว้ ระบบจะส่งสัญญาณแจ้งเตือนไปยังแผงควบคุมระบบแจ้งเหตุเพลิงไหม้ (fire alarm control panel)

เมื่อเกิดเพลิงไหม้ อนุภาคควันที่ลอยอยู่ในอากาศจะเคลื่อนผ่านแนวลำแสง ทำให้เกิดการดูดกลืน (absorption) และการกระเจิงของแสง (scattering) ส่งผลให้ปริมาณแสงที่เดินทางถึงตัวรับลดลง วงจรประมวลผลจะตรวจวัดการเปลี่ยนแปลงดังกล่าวและคำนวณเปอร์เซ็นต์การบดบังลำแสง (beam obscuration) หากค่าการบดบังสูงกว่าค่าที่กำหนดไว้ ระบบจะสั่งงานวงจรแจ้งเตือนและส่งสัญญาณไปยังแผงควบคุมเพื่อแจ้งเหตุเพลิงไหม้ นอกจากนี้ อุปกรณ์ยังประกอบด้วยชุดควบคุมและแสดงผล (control and indication unit) ซึ่งใช้สำหรับแสดงสถานะการทำงานของระบบ เช่น power แสดงการจ่ายไฟ alarm แสดงสถานะการแจ้งเตือน และ fault แสดงความผิดปกติของอุปกรณ์ เช่น การสูญเสียแนวลำแสง การจัดแนวตัวส่งและตัวรับไม่ตรงกัน หรือความสกปรกของเลนส์ ทั้งนี้ชุดควบคุมยังสามารถใช้ในการปรับตั้งค่าความไว (sensitivity adjustment) การสอบเทียบ (calibration) และการทดสอบระบบ (system test) เพื่อให้การตรวจจับมีความแม่นยำและเป็นไปตามมาตรฐานการติดตั้งระบบแจ้งเหตุเพลิงไหม้



รูปที่ 2.14 โครงสร้างของอุปกรณ์ตรวจจับควันแบบลำแสง

2.4.4 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับควัน

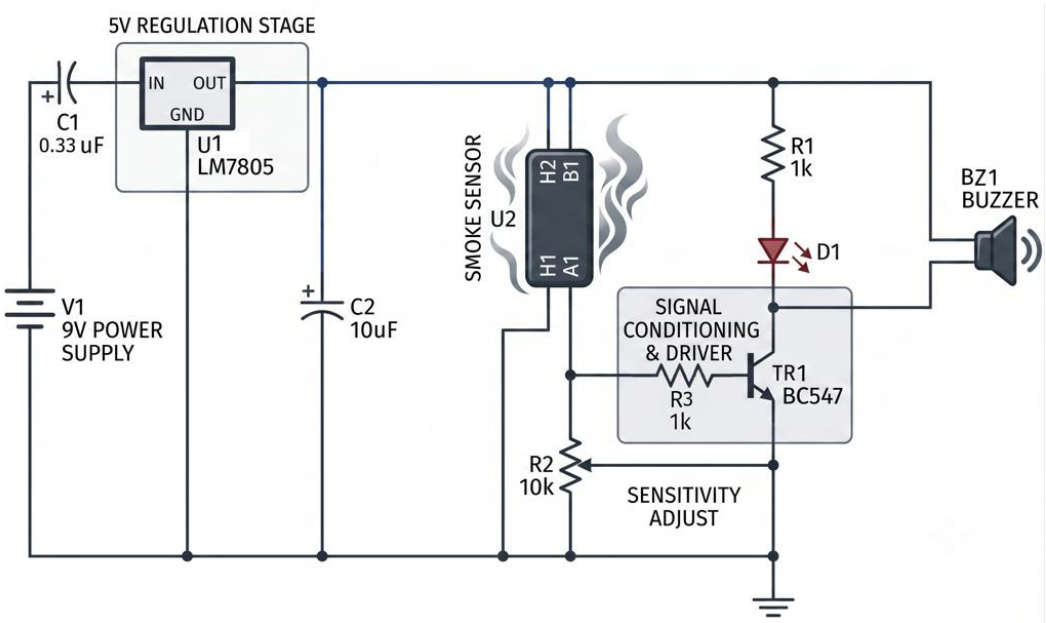
1) วงจรตรวจจับควันด้วยเซนเซอร์ MQ และแจ้งเตือน

วงจรนี้เป็นระบบตรวจจับควันที่ใช้ เซนเซอร์ตรวจจับก๊าซและควันตระกูล MQ เช่น MQ-2 หรือ MQ-6 ร่วมกับ ทรานซิสเตอร์ BC547 เพื่อขับอุปกรณ์แจ้งเตือน ได้แก่ หลอด LED

และบัซเซอร์ โดยมีวงจรควบคุมแรงดันให้คงที่ที่ 5 V ด้วยตัวควบคุมแรงดัน LM7805 แสดงดังรูปที่ 2.15 เมื่อจ่ายไฟจากแบตเตอรี่ 9 V (V1) แรงดันจะถูกส่งเข้าสู่ LM7805 (U1) เพื่อปรับลดแรงดันให้เหลือ 5 V ซึ่งเป็นแรงดันที่เหมาะสมสำหรับการทำงานของเซนเซอร์และวงจรอิเล็กทรอนิกส์ ภายในวงจรมีตัวเก็บประจุ C1 (0.33 μF) ที่ด้านอินพุตของ LM7805 ทำหน้าที่ลดสัญญาณรบกวนและเพิ่มเสถียรภาพของแรงดันไฟฟ้าขาเข้า ส่วน C2 (10 μF) ที่ด้านเอาต์พุตช่วยกรองแรงดันไฟฟ้าและลดการแกว่งของแรงดัน เพื่อให้วงจรได้รับแรงดันไฟฟ้าที่เรียบและคงที่

เซนเซอร์ตรวจจับควัน U2 ได้รับแรงดันไฟเลี้ยง 5 V จากเอาต์พุตของ LM7805 โดยองค์ประกอบตรวจจับภายในเซนเซอร์จะเปลี่ยนค่าความต้านทานเมื่อสัมผัสกับควันหรือก๊าซไวไฟ ส่งผลให้แรงดันที่ขาสัญญาณเปลี่ยนแปลงตามความเข้มข้นของก๊าซที่ตรวจพบ วงจรใช้ตัวต้านทานปรับค่าได้ R2 (10 kΩ) เป็นตัวปรับระดับแรงดันอ้างอิงหรือความไวในการตรวจจับ (sensitivity adjustment) ทำให้สามารถกำหนดระดับความเข้มข้นของควันที่ต้องการให้ระบบเริ่มแจ้งเตือนได้

เมื่อแรงดันจากเซนเซอร์สูงกว่าค่าที่กำหนด กระแสไฟฟ้าจะไหลผ่านตัวต้านทาน R3 (1kΩ) เข้าสู่ขา B ของทรานซิสเตอร์ BC547 (TR1) ซึ่งทำหน้าที่เป็นสวิตช์อิเล็กทรอนิกส์แบบ low-side switching เมื่อทรานซิสเตอร์เข้าสู่สภาวะอิ่มตัว จะทำให้เกิดการนำกระแสระหว่างขา C และขา E กระแสไฟฟ้าจึงไหลจากแหล่งจ่าย 5 V ผ่านตัวต้านทาน R1 (1 kΩ) และ LED (D1) ลงสู่ทรานซิสเตอร์ ทำให้ LED สว่างขึ้นเพื่อแสดงสถานะการตรวจพบควัน พร้อมกันนั้น กระแสไฟฟ้าจะไหลผ่าน BZ1 ลงสู่ทรานซิสเตอร์เช่นเดียวกัน ทำให้บัซเซอร์ส่งเสียงเตือนเพื่อแจ้งให้ผู้ใช้งานทราบถึงการเกิดควันหรือก๊าซที่มีความเข้มข้นเกินกว่าค่าที่กำหนด



รูปที่ 2.15 วงจรตรวจจับควันด้วยเซนเซอร์ MQ และแจ้งเตือนด้วย LED และบัซเซอร์

เมื่อความเข้มข้นของควันลดลงต่ำกว่าค่าที่ตั้งไว้ เซนเซอร์จะส่งแรงดันกลับสู่ระดับปกติ ทำให้กระแสที่ไหลเข้าสู่ขาเบสของทรานซิสเตอร์ลดลง ทรานซิสเตอร์จึงเข้าสู่สภาวะปิด (cut-off)

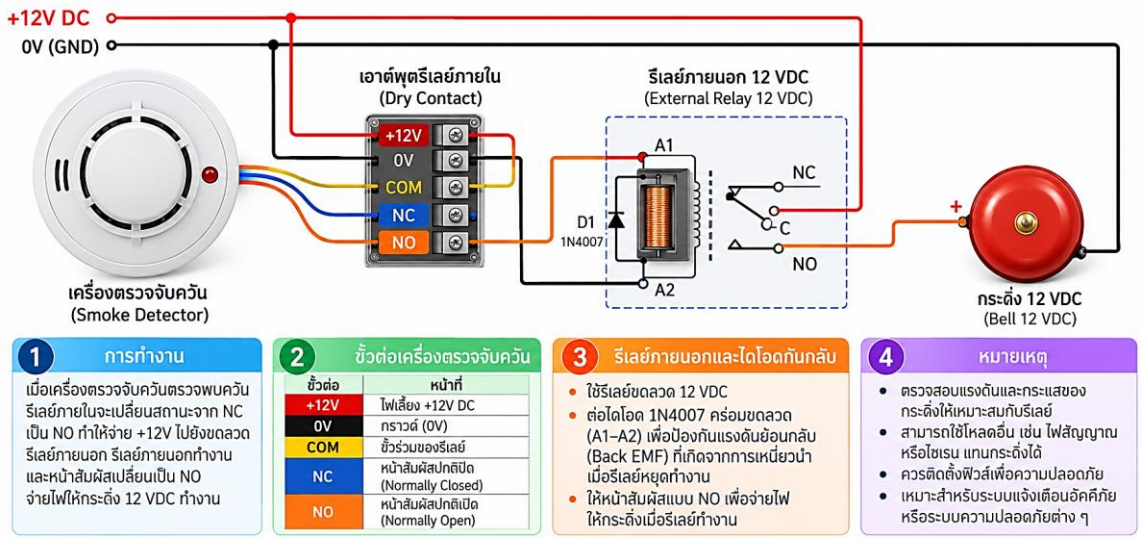
ส่งผลให้กระแสไฟฟ้าไม่สามารถไหลผ่าน LED และบัซเซอร์ได้ ทั้งสองอุปกรณ์จึงหยุดทำงาน และวงจรกลับเข้าสู่สถานะเฝ้าระวัง (standby) เพื่อรอการตรวจจับควันในรอบถัดไป

2) วงจรเครื่องตรวจจับควันแบบ 4 สายร่วมกับรีเลย์ภายนอก

การต่อวงจรเครื่องตรวจจับควันแบบ 4 สาย (4-wire smoke detector) ร่วมกับรีเลย์ภายนอก (external relay) เพื่อควบคุมการทำงานของกระดิ่งแจ้งเตือน (bell) ซึ่งเหมาะสำหรับกรณีที่กระดิ่งหรืออุปกรณ์แจ้งเตือนใช้กระแสไฟฟ้าสูงกว่าที่รีเลย์ภายในเครื่องตรวจจับควันสามารถรองรับได้ หลักการทำงาน รูปที่ 2.16

สถานะปกติ (normal condition) เมื่อระบบทำงานในสภาวะปกติ จะมีการจ่ายแรงดันไฟฟ้า 12 VDC ให้กับเครื่องตรวจจับควันผ่านขั้ว +12V และ 0V (GND) เพื่อเลี้ยงวงจรอิเล็กทรอนิกส์ภายในเครื่องตรวจจับควัน ขณะเดียวกัน หน้าสัมผัสรีเลย์ภายในเครื่องตรวจจับควันยังอยู่ในสถานะปกติ โดยหน้าสัมผัส COM ยังไม่เชื่อมต่อกับ NO ทำให้ไม่มีแรงดันไฟฟ้าถูกส่งไปยังขดลวดของรีเลย์ภายนอกดังนั้น รีเลย์ภายนอกจึงยังไม่ทำงาน หน้าสัมผัสของรีเลย์ภายนอกยังคงอยู่ในตำแหน่งปกติ ส่งผลให้กระดิ่งไม่ได้รับแรงดันไฟฟ้าและไม่ส่งเสียงเตือน เมื่อเครื่องตรวจจับควันตรวจพบควัน (alarm condition) เมื่อมีควันเข้าสู่ห้องตรวจจับ เซนเซอร์ภายในเครื่องตรวจจับควันจะตรวจพบอนุภาคของควันและส่งสัญญาณไปยังวงจรควบคุมภายใน จากนั้นวงจรจะสั่งให้รีเลย์ภายในเครื่องตรวจจับควันทำงาน ทำให้หน้าสัมผัส COM เชื่อมต่อกับ NO เมื่อหน้าสัมผัส COM–NO ปิดวงจร แรงดันไฟฟ้า +12 VDC ที่ต่ออยู่กับขั้ว COM จะถูกส่งผ่านไปยังขั้ว NO และเข้าสู่ขั้ว A1 ของขดลวดรีเลย์ภายนอก ขณะที่ขั้ว A2 ต่ออยู่กับ GND ทำให้เกิดกระแสไฟฟ้าไหลผ่านขดลวดของรีเลย์ภายนอก ส่งผลให้รีเลย์ภายนอกทำงาน (relay energized) เมื่อขดลวดของรีเลย์ภายนอกได้รับแรงดันไฟฟ้า หน้าสัมผัสเคลื่อนที่ (moving contact) จะเปลี่ยนตำแหน่งจาก NC ไปเชื่อมต่อกับ NO ในวงจรนี้ ขั้ว COM ของรีเลย์ภายนอกต่อกับแหล่งจ่าย +12 VDC ส่วนขั้ว NO ต่อเข้ากับขั้วบวกของกระดิ่ง ดังนั้น เมื่อรีเลย์ทำงาน หน้าสัมผัส COM–NO จะปิดวงจร ทำให้แรงดันไฟฟ้า 12 VDC ถูกส่งไปยังกระดิ่ง กระแสไฟฟ้าจะไหลจากแหล่งจ่าย ผ่านหน้าสัมผัสรีเลย์ภายนอก ผ่านกระดิ่ง และไหลกลับสู่ GND ทำให้กระดิ่งส่งเสียงเตือนเพื่อแจ้งเหตุเพลิงไหม้หรือการเกิดควัน เมื่อสภาพแวดล้อมกลับสู่ภาวะปกติ เครื่องตรวจจับควันจะยกเลิกสัญญาณเตือน รีเลย์ภายในและรีเลย์ภายนอกจะกลับสู่ตำแหน่งเดิม ส่งผลให้วงจรของกระดิ่งถูกตัดออกและกระดิ่งหยุดทำงาน

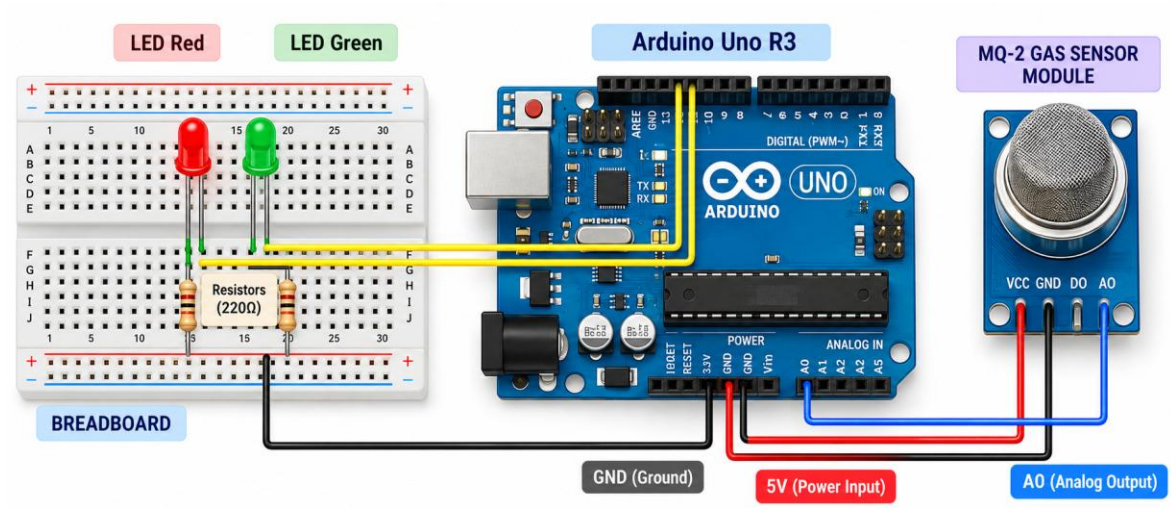
ไดโอด D1 (1N4007) ต่อคร่อมขดลวดของรีเลย์ภายนอก ทำหน้าที่เป็น flyback diode หรือ freewheeling diode เพื่อป้องกันแรงดันไฟฟ้าย้อนกลับ (Back Electromotive Force: Back EMF) ที่เกิดขึ้นเมื่อรีเลย์หยุดทำงาน เมื่อขดลวดของรีเลย์ถูกตัดกระแส จะเกิดแรงดันไฟฟ้าย้อนกลับซึ่งอาจมีค่าหลายสิบถึงหลายร้อยโวลต์ แรงดันดังกล่าวอาจทำให้หน้าสัมผัสของรีเลย์ภายในเครื่องตรวจจับควันหรืออุปกรณ์อิเล็กทรอนิกส์เสียหายได้ ไดโอด D1 จะทำหน้าที่ระบายพลังงานที่สะสมอยู่ในสนามแม่เหล็กของขดลวด จึงช่วยป้องกันแรงดันย้อนและเพิ่มอายุการใช้งานของระบบ



รูปที่ 2.16 การต่อวงจรใช้งานตัวตรวจจับควันแบบ 4 สาย

3) วงจรตรวจจับก๊าซด้วยเซนเซอร์ MQ-2 และแสดงสถานะด้วย LED โดยใช้ Arduino

วงจรในรูปเป็นระบบตรวจจับก๊าซโดยใช้ เซนเซอร์ตรวจจับก๊าซ MQ-2 ร่วมกับ Arduino Uno เพื่อวัดความเข้มข้นของก๊าซไวไฟและควันที่อยู่ในอากาศ พร้อมแสดงผลสถานะผ่านหลอดไฟ LED สีเขียว และ LED สีแดง โดย Arduino ทำหน้าที่เป็นหน่วยประมวลผลหลักของระบบ เริ่มต้นจากการจ่ายแรงดันไฟฟ้า 5 VDC ให้กับโมดูลเซนเซอร์ MQ-2 ผ่านขั้ว VCC และเชื่อมต่อขั้ว GND ร่วมกันเพื่อเป็นจุดอ้างอิงของวงจร ขณะที่ขา A0 ของเซนเซอร์เชื่อมต่อกับขาอินพุตแอนะล็อกของ Arduino เพื่อส่งค่าความเข้มข้นของก๊าซในรูปของสัญญาณแรงดันไฟฟ้าแบบแอนะล็อกเข้าสู่ไมโครคอนโทรลเลอร์



รูปที่ 2.17 วงจรตรวจจับก๊าซโดยใช้ เซนเซอร์ตรวจจับก๊าซ MQ-2 ร่วมกับ Arduino

ภายในเซนเซอร์ MQ-2 ประกอบด้วยวัสดุเซมิคอนดักเตอร์ชนิด ดีบุกออกไซด์ (Tin Dioxide: SnO_2) ซึ่งมีคุณสมบัติในการเปลี่ยนค่าความต้านทานไฟฟ้าตามความเข้มข้นของก๊าซ เมื่อมีก๊าซไวไฟหรือควัน เช่น ก๊าซปิโตรเลียมเหลว (LPG) มีเทน (CH_4) โพรเพน (C_3H_8) ไฮโดรเจน (H_2) หรือควันจากการเผาไหม้เข้าสัมผัสผิวเซนเซอร์ ความต้านทานของวัสดุ SnO_2 จะลดลง ส่งผลให้แรงดันไฟฟ้าที่เอาต์พุตแอนะล็อกเปลี่ยนแปลงตามระดับความเข้มข้นของก๊าซ จากนั้น Arduino จะอ่านค่าแรงดันดังกล่าวผ่านตัวแปลงสัญญาณแอนะล็อกเป็นดิจิทัล (ADC) ซึ่งมีความละเอียด 10 บิต และนำค่าที่ได้ไปเปรียบเทียบกับค่าขีดจำกัด (threshold) ที่กำหนดไว้ในโปรแกรม เมื่อค่าความเข้มข้นของก๊าซต่ำกว่าค่าขีดจำกัด Arduino จะสั่งให้ LED สีเขียว ติดสว่าง เพื่อแสดงว่าสภาพแวดล้อมอยู่ในสภาวะปกติและปลอดภัย ขณะที่ LED สีแดง จะดับ แต่เมื่อค่าความเข้มข้นของก๊าซสูงกว่าค่าขีดจำกัด Arduino จะสั่งให้ LED สีแดง ติดสว่างและ LED สีเขียว ดับ เพื่อแจ้งเตือนว่าตรวจพบก๊าซหรือควันที่มีความเข้มข้นสูง ซึ่งอาจก่อให้เกิดอันตรายและควรดำเนินการตรวจสอบหรือระบายอากาศทันที ทั้งนี้ หลอด LED ทั้งสองดวงต่ออนุกรมกับตัวต้านทาน 220 Ω เพื่อจำกัดกระแสไฟฟ้าที่ไหลผ่าน LED ไม่ให้เกินค่าที่กำหนด ช่วยป้องกันความเสียหายของหลอด LED และขาเอาต์พุตดิจิทัลของ Arduino

2.5 เซนเซอร์ตรวจจับก๊าซ (Gas Sensors)

2.5.1 ความหมายของเซนเซอร์ตรวจจับก๊าซ

เซนเซอร์ตรวจจับก๊าซ (gas sensor) เป็นอุปกรณ์ที่ใช้ตรวจวัดชนิดหรือความเข้มข้นของก๊าซในบรรยากาศ โดยอาศัยการเปลี่ยนแปลงสมบัติทางเคมี ทางไฟฟ้า ทางความร้อน หรือทางแสง แล้วแปลงเป็นสัญญาณไฟฟ้าสำหรับการประมวลผล เซนเซอร์ชนิดนี้มีบทบาทสำคัญในระบบความปลอดภัย ระบบตรวจจับอัคคีภัย ระบบควบคุมคุณภาพอากาศ ระบบอุตสาหกรรม ระบบการแพทย์ และระบบอาคารอัจฉริยะ ตลอดจนระบบ IoT (Yunusa et al., 2014; Nagpal et al., 2025)

2.5.2 ชนิดของเซนเซอร์ตรวจจับก๊าซ

โดยทั่วไปเซนเซอร์ตรวจจับก๊าซ สามารถแบ่งออกเป็น 6 ประเภทหลัก ดังนี้

1) เซนเซอร์ตรวจจับก๊าซแบบตัวเร่งปฏิกิริยา (Catalytic Gas Sensors)

Catalytic gas sensor เป็นเซนเซอร์ที่ใช้ตรวจจับก๊าซไวไฟ (combustible gas) เช่น methane (CH_4), propane (C_3H_8), butane (C_4H_{10}), และ hydrogen (H_2) หลักการทำงานอาศัยปฏิกิริยาออกซิเดชันของก๊าซบนผิวตัวเร่งปฏิกิริยา (catalyst) เช่น platinum หรือ palladium เมื่อก๊าซเผาไหม้บนผิวเซนเซอร์จะเกิดความร้อน ทำให้อุณหภูมิและค่าความต้านทานของตัวตรวจจับเปลี่ยนแปลง จากนั้นวงจร Wheatstone bridge จะวัดการเปลี่ยนแปลงดังกล่าวและแปลงเป็นสัญญาณไฟฟ้า โดยมีข้อดี คือ ตรวจจับก๊าซไวไฟได้ดี ความไวสูง ราคาค่อนข้างต่ำ ส่วนข้อจำกัด คือ ต้องใช้อุณหภูมิสูงในการทำงาน ใช้พลังงานมาก ตัวเร่งปฏิกิริยาเสื่อมสภาพได้เมื่อสัมผัสสารพิษบางชนิด เช่น ซิลิโคนหรือกำมะถัน (Yunusa et al., 2014)

2) เซนเซอร์ตรวจจับก๊าซแบบการนำความร้อน (Thermal Conductivity Gas Sensors)

เซนเซอร์ชนิดนี้ตรวจจับก๊าซโดยวัดการเปลี่ยนแปลงของการนำความร้อน (thermal conductivity) ระหว่างก๊าซตัวอย่างกับก๊าซอ้างอิง หากก๊าซมีค่าการนำความร้อนแตกต่างจากอากาศ เช่น hydrogen หรือ methane จะทำให้อัตราการสูญเสียความร้อนของตัวทำความร้อนเปลี่ยนไป และสามารถนำไปคำนวณความเข้มข้นของก๊าซได้ โดยมีข้อดี ตรวจจับก๊าซได้แม้ไม่มีออกซิเจน มีอายุการใช้งานยาว ส่วนข้อข้อจำกัด คือ ความไวต่ำกว่าชนิดอื่น ไม่เหมาะกับก๊าซที่มีค่าการนำความร้อนใกล้เคียงอากาศ (Yunusa et al., 2014)

3) เซนเซอร์ตรวจจับก๊าซแบบไฟฟ้าเคมี (Electrochemical Gas Sensors)

เซนเซอร์ไฟฟ้าเคมี เป็นเซนเซอร์ที่ได้รับความนิยมมากที่สุดในระบบตรวจจับก๊าซพิษโดยเฉพาะในระบบตรวจจับอัคคีภัย เนื่องจากสามารถตรวจวัดก๊าซที่เกิดขึ้นในระยะเริ่มต้นของการเผาไหม้ เช่น carbon monoxide (CO), hydrogen cyanide (HCN), nitrogen oxides (NO_X), และ sulfur dioxide (SO_2) (Yunusa et al., 2014; Wu et al., 2025)

เซนเซอร์ประกอบด้วย Working Electrode (WE), Counter Electrode (CE), Reference Electrode (RE), และ electrolyte เมื่อก๊าซแพร่ผ่านเยื่อพรุนเข้าสู่ WE จะเกิดปฏิกิริยาออกซิเดชันหรือรีดักชัน ส่งผลให้เกิดกระแสไฟฟ้าซึ่งมีค่าแปรผันตรงกับความเข้มข้นของก๊าซ ตามกฎของฟาราเดย์ (Faraday's law) มีข้อดี คือ ความไวสูงมาก ใช้พลังงานต่ำ ความจำเพาะต่อก๊าซสูง เหมาะกับระบบตรวจสอบไฟ ส่วนข้อจำกัด คือ อายุของอิเล็กโทรไลต์จำกัด ต้องสอบเทียบ (calibration) อาจเกิด cross-sensitivity กับก๊าซบางชนิด

4) เซนเซอร์ตรวจจับก๊าซแบบเชิงแสง (Optical Gas Sensors)

เซนเซอร์เชิงแสง ตรวจจับก๊าซจากการดูดกลืนหรือการเปลี่ยนแปลงของแสง เช่น Infrared (IR), Ultraviolet (UV), laser absorption, และ fiber optic sensor ก๊าซแต่ละชนิดจะดูดกลืนพลังงานของแสงที่ความยาวคลื่นเฉพาะ ทำให้สามารถวิเคราะห์ชนิดและปริมาณก๊าซได้อย่างแม่นยำ มีข้อดี คือ ไม่สัมผัสก๊าซโดยตรง อายุการใช้งานยาว และความแม่นยำสูง ส่วนข้อจำกัด คือ ราคาสูง วงจรมีความซับซ้อน (Yunusa et al., 2014)

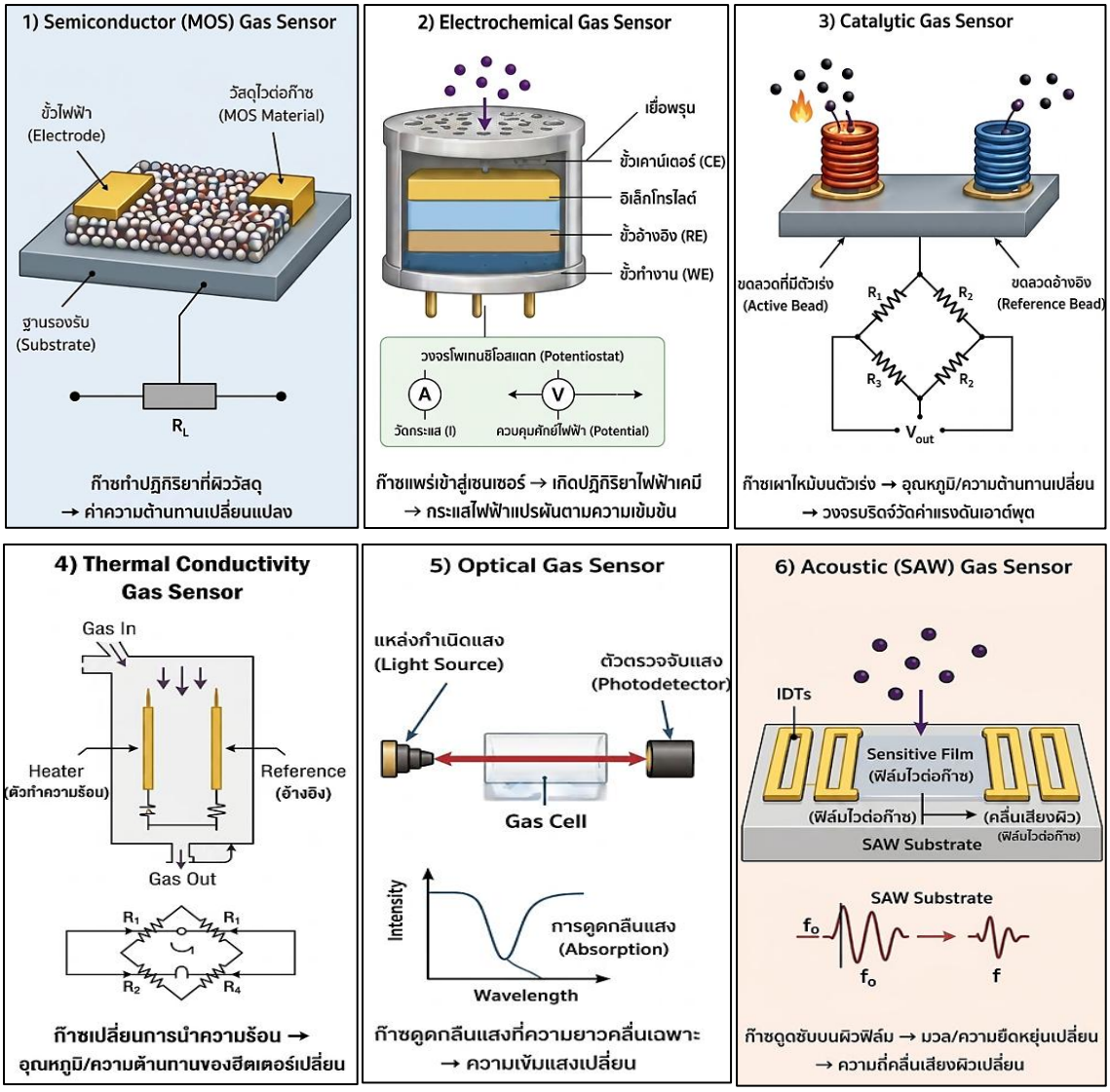
5) เซนเซอร์ตรวจจับก๊าซแบบคลื่นเสียง (Acoustic Gas Sensors)

เซนเซอร์ตรวจจับก๊าซแบบคลื่นเสียงใช้หลักการเปลี่ยนแปลงของคลื่นเสียง หรือคลื่นผิว (Surface Acoustic Wave: SAW) เมื่อโมเลกุลของก๊าซดูดซับบนผิววัสดุไวต่อก๊าซ จะทำให้มวลและความเร็วของคลื่นเปลี่ยนแปลง ส่งผลให้ความถี่ของคลื่นเปลี่ยนไป สามารถนำไปวิเคราะห์ชนิดของก๊าซได้อย่างแม่นยำ ข้อดี คือ ความไวสูงมาก ตรวจจับระดับส่วนในพันล้านส่วน (parts per billion; ppb) ได้ ส่วนข้อจำกัด มีราคาแพง ต้องการวงจรอิเล็กทรอนิกส์ความละเอียดสูง (Yunusa et al., 2014)

6) เซนเซอร์ตรวจจับก๊าซแบบสารกึ่งตัวนำออกไซด์โลหะ (Metal Oxide Semiconductor: MOS)

ปัจจุบันซนเซอร์ก๊าซแบบ MOS เป็นเซนเซอร์ที่ได้รับความนิยมอย่างแพร่หลาย เนื่องจากมีต้นทุนต่ำ ผลิตง่าย และสามารถประยุกต์ใช้งานร่วมกับเทคโนโลยีนาโน วัสดุไวต่อก๊าซที่ใช้ในเซนเซอร์ MOS ส่วนใหญ่ประกอบด้วยสารกึ่งตัวนำประเภทโลหะออกไซด์ เช่น ดีบุกไดออกไซด์

(SnO_2) สังกะสีออกไซด์ (ZnO) ทังสเตนไตรออกไซด์ (WO_3) และ ไทเทเนียมไดออกไซด์ (TiO_2) ซึ่งสามารถเกิดการเปลี่ยนแปลงค่าความต้านทานไฟฟ้าเมื่อโมเลกุลของก๊าซทำปฏิกิริยากับออกซิเจนที่ดูดซับอยู่บนผิววัสดุ จึงสามารถนำมาใช้ตรวจวัดชนิดและความเข้มข้นของก๊าซได้อย่างมีประสิทธิภาพ (Nagpal et al., 2025; Yunusa et al., 2014) เมื่อก๊าซทำปฏิกิริยากับออกซิเจนที่ดูดซับบนผิวเซนเซอร์ จะทำให้จำนวนอิเล็กตรอนและค่าความต้านทานไฟฟ้าเปลี่ยนแปลง ซึ่งสามารถนำไปคำนวณความเข้มข้นของก๊าซได้ ปัจจุบันมีการพัฒนาโดยใช้วัสดุนาโน เช่น graphene, Carbon Nanotubes (CNTs), Metal-Organic Frameworks (MOFs) และตัวเร่งปฏิกิริยาโลหะมีค่า แพลทินัม (Pt) พัลลาเดียม (Pd) และทองคำ (Au) เพื่อเพิ่มความไว ความจำเพาะ ลดอุณหภูมิการทำงาน และลดการใช้พลังงาน ข้อดี ได้แก่ ราคาถูก อายุการใช้งานยาว ผลิตได้ง่าย เหมาะสำหรับ IoT และ smart sensors ส่วนข้อจำกัด ได้แก่ ต้องใช้ความร้อนในการทำงาน มีผลกระทบจากอุณหภูมิและความชื้น อาจเกิด cross-sensitivity (Yunusa et al., 2014; Wu et al., 2025)



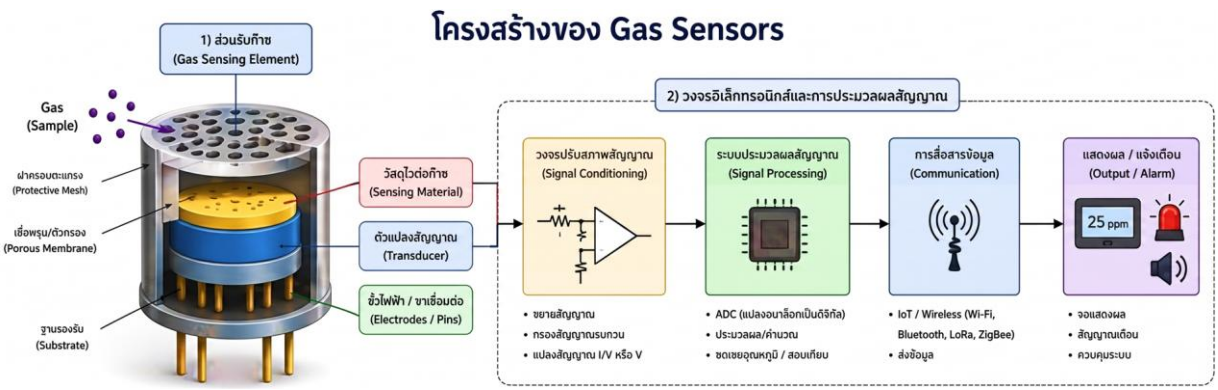
รูปที่ 2.18 เซนเซอร์ตรวจจับก๊าซชนิดต่าง ๆ

ตารางที่ 2.1 การเปรียบเทียบชนิดของเซนเซอร์ตรวจจับก๊าซ (Yunusa et al., 2014; Nagpal et al., 2025; Wu et al., 2025)

ชนิดเซนเซอร์	หลักการตรวจจับ	ก๊าซที่เหมาะสม	ข้อดี	ข้อจำกัด
Catalytic	ความร้อนจากเผาไหม้	CH_4, LPG, H_2	ราคาถูก, ความไวสูง	ใช้พลังงานสูง
Thermal Conductivity	การนำความร้อน	H_2, He	อายุยาว	ความไวต่ำ
Electrochemical	ปฏิกิริยารีดอกซ์	CO, H_2S, HCN, NO_2	ความจำเพาะสูง	ต้องสอบเทียบ
Optical	การดูดกลืนแสง	CO_2, CH_4	แม่นยำสูง	ราคาแพง
SAW	การเปลี่ยนความถี่คลื่น	VOCs	ความไวสูงมาก	วงจรซับซ้อน
MOS	ความต้านทานของสารกึ่งตัวนำ	VOCs, CO, NH_3, H_2	ราคาถูก ผลิตง่าย	ต้องให้ความร้อน

2.5.3 โครงสร้างของเซนเซอร์ตรวจจับก๊าซ

เซนเซอร์ตรวจจับก๊าซ มีโครงสร้างที่แตกต่างกันไปตามหลักการตรวจจับและเทคโนโลยีที่ใช้ เซนเซอร์ตรวจจับก๊าซทุกชนิดประกอบด้วยองค์ประกอบพื้นฐาน ได้แก่ ส่วนรับก๊าซ (gas sensing element) วัสดุไวต่อก๊าซ (sensing material) ชุดแปลงสัญญาณ (transducer) วงจรปรับสภาพสัญญาณ (signal conditioning circuit) และวงจรประมวลผลสัญญาณ (signal processing unit) ซึ่งทำงานร่วมกันเพื่อแปลงการเปลี่ยนแปลงทางเคมีหรือทางกายภาพของก๊าซให้เป็นสัญญาณไฟฟ้าและนำไปประมวลผล (Yunusa et al., 2014; Nagpal et al., 2025; Wu et al., 2025) จากการศึกษาของ Yunusa et al. (2014) โครงสร้างของเซนเซอร์ตรวจจับก๊าซแบ่งออกเป็น 3 ส่วน ได้แก่ (1) ส่วนตรวจจับ (sensing layer) ซึ่งเป็นบริเวณที่ก๊าซเป้าหมายทำปฏิกิริยากับวัสดุไวต่อก๊าซ (2) ตัวแปลงสัญญาณ (transducer) ทำหน้าที่เปลี่ยนแปลงทางเคมีให้เป็นสัญญาณไฟฟ้า เช่น ความต้านทาน กระแสไฟฟ้า แรงดันไฟฟ้า หรือความถี่ และ (3) วงจรอิเล็กทรอนิกส์ (electronic interface) สำหรับขยาย กรอง และประมวลผลก่อนส่งไปยังระบบแสดงผลหรือระบบควบคุม



รูปที่ 2.19 โครงสร้างของเซนเซอร์ตรวจจับก๊าซ

1) ส่วนรับก๊าซและวัสดุไวต่อก๊าซ (Gas Sensing Element)

ส่วนรับก๊าซเป็นองค์ประกอบสำคัญที่สุดของเซนเซอร์ โดยทำหน้าที่สัมผัสกับก๊าซเป้าหมายโดยตรง วัสดุไวต่อก๊าซจะเกิดการเปลี่ยนแปลงสมบัติทางไฟฟ้าหรือทางเคมีเมื่อเกิดการดูดซับ (adsorption) หรือการทำปฏิกิริยากับโมเลกุลของก๊าซ ซึ่งวัสดุที่นิยมใช้ ได้แก่ โลหะออกไซด์เซมิคอนดักเตอร์ แบบ MOS เช่น SnO_2, ZnO, WO_3 และ TiO_2 รวมถึงวัสดุนาโน เช่น กราฟีน (graphene) คาร์บอนนาโนทิวบ์ (CNTs) และ Metal–Organic Frameworks (MOFs) ซึ่งช่วยเพิ่มพื้นที่ผิว เพิ่มจำนวนตำแหน่งออกฤทธิ์ และปรับปรุงความไวและความจำเพาะของเซนเซอร์ (Nagpal et al., 2025) ส่วน Nagpal et al. (2025) รายงานว่า เซนเซอร์ตรวจจับก๊าซสมัยใหม่มีการพัฒนาโครงสร้างระดับนาโน เช่น core–shell structure, heterojunction, MOF coating และการเติมโลหะมีค่า ได้แก่ แพลทินัม (Pt) พัลลาเดียม (Pd) และทองคำ (Au) เพื่อเพิ่มประสิทธิภาพในการดูดซับก๊าซ ลดขีดจำกัดการตรวจจับ (Limit of Detection: LOD) เพิ่มความไว และเพิ่มความจำเพาะต่อก๊าซเป้าหมาย (Nagpal et al., 2025)

2) ตัวแปลงสัญญาณ (Transducer)

ตัวแปลงสัญญาณทำหน้าที่เปลี่ยนการเปลี่ยนแปลงที่เกิดขึ้นบนวัสดุไวต่อก๊าซให้เป็นสัญญาณไฟฟ้าที่สามารถวัดได้ โดยรูปแบบของสัญญาณขึ้นอยู่กับชนิดของเซนเซอร์ เช่น การเปลี่ยนแปลงค่าความต้านทานไฟฟ้า (resistive sensor) การเปลี่ยนแปลงกระแสไฟฟ้า (amperometric sensor) การเปลี่ยนแปลงแรงดันไฟฟ้า (potentiometric sensor) การเปลี่ยนแปลงความถี่ (acoustic sensor) และการเปลี่ยนแปลงความเข้มของแสง (optical sensor) ซึ่งแต่ละชนิดจะเลือกใช้ตัวแปลงสัญญาณที่เหมาะสมกับหลักการตรวจจับ (Yunusa et al., 2014)

3) โครงสร้างของเซนเซอร์ไฟฟ้าเคมี (Electrochemical Gas Sensor)

เซนเซอร์ไฟฟ้าเคมีเป็นเซนเซอร์ที่ได้รับความนิยมสูงสำหรับการตรวจจับก๊าซพิษและก๊าซที่เกิดจากเพลิงไหม้ เช่น คาร์บอนมอนอกไซด์ (CO) ไฮโดรเจนไซยาไนด์ (HCN) ซัลเฟอร์ไดออกไซด์ (SO_2) และไนโตรเจนออกไซด์ (NO_X) เนื่องจากมีความไวสูง ใช้พลังงานต่ำ และสามารถตรวจวัดก๊าซในระดับส่วนในล้านส่วน (ppm) ได้อย่างแม่นยำ (Wu et al., 2025)

โครงสร้างของเซนเซอร์ชนิดนี้ประกอบด้วย ตัวเรือนเซนเซอร์ (sensor housing) เยื่อพรุนควบคุมการแพร่ของก๊าซ (porous membrane) ขั้วทำงาน (WE) ขั้วอ้างอิง (RE) ขั้วเคาน์เตอร์ (CE) อิเล็กโทรไลต์ (electrolyte) และวงจรโพเทนชิโอสแตต (potentiostatic circuit) ซึ่งทำงานร่วมกันเพื่อแปลงปฏิกิริยาไฟฟ้าเคมีให้เป็นกระแสไฟฟ้าที่สัมพันธ์กับความเข้มข้นของก๊าซ (Wu et al., 2025) เมื่อก๊าซเป้าหมายแพร่ผ่านเยื่อพรุนเข้าสู่เซนเซอร์ จะเกิดปฏิกิริยาออกซิเดชันหรือรีดักชันที่ขั้วทำงาน ทำให้อิเล็กตรอนเคลื่อนที่ผ่านวงจรภายนอก ขณะที่ไอออนเคลื่อนที่ผ่านอิเล็กโทรไลต์ กระแสไฟฟ้าที่เกิดขึ้นมีค่าเป็นสัดส่วนโดยตรงกับความเข้มข้นของก๊าซตามกฎของฟาราเดย์ (Faraday's law) จากนั้นวงจรโพเทนชิโอสแตตจะขยาย กรอง และแปลงกระแสไฟฟ้าให้เป็นแรงดันสำหรับการประมวลผลต่อไป (Wu et al., 2025)

4) วงจรปรับสภาพสัญญาณ (Signal Conditioning Circuit)

สัญญาณที่ได้จากเซนเซอร์มักมีขนาดเล็กมาก โดยเฉพาะเซนเซอร์ไฟฟ้าเคมีซึ่งให้กระแสในระดับไมโครแอมแปร์ (μA) ดังนั้นจึงจำเป็นต้องมีวงจรขยายสัญญาณ (amplifier) วงจร

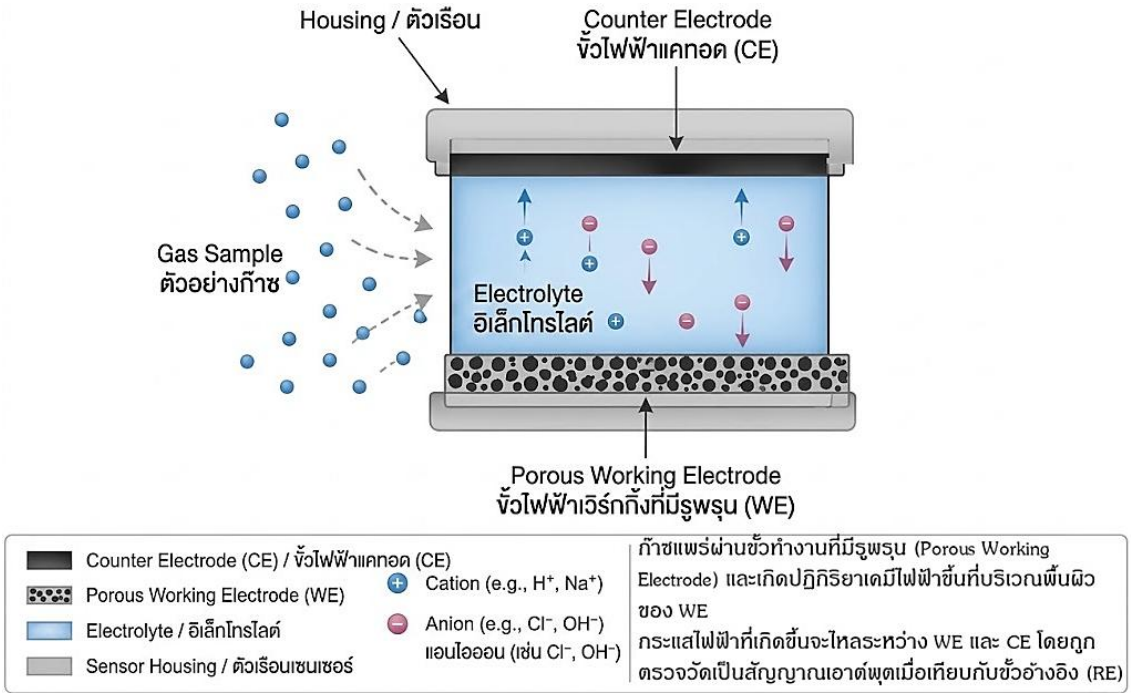
กรองสัญญาณ (filter) และวงจรแปลงกระแสเป็นแรงดัน (current-to-voltage converter) ก่อนส่งเข้าสู่ไมโครคอนโทรลเลอร์หรือระบบประมวลผล เพื่อเพิ่มความแม่นยำ ลดสัญญาณรบกวน และทำให้การวัดมีความเสถียร (Wu et al., 2025)

5) ระบบประมวลผลและการสื่อสารข้อมูล (Signal Processing and Communication)

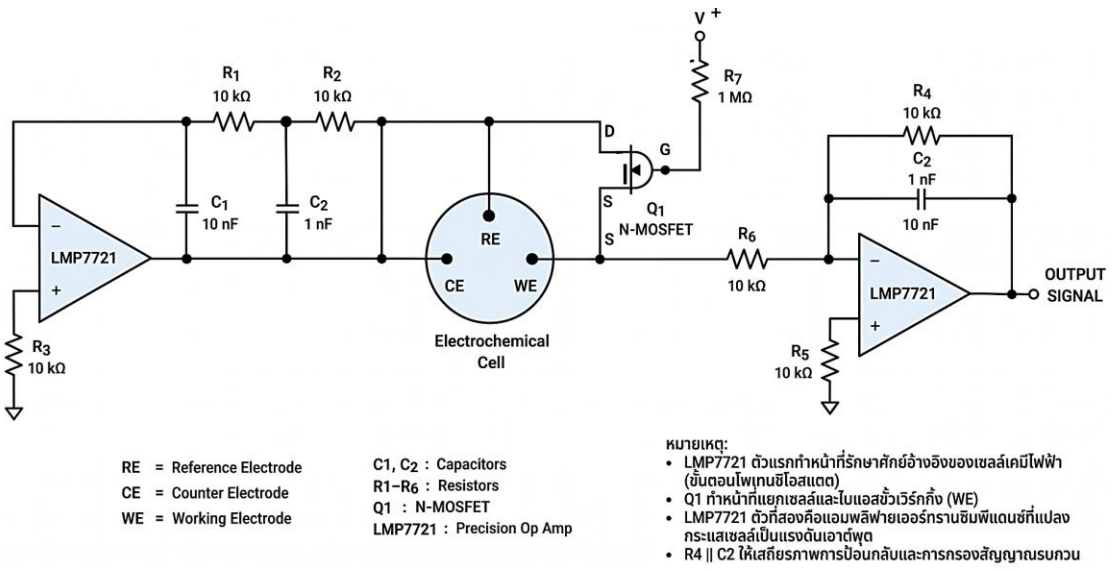
เซนเซอร์ตรวจจับก๊าซสมัยใหม่มักเชื่อมต่อกับไมโครคอนโทรลเลอร์หรือระบบฝังตัว (embedded system) เพื่อประมวลผลข้อมูลแบบเรียลไทม์ พร้อมทั้งใช้เทคนิคการชดเชยอุณหภูมิ การสอบเทียบอัตโนมัติ และอัลกอริทึมปัญญาประดิษฐ์ (AI) หรือการเรียนรู้ของเครื่อง (ML) เพื่อเพิ่มความแม่นยำ ลดการแจ้งเตือนผิดพลาด และรองรับการเชื่อมต่อกับ IoT ผ่านเทคโนโลยีไร้สาย เช่น Wi-Fi, Bluetooth, Zigbee และ LoRaWAN สำหรับการเฝ้าระวังคุณภาพอากาศและความปลอดภัยจากระยะไกล (Nagpal et al., 2025; Wu et al., 2025)

โดยสรุปโครงสร้างของเซนเซอร์ตรวจจับก๊าซประกอบด้วยส่วนรับก๊าซ วัสดุไวต่อก๊าซ ตัวแปลงสัญญาณ วงจรปรับสภาพสัญญาณ และระบบประมวลผล ซึ่งทำงานร่วมกันเพื่อเปลี่ยนการเปลี่ยนแปลงทางเคมีของก๊าซให้เป็นข้อมูลทางไฟฟ้าที่สามารถนำไปใช้ในระบบตรวจจับก๊าซ ระบบรักษาความปลอดภัยอัจฉริยะ ระบบตรวจจับอัคคีภัย และระบบ IoT ได้อย่างมีประสิทธิภาพ การพัฒนาวัสดุนาโน โครงสร้างเฮเทอโรจังก์ชัน และการประยุกต์ใช้ปัญญาประดิษฐ์ทำให้เซนเซอร์ตรวจจับก๊าซในปัจจุบันมีความไวสูง ตอบสนองรวดเร็ว และมีความจำเพาะต่อก๊าซเป้าหมายมากขึ้น (Nagpal et al., 2025; Wu et al., 2025; Yunusa et al., 2014)

โครงสร้างและวงจรอ่านสัญญาณของเซนเซอร์ก๊าซแบบไฟฟ้าเคมี (electrochemical gas sensor) ซึ่งแบ่งออกเป็น 2 ส่วน ดังรูปที่ 2.20 รายละเอียดดังนี้



(ก) โครงสร้างของเซนเซอร์ก๊าซแบบไฟฟ้าเคมี



(ข) วงจรประมวลผลสัญญาณ

รูปที่ 2.20 โครงสร้างและวงจรอ่านสัญญาณของเซนเซอร์ก๊าซแบบไฟฟ้าเคมี

1) โครงสร้างของเซนเซอร์ก๊าซแบบไฟฟ้าเคมี (Electrochemical Gas Sensor)

รูปที่ 2.20 (ก) แสดงองค์ประกอบภายในของเซนเซอร์ก๊าซแบบไฟฟ้าเคมี ซึ่งประกอบด้วย ตัวเรือนเซนเซอร์ ทำหน้าที่ป้องกันอุปกรณ์ภายในและควบคุมการแพร่ของก๊าซเข้าสู่เซนเซอร์ เมื่อก๊าซตัวอย่าง (gas sample) แพร่ผ่าน ขั้วทำงานชนิดพรุน (porous working electrode: WE) โมเลกุลของก๊าซจะสัมผัสกับตัวเร่งปฏิกิริยาบนผิวขั้วไฟฟ้าและเกิดปฏิกิริยาออกซิเดชันหรือรีดักชัน ส่งผลให้เกิดการแลกเปลี่ยนอิเล็กตรอนภายในเซนเซอร์บรรจุ อิเล็กโทรไลต์ (electrolyte) ซึ่งเป็นตัวกลางให้ไอออนเคลื่อนที่ระหว่างขั้วไฟฟ้า ในภาพแสดงตัวอย่างของ แคตไอออน (cation) เช่น H^+ หรือ Na^+ และ แอนไอออน (anion) เช่น Cl^- หรือ OH^- ที่เคลื่อนที่ภายในอิเล็กโทรไลต์เพื่อรักษาสมดุลของประจุไฟฟ้าระหว่างปฏิกิริยา เซนเซอร์ชนิดนี้ใช้ระบบ สามขั้วไฟฟ้า (three-electrode system) ได้แก่

1.1) ขั้วทำงาน (Working Electrode: WE) เป็นบริเวณที่เกิดปฏิกิริยาไฟฟ้าเคมีกับก๊าซเป้าหมาย และเป็นขั้วที่สร้างกระแสไฟฟ้าตามความเข้มข้นของก๊าซ

1.2) ขั้วอ้างอิง (Reference Electrode: RE) ทำหน้าที่รักษาศักย์ไฟฟ้าของขั้วทำงานให้คงที่ โดยแทบไม่มีกระแสไฟฟ้าไหลผ่าน จึงใช้เป็นจุดอ้างอิงในการควบคุมศักย์ไฟฟ้า

1.3) ขั้วเคาน์เตอร์ (Counter Electrode: CE) ทำหน้าที่เกิดปฏิกิริยาตรงข้ามกับขั้วทำงาน เพื่อให้วงจรไฟฟ้าเคมีสมบูรณ์และรักษาสมดุลของประจุ

เมื่อความเข้มข้นของก๊าซเพิ่มขึ้น อัตราการเกิดปฏิกิริยาไฟฟ้าเคมีที่ขั้วทำงานจะเพิ่มขึ้น ส่งผลให้กระแสไฟฟ้าที่ไหลระหว่าง WE และ CE เพิ่มขึ้นตาม โดยมี RE เป็นขั้วอ้างอิงสำหรับควบคุมศักย์ไฟฟ้า กระแสไฟฟ้าที่เกิดขึ้นจึงมีค่าเป็นสัดส่วนโดยตรงกับความเข้มข้นของก๊าซ

2) วงจรประมวลผลสัญญาณของเซนเซอร์ (Signal Conditioning Circuit)

จากรูปที่ 2.20 (ข) แสดงวงจรอิเล็กทรอนิกส์ที่ใช้รับและประมวลผลสัญญาณจากเซลล์

ไฟฟ้าเคมี โดยประกอบด้วย Op-amp (LMP7721) จำนวน 2 ตัว การทำงานเป็น 2 ขั้นตอน

2.1) วงจรควบคุมศักย์ไฟฟ้า (Potentiostat)

Operational Amplifier ตัวแรกทำหน้าที่เป็นโพเทนชิโอสแตต (potentiostat) เพื่อควบคุมให้ศักย์ไฟฟ้าระหว่าง WE และ RE คงที่ตลอดเวลา ทำให้ปฏิกิริยาไฟฟ้าเคมีเกิดขึ้นภายใต้เงื่อนไขที่เหมาะสม ส่งผลให้ค่ากระแสที่วัดได้มีความแม่นยำและเสถียร

2.2) วงจรแปลงกระแสเป็นแรงดัน (Transimpedance Amplifier)

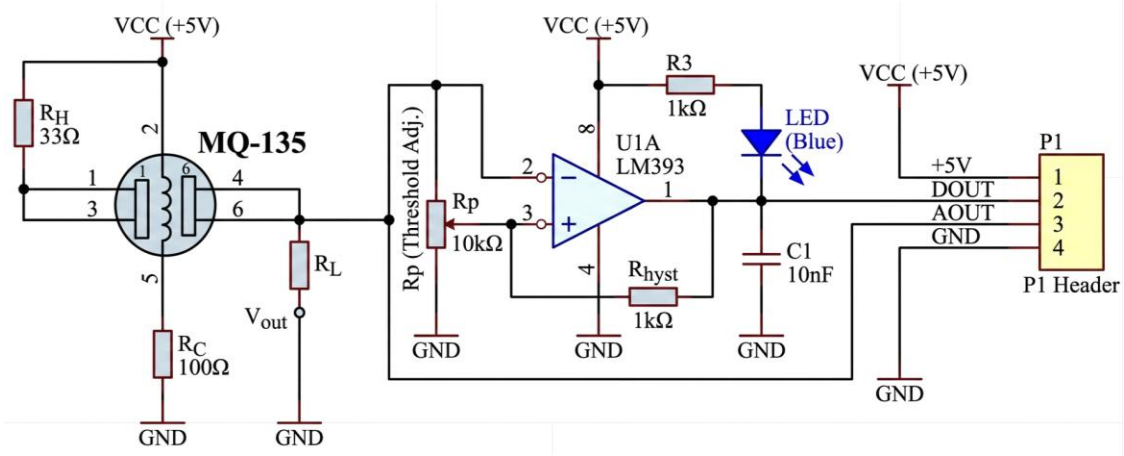
กระแสไฟฟ้าที่เกิดขึ้นจากเซนเซอร์มีค่าต่ำมาก (ηA) จึงไม่สามารถนำไปประมวลผลได้โดยตรง Op-Amp ตัวที่สองจึงทำหน้าที่เป็น Transimpedance Amplifier (TIA) เพื่อแปลงกระแสไฟฟ้าเป็นแรงดันไฟฟ้า โดยค่าความต้านทาน R6 เป็นตัวกำหนดอัตราการแปลงกระแสเป็นแรงดัน (current-to-voltage conversion gain) ส่วน R4 และ C2 ทำหน้าที่เป็นวงจรป้อนกลับ (feedback network) เพื่อรักษาเสถียรภาพของวงจร ลดสัญญาณรบกวน และป้องกันการเกิดการสั่นของสัญญาณนอกจากนี้ Q1(N-MOSFET) และ R7 ใช้สำหรับควบคุมแรงดันไบอัสและช่วงการทำงานของเซนเซอร์ ขณะที่ R1–R3 และ C1–C2 ทำหน้าที่กรองสัญญาณและลดสัญญาณรบกวนก่อนเข้าสู่วงจรขยาย ท้ายสุดแรงดันเอาต์พุต (output signal) ที่ได้จะมีค่าเป็นสัดส่วนกับความเข้มข้นของก๊าซ และสามารถส่งต่อไปยังไมโครคอนโทรลเลอร์ ระบบเก็บข้อมูล หรือระบบแจ้งเตือนเพื่อแสดงผลและสั่งงานระบบความปลอดภัยได้

2.5.3 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับก๊าซ

1) วงจรตรวจจับแก๊สและคุณภาพอากาศด้วยเซนเซอร์ MQ-135

ปัจจุบันปัญหามลพิษทางอากาศและการสะสมของแก๊สในพื้นที่ต่าง ๆ เป็นปัจจัยสำคัญที่อาจส่งผลต่อสุขภาพและความปลอดภัยของผู้ใช้งาน ดังนั้น การตรวจสอบคุณภาพอากาศและการตรวจจับแก๊สจึงมีความสำคัญ โดยเฉพาะในบริเวณที่มีโอกาสเกิดการสะสมหรือรั่วไหลของแก๊ส เช่น ภายในอาคาร ห้องปฏิบัติการ โรงงาน และพื้นที่ปิด การนำเซนเซอร์ตรวจจับแก๊สมาใช้จึงช่วยให้สามารถตรวจสอบความผิดปกติและแจ้งเตือนได้อย่างรวดเร็ว วงจรตรวจวัดแก๊สด้วย เซนเซอร์ MQ-135 เป็นวงจรที่ใช้สำหรับตรวจสอบการเปลี่ยนแปลงของแก๊สและสารมลพิษในอากาศ โดย MQ-135 มีความไวต่อแก๊สหลายชนิดและสามารถเปลี่ยนการตอบสนองต่อแก๊สให้เป็นสัญญาณไฟฟ้า เพื่อนำไปประมวลผลหรือใช้ควบคุมอุปกรณ์อื่น ๆ ได้

วงจรนี้มีการใช้ LM393 เป็นวงจรเปรียบเทียบแรงดัน (comparator) เพื่อเปรียบเทียบสัญญาณจากเซนเซอร์กับระดับอ้างอิงที่กำหนดไว้ โดยผู้ใช้งานสามารถปรับระดับการตรวจจับหรือค่า Threshold ได้ เมื่อค่าที่ตรวจวัดถึงระดับที่กำหนด วงจรจะเปลี่ยนสถานะของสัญญาณเอาต์พุตและแสดงผลผ่าน LED นอกจากนี้ยังมีเอาต์พุตทั้งแบบแอนะล็อก (AOUT) และ ดิจิทัล (DOUT) ทำให้สามารถนำไปเชื่อมต่อกับไมโครคอนโทรลเลอร์ เพื่อพัฒนาเป็นระบบตรวจจับและแจ้งเตือนแก๊สได้ ดังนั้นวงจรตรวจวัดแก๊สด้วยเซนเซอร์ MQ-135 และ LM393 จึงเป็นส่วนสำคัญของระบบตรวจจับแก๊ส ทำหน้าที่รับรู้การเปลี่ยนแปลงของสภาพอากาศและส่งสัญญาณไปยังส่วนควบคุมเพื่อให้ระบบสามารถแจ้งเตือนเมื่อพบระดับแก๊สที่ผิดปกติและช่วยเพิ่มความปลอดภัยในการใช้งาน



รูปที่ 2.21 วงจรตรวจจับแก๊สและคุณภาพอากาศด้วยเซนเซอร์ MQ-135

จากรูปที่ 2.21 เป็นวงจรตรวจจับแก๊สโดยใช้เซนเซอร์ MQ-135 ร่วมกับวงจรเปรียบเทียบ LM393 สามารถอธิบายการทำงานของวงจรเป็นส่วนต่าง ๆ ได้ดังนี้

1.1) ส่วนเซนเซอร์ MQ-135

MQ-135 เป็นเซนเซอร์ตรวจจับคุณภาพอากาศที่ตอบสนองต่อแก๊สและสารระเหยหลายชนิด ภายในเซนเซอร์ประกอบด้วย ฮีตเตอร์ (heater) และวัสดุไวต่อแก๊ส เมื่อจ่ายแรงดัน +5V ให้กับวงจร กระแสจะไหลผ่านส่วนฮีตเตอร์ ทำให้เซนเซอร์มีอุณหภูมิที่เหมาะสมต่อการตรวจจับแก๊ส โดยมีตัวต้านทาน (RH) และ (RC) อยู่ในส่วนของวงจรฮีตเตอร์เมื่อความเข้มข้นของแก๊สในอากาศเปลี่ยนแปลง ความต้านทานภายในของส่วนตรวจจับ MQ-135 จะเปลี่ยนแปลงตามไปด้วย การเปลี่ยนแปลงดังกล่าวจะถูกแปลงเป็นแรงดันไฟฟ้าด้วยตัวต้านทานโหลด (RL) ทำให้เกิดแรงดัน (VOUT) ดังนั้น ค่า VOUT ที่ได้ เป็นสัญญาณแอนะล็อกที่สัมพันธ์กับสภาวะแก๊สที่เซนเซอร์ตรวจจับได้และถูกส่งออกทางขา AOUT

1.2) ส่วนปรับค่าระดับการตรวจจับ

วงจรมีตัวต้านทานปรับค่าได้ Rp ขนาด 10 kΩ ทำหน้าที่กำหนด threshold หรือระดับอ้างอิงสำหรับการตรวจจับ เมื่อหมุนปรับ Rp ค่าแรงดันที่ส่งเข้าสู่อินพุตของ LM393 จะเปลี่ยนไป ทำให้ผู้ใช้งานสามารถกำหนดได้ว่า ต้องการให้ขา DOUT เปลี่ยนสถานะเมื่อปริมาณแก๊สอยู่ที่ระดับใด กล่าวง่าย ๆ คือ Rp ใช้ปรับความไวหรือจุดเตือนของวงจร

1.3) ส่วนเปรียบเทียบสัญญาณ LM393

LM393 ทำหน้าที่เป็นวงจรเปรียบเทียบแรงดัน โดยเปรียบเทียบแรงดันที่สัมพันธ์กับค่าจากเซนเซอร์ กับแรงดัน threshold ที่กำหนดจาก Rp เมื่อแรงดันทั้งสองมีความสัมพันธ์ถึงจุดที่กำหนดไว้ เอาต์พุตของ LM393 จะเปลี่ยนสถานะ ทำให้ได้สัญญาณดิจิทัลที่ขา DOUT เนื่องจากเอาต์พุตของ LM393 เป็นแบบ open-collector การทำงานจึงเป็นลักษณะดึงระดับสัญญาณลงต่ำเมื่อวงจร comparator ทำงาน ส่วนวงจร LED และตัวต้านทาน R3 ช่วยทำหน้าที่เป็นโหลดพร้อมแสดงสถานะ ดังนั้นการตีความว่า DOUT เป็น HIGH หรือ LOW เมื่อ “ตรวจพบแก๊ส” จะขึ้นอยู่กับการตั้ง ค่า threshold และการต่อวงจร comparator นี้

1.4) ส่วน LED แสดงสถานะ

LED ทำหน้าที่แสดงสถานะของเอาต์พุตจาก LM393 โดยมี R3 ขนาด 1 kΩ ทำหน้าที่จำกัดกระแสที่ไหลผ่าน LED เพื่อป้องกันไม่ให้ LED ได้รับกระแสมากเกินไป เมื่อเอาต์พุตของ LM393 ดึงสัญญาณลงต่ำ กระแสสามารถไหลจาก +5V ผ่าน R3 และ LED ไปยังเอาต์พุตของ LM393 ทำให้ LED ติด แสดงว่าวงจร Comparator อยู่ในสถานะที่กำหนดไว้สำหรับการตรวจจับ

1.5) ตัวต้านทาน Rhyst

ตัวต้านทาน Rhyst ขนาด 1 kΩ เป็นส่วนของวงจรป้อนกลับเพื่อสร้าง hysteresis ให้ comparator หน้าที่ของ hysteresis คือช่วยป้องกันไม่ให้เอาต์พุตของ LM393 สลับ HIGH และ LOW อย่างรวดเร็วในกรณีที่ค่าจากเซนเซอร์อยู่ใกล้กับค่า threshold เช่น เมื่อความเข้มข้นของแก๊สเปลี่ยนแปลงเล็กน้อยบริเวณจุดตัด จึงช่วยให้สัญญาณ DOUT มีความเสถียรมากขึ้น

1.6) ตัวเก็บประจุ C1

C1 ขนาด 10 nF ต่ออยู่เอาต์พุตของ comparator ทำหน้าที่ช่วยลดสัญญาณรบกวนและการเปลี่ยนแปลงของสัญญาณที่รวดเร็วมาก ทำให้สัญญาณ DOUT ที่ส่งออกมีความเสถียรขึ้น

1.7) ขาเอาต์พุตของวงจร

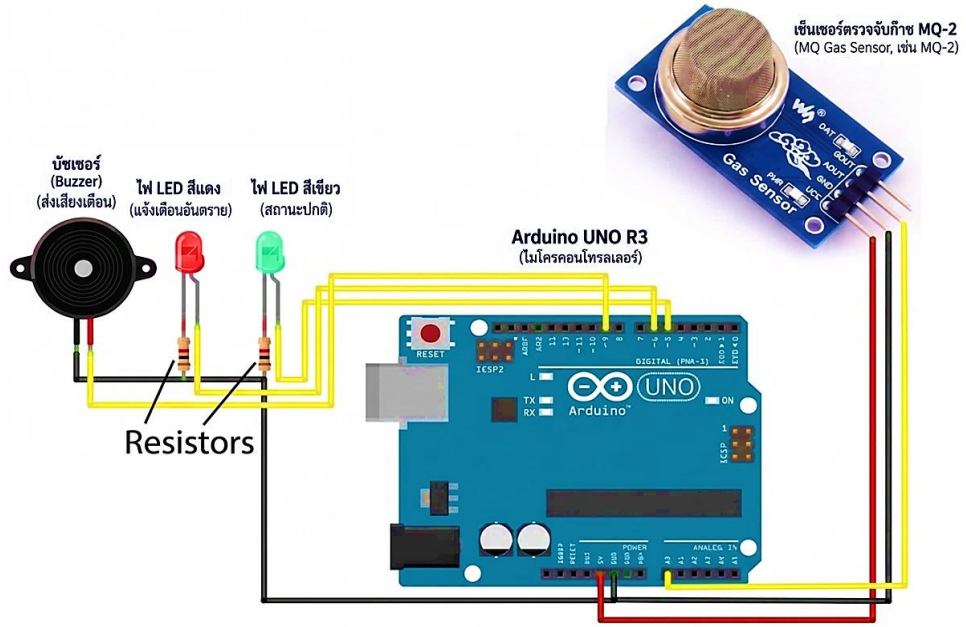
วงจรมีขั้วต่อ P1 จำนวน 4 ขา ได้แก่

- +5V รับแรงดันไฟเลี้ยง 5 V
- DOUT สัญญาณเอาต์พุตแบบดิจิทัลจากวงจร LM393 เหมาะสำหรับต่อเข้าขา digital input ของไมโครคอนโทรลเลอร์
- AOUT สัญญาณแอนะล็อกจากส่วนตรวจจับ MQ-135 เหมาะสำหรับต่อเข้าขา analog input เพื่ออ่านระดับสัญญาณและนำไปประมวลผล
- GND กราวด์ของวงจร

สรุปการทำงานของวงจร เมื่อจ่ายไฟ 5 V ให้กับวงจร ฮีตเตอร์ของ MQ-135 จะทำให้เซนเซอร์อยู่ในสภาวะพร้อมตรวจจับแก๊ส เมื่อปริมาณแก๊สเปลี่ยนแปลง ความต้านทานของส่วนตรวจจับจะเปลี่ยน ส่งผลให้แรงดัน V_{OUT} เปลี่ยนตาม แรงดันนี้สามารถนำออกไปใช้งานโดยตรงผ่านขา AOUT ในขณะเดียวกัน วงจร LM393 จะเปรียบเทียบสัญญาณที่เกี่ยวข้องกับเซนเซอร์กับระดับ threshold ที่ปรับด้วย Rp เมื่อค่าถึงจุดที่กำหนด เอาต์พุตของ comparator จะเปลี่ยนสถานะ ทำให้ DOUT เปลี่ยนระดับลอจิกและ LED แสดงสถานะ ส่วน Rhyst และ C1 ช่วยให้การเปลี่ยนสถานะมีความเสถียรและลดผลกระทบจากสัญญาณรบกวน

2) วงจรตรวจจับแก๊สด้วยเซนเซอร์ MQ-2 ร่วมกับ Arduino

การออกแบบระบบตรวจจับและแจ้งเตือนแก๊สนี้ เป็นการนำโมดูลเซนเซอร์ตรวจจับแก๊สมาใช้ร่วมกับ Arduino Uno ซึ่งทำหน้าที่เป็นหน่วยควบคุมและประมวลผลหลักของระบบ เมื่อเซนเซอร์ตรวจพบการเปลี่ยนแปลงของปริมาณแก๊ส จะส่งสัญญาณไปยัง Arduino เพื่อเปรียบเทียบกับค่าที่กำหนดไว้ จากนั้น Arduino จะควบคุมอุปกรณ์แสดงสถานะ ได้แก่ LED สีเขียว สำหรับแสดงสภาวะปกติ และ LED สีแดงพร้อม buzzer สำหรับแจ้งเตือนเมื่อระดับแก๊สสูงกว่าค่าที่กำหนด โดยอุปกรณ์ทั้งหมดเชื่อมต่อร่วมกัน ดังรูปที่ 2.22



รูปที่ 2.22 วงจรตรวจจับและแจ้งเตือนแก๊สด้วยเซนเซอร์ MQ-2 ร่วมกับ Arduino

จากรูปที่ 2.22 หลักการทำงานของวงจร เมื่อเปิดระบบ Arduino จะจ่ายไฟให้กับ gas sensor และเริ่มอ่านค่าที่เซนเซอร์ตรวจจับได้อย่างต่อเนื่อง โดย gas sensor จะตรวจสอบความเข้มข้นของแก๊สในอากาศและเปลี่ยนปริมาณแก๊สที่ตรวจพบเป็นสัญญาณไฟฟ้าส่งเข้าสู่ Arduino จากนั้น Arduino จะนำค่าที่อ่านได้มา เปรียบเทียบกับค่าระดับแก๊สที่กำหนดไว้ในโปรแกรม (threshold) จากนั้นจึงควบคุม LED และ buzzer ตามเงื่อนไขที่กำหนด

➲ กรณีปริมาณแก๊สอยู่ในระดับปกติ Arduino จะสั่งให้ LED สีเขียวติด เพื่อแสดงว่าสภาพแวดล้อมอยู่ในระดับปลอดภัย พร้อมกับสั่งให้ LED สีแดงดับและ buzzer ไม่ส่งเสียง

➲ กรณีตรวจพบปริมาณแก๊สสูงเกินค่าที่กำหนด Arduino จะสั่งให้ LED สีแดงติด เพื่อแสดงสถานะอันตราย และสั่งให้ buzzer ส่งเสียงเตือน เพื่อแจ้งให้ผู้ใช้งานทราบว่ามีปริมาณแก๊สสูงผิดปกติ ส่วน LED สีเขียวจะดับลง

2.1) การต่อ gas sensor

➲ ขา VCC ของ gas sensor ต่อเข้ากับขา 5V ของ Arduino เพื่อจ่ายไฟให้เซนเซอร์

➲ ขา GND ต่อเข้ากับขา GND ของ Arduino

➲ ขาสัญญาณ AOUT (analog output) ต่อเข้ากับขา analog input ของ Arduino เพื่อส่งค่าปริมาณแก๊สที่ตรวจจับได้ให้ Arduino นำไปประมวลผล

➲ หากโมดูลมีขา DOUT สามารถใช้เป็นสัญญาณดิจิทัลได้ แต่ในวงจรนี้หลักการตรวจวัดสามารถใช้สัญญาณจาก AOUT เพื่อเปรียบเทียบกับค่าที่กำหนดในโปรแกรม

2.2) การต่อ LED

สีเขียวLED สีเขียวใช้สำหรับแสดงสถานะว่า ปริมาณแก๊สอยู่ในระดับปกติหรือปลอดภัย โดยต่อขาหนึ่งของ LED เข้ากับขา digital output ของ Arduino และอีกขาต่อผ่านตัวต้านทานลง GND ตัวต้านทานทำหน้าที่จำกัดกระแสเพื่อป้องกัน LED เสียหาย

การต่อ LED สีแดง ใช้สำหรับแสดง สถานะเตือนภัย เมื่อตรวจพบปริมาณแก๊สสูงกว่าค่าที่กำหนด โดยต่อเข้ากับขา digital output ของ Arduino และต่อร่วมกับตัวต้านทานเพื่อจำกัดกระแสเช่นเดียวกับ LED สีเขียว

2.3)การต่อ buzzer

Buzzer ทำหน้าที่ส่งเสียงเตือน โดยต่อขาสัญญาณเข้ากับขา digital output ของ Arduino ส่วนอีกขาต่อเข้ากับ GND เมื่อ Arduino ตรวจพบปริมาณแก๊สเกินค่าที่กำหนด จะส่งสัญญาณไปยัง buzzer เพื่อให้เกิดเสียงเตือน

2.4) การต่อกราวด์ (GND)

อุปกรณ์ต่าง ๆ ในวงจรจะใช้ GND ร่วมกันกับ Arduino เพื่อให้วงจรมีจุดอ้างอิงแรงดันเดียวกันและสามารถทำงานร่วมกันได้อย่างถูกต้อง

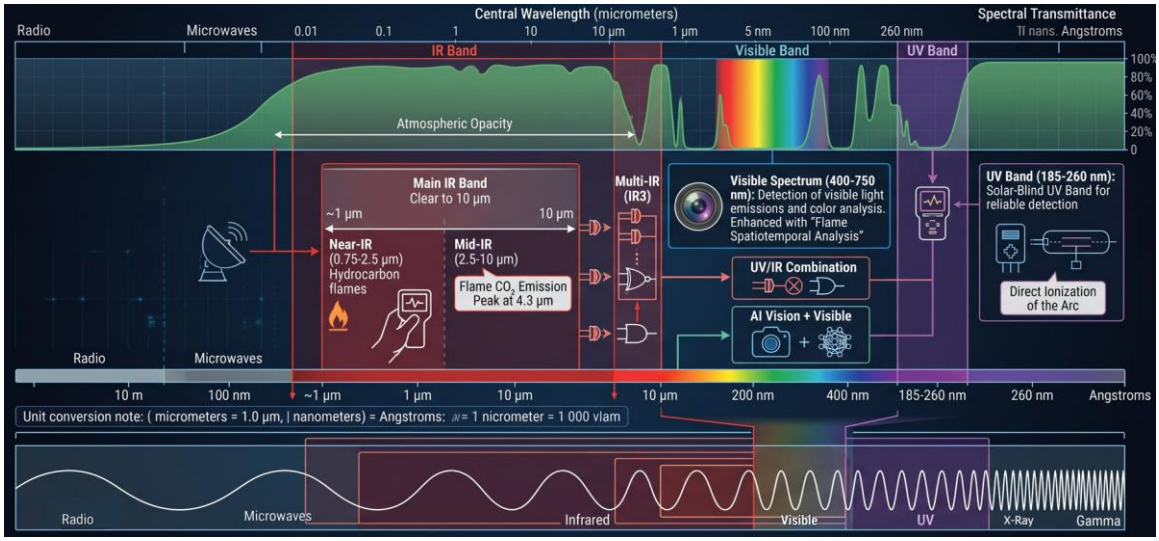
2.6 เซนเซอร์ตรวจจับเปลวไฟ (Flame Sensors)

เซนเซอร์ตรวจจับเปลวไฟ (flame sensor หรือ flame detector) เป็นอุปกรณ์ตรวจจับอัคคีภัยที่ออกแบบมาเพื่อรับรู้การเกิดเปลวไฟโดยตรงจากพลังงานรังสีแม่เหล็กไฟฟ้า (electromagnetic radiation) ที่แผ่ออกมาระหว่างกระบวนการเผาไหม้ แตกต่างจากเครื่องตรวจจับควัน (smoke detector) และเครื่องตรวจจับความร้อน (heat detector) ซึ่งอาศัยผลิตภัณฑ์ที่เกิดขึ้นภายหลังการเผาไหม้ เช่น ควันหรืออุณหภูมิที่เพิ่มสูงขึ้น ทำให้เซนเซอร์ตรวจจับเปลวไฟสามารถตรวจจับเหตุการณ์ได้รวดเร็วกว่า โดยเฉพาะในพื้นที่ที่เกิดการลุกไหม้อย่างรวดเร็วหรือมีความเสี่ยงสูง เช่น โรงกลั่นน้ำมัน โรงงานปิโตรเคมี คลังเชื้อเพลิง โรงงานผลิตสารเคมี หรือโรงงานผลิตวัตถุระเบิด (Hosch, 2020; National Fire Protection Association: NFPA, 2022)

หลักการตรวจจับเปลวไฟอาศัยการวิเคราะห์รังสีแม่เหล็กไฟฟ้าที่ปล่อยออกมาจากเปลวไฟในช่วงความยาวคลื่นที่แตกต่างกัน ได้แก่ รังสีอัลตราไวโอเลต (UV) แสงที่มองเห็นได้ (visible light) และรังสีอินฟราเรด (IR) โดยเปลวไฟของเชื้อเพลิงแต่ละชนิดจะมีลักษณะการแผ่รังสี (spectral emission) ที่แตกต่างกัน เซนเซอร์จึงถูกออกแบบให้ตอบสนองเฉพาะช่วงความยาวคลื่นที่เป็นลักษณะเฉพาะของการเผาไหม้ พร้อมใช้วงจรประมวลผลในการวิเคราะห์ความเข้มของรังสี ความถี่การกะพริบของเปลวไฟ (flame flicker frequency) และรูปแบบสัญญาณ เพื่อแยกแยะเปลวไฟจริงออกจากแหล่งกำเนิดรังสีอื่น เช่น แสงอาทิตย์ งานเชื่อมโลหะ หรือวัตถุที่มีอุณหภูมิสูง ซึ่งช่วยลดการแจ้งเตือนผิดพลาด (false alarm) ได้อย่างมีประสิทธิภาพ (Hosch, 2020) ปัจจุบันเซนเซอร์ตรวจจับเปลวไฟมีการพัฒนาอย่างต่อเนื่อง จากเซนเซอร์ที่ตรวจจับเพียงช่วงคลื่นเดียว เช่น UV หรือ IR ไปสู่เซนเซอร์หลายสเปกตรัม เช่น UV/IR, multi-IR (IR3), triple spectrum และ AI vision flame detector ซึ่งสามารถประมวลผลข้อมูลจากหลายช่วงคลื่นร่วมกับอัลกอริทึมอัจฉริยะ ทำให้มีความแม่นยำสูง สามารถตรวจจับเปลวไฟได้รวดเร็ว ลดการแจ้งเตือนผิดพลาด และเหมาะสำหรับระบบป้องกันอัคคีภัยสมัยใหม่ (Hosch, 2020; NFPA, 2022)

2.6.1 คุณสมบัติของคลื่นแม่เหล็กไฟฟ้าที่ตรวจพบจากเปลวไฟ

ในระหว่างกระบวนการเผาไหม้ พลังงานเคมีของเชื้อเพลิงจะถูกเปลี่ยนเป็นพลังงานความร้อนและพลังงานรังสี ทำให้เปลวไฟแผ่คลื่นแม่เหล็กไฟฟ้าออกมาในหลายช่วงความยาวคลื่น ตั้งแต่รังสีอัลตราไวโอเลตจนถึงรังสีอินฟราเรด โดยแต่ละช่วงคลื่นมีคุณสมบัติและความเหมาะสมในการตรวจจับแตกต่างกัน ดังแสดงในรูปคลื่นแม่เหล็กไฟฟ้าของเซนเซอร์ตรวจจับเปลวไฟ



รูปที่ 2.23 คลื่นแม่เหล็กไฟฟ้าที่ตรวจพบจากเปลวไฟ

1) รังสีอัลตราไวโอเลต (Ultraviolet: UV)

รังสีอัลตราไวโอเลตที่เกิดจากเปลวไฟมีช่วงความยาวคลื่นประมาณ 185–260 ηm (1,850–2,600 Å) ซึ่งเป็นช่วง solar-blind UV ที่แสงอาทิตย์ไม่สามารถผ่านชั้นบรรยากาศมายังพื้นโลกได้ จึงช่วยลดผลกระทบจากแสงอาทิตย์และทำให้สามารถตรวจจับเปลวไฟได้อย่างรวดเร็ว โดยเฉพาะเปลวไฟจากก๊าซ ไฮโดรเจน และเชื้อเพลิงไฮโดรคาร์บอน (Hosch, 2020)

2) แสงที่มองเห็นได้ (Visible Light)

แสงที่มองเห็นได้มีช่วงความยาวคลื่นประมาณ 400–700 ηm เป็นช่วงที่ดวงตามนุษย์สามารถรับรู้ได้ อย่างไรก็ตาม แสงในช่วงนี้ได้รับผลกระทบจากแสงอาทิตย์ แสงสว่างในโรงงานและแหล่งกำเนิดแสงอื่น ๆ ได้ง่าย จึงไม่ค่อยนำมาใช้เพียงอย่างเดียวในการตรวจจับเปลวไฟ แต่จะใช้ร่วมกับการประมวลผลภาพในระบบ Video Flame Detector (VFD) และ AI vision flame detector (NFPA, 2022)

3) รังสีอินฟราเรด (Infrared: IR)

รังสีอินฟราเรดที่ปล่อยออกจากเปลวไฟมีช่วงความยาวคลื่นกว้าง แต่เซนเซอร์ตรวจจับเปลวไฟมักเลือกตรวจจับบริเวณ 4.2–4.8 µm หรือประมาณ 4.45 µm ซึ่งเป็นช่วงการแผ่รังสีของก๊าซคาร์บอนไดออกไซด์ (CO_2 emission band) ที่เกิดขึ้นจากการเผาไหม้ จึงสามารถตรวจจับเปลวไฟได้อย่างแม่นยำ และลดผลกระทบจากแหล่งกำเนิดความร้อนทั่วไป (Hosch, 2020)

4) ความถี่การกะพริบของเปลวไฟ (Flame Flicker Frequency)

นอกจากช่วงความยาวคลื่นแล้ว เปลวไฟยังมีลักษณะการกะพริบของความเข้มแสงที่ความถี่ประมาณ 2–20 Hz ซึ่งเกิดจากความปั่นป่วนของกระบวนการเผาไหม้ เซนเซอร์ตรวจจับเปลวไฟจะนำข้อมูลดังกล่าวมาวิเคราะห์ร่วมกับข้อมูลเชิงสเปกตรัม เพื่อช่วยแยกเปลวไฟจริงออกจากแหล่งกำเนิดรังสีคงที่ เช่น หลอดไฟหรือวัตถุร้อน ส่งผลให้ลดการแจ้งเตือนผิดพลาดและเพิ่มความน่าเชื่อถือของระบบตรวจจับ (Hosch, 2020; NFPA, 2022)

ตารางที่ 2.2 สรุปคุณสมบัติของคลื่นแม่เหล็กไฟฟ้าที่ใช้ในการตรวจจับเปลวไฟ

ช่วงคลื่น	ความยาวคลื่น	ลักษณะเด่น	การประยุกต์ใช้
Ultraviolet (UV)	185–260 ηm	ตรวจจับได้รวดเร็ว ไม่ถูกรบกวนจากแสงอาทิตย์	UV Detector, UV/IR
Visible Light	400–700 ηm	ใช้วิเคราะห์ภาพเปลวไฟ	VFD, AI Vision
Infrared (IR)	4.2–4.8 μm	ตรวจจับการแผ่รังสีจาก CO_2 ในเปลวไฟ	IR Detector, IR3, UV/IR
Flicker Frequency	2–20 Hz	วิเคราะห์การกะพริบของเปลวไฟ	IR, IR3, AI Vision

2.6.2 ชนิดของเซนเซอร์ตรวจจับเปลวไฟ (Types of Flame Sensors)

เซนเซอร์ตรวจจับเปลวไฟ (flame sensor) เป็นอุปกรณ์ที่ใช้ตรวจจับรังสีแม่เหล็กไฟฟ้าที่เกิดจากการเผาไหม้ โดยอาศัยการตรวจจับรังสีในช่วงอัลตราไวโอเลต (UV) อินฟราเรด (IR) หรือแสงที่ตามองเห็น (visible light) เพื่อแจ้งเตือนเมื่อเกิดเพลิงไหม้ ซึ่งเซนเซอร์แต่ละชนิดมีหลักการทำงาน ช่วงคลื่นที่ตรวจจับ และความเหมาะสมในการใช้งานแตกต่างกัน (Xiao et al., 2020)

1) เซนเซอร์ตรวจจับเปลวไฟแบบอัลตราไวโอเลต (Ultraviolet Flame Sensor: UV)

เปลวไฟจะปลดปล่อยรังสีอัลตราไวโอเลตในช่วง solar-blind UV ประมาณ 200–280 ηm ตั้งแต่เริ่มเกิดการเผาไหม้ จึงทำให้เซนเซอร์ชนิดนี้สามารถตรวจจับเพลิงไหม้ได้อย่างรวดเร็วภายในเวลาเพียงไม่กี่มิลลิวินาที เหมาะสำหรับการตรวจจับไฟที่เกิดจากก๊าซ เชื้อเพลิงเหลว และสารเคมีไวไฟ อย่างไรก็ตาม เซนเซอร์ชนิดนี้อาจเกิดการแจ้งเตือนผิดพลาดจากแหล่งกำเนิดรังสี UV เช่น งานเชื่อมโลหะหรือฟ้าผ่าได้ (Wei et al., 2026)

2) เซนเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด (Infrared Flame Sensor: IR Sensor)

เปลวไฟจากการเผาไหม้ของเชื้อเพลิงไฮโดรคาร์บอน จะมีการแผ่รังสีอินฟราเรดที่มีลักษณะเฉพาะ โดยเฉพาะบริเวณ 4.3–4.4 μm ซึ่งเกิดจากการแผ่รังสีของก๊าซคาร์บอนไดออกไซด์ (CO_2) ทำให้สามารถแยกความแตกต่างระหว่างเปลวไฟกับวัตถุร้อนทั่วไปได้อย่างมีประสิทธิภาพ จึงนิยมนำไปใช้ในโรงงานอุตสาหกรรม โรงกลั่นน้ำมัน และคลังเก็บเชื้อเพลิง (Bordbar et al., 2022)

3) เซนเซอร์ตรวจจับเปลวไฟแบบอัลตราไวโอเลต/อินฟราเรด (UV/IR Flame Sensor)

เซนเซอร์ที่ใช้ตัวรับสัญญาณทั้งรังสี UV และ IR เพื่อยืนยันการเกิดเปลวไฟจากทั้งสองช่วงคลื่นพร้อมกัน ส่งผลให้ลดโอกาสการแจ้งเตือนผิดพลาดจากแหล่งกำเนิดรังสีเพียงชนิดเดียว และเพิ่มความน่าเชื่อถือของระบบตรวจจับเปลวไฟ (Xiao et al., 2020)

4) เซนเซอร์ตรวจจับเปลวไฟแบบหลายช่วงคลื่นอินฟราเรด (Multi-Spectrum Infrared หรือ IR3)

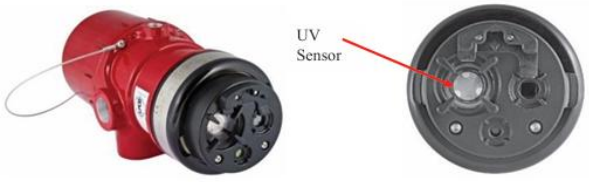
เซนเซอร์แบบหลายช่วงคลื่นอินฟราเรดใช้ตัวกรองแสงและตัวรับสัญญาณหลายช่วงคลื่นเพื่อวิเคราะห์รูปแบบการแผ่รังสีของเปลวไฟ โดยเปรียบเทียบสัญญาณที่ได้รับจากหลายช่วงคลื่นพร้อมกัน ทำให้สามารถแยกเปลวไฟออกจากแสงอาทิตย์หรือวัตถุที่มีอุณหภูมิสูงได้อย่างแม่นยำ จึงได้รับความนิยมในอุตสาหกรรมปิโตรเคมีและพลังงาน (Bordbar et al., 2022)

5) เซนเซอร์ตรวจจับเปลวไฟแบบภาพ (Vision-Based Flame Sensor)

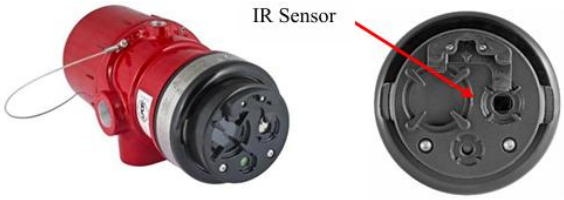
วิธีตรวจจับเปลวไฟด้วยกล้องดิจิทัลร่วมกับเทคนิคปัญญาประดิษฐ์ โดยพัฒนาอัลกอริทึมบนพื้นฐานของ YOLOv5 ร่วมกับการวิเคราะห์ลำดับเวลา (time sequence analysis) เพื่อวิเคราะห์สี รูปร่าง การเคลื่อนไหว และการเปลี่ยนแปลงของเปลวไฟในภาพวิดีโอ ส่งผลให้สามารถตรวจจับเปลวไฟแบบเรียลไทม์ได้อย่างแม่นยำ พร้อมลดการแจ้งเตือนผิดพลาดจากวัตถุที่มีลักษณะคล้ายเปลวไฟ (Zhang et al., 2023)

ตารางที่ 2.3 การเปรียบเทียบชนิดของเซนเซอร์ตรวจจับเปลวไฟ (Xiao et al., 2020; Bordbar et al., 2022; Zhang et al., 2023; Wei et al., 2026)

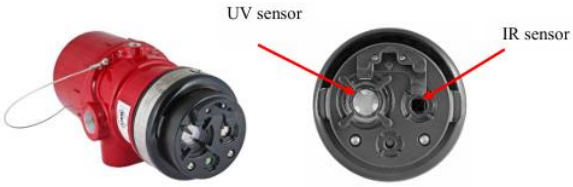
ชนิดของ Flame Sensor	หลักการตรวจจับ	การใช้งาน
1. Ultraviolet (UV)	ตรวจจับรังสี UV ประมาณ 180–280 nm	ตรวจจับได้รวดเร็ว เหมาะกับก๊าซและเชื้อเพลิงเหลว
2. Infrared (IR)	ตรวจจับรังสีอินฟราเรดจากเปลวไฟ โดยเฉพาะ CO_2 ที่ประมาณ 4.3 μm	ใช้ในโรงงานอุตสาหกรรม
3. UV/IR Combination	ตรวจจับ UV และ IR พร้อมกัน	ลดการแจ้งเตือนผิดพลาด
4. Multi-IR (IR3, Triple IR)	เปรียบเทียบหลายช่วงคลื่นอินฟราเรด	ความแม่นยำสูง ใช้ในอุตสาหกรรมน้ำมันและก๊าซ
5. UV/IR + Visible (Triple Spectrum)	ตรวจจับ UV, IR และแสงที่ตามองเห็น	ใช้ในพื้นที่ที่มีแสงรบกวนมาก
6. Video Flame Detector (VFD)	ใช้กล้องและการประมวลผลภาพ	ตรวจจับพื้นที่กว้างและระบุตำแหน่งเปลวไฟ
7. AI Vision Flame Detector	ใช้ AI วิเคราะห์ภาพหรือวิดีโอ	ระบบ Smart Fire Detection และ Smart Building



(ก) Ultraviolet (UV) (Hosch, 2020)



(ข) Infrared (IR) (Hosch, 2020)

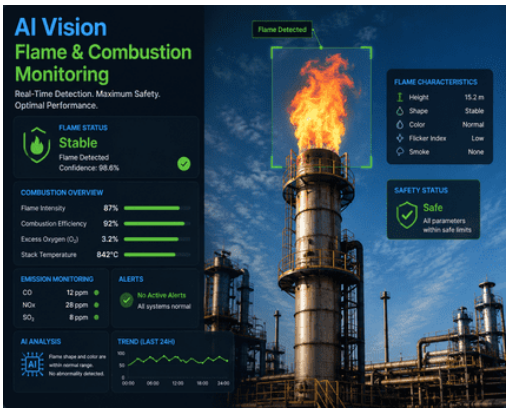


(ค) UV/IR Combination (Hosch, 2020)

(ง) Video Flame Detector (VFD)

(จ) Multi-IR (IR3, Triple IR) (Hosch, 2020)

(ฉ) UV/IR/Visible (Triple Spectrum) (Hosch, 2020)



(ช) AI Vision Flame Detector (Austin, 2026)

รูปที่ 2.24 เซนเซอร์ตรวจจับเปลวไฟชนิดต่าง ๆ

เซนเซอร์ตรวจจับเปลวไฟแต่ละประเภทมีจุดเด่นแตกต่างกัน ได้แก่ เซนเซอร์ UV ที่ตอบสนองรวดเร็ว เซนเซอร์ IR ที่เหมาะสำหรับการตรวจจับระยะไกล เซนเซอร์ UV/IR ที่ช่วยลดการแจ้งเตือนผิดพลาด เซนเซอร์ multi-IR ที่มีความแม่นยำสูงในงานอุตสาหกรรม และเซนเซอร์แบบภาพที่ใช้เทคโนโลยีปัญญาประดิษฐ์สำหรับระบบเฝ้าระวังอัจฉริยะ ดังนั้นการเลือกใช้เซนเซอร์ควรพิจารณาจากลักษณะการใช้งาน สภาพแวดล้อม และระดับความเสี่ยงของพื้นที่ติดตั้ง (Xiao et al., 2020; Bordbar et al., 2022; Zhang et al., 2023; Wei et al., 2026)

2.6.3 โครงสร้างของเซนเซอร์ตรวจจับเปลวไฟ (Structure of Flame Sensors)

เซนเซอร์ตรวจจับเปลวไฟ ประกอบด้วยองค์ประกอบหลักหลายส่วนที่ทำงานร่วมกันเพื่อรับรังสีแม่เหล็กไฟฟ้าที่เกิดจากการเผาไหม้ แปลงเป็นสัญญาณไฟฟ้า ประมวลผล และส่งสัญญาณแจ้งเตือนเมื่อเกิดเพลิงไหม้ โดยแม้เซนเซอร์แต่ละชนิด เช่น UV, IR, UV/IR และ Multi-IR จะมีหลักการตรวจจับแตกต่างกัน แต่โครงสร้างพื้นฐานของอุปกรณ์มีองค์ประกอบที่คล้ายคลึงกัน ได้แก่ ตัวเรือนเซนเซอร์ เลนส์หรือหน้าต่างกรองแสง ชุดตรวจจับรังสี วงจรขยายสัญญาณ วงจรประมวลผล และ

วงจรเอาต์พุต (Bordbar et al., 2022; Xiao et al., 2020) โครงสร้างทั่วไปของเซนเซอร์ตรวจจับเปลวไฟประกอบด้วยองค์ประกอบสำคัญ ดังนี้

1) ตัวเรือนเซนเซอร์ (Sensor Housing)

ตัวเรือนทำหน้าที่ป้องกันอุปกรณ์อิเล็กทรอนิกส์ภายในจากฝุ่น ความชื้น สารเคมี และแรงกระแทก โดยทั่วไปผลิตจากอะลูมิเนียมอัลลอยหรือสเตนเลสที่มีความแข็งแรงและทนต่อการกัดกร่อน ในงานอุตสาหกรรมมักออกแบบให้มีมาตรฐานป้องกันฝุ่นและน้ำ เช่น IP66 หรือ IP67 และอาจได้รับการรับรองมาตรฐานป้องกันการระเบิด (explosion-proof) สำหรับใช้งานในพื้นที่อันตราย (hazardous area) (Bordbar et al., 2022)

2) หน้าต่างรับรังสีหรือเลนส์กรองแสง (Optical Window / Optical Filter)

หน้าต่างรับรังสีอยู่บริเวณด้านหน้าของเซนเซอร์ ทำหน้าที่ให้รังสีจากเปลวไฟผ่านเข้าสู่ตัวตรวจจับ พร้อมทั้งกรองช่วงความยาวคลื่นที่ไม่ต้องการออก เพื่อลดผลกระทบจากแสงอาทิตย์ แสงจากหลอดไฟ หรือแหล่งกำเนิดความร้อนอื่น ๆ วัสดุที่ใช้ผลิตหน้าต่างรับรังสีจะแตกต่างกันตามชนิดของเซนเซอร์ เช่น ควอตซ์ (quartz) สำหรับเซนเซอร์ UV และเจอร์เมเนียม (germanium) หรือแซฟไฟร์ (sapphire) สำหรับเซนเซอร์อินฟราเรด (Wei et al., 2026)

3) ตัวตรวจจับรังสี (Radiation Detector)

ตัวตรวจจับรังสีเป็นส่วนสำคัญที่สุดของเซนเซอร์ ทำหน้าที่แปลงพลังงานรังสีจากเปลวไฟให้เป็นสัญญาณไฟฟ้า โดยชนิดของตัวตรวจจับขึ้นอยู่กับหลักการตรวจจับ ได้แก่

3.1) UV detector ใช้หลอดตรวจจับรังสี UV หรือโฟโตไดโอดที่ไวต่อรังสี UV

3.2) IR detector ใช้โฟโตไดโอดอินฟราเรดเทอร์โมไพล์ (thermopile) หรือไพโรอิเล็กทริกเซนเซอร์ (pyroelectric sensor)

3.3) Multi-IR detector ใช้ตัวรับอินฟราเรดหลายตัวร่วมกับตัวกรองแสงหลายช่วงคลื่น เพื่อเปรียบเทียบลักษณะการแผ่รังสีของเปลวไฟ (Bordbar et al., 2022)

4) วงจรขยายสัญญาณ (Signal Amplifier)

สัญญาณที่ได้จากตัวตรวจจับรังสีมีขนาดเล็กมาก จึงต้องผ่านวงจรขยายสัญญาณเพื่อเพิ่มระดับแรงดันหรือกระแสไฟฟ้าให้เหมาะสมสำหรับการประมวลผลในขั้นตอนถัดไป พร้อมทั้งลดสัญญาณรบกวนจากสภาพแวดล้อม (Xiao et al., 2020)

5) วงจรประมวลผลสัญญาณ (Signal Processing Unit)

วงจรประมวลผลทำหน้าที่วิเคราะห์ลักษณะของสัญญาณที่ได้รับ เช่น ความเข้มของรังสี ความถี่การกะพริบของเปลวไฟ (flame flicker frequency) และรูปแบบของคลื่นอินฟราเรด เพื่อจำแนกว่ารังสีที่ตรวจพบเกิดจากเปลวไฟจริงหรือเกิดจากแหล่งกำเนิดอื่น ช่วยลดการแจ้งเตือนผิดพลาด (false alarm) ได้อย่างมีประสิทธิภาพ (Bordbar et al., 2022)

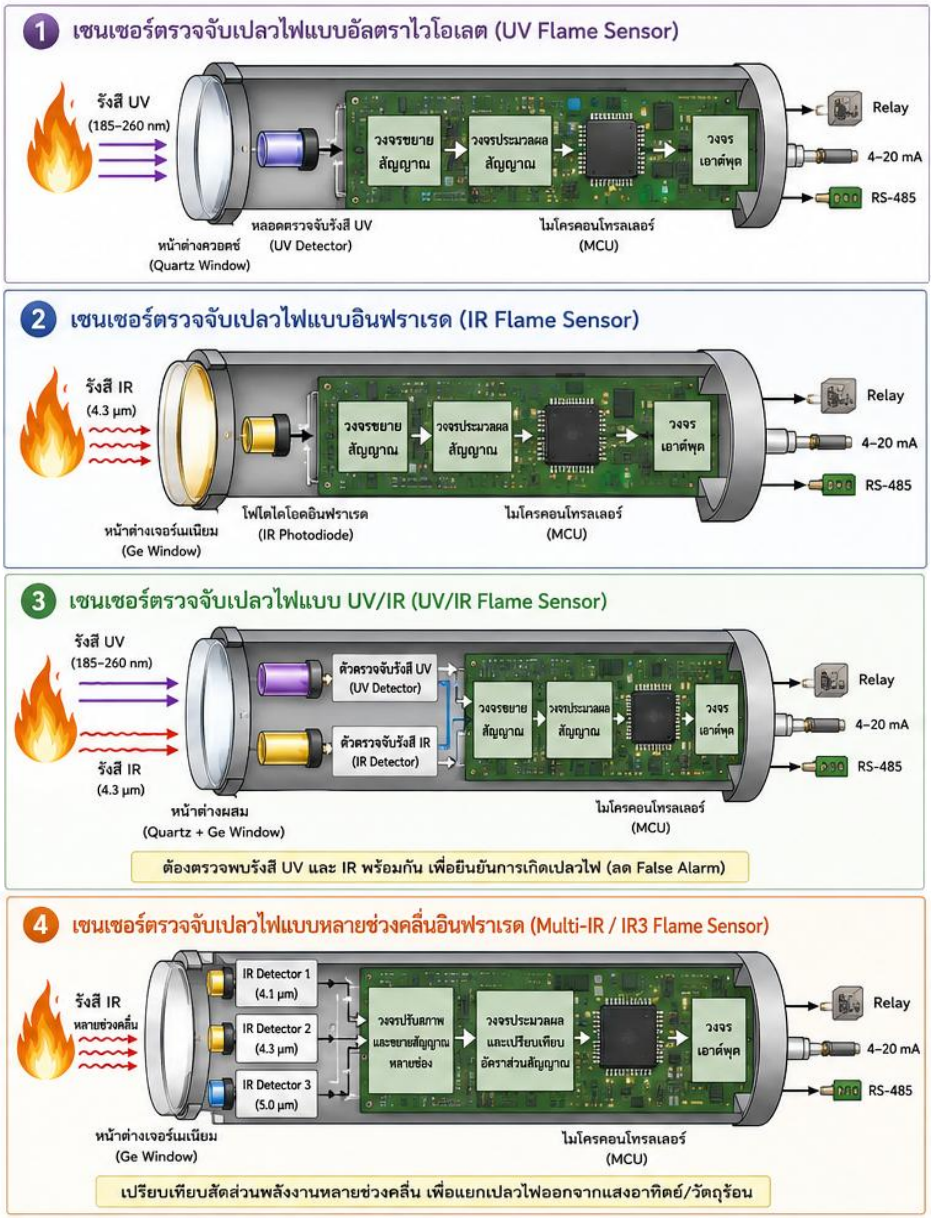
6) ไมโครคอนโทรลเลอร์หรือหน่วยประมวลผล (Microcontroller / Processor)

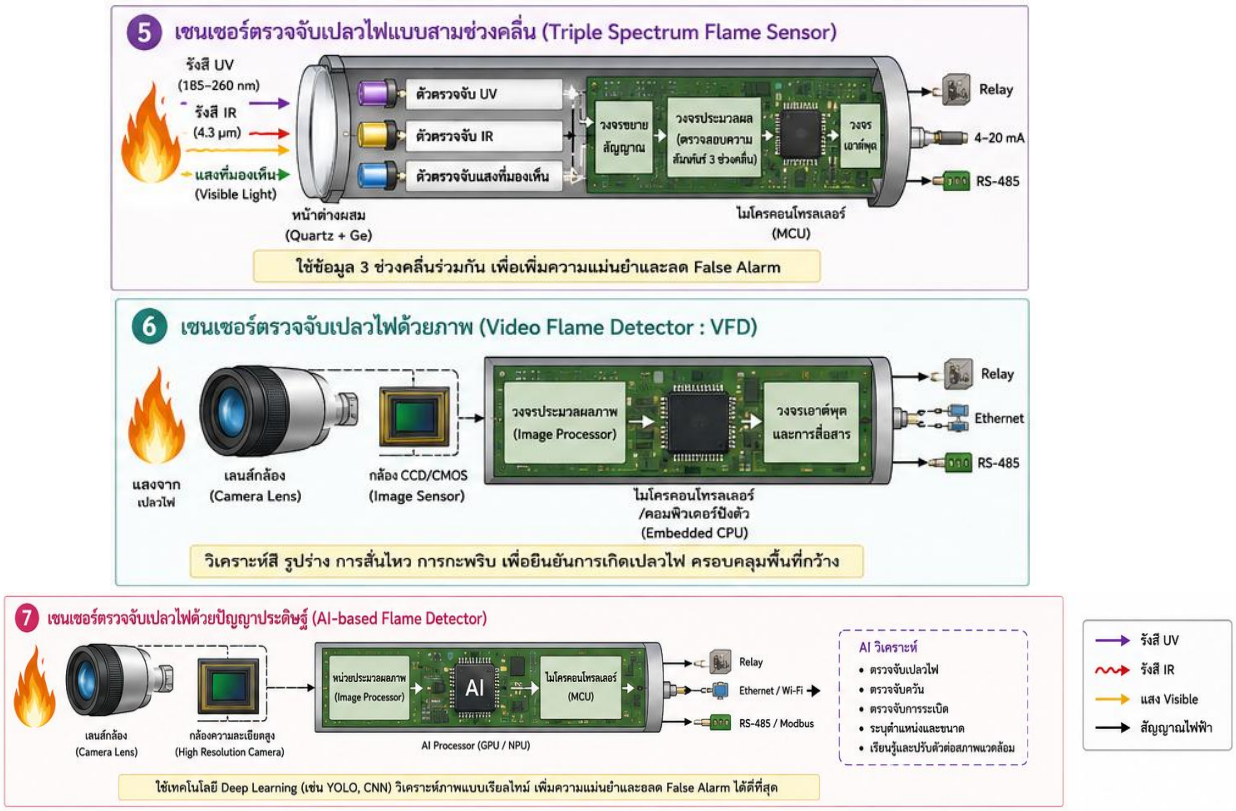
เซนเซอร์รุ่นใหม่จะใช้ไมโครคอนโทรลเลอร์หรือไมโครโปรเซสเซอร์ประมวลผลข้อมูลจากตัวตรวจจับรังสี และควบคุมการทำงานทั้งหมดของอุปกรณ์ เช่น การตรวจสอบสถานะเซนเซอร์ การวิเคราะห์สัญญาณ และการสื่อสารกับระบบแจ้งเหตุเพลิงไหม้ สำหรับเซนเซอร์อัจฉริยะบางรุ่นจะใช้เทคนิคปัญญาประดิษฐ์ เพื่อเพิ่มความแม่นยำในการตรวจจับเปลวไฟ (Zhang et al., 2023)

7) วงจรเอาต์พุตและการสื่อสาร (Output and Communication Interface)

เมื่อระบบประมวลผลยืนยันว่ามีการเกิดเปลวไฟ วงจรเอาต์พุตจะส่งสัญญาณแจ้งเตือนไปยังอุปกรณ์ภายนอก เช่น รีเลย์ ระบบแจ้งเหตุเพลิงไหม้ (Fire Alarm Control Panel: FACP) หรือระบบควบคุมอาคาร (Building Management System: BMS) โดยอาจรองรับเอาต์พุตหลายรูปแบบ เช่น รีเลย์คอนแทกต์ (relay contact), 4–20 mA, RS-485 หรือ Modbus เพื่อให้สามารถเชื่อมต่อกับระบบควบคุมและระบบเฝ้าระวังในโรงงานอุตสาหกรรมได้ (Xiao et al., 2020)

โครงสร้างของเซนเซอร์ตรวจจับเปลวไฟประกอบด้วย ตัวเรือนเซนเซอร์ หน้าต่างรับรังสี ตัวตรวจจับรังสี วงจรขยายสัญญาณ วงจรประมวลผล ไมโครคอนโทรลเลอร์ และวงจรเอาต์พุต ซึ่งทำงานร่วมกันเพื่อรับรังสีจากเปลวไฟ วิเคราะห์สัญญาณ และส่งสัญญาณแจ้งเตือนเมื่อเกิดเพลิงไหม้ (Xiao et al., 2020; Bordbar et al., 2022; Wei et al., 2026)





รูปที่ 2.25 โครงสร้างของเซนเซอร์ตรวจจับเปลวไฟแต่ละชนิด

2.6.4 หลักการทำงานของเซนเซอร์ตรวจจับเปลวไฟ (Flame Sensors Operating Principle)

1) หลักการทำงานของเซ็นเซอร์อินฟราเรดในการตรวจจับเปลวไฟ (Infrared Flame Sensor Operating Principle)

เซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด (infrared flame sensor/IR flame detector) ทำงานโดยอาศัยหลักการตรวจจับรังสีอินฟราเรดที่แผ่ออกมาจากเปลวไฟ ซึ่งเกิดขึ้นในระหว่างกระบวนการเผาไหม้ของเชื้อเพลิง โดยเฉพาะเชื้อเพลิงประเภทไฮโดรคาร์บอน (hydrocarbon fuels) ที่จะปล่อยพลังงานอินฟราเรดออกมาอย่างเด่นชัดบริเวณช่วงความยาวคลื่นประมาณ 4.3–4.5 μm ซึ่งเป็นช่วงการแผ่รังสีของก๊าซคาร์บอนไดออกไซด์ (CO_2 emission band) ที่เกิดขึ้นจากการเผาไหม้ (Hosch, 2020) หลักการทำงานของเซ็นเซอร์อินฟราเรดดังนี้

1.1) การรับรังสีอินฟราเรดจากเปลวไฟ (Incident Infrared Radiation)

เมื่อเกิดเปลวไฟ รังสีอินฟราเรดที่มีความยาวคลื่นประมาณ 4.45 μm จะเดินทางเข้าสู่เซนเซอร์พร้อมกับรังสีอินฟราเรดจากแหล่งกำเนิดความร้อนอื่นในสภาพแวดล้อม อย่างไรก็ตาม เซนเซอร์ได้รับการออกแบบให้ตอบสนองเฉพาะช่วงคลื่นที่เป็นลักษณะเฉพาะของการเผาไหม้ จึงช่วยลดผลกระทบจากแหล่งรบกวนภายนอก (Hosch, 2020)

1.2) การคัดเลือกช่วงความยาวคลื่นด้วยตัวกรองแสง (Optical Bandpass Filter)

รังสีอินฟราเรดที่เข้าสู่เซนเซอร์จะผ่าน ตัวกรองแสงแบบแบนด์พาส (optical bandpass filter) ซึ่งทำหน้าที่คัดเลือกเฉพาะช่วงความยาวคลื่นประมาณ 4.2–4.8 μm โดยมีค่า

กลาง (center wavelength) ประมาณ 4.45 μm ทำให้รังสีจากแหล่งกำเนิดอื่นที่อยู่นอกช่วงดังกล่าวถูกกรองออก ส่งผลให้เซนเซอร์มีความจำเพาะต่อเปลวไฟของเชื้อเพลิงไฮโดรคาร์บอนมากขึ้น (Hosch, 2020)

1.3) การแปลงรังสีเป็นสัญญาณไฟฟ้า (Pyroelectric Infrared Sensor)

หลังผ่านตัวกรองแสง รังสีอินฟราเรดจะตกกระทบบน เซนเซอร์ไพโรอิเล็กทริก (pyroelectric infrared sensor) ซึ่งทำหน้าที่แปลงการเปลี่ยนแปลงของพลังงานรังสีอินฟราเรดให้เป็นสัญญาณไฟฟ้า เซนเซอร์ชนิดนี้ตอบสนองต่อการเปลี่ยนแปลงของพลังงานรังสี จึงเหมาะสำหรับการตรวจจับเปลวไฟที่มีการกะพริบตามธรรมชาติ

1.4) การกรองสัญญาณการกะพริบของเปลวไฟ (Flicker Filter Circuit)

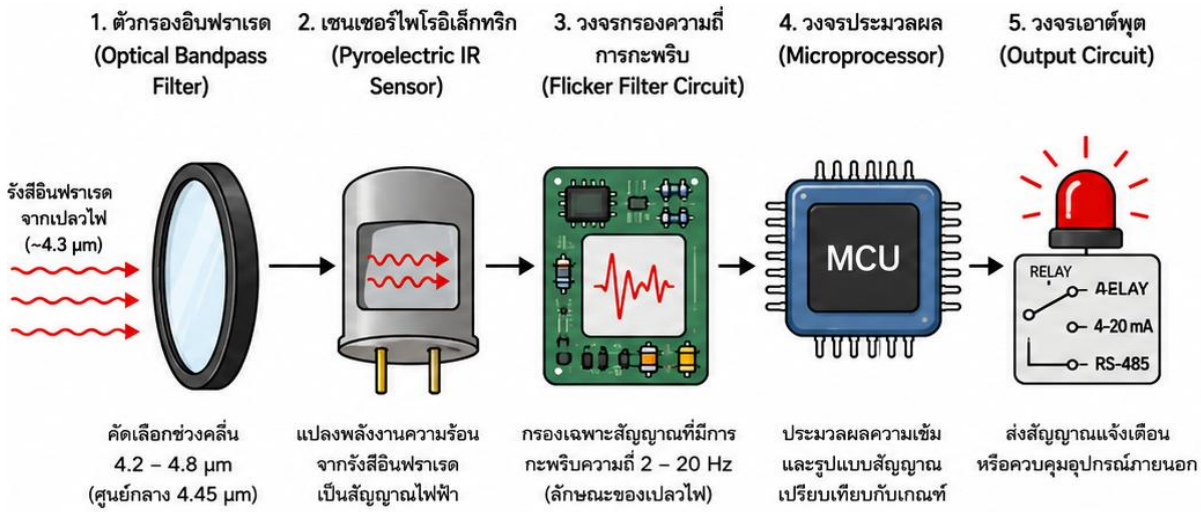
สัญญาณไฟฟ้าที่ได้จะถูกส่งเข้าสู่วงจร flicker filter หรือวงจรกรองความถี่ ซึ่งทำหน้าที่แยกสัญญาณการกะพริบของเปลวไฟ ที่มีความถี่โดยทั่วไปประมาณ 2–20 Hz ออกจากรังสีอินฟราเรดคงที่ (steady-state infrared) ที่เกิดจากแสงอาทิตย์ เครื่องจักร หรือพื้นผิวที่มีอุณหภูมิสูง จึงช่วยลดการแจ้งเตือนผิดพลาด (false alarm) ได้อย่างมีประสิทธิภาพ (Hosch, 2020)

1.5) การประมวลผลสัญญาณ (Signal Processing)

สัญญาณที่ผ่านการกรองจะถูกส่งเข้าสู่หน่วยประมวลผล ซึ่งประกอบด้วยวงจรแปลงสัญญาณแอนะล็อกเป็นดิจิทัล (A/D converter) และอัลกอริทึมวิเคราะห์สัญญาณ เพื่อประเมินความเข้มของรังสี รูปแบบการกะพริบ และระยะเวลาที่ตรวจพบ หากข้อมูลตรงตามเกณฑ์ที่กำหนด ระบบจะยืนยันการเกิดเปลวไฟ

1.6) การส่งสัญญาณแจ้งเตือน (Output Circuit)

เมื่อระบบยืนยันว่ามีเปลวไฟจริง วงจรเอาต์พุตจะส่งสัญญาณไปยังระบบแจ้งเหตุเพลิงไหม้หรือระบบควบคุมภายนอก เช่น รีเลย์ เอาต์พุตแบบ 4–20 mA, RS-485 หรือ Modbus พร้อมทั้งแสดงสถานะการทำงานผ่านไฟแสดงผล LED เพื่อแจ้งเตือนผู้ปฏิบัติงานและสั่งงานระบบป้องกันอัคคีภัยต่อไป



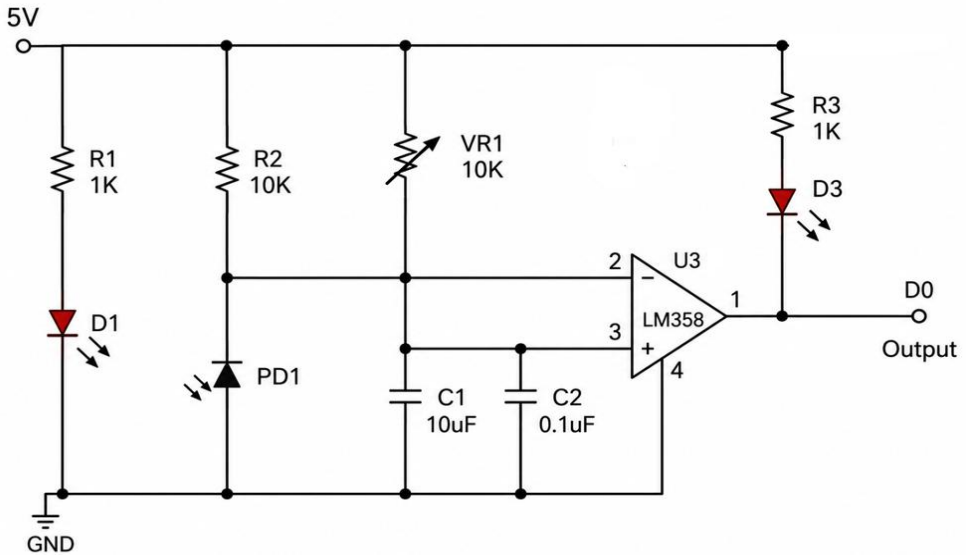
รูปที่ 2.26 หลักการทำงานของเซนเซอร์ตรวจจับเปลวไฟ

โดยสรุปเซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรดอาศัยการตรวจจับรังสีอินฟราเรดในช่วงความยาวคลื่นที่เป็นลักษณะเฉพาะของการเผาไหม้ ร่วมกับการวิเคราะห์ความถี่การกะพริบของเปลวไฟและการประมวลผลสัญญาณดิจิทัล ทำให้สามารถตรวจจับเปลวไฟได้อย่างรวดเร็ว มีความแม่นยำสูง และลดโอกาสการแจ้งเตือนผิดพลาดจากแหล่งกำเนิดความร้อนทั่วไปได้อย่างมีประสิทธิภาพ (Hosch, 2020)

2.6.4 วงจรประยุกต์ใช้งานเซนเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด

1) วงจรเซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด

วงจรเซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรดเป็นวงจรตรวจจับรังสีอินฟราเรดที่แผ่ออกมาจากเปลวไฟ และแปลงเป็นสัญญาณดิจิทัลเพื่อใช้ควบคุมไมโครคอนโทรลเลอร์หรือระบบแจ้งเตือน โดยภายในโมดูลประกอบด้วยตัวรับรังสีอินฟราเรด (PD1) วงจรเปรียบเทียบแรงดัน (comparator) ซึ่งใช้ไอซี LM358 หรือ LM393 ตัวต้านทาน ตัวเก็บประจุ และตัวปรับค่าความไว (VR1) เพื่อกำหนดระดับการตรวจจับเปลวไฟ ดังแสดงในรูปที่ 2.27



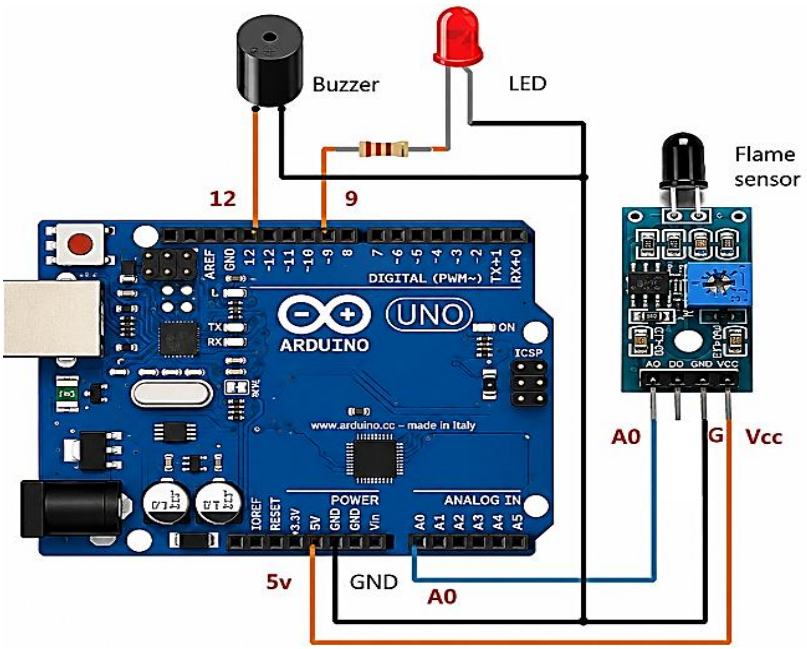
รูปที่ 2.27 วงจรเซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด

หลักการทำงานของวงจร เมื่อวงจรได้รับแรงดันไฟเลี้ยง 5 VDC ตัวต้านทาน R1 ทำหน้าที่จำกัดกระแสให้กับไดโอดแสดงสถานะ D1 (power LED) เพื่อแสดงว่ามีการจ่ายไฟเข้าสู่วงจรเรียบร้อยแล้ว ส่วน PD1 (infrared photodiode) ทำหน้าที่รับรังสีอินฟราเรดจากเปลวไฟ ซึ่งโดยทั่วไปเปลวไฟของเชื้อเพลิงไฮโดรคาร์บอนจะปล่อยรังสีอินฟราเรดในช่วงประมาณ 760–1100 ηm สำหรับโมดูลตรวจจับเปลวไฟทั่วไป เมื่อปริมาณรังสีอินฟราเรดที่ตกกระทบเพิ่มขึ้น กระแสโฟโตอิเล็กทริก (photocurrent) ของโฟโตไดโอดจะเปลี่ยนแปลง ส่งผลให้แรงดันไฟฟ้าที่จุดตรวจวัดเปลี่ยนแปลงตามไปด้วย

แรงดันจากโฟโตไดโอดจะถูกส่งเข้าสู่ขาอินพุตของวงจรเปรียบเทียบแรงดัน LM358 (U3) โดยแรงดันอ้างอิง (reference voltage) ถูกกำหนดจากตัวต้านทานปรับค่า VR1 ซึ่งผู้ใช้งานสามารถปรับระดับความไวของการตรวจจับได้ตามความเหมาะสม หากแรงดันจากโฟโตไดโอดสูงหรือต่ำกว่าค่าอ้างอิงที่กำหนด (ขึ้นอยู่กับการต่อวงจรของผู้ผลิต) วงจรเปรียบเทียบจะเปลี่ยนสถานะของเอาต์พุตทันที ตัวเก็บประจุ C1 (10 μF) และ C2 (0.1 μF) ทำหน้าที่กรองสัญญาณรบกวนและลดการแกว่งของแรงดันไฟฟ้า (noise filtering) ทำให้การตรวจจับมีความเสถียรมากขึ้นและลดการทำงานผิดพลาดจากสัญญาณรบกวนภายนอก เมื่อวงจรตรวจพบเปลวไฟ เอาต์พุต DO (digital output) จะเปลี่ยนสถานะเป็นลอจิก HIGH หรือ LOW ตามรูปแบบการออกแบบของโมดูลแต่ละรุ่น ซึ่งสามารถนำไปเชื่อมต่อกับไมโครคอนโทรลเลอร์ เช่น Arduino หรือ ESP8266 เพื่อควบคุมการแจ้งเตือน การสั่งงานรีเลย์ หรือระบบดับเพลิงอัตโนมัติ พร้อมกันนั้น D3 (output LED) จะติดสว่างเพื่อแสดงสถานะว่ามีการตรวจพบเปลวไฟ ทำให้ผู้ใช้งานสามารถตรวจสอบการทำงานของเซ็นเซอร์ได้โดยตรง

2) วงจรเซนเซอร์ตรวจจับเปลวไฟร่วมกับ Arduino UNO เพื่อการแจ้งเตือน

วงจรนี้ใช้ Arduino UNO เป็นหน่วยประมวลผลหลัก โดยเชื่อมต่อกับโมดูลเซนเซอร์ตรวจจับเปลวไฟ (flame sensor module) พร้อมอุปกรณ์แจ้งเตือน ได้แก่ LED และ buzzer เพื่อแจ้งเตือนเมื่อมีการตรวจพบเปลวไฟ การเชื่อมต่ออุปกรณ์มีรายละเอียดดังนี้



รูปที่ 2.28 วงจรเซนเซอร์ตรวจจับเปลวไฟร่วมกับ Arduino UNO เพื่อการแจ้งเตือน

2.1) ขา VCC ของโมดูลเซนเซอร์ต่อเข้ากับขา 5 V ของ Arduino UNO เพื่อจ่ายแรงดันไฟเลี้ยงให้กับโมดูล

2.2) ขา GND ของเซนเซอร์ต่อเข้ากับ GND ของ Arduino เพื่อใช้เป็นกราวด์ร่วม

2.3) ขา A0 (analog output) ของเซนเซอร์ต่อเข้ากับขา A0 ของ Arduino สำหรับอ่านค่าแรงดันแอนะล็อกจากเซนเซอร์

2.4) ขา Digital 12 (D12) ของ Arduino Uno ต่อเข้ากับขั้วบวกของ buzzer เพื่อใช้เป็นสัญญาณควบคุมการส่งเสียงเตือน

2.5) ขา Digital 9 (D9) ต่อเข้ากับขั้วบวกของ LED เพื่อใช้แสดงสถานะการตรวจพบเปลวไฟ ส่วนขั้วลบของ LED และ buzzer ต่อร่วมกับกราวด์ (GND)

หลักการทำงานของวงจร เมื่อระบบเริ่มทำงาน Arduino Uno จะจ่ายแรงดันไฟ 5 VDC ให้กับโมดูลเซนเซอร์ตรวจจับเปลวไฟ จากนั้นเซนเซอร์จะตรวจจับรังสีอินฟราเรดที่แผ่ออกมาจากเปลวไฟ หากไม่มีเปลวไฟ ค่าที่ส่งออกจากขา A0 จะอยู่ในช่วงค่าปกติ ซึ่ง Arduino จะอ่านค่าแรงดันดังกล่าวผ่านตัวแปลงสัญญาณแอนะล็อกเป็นดิจิทัล (Analog-to-Digital Converter: ADC) ภายในไมโครคอนโทรลเลอร์ โดยเมื่อเกิดเปลวไฟ รังสีอินฟราเรดจะตกกระทบตัวรับรังสีภายในเซนเซอร์ ทำให้แรงดันไฟฟ้าขา A0 เปลี่ยนแปลง Arduino จะอ่านค่าดังกล่าวและนำไปเปรียบเทียบกับค่าระดับอ้างอิง (threshold) ที่กำหนดไว้ในโปรแกรม หากค่าที่อ่านได้เกินหรืออยู่ต่ำกว่าค่าที่กำหนด (ขึ้นอยู่กับลักษณะการตอบสนองของโมดูลเซนเซอร์ที่ใช้) Arduino จะสั่งให้ขา D9 อยู่ในสถานะ HIGH เพื่อให้ LED ติดสว่าง และสั่งให้ขา D12 อยู่ในสถานะ HIGH เพื่อให้ Buzzer ส่งเสียงแจ้งเตือนผู้ใช้งานว่ามีการตรวจพบเปลวไฟ เมื่อไม่พบเปลวไฟ ค่าที่อ่านจากเซนเซอร์จะกลับเข้าสู่ช่วงปกติ Arduino จะปิดการทำงานของ LED และ buzzer ทำให้ระบบกลับเข้าสู่สถานะเฝ้าระวังพร้อมตรวจจับเหตุการณ์ต่อไป

บรรณานุกรมบทที่ 2

Al-Qutayri, M. (Ed.). (2010). *Smart Home Systems*. InTech. https://doi.org/10.5772/182.

Austin. (2026). *AI Vision Flame & Combustion Monitoring*. https://ifactoryapp.com/ai-vision-camera/ai-vision-flame-burner-combustion-monitoring.

Bentley, J. P. (2005). *Principles of measurement systems* (4th ed.). Pearson Education.

Bordbar, H., Alinejad, F., Conley, K., Ala-Nissila, T., & Hostikka, S. (2022). Flame detection by heat from the infrared spectrum: Optimization and sensitivity analysis. *Fire Safety Journal*, *133*,103673. https://doi.org/10.1016/j.firesaf.2022.103673.

Carletti, V., Greco, A., Saggese, A., & Vento, B. (2024). A smart visual sensor for smoke detection based on deep neural networks. *Sensors, 24*(14), 4519. https://doi.org/10.3390/s24144519.

Crescentini, M., Syeda, S. F., & Gibiino, G. P. (2022). Hall-Effect Current Sensors: Principles of Operation and Implementation Techniques. *IEEE Sensors Journal*, *22*(11), 10137-10151. https://doi.org/10.1109/JSEN.2021.3119766.

Dempsey, B. (2022). *Door and window sensor evaluation platform: Introduction and performance overview.* Texas Instruments, Dallas, Texas, USA. https://www.ti.com/lit/an/slya073/slya073.pdf?ts=1788623804972&ref_url=https%253A%252F%252Fwww.google.com%252F.

Elhanashi, A., Essahraui, S., Dini, P., & Saponara, S. (2025). Early fire and smoke detection using deep learning: A comprehensive review of models, datasets, and challenges. *Applied Sciences, 15*(18), 10255. https://doi.org/10.3390/app151810255.

Gagote, E. O., Gapol, K. J. D., Murillo, S. K. G., Velasquez, H. U., & Fabro, M. N. (2026). Autolight: Smart motion detection lighting system (Passive Infrared Sensor). *International Journal of Research and Scientific Innovation, 13*(1). https://doi.org/10.51244/IJRSI.2026.13010052.

Hosch, M. J. (2020). *Ultra-high-speed optical flame detection and releasing system solutions*. Det-Tronics. https://www.det-tronics.com/wp-content/uploads/sites/8/2025/04/HSDM-technical-paper-86-1000-1.1.pdf.

Hwang, W. Y., Lee, H. J., Jin, J., Ryou, H. S., Choi, C. K., Hong, S. H., & Lee, S. H. (2024). Computational design of a smoke detector with high sensitivity considering three-dimensional flow characteristics. *Case Studies in Thermal Engineering, 53*, 103896. https://doi.org/10.1016/j.csite.2023.103896.

Ismail, Y. (Ed.). (2019). *Internet of Things (IoT) for automated and smart applications*. IntechOpen. https://doi.org/10.5772/intechopen.90022.

Kadum, I. A., Hassan, A. S., & Altimimy, A. H. (2018). Computer-based intruder detection alarm system. *Iraqi Journal of Information Technology, 8*(3), 97–108.

Kumar, R. (2024). *Enhancing home security: Mechanisms of ionization smoke detectors*. OEMSecrets. https://www.oemsecrets.com/articles/enhancing-home-security-mechanisms-of-ionization-smoke-detectors.

Kuznetsov, G., Kopylov, N., Sushkina, E., & Zhdanova, A. (2022). Adaptation of fire-fighting systems to localization of fires in the premises: Review. *Energies, 15*(2), 522. https://doi.org/10.3390/en15020522.

Leslie, L. (2024, April 4). *What is the wireless door & window sensor, and how does it work?* Disruptive Technologies. https://www.disruptive-technologies.com/explore/what-is-the-wireless-door-and-window-sensor-and-how-does-it-work.

Nagpal, R., Ababii, N., & Lupan, O. (2025). Comprehensive advances in gas sensing: Mechanisms, material innovations, and applications in environmental and health monitoring. *Materials Today Electronics, 15*, 100192. https://doi.org/10.1016/j.mtelec.2025.100192.

National Fire Protection Association. (2022). *NFPA 72: National Fire Alarm and Signaling Code*. NFPA.

Pawar, Y., Chopde, A., & Nandre, M. (2018). Motion detection using PIR sensor. *International Research Journal of Engineering and Technology (IRJET), 5*(4), *4753–4756.*

Sahasika, M. P., Pratiwi, D., & Santoso, G. B. (2023). Visualization of home security sensor system based on IoT server. *Qeios, Preprint*, 1-19. https://doi.org/10.32388/ZC810D.

Selvolini, G., & Marrazza, G. (2023). *Sensor principles and basic designs*. In A. Barhoum & Z. Altintas (Eds.), Fundamentals of sensor technology (pp. 17–43). Woodhead Publishing. https://doi.org/10.1016/B978-0-323-88431-0.00018-1.

System Sensor Europe. (2011). *Beam detection systems: Application guide*. Pittway Tecnologica S.r.l. https://www.systemsensoreurope.com/wp-content/uploads/2019/12/Beam_application_guide_compressed.pd.

Thu, M. M., Swe, S. S., & Zaw, T. T. (2020). Security system with PIR sensor. *IRE Journals, 4*(6), 77–88.

Vega-Luna, J. I., Sánchez-Rangel, F. J., & Cosme-Aceves, J. F. (2019). Monitoring system for doors and windows of a data center with IoT. *Ingenius: Revista de Cienciay Tecnología, 22*, 43–53. https://doi.org/10.17163/ings.n22.2019.07.

Wang, Z., Li, B., Wang, L., Cao, Z., & Zhang, X. (2025). Dual-GRU perception accumulation model for linear beam smoke detector. *Fire, 8*(6), 229. https://doi.org/10.3390/fire8060229.

Wei, J., Ma, G., Liang, R., Wang, W., Chen, J., Guan, S., Jiang, J., Zhu, X., Cheng, Q., Shen, Y., Xia, Q., Wu, S., Wan, H., Zeng, L., Li, M., Wang, Y., Shen, L., Han, W., & Wang, H. (2026). Ferroelectric optoelectronic sensor for intelligent flame detection and in-sensor motion perception. *Nano-Micro Letters, 18*, 123. https://doi.org/10.1007/s40820-025-01968-x.

Wu, Q., Ding, Z., & Zhang, W. (2025). Research progress on electrochemical gas sensors for fire detection. *International Journal of Electrochemical Science, 20*, 101043. https://doi.org/10.1016/j.ijoes.2025.101043.

Xiao, G., Weng, H., Ge, L., & Huang, Q. (2020). Application status of carbon nanotubes in fire detection sensors. *Frontiers in Materials, 7*, 588521. https://doi.org/10.3389/fmats.2020.588521.

Yunusa, Z., Hamidon, M. N., Kaiser, A., & Awang, Z. (2014). Gas sensors: A review. *Sensors & Transducers, 168*(4), 61–75.

Zhang, J., Shi, B., Chen, B., Chen, H., & Xu, W. (2023). A real-time flame detection method using deformable object detection and time sequence analysis. *Sensors, 23*(20), 8616. https://doi.org/10.3390/s23208616.

สรุปสาระสำคัญของบทที่ 2
อุปกรณ์เซนเซอร์สำหรับระบบรักษาความปลอดภัย

หลักการพื้นฐานของเซ็นเซอร์ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ ตั้งแต่หลักการทำงาน การแปลงสัญญาณ คุณลักษณะสำคัญของเซ็นเซอร์ ตลอดจนโครงสร้าง หลักการทำงาน และการประยุกต์ใช้งานของเซ็นเซอร์ชนิดต่าง ๆ ที่นิยมใช้ในระบบ smart security โดยเน้นการประยุกต์ใช้งานทั้งในระบบป้องกันการบุกรุก ระบบแจ้งเหตุเพลิงไหม้ และระบบ Internet of Things (IoT) เพื่อเพิ่มประสิทธิภาพในการตรวจจับและแจ้งเตือนแบบอัตโนมัติ

เซ็นเซอร์ (sensor) เป็นอุปกรณ์ที่ทำหน้าที่ตรวจจับการเปลี่ยนแปลงของปริมาณทางกายภาพ ทางเคมี หรือทางชีวภาพ แล้วแปลงข้อมูลดังกล่าวให้เป็นสัญญาณไฟฟ้าเพื่อส่งเข้าสู่ระบบประมวลผล การทำงานของเซ็นเซอร์ประกอบด้วย 3 ขั้นตอนหลัก ได้แก่ การตรวจจับ (detection) การแปลงสัญญาณ (transduction) และการปรับสภาพสัญญาณ (signal conditioning) นอกจากนี้ยังอธิบายหลักการแปลงสัญญาณของเซ็นเซอร์ประเภทต่าง ๆ เช่น เซ็นเซอร์แบบความต้านทาน แบบความจุไฟฟ้า แบบเพียโซอิเล็กทริก และแบบออปติคัล รวมถึงการจำแนกเซ็นเซอร์ตามแหล่งพลังงานเป็น active sensor และ passive sensor พร้อมทั้งอธิบายสมรรถนะที่สำคัญ ได้แก่ ความไว (sensitivity) ความละเอียด (resolution) ความถูกต้อง (accuracy) และช่วงการวัด (dynamic range) ซึ่งเป็นปัจจัยสำคัญในการเลือกใช้งานเซ็นเซอร์ให้เหมาะสมกับลักษณะงาน

เซ็นเซอร์ตรวจจับการเคลื่อนไหว (Motion Sensor)

โดยมุ่งเน้นเซ็นเซอร์อินฟราเรดแบบพาสซีฟ (Passive Infrared: PIR) ซึ่งทำงานโดยตรวจจับการเปลี่ยนแปลงของรังสีอินฟราเรดที่แผ่ออกมาจากร่างกายมนุษย์หรือวัตถุที่มีอุณหภูมิแตกต่างจากสภาพแวดล้อม พร้อมอธิบายโครงสร้างภายใน หลักการตรวจจับด้วยวัสดุไพโรอิเล็กทริก (pyroelectric material) บทบาทของเลนส์เฟรสเนล (Fresnel lens) ปัจจัยที่มีผลต่อประสิทธิภาพการตรวจจับ ตัวอย่างวงจรการประยุกต์ใช้งานร่วมกับรีเลย์และไมโครคอนโทรลเลอร์ Arduino เพื่อควบคุมอุปกรณ์แจ้งเตือนหรือระบบอัตโนมัติในอาคารอัจฉริยะ

เซ็นเซอร์ตรวจจับประตูและหน้าต่าง (Door and Window Sensor)

หลักการตรวจจับการเปิด–ปิดด้วยสนามแม่เหล็ก พร้อมเปรียบเทียบการทำงานของสวิตช์แม่เหล็ก (reed switch) และ Hall effect sensor โดยอธิบายโครงสร้าง จุดเด่น ข้อจำกัด และหลักการตรวจจับสนามแม่เหล็กของแต่ละชนิด รวมทั้งแนวทางการเลือกใช้งานในระบบรักษาความปลอดภัย ซึ่ง Hall effect sensor มีข้อได้เปรียบด้านความทนทาน ไม่มีหน้าสัมผัสเชิงกล อายุการใช้งานยาวนาน และตอบสนองได้รวดเร็ว ขณะที่ reed switch มีโครงสร้างเรียบง่าย ราคาประหยัด และนิยมใช้ในงานตรวจจับการเปิด–ปิดประตูและหน้าต่างทั่วไป

เซ็นเซอร์ตรวจจับควัน (Smoke Sensor)

เซ็นเซอร์แบบโฟโตอิเล็กทริก (photoelectric smoke detector) ซึ่งอาศัยหลักการกระเจิงของแสง (light scattering) และเซ็นเซอร์แบบไอออไนเซชัน (ionization smoke detector) ที่ตรวจจับการเปลี่ยนแปลงของกระแสไฟฟ้าภายในห้องไอออไนเซชันเมื่อมีอนุภาคควันเข้าสู่ห้องตรวจจับ นอกจากนี้ยังอธิบายเซ็นเซอร์ตรวจจับควันแบบลำแสง (beam smoke detector) ซึ่งเหมาะสำหรับพื้นที่ขนาดใหญ่ โดยใช้ลำแสงอินฟราเรดตรวจสอบการลดลงของความเข้มแสงจากการบดบังของควัน พร้อมอธิบายองค์ประกอบของระบบและการเชื่อมต่อเข้ากับแผงควบคุมระบบแจ้งเหตุเพลิงไหม้

เซ็นเซอร์ตรวจจับก๊าซ (Gas Sensor)

โครงสร้างของเซ็นเซอร์แบบโลหะออกไซด์ (Metal Oxide Semiconductor: MOS) และเซ็นเซอร์แบบไฟฟ้าเคมี (electrochemical gas sensor) ซึ่งประกอบด้วยส่วนตรวจจับ ตัวแปลงสัญญาณ และวงจรปรับสภาพสัญญาณ พร้อมอธิบายหลักการเกิดปฏิกิริยาเคมีที่ผิวอิเล็กโทรด การประมวลผลสัญญาณ และการประยุกต์ใช้ในการตรวจจับก๊าซรั่วไหล ระบบแจ้งเหตุเพลิงไหม้ และระบบเฝ้าระวังคุณภาพอากาศร่วมกับเทคโนโลยี IoT

เซ็นเซอร์ตรวจจับเปลวไฟ (Flame Sensor)

เซ็นเซอร์ตรวจจับเปลวไฟแบบอินฟราเรด (IR flame detector) โดยอธิบายหลักการตรวจจับรังสีอินฟราเรดที่แผ่ออกมาจากเปลวไฟในช่วงความยาวคลื่นเฉพาะ การประมวลผลรูปแบบการกะพริบของเปลวไฟ การกรองสัญญาณรบกวน และการส่งสัญญาณแจ้งเตือนไปยังระบบควบคุม เพื่อให้สามารถตรวจจับเหตุเพลิงไหม้ได้อย่างรวดเร็วและลดการแจ้งเตือนผิดพลาด

โดยสรุป เซ็นเซอร์เป็นองค์ประกอบพื้นฐานของระบบรักษาความปลอดภัยอัจฉริยะ ทุกชนิดมีหลักการทำงาน โครงสร้าง และคุณสมบัติที่แตกต่างกัน การเลือกใช้เซ็นเซอร์ให้เหมาะสมกับลักษณะงานจะช่วยเพิ่มความแม่นยำในการตรวจจับ ลดความผิดพลาดในการแจ้งเตือน และยกระดับประสิทธิภาพของระบบ smart security, smart home และระบบ IoT ให้สามารถเฝ้าระวัง วิเคราะห์ และตอบสนองต่อเหตุการณ์ต่าง ๆ ได้อย่างรวดเร็ว มีความน่าเชื่อถือ และรองรับการพัฒนาไปสู่ระบบอัจฉริยะในอนาคต

แบบฝึกหัดท้ายบทที่ 2
อุปกรณ์เซนเซอร์สำหรับระบบรักษาความปลอดภัย

ตอนที่ 1 เลือกตอบ

คำสั่ง จงเลือกคำตอบที่ถูกต้องที่สุด

1. ข้อใดอธิบายหน้าที่ของเซ็นเซอร์ได้ถูกต้องที่สุด
   ก. แปลงพลังงานไฟฟ้าเป็นพลังงานกล
   ข. ตรวจจับการเปลี่ยนแปลงของสิ่งแวดล้อมและแปลงเป็นสัญญาณไฟฟ้า
   ค. เพิ่มแรงดันไฟฟ้าให้วงจร
   ง. เก็บข้อมูลลงฐานข้อมูล
2. ขั้นตอนแรกของการทำงานของเซ็นเซอร์คือข้อใด
   ก. Signal Conditioning
   ข. Detection
   ค. Amplification
   ง. Analog-to-Digital Conversion
3. เซ็นเซอร์แบบใดต้องอาศัยแหล่งจ่ายไฟภายนอกในการทำงาน
   ก. Active Sensor
   ข. Passive Sensor
   ค. Piezoelectric Sensor
   ง. Thermocouple
4. ค่าใดใช้บอกความสามารถของเซ็นเซอร์ในการตรวจจับการเปลี่ยนแปลงเพียงเล็กน้อย
   ก. Accuracy
   ข. Resolution
   ค. Sensitivity
   ง. Dynamic Range
5. เซ็นเซอร์ PIR ตรวจจับสิ่งใด
   ก. เสียง
   ข. สนามแม่เหล็ก
   ค. การเปลี่ยนแปลงของรังสีอินฟราเรด
   ง. ความชื้น
6. เลนส์ Fresnel ของเซ็นเซอร์ PIR มีหน้าที่หลักคือข้อใด
   ก. ขยายแรงดันไฟฟ้า
   ข. รวมและกระจายรังสีอินฟราเรดเข้าสู่เซ็นเซอร์
   ค. ลดแรงดันไฟฟ้า
   ง. ควบคุมเวลา Delay
7. เมื่อ PIR ตรวจพบการเคลื่อนไหว ขา OUT จะเป็นระดับใด
   ก. LOW
   ข. Floating
   ค. HIGH
   ง. Ground
8. ไดโอด 1N4007 ที่ต่อคร่อมรีเลย์ในวงจร PIR มีหน้าที่อะไร
   ก. เพิ่มแรงดันไฟฟ้า
   ข. ป้องกันแรงดันย้อนกลับ (Back EMF)
   ค. เพิ่มกระแส
   ง. ลดสัญญาณรบกวนจากเซ็นเซอร์
9. เซ็นเซอร์ตรวจจับประตูและหน้าต่างทั่วไปใช้หลักการใด
   ก. อัลตราโซนิก
   ข. สนามแม่เหล็ก
   ค. คลื่นไมโครเวฟ
   ง. คลื่นวิทยุ
10. Reed Switch จะเปลี่ยนสถานะเมื่อ
   ก. มีแสงตกกระทบ
   ข. มีควัน
   ค. สนามแม่เหล็กเข้าใกล้
   ง. อุณหภูมิสูงขึ้น

11. Hall Effect Sensor ตรวจจับสิ่งใด

ก. แสง

ข. สนามแม่เหล็ก

ค. เสียง

ง. ความชื้น

12. เซ็นเซอร์ตรวจจับควันแบบ Photoelectric เหมาะสำหรับตรวจจับ

ก. ควันจากการลุกไหม้แบบคุกรุ่น

ข. ก๊าซ LPG

ค. ความร้อน

ง. สนามแม่เหล็ก

13. เซ็นเซอร์ตรวจจับควันแบบ Ionization มีความไวต่อ

ก. ควันจากการเผาไหม้ที่มีเปลวไฟ

ข. ความชื้น

ค. การเคลื่อนไหว

ง. ก๊าซพิษ

14. MQ-2 เป็นเซ็นเซอร์ตรวจจับ

ก. เปลวไฟ

ข. ก๊าซไวไฟและควัน

ค. ความเร่ง

ง. สนามแม่เหล็ก

15. เซ็นเซอร์ตรวจจับเปลวไฟแบบ IR ตรวจจับรังสีชนิดใด

ก. Ultraviolet

ข. Infrared

ค. Microwave

ง. X-ray

16. Flame Sensor แบบ UV/IR มีข้อดีเหนือแบบเดี่ยวคือข้อใด

ก. ใช้พลังงานน้อยกว่าเสมอ

ข. ลดการแจ้งเตือนผิดพลาด (False Alarm)

ค. ไม่ต้องใช้วงจรประมวลผล

ง. ตรวจจับได้เฉพาะในที่มืด

17. ข้อใดเป็นตัวอย่างการประยุกต์ใช้ PIR Sensor

ก. ระบบเปิดไฟอัตโนมัติ

ข. เครื่องวัดอุณหภูมิ

ค. เครื่องวัดแรงดัน

ง. เครื่องชั่งน้ำหนัก

18. ระบบ Smart Home นิยมใช้เซ็นเซอร์ชนิดใดในการตรวจจับการบุกรุก

ก. PIR และ Door Sensor

ข. pH Sensor

ค. Load Cell

ง. Flow Sensor

19. หากต้องการตรวจจับการรั่วไหลของก๊าซหุงต้ม ควรเลือกใช้เซ็นเซอร์ชนิดใด

ก. PIR

ข. MQ-2

ค. Reed Switch

ง. UV Flame Sensor

20. หากต้องการตรวจจับเปลวไฟในโรงงานอุตสาหกรรมที่มีแสงรบกวนสูง ควรเลือกใช้เซ็นเซอร์ชนิดใด

ก. UV

ข. IR

ค. Multi-IR หรือ Triple Spectrum

ง. PIR

ตอนที่ 2 จับคู่

คำสั่ง จงจับคู่ให้ถูกต้อง

ข้อ	เซ็นเซอร์	คำตอบ	ตัวเลือก
1	PIR Sensor	_____	ก. ตรวจจับสนามแม่เหล็กแบบไม่สัมผัส
2	Reed Switch	_____	ข. ตรวจจับการเคลื่อนไหวจากรังสีอินฟราเรด
3	Hall Effect Sensor	_____	ค. ตรวจจับก๊าซและควัน
4	MQ-2	_____	ง. ตรวจจับควันจากการกระเจิงของแสง
5	Photoelectric Smoke Detector	_____	จ. ตรวจจับควันจากการเปลี่ยนแปลงกระแสไอออน
6	Ionization Smoke Detector	_____	ฉ. ตรวจจับรังสีอัลตราไวโอเลตจากเปลวไฟ
7	UV Flame Detector	_____	ช. ตรวจจับรังสีอินฟราเรดจากเปลวไฟ
8	IR Flame Detector	_____	ซ. สวิตช์แม่เหล็กสำหรับประตูและหน้าต่าง

ตอนที่ 3 เติมคำ

คำสั่ง จงเติมคำให้ถูกต้อง

1. เซ็นเซอร์ทำหน้าที่ตรวจจับ _____
2. การทำงานของเซ็นเซอร์ประกอบด้วย _____, _____ และ _____
3. เซ็นเซอร์ PIR ย่อมาจาก _____
4. Reed Switch ทำงานร่วมกับ _____
5. MQ-2 ใช้ตรวจจับ _____
6. Photoelectric Smoke Detector ใช้หลักการ _____
7. Hall Effect Sensor ใช้ตรวจจับ _____
8. Flame Sensor แบบ UV ตรวจจับรังสี _____
9. เซ็นเซอร์ PIR ไม่ปล่อยคลื่นออกไปตรวจจับ จึงจัดเป็น _____ Sensor
10. ระบบ Smart Security มักเชื่อมต่อเซ็นเซอร์เข้ากับ _____ เพื่อประมวลผลข้อมูล

ตอนที่ 4 คำถามอธิบาย

1. อธิบายหลักการทำงานของเซ็นเซอร์ พร้อมอธิบายกระบวนการ Detection, Transduction และ Signal Conditioning

_____

_____

_____

_____

_____

2. อธิบายหลักการทำงานของเซ็นเซอร์ PIR พร้อมยกตัวอย่างการประยุกต์ใช้งานในระบบ Smart Home

_____

_____

_____

_____

_____

_____

_____

_____

_____

เปรียบเทียบ Reed Switch และ Hall Effect Sensor พร้อมอธิบายข้อดี ข้อจำกัด และการเลือกใช้งาน

_____

_____

_____

_____

_____

_____

_____

_____

_____

3. เปรียบเทียบเซ็นเซอร์ตรวจจับควันแบบ Photoelectric และ Ionization พร้อมยกตัวอย่างสถานการณ์ที่เหมาะสมในการใช้งาน

_____

_____

_____

_____

_____

_____

_____

_____

_____

4. อธิบายหลักการทำงานของ MQ-2 Gas Sensor และยกตัวอย่างการนำไปประยุกต์ใช้ในระบบรักษาความปลอดภัย

_____

_____

_____

_____

_____

_____

_____

_____

_____

5. เปรียบเทียบ Flame Sensor แบบ UV, IR, UV/IR และ Multi-IR พร้อมอธิบายข้อดีของแต่ละชนิด

_____

_____

_____

_____

_____

_____

_____

_____

_____

6. ออกแบบระบบ Smart Security สำหรับบ้านพักอาศัย โดยเลือกใช้เซ็นเซอร์อย่างน้อย 4 ชนิด พร้อมอธิบายเหตุผลในการเลือกใช้งาน

_____

_____

_____

_____

_____

_____

_____

_____

_____

3 ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

31

พื้นฐานของระบบกล้องโทรทัศน์วงจรปิด

3.1.1 ความหมายของกล้องโทรทัศน์วงจรปิด
3.1.2 ความเป็นมาของกล้องโทรทัศน์วงจรปิด
3.1.3 องค์ประกอบของระบบกล้องโทรทัศน์วงจรปิด
3.1.4 ระบบเครือข่ายคอมพิวเตอร์ในระบบกล้องวงจรปิด
3.1.5 มาตรฐาน Ingress Protection Rating
3.1.6 หน่วยวัดความละเอียดภาพ

32

ประเภทของกล้องวงจรปิด

3.2.1 กล้องโทรทัศน์วงจรปิดระบบแอนะล็อก
3.2.2 กล้องโทรทัศน์วงจรปิดระบบดิจิทัล

33

อุปกรณ์ของระบบกล้องโทรทัศน์วงจรปิด

3.3.1 กล้องโทรทัศน์วงจรปิด
3.3.2 เซ็นเซอร์รับภาพ
3.3.3 เลนส์ของกล้องโทรทัศน์วงจรปิด
3.3.4 เครื่องบันทึกภาพ
3.3.5 ฮาร์ดดิสก์สำหรับงานระบบกล้องโทรทัศน์วงจรปิด
3.3.6 จอภาพ
3.3.7 สายนำสัญญาณ
3.3.8 เครื่องสลับภาพ
3.3.9 เครื่องแบ่งสัญญาณภาพ
3.3.10 อุปกรณ์แปลงสัญญาณภาพ
3.3.11 อุปกรณ์เชื่อมต่อระบบเครือข่าย
3.3.12 ขั้วต่อสายสัญญาณในงานกล้องโทรทัศน์วงจรปิด
3.3.13 อุปกรณ์เสริมในงานกล้องโทรทัศน์วงจรปิด

34 **การออกแบบและติดตั้งระบบกล้องโทรทัศน์วงจรปิด**

3.4.1 เครื่องมือพื้นฐานสำหรับงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด
3.4.2 การสำรวจพื้นที่การติดตั้งระบบกล้องโทรทัศน์วงจรปิด
3.4.3 การเลือกอุปกรณ์สำหรับการติดระบบกล้องโทรทัศน์วงจรปิด
3.4.4 การคำนวณระยะเลนส์กล้องโทรทัศน์วงจรปิด
3.4.5 การคำนวณความกว้างของพื้นที่ที่กล้องมองเห็นได้
3.4.6 การคำนวณความจุฮาร์ดดิสก์และแบนด์วิดท์ของระบบกล้องโทรทัศน์วงจรปิด

35 **โปรแกรมบริหารจัดการระบบกล้องโทรทัศน์วงจรปิด**

3.5.1 ความหมายของโปรแกรมบริหารจัดการ
3.5.2 ซอฟแวร์ Central Management System
3.5.3 การติดตั้งโปรแกรมบริหารจัดการ
3.5.4 การทดสอบการใช้งานโปรแกรมบริหารจัดการ
3.5.5 เมนูหลักของโปรแกรม CMS

36 **การแก้ไขปัญหาและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด**

3.6.1 อาการภาพดับหรือไม่เกิดภาพ
3.6.2 อาการภาพเป็นคลื่น
3.6.3 อาการภาพเบลอ
3.6.4 การบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด

บทที่ 3 ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

Smart Close-Circuit Television Systems

3.1 พื้นฐานของระบบกล้องโทรทัศน์วงจรปิด (Fundamentals of CCTV Systems)

3.1.1 ความหมายของกล้องโทรทัศน์วงจรปิด

กล้องโทรทัศน์วงจรปิด (Close-Circuit Television: CCTV) คือ ระบบการบันทึกภาพเคลื่อนไหวด้วยกล้องโดยทำงานผ่านเครือข่ายแบบปิด ซึ่งเป็นระบบสำหรับการใช้เพื่อรักษาความปลอดภัย หรือที่ใช้เพื่อการสอดส่องดูแลเหตุการณ์ สถานการณ์ต่าง ๆ ที่เกิดขึ้นนอกเหนือจากการรักษาความปลอดภัย

3.1.2 ความเป็นมาของกล้องโทรทัศน์วงจรปิด

ระบบกล้องโทรทัศน์วงจรปิดเริ่มติดตั้งครั้งแรกในปี 1942 ในประเทศเยอรมนี ในยุคสงครามโลกครั้งที่ 2 ซึ่งวัตถุประสงค์ในช่วงแรกติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อสังเกตการณ์ความเคลื่อนไหวของขีปนาวุธ จากนั้นในปี 1968 ที่ประเทศสหรัฐอเมริกาได้มีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อสอดส่งดูแลและระแวดระวังเรื่องการก่อการร้าย จากนั้นมาได้มีการพัฒนาการกล้องโทรทัศน์วงจรปิดอย่างต่อเนื่อง กล้องโทรทัศน์วงจรปิดแบ่งตามเทคโนโลยีที่พัฒนาอย่างต่อเนื่องจะถูกแบ่งออกเป็น 4 ยุค ดังนี้ คือ

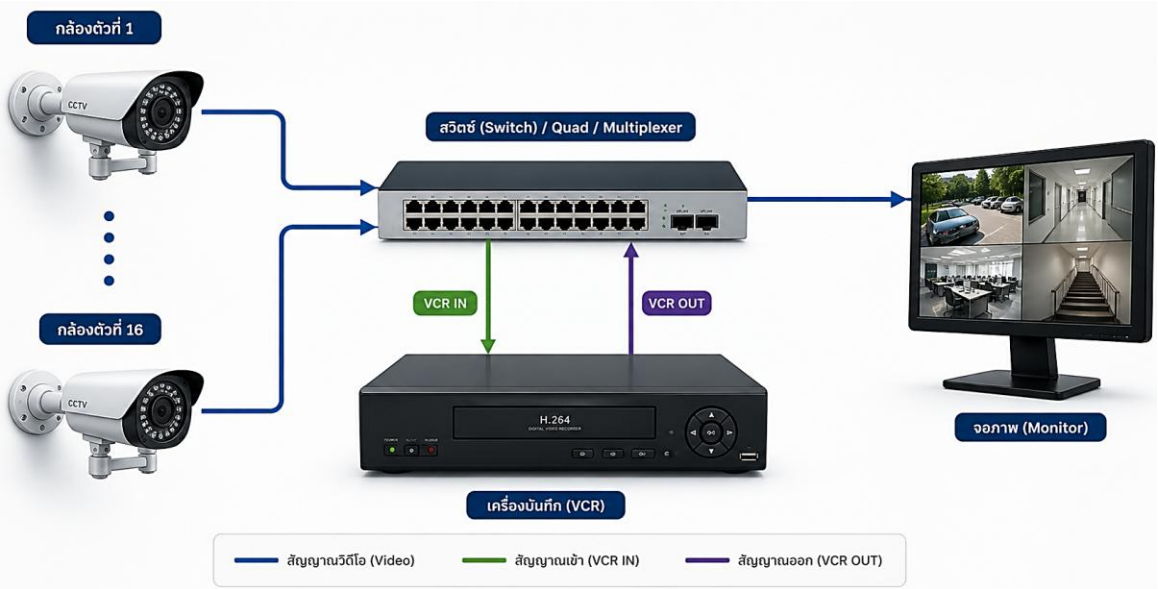
1) ยุคที่ 1 ของกล้องโทรทัศน์วงจรปิด เป็นการต่อกล้องโทรทัศน์วงจรปิดไปยังจอเพื่อดูภาพเท่านั้น ดังนั้นจะเห็นกล้องโทรทัศน์วงจรปิดต่อกับทีวีเป็นระบบ 1 ต่อ 1 ซึ่งไม่สามารถบันทึกภาพได้ ดังรูปที่ 3.1

รูปที่ 3.1 กล้องโทรทัศน์วงจรปิดยุคที่ 1

2) ยุคที่ 2 ของกล้องโทรทัศน์วงจรปิด เป็นต่อกล้องส่งการบันทึกภาพเก็บเอาไว้ดูในภายหลังผ่านเครื่องวีซีอาร์ (Video Cassette Recorder: VCR) แสดงภาพบนจอมอนิเตอร์ ระบบแบบนี้ ปัจจุบันไม่ค่อยได้รับความนิยมแต่ยังมีใช้งานอยู่บ้าง ดังรูปที่ 3.2

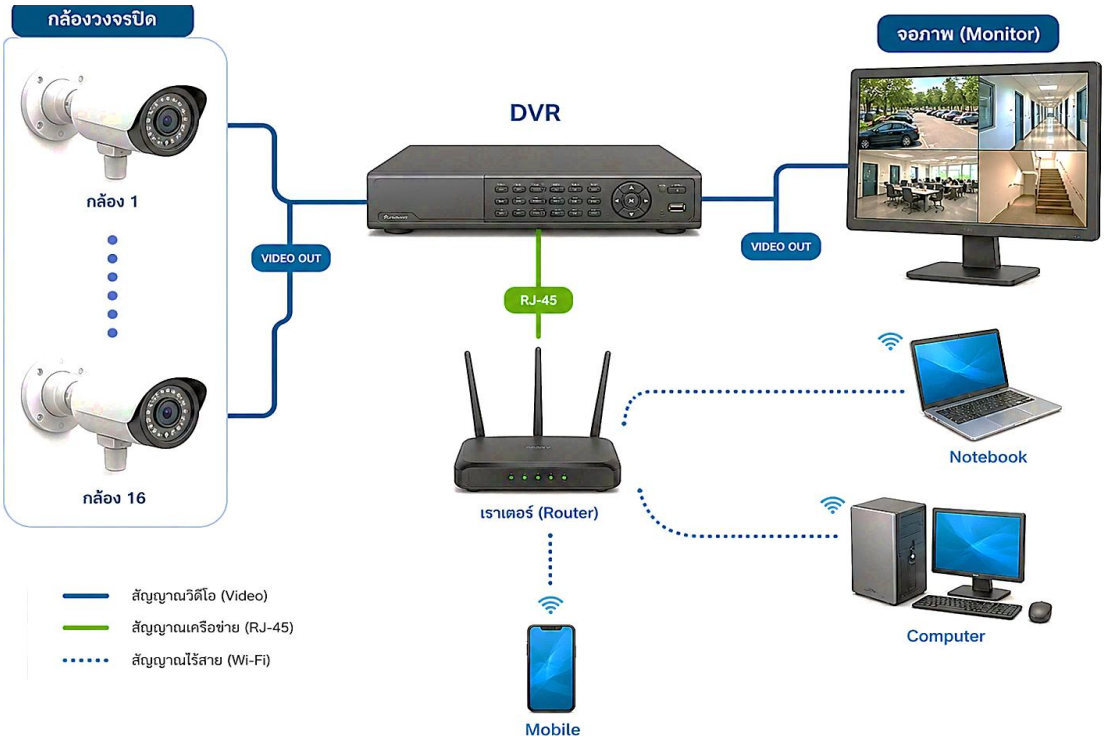
รูปที่ 3.2 กล้องโทรทัศน์วงจรปิดยุคที่ 2

3) ยุคที่ 3 ของกล้องโทรทัศน์วงจรปิด เป็นการบันทึกภาพ และต่อกล้องโทรทัศน์วงจรปิดมากกว่า 1 ตัว โดยใช้อุปกรณ์รวมสัญญาณเข้ามา ระบบแบบนี้จะพบอยู่ 2 ลักษณะนั้น คือ ต่อกับเครื่องบันทึกภาพ และไม่ต่อกับเครื่องบันทึกภาพ ดังรูปที่ 3.3



รูปที่ 3.3 กล้องโทรทัศน์วงจรปิดยุคที่ 3

4) ยุคที่ 4 ของกล้องโทรทัศน์วงจรปิด เป็นต่อกล้องโทรทัศน์วงจรปิดมากกว่า 1 ตัว ทำการบันทึกภาพด้วยเครื่องบันทึกสัญญาณวิดีโอแบบดิจิทัล (Digital Video Recorder: DVR) (ใช้ในระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก) และเครื่องบันทึกวิดีโอสำหรับกล้องโทรทัศน์วงจรปิดแบบเครือข่าย (Network Video Recorder: NVR) ใช้ในระบบกล้องโทรทัศน์วงจรปิดแบบดิจิทัล ปัจจุบันนิยมใช้โดยสามารถเชื่อมต่ออินเทอร์เน็ตจากอุปกรณ์โครงข่ายเพื่อดูภาพจากทุก ๆ ที่ ดังรูปที่ 3.4



รูปที่ 3.4 กล้องโทรทัศน์วงจรปิดยุคที่ 4

3.1.3 องค์ประกอบของระบบกล้องโทรทัศน์วงจรปิด

องค์ประกอบของระบบกล้องโทรทัศน์วงจรปิด สามารถอธิบายได้เป็นส่วนหลัก ๆ ดังนี้

1) กล้องโทรทัศน์วงจรปิด (Camera)

ทำหน้าที่จับภาพเหตุการณ์ในพื้นที่ที่ต้องการเฝ้าระวัง โดยมีหลายประเภท เช่น กล้องมาตรฐาน (standard) กล้องโดม (dome) กล้องกระบอก (bullet) และกล้องอินฟราเรด (Infrared: IR) สำหรับใช้งานในที่มืด รูปที่ได้จะถูกส่งต่อไปยังเครื่องบันทึกต่อไป

2) เครื่องบันทึกภาพ (DVR/NVR) เป็นอุปกรณ์ที่ใช้บันทึก จัดเก็บข้อมูลภาพจากกล้อง

2.1) DVR ใช้กับกล้องระบบแอนะล็อก

2.2) NVR ใช้กับกล้องระบบ IP สามารถดูภาพย้อนหลัง ควบคุม และตั้งค่าระบบได้

3) อุปกรณ์จัดเก็บข้อมูล (Hard Disk)

ติดตั้งอยู่ภายในเครื่องบันทึก ใช้สำหรับเก็บข้อมูลวิดีโอ โดยความจุจะมีผลต่อระยะเวลาในการเก็บบันทึกภาพ

4) จอแสดงผล (Monitor)

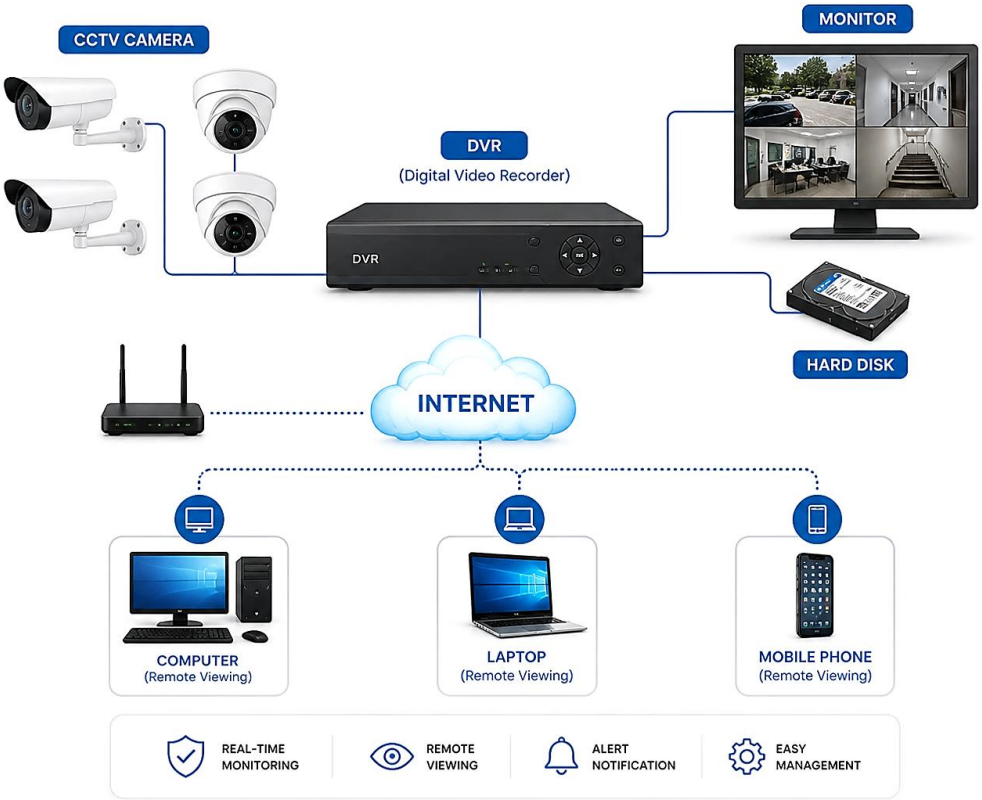
ใช้สำหรับแสดงภาพจากกล้องแบบเรียลไทม์ และดูภาพย้อนหลัง ช่วยให้ผู้ใช้งานสามารถตรวจสอบเหตุการณ์ได้สะดวก

5) ระบบเครือข่าย (Network/Internet)

ช่วยให้สามารถดูภาพจากระยะไกลผ่านคอมพิวเตอร์ โทรศัพท์มือถือ หรือแท็บเล็ต รองรับการเชื่อมต่อแบบออนไลน์

6) อุปกรณ์เชื่อมต่อ (Cabling and Accessories)

สายนำสัญญาณ เช่น สายโคแอกเชียล สายสัญญาณเครือข่าย แหล่งจ่ายไฟ สวิชต์ หรือเราเตอร์ ทำหน้าที่เชื่อมโยงอุปกรณ์ทั้งหมดเข้าด้วยกัน



รูปที่ 3.5 องค์ประกอบระบบกล้องโทรทัศน์วงจรปิด

ระบบกล้องโทรทัศน์วงจรปิดทำงานโดย กล้องจับภาพ จากนั้นส่งไปยังเครื่องบันทึก ทำการจัดเก็บข้อมูล และแสดงผลผ่านจอ และสามารถดูผ่านอินเทอร์เน็ตได้ ซึ่งทุกองค์ประกอบต้องทำงานร่วมกันอย่างเป็นระบบเพื่อให้เกิดประสิทธิภาพสูงสุดในการรักษาความปลอดภัย

3.1.4 ระบบเครือข่ายคอมพิวเตอร์ในระบบกล้องโทรทัศน์วงจรปิด

เครือข่ายเฉพาะที่ (Local Area Network: LAN) คือเครือข่ายคอมพิวเตอร์ขนาดเล็กที่เชื่อมต่ออุปกรณ์ต่าง ๆ ภายในพื้นที่จำกัด เช่น ภายในอาคาร สำนักงาน หรือสถานศึกษา โดยใช้อุปกรณ์เครือข่าย เช่น สวิตช์ (switch) และเราเตอร์ (router) เชื่อมต่อผ่านสายสัญญาณหรือสัญญาณไร้สาย ทำให้อุปกรณ์สามารถสื่อสารแลกเปลี่ยนข้อมูล และใช้ทรัพยากรร่วมกันได้อย่างรวดเร็วและมีประสิทธิภาพ ทั้งนี้ระบบ LAN สามารถออกแบบและติดตั้งได้ตามความต้องการของแต่ละองค์กร ตั้งแต่ระบบขนาดเล็กไปจนถึงระบบขนาดใหญ่ภายในหน่วยงานเดียวกัน (กิตติศักดิ์ เฮงสว่าง, 2553; Forouzan, 2013; CS Odessa, 2025a)

1) รูปแบบการเชื่อมต่อของระบบเครือข่ายเฉพาะที่ (LAN Topology)

รูปแบบการเชื่อมต่อเครือข่าย (topology) เป็นโครงสร้างการจัดวางอุปกรณ์และเส้นทางการสื่อสารข้อมูลในระบบเครือข่าย ซึ่งมีผลต่อประสิทธิภาพ ความเสถียร และความง่ายในการดูแลรักษาระบบ โดยแบ่งออกเป็นรูปแบบหลัก (Forouzan, 2013; CS Odessa, 2025a) ดังนี้

1.1) แบบบัส (Bus Topology)

เป็นรูปแบบการเชื่อมต่อที่อุปกรณ์ทุกเครื่องเชื่อมต่ออยู่บนสายสัญญาณหลักเพียงเส้นเดียว (bus) โดยปลายสายทั้งสองด้านต้องติดตั้งอุปกรณ์ที่ใช้ต่อปิดหัวสาย (terminator) เพื่อป้องกันสัญญาณสะท้อนกลับ ไม่มีอุปกรณ์ใดทำหน้าที่เป็นศูนย์กลางของระบบ การส่งข้อมูลจะวิ่งไปตามสายหลักและกระจายไปยังทุกอุปกรณ์

1.1.1) ข้อดี โครงสร้างไม่ซับซ้อน ติดตั้งง่าย ใช้สายน้อย ประหยัดค่าใช้จ่าย

1.1.2) ข้อเสีย หากสายหลักขาดหรือเสียหาย ระบบทั้งหมดจะหยุดทำงาน การตรวจสอบและแก้ไขปัญหาทำได้ยาก โดยเฉพาะในระบบขนาดใหญ่

การประยุกต์ใช้ในระบบ CCTV ในอดีต ระบบแอนะล็อกมีลักษณะใกล้เคียง bus topology เนื่องจากใช้สาย coaxial เป็นสายหลักในการส่งสัญญาณ แต่ในปัจจุบันไม่นิยมใช้โครงสร้างนี้ในระบบเครือข่าย IP เนื่องจากมีข้อจำกัดด้านความเสถียร

รูปที่ 3.6 รูปแบบการเชื่อมต่อเครือข่ายแบบบัส

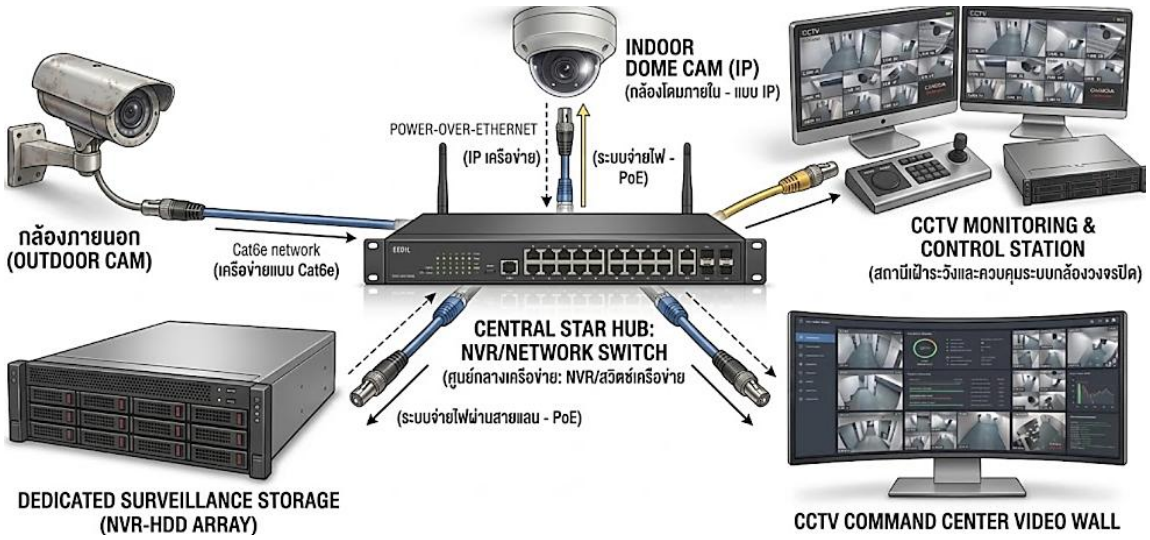
1.2) แบบดาว (Star Topology)

เป็นรูปแบบที่อุปกรณ์ทุกตัวเชื่อมต่อเข้ากับอุปกรณ์ศูนย์กลาง เช่น switch หรือ hub แต่ละอุปกรณ์ใช้สายสัญญาณแยกของตนเอง หากอุปกรณ์ใดเสียหาย จะไม่กระทบกับอุปกรณ์อื่น

1.2.1) ข้อดี คือ ระบบมีความเสถียรสูง ง่ายต่อการบริหารจัดการและแก้ไขปัญหา และรองรับการขยายระบบได้ดี

1.2.2) ข้อเสีย คือ ใช้สายสัญญาณจำนวนมาก หากอุปกรณ์ศูนย์กลางเสียหายระบบทั้งหมดจะหยุดทำงาน

การประยุกต์ใช้ในระบบ CCTV เป็นรูปแบบที่นิยมมากที่สุดในระบบ IP โดยกล้องทุกตัวจะเชื่อมต่อเข้าสู่ switch และส่งข้อมูลไปยัง NVR ควบคุมและดูภาพได้อย่างมีประสิทธิภาพ



รูปที่ 3.7 รูปแบบการเชื่อมต่อเครือข่ายแบบดาว

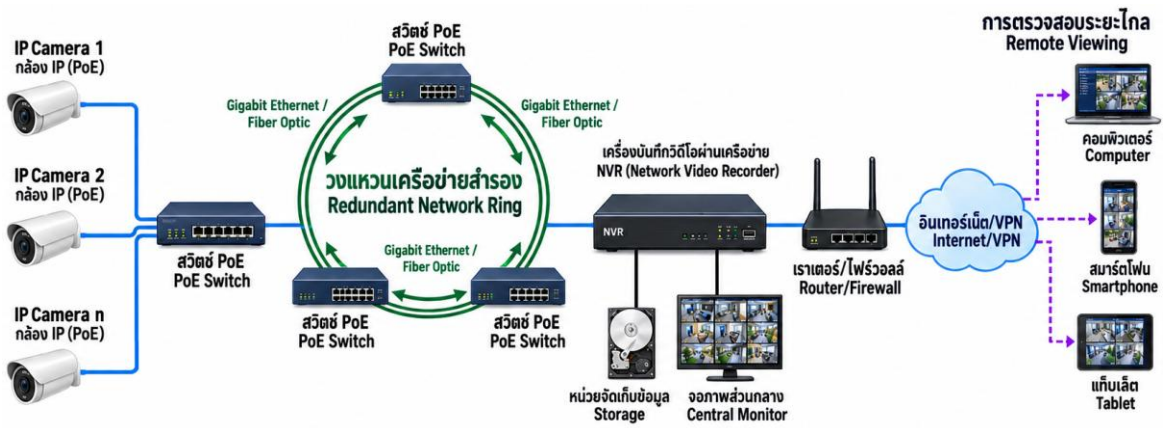
1.3) แบบวงแหวน (Ring Topology)

เป็นการเชื่อมต่ออุปกรณ์เป็นวงปิด โดยข้อมูลจะถูกส่งผ่านจากอุปกรณ์หนึ่งไปยังอีกอุปกรณ์หนึ่งตามลำดับจนถึงปลายทาง ทุกอุปกรณ์จะมีหน้าที่รับและส่งต่อข้อมูล

1.3.1) ข้อดี คือ ใช้สายสัญญาณน้อยกว่าแบบดาว ส่งข้อมูลมีลำดับชัดเจน

1.3.2) ข้อเสีย ได้แก่ หากอุปกรณ์ใดอุปกรณ์หนึ่งเสีย จะส่งผลต่อทั้งระบบ การขยายระบบและการแก้ไขปัญหาทำได้ยาก

การประยุกต์ใช้ในระบบ CCTV พบได้ในระบบเครือข่ายเฉพาะทาง เช่น ระบบกล้องในโรงงานหรือโครงสร้าง fiber optic ring เพื่อเพิ่มความต่อเนื่องของระบบ (redundancy) คือ การมี “อุปกรณ์หรือเส้นทางสำรอง” เผื่อกรณีที่อุปกรณ์หลักหรือเส้นทางหลักเกิดปัญหา



รูปที่ 3.8 การเชื่อมต่อเครือข่ายแบบวงแหวน

1.4) แบบผสมผสาน (Hybrid Topology)

เป็นการนำรูปแบบต่าง ๆ เช่น bus, star, และ ring มาผสมผสานกัน เพื่อเพิ่มประสิทธิภาพและลดข้อจำกัดของแต่ละรูปแบบ

1.4.1) ข้อดี มีความยืดหยุ่นสูง และสามารถออกแบบให้เหมาะกับพื้นที่ใช้งานจริง

1.4.2) ข้อเสีย มีความซับซ้อนในการออกแบบและติดตั้ง ค่าใช้จ่ายสูงกว่าระบบพื้นฐาน

การประยุกต์ใช้ในระบบ CCTV นิยมใช้ในระบบขนาดใหญ่ เช่น มหาวิทยาลัย สนามบิน โรงงานอุตสาหกรรม โดยอาจใช้ star topology เป็นหลัก และเสริมด้วย ring สำหรับสำรองข้อมูลเพื่อให้ระบบมีความเสถียรสูง

สรุปรูปแบบเครือข่าย LAN topology มีบทบาทสำคัญต่อการออกแบบระบบ CCTV โดยเฉพาะในระบบกล้อง IP ที่นิยมใช้โครงสร้างแบบ star และ hybrid เนื่องจากมีความเสถียร รองรับการขยายระบบ และสามารถจัดการเครือข่ายได้อย่างมีประสิทธิภาพ

2) ส่วนประกอบพื้นฐานของระบบเครือข่ายเฉพาะที่ (LAN)

ระบบเครือข่าย LAN ประกอบด้วยองค์ประกอบสำคัญหลายส่วนที่ทำงานร่วมกัน เพื่อให้สามารถสื่อสารและแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิภาพ (Forouzan, 2013) รายละเอียดดังนี้

2.1) ระบบปฏิบัติการเครือข่าย (Network Operating System: NOS)

ระบบปฏิบัติการเครือข่ายเป็นซอฟต์แวร์ที่ทำหน้าที่ควบคุมและบริหารจัดการการทำงานของเครือข่าย เช่น การจัดการผู้ใช้งาน การควบคุมสิทธิ์การเข้าถึงข้อมูล และการแบ่งปันทรัพยากรในระบบ โดยในเครือข่ายแบบจุดต่อจุด (peer-to-peer) เครื่องคอมพิวเตอร์แต่ละเครื่องจะมีระบบปฏิบัติการที่สามารถทำหน้าที่เป็นทั้งผู้ให้และผู้ใช้บริการได้ ส่วนในเครือข่ายแบบไคลเอนต์-เซิร์ฟเวอร์ (client-server) ระบบปฏิบัติการเครือข่ายจะติดตั้งอยู่บนเครื่องเซิร์ฟเวอร์ เช่น Windows server หรือ Linux server ทำหน้าที่เป็นศูนย์กลางในการให้บริการแก่เครื่องลูกข่าย

2.2) เครื่องบริการและสถานีงาน (Server and Workstation)

เครื่องบริการ (server) คือ คอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่าง ๆ ภายในเครือข่าย เช่น การจัดเก็บข้อมูล (file server) การพิมพ์งาน (print server) หรือการจัดการฐานข้อมูล (database server) ส่วนสถานีงาน (workstation) หรือเครื่องลูกข่าย คือ เครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อเข้ากับเครือข่ายเพื่อใช้งานบริการจากเซิร์ฟเวอร์

2.3) แผงวงจรเชื่อมต่อเครือข่าย (Network Interface Card: NIC)

NIC เป็นอุปกรณ์ฮาร์ดแวร์ที่ติดตั้งอยู่ในคอมพิวเตอร์ ทำหน้าที่เชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับเครือข่าย โดยทำหน้าที่แปลงข้อมูลจากคอมพิวเตอร์ให้อยู่ในรูปแบบสัญญาณที่สามารถส่งผ่านสื่อกลางเครือข่ายได้ และในทางกลับกัน NIC ยังทำหน้าที่รับสัญญาณจากเครือข่ายกลับมาเป็นข้อมูลที่คอมพิวเตอร์เข้าใจได้

2.4) ระบบสื่อกลางและการเดินสาย (Transmission Media/Cabling System)

สื่อกลางเครือข่ายเป็นส่วนที่ใช้เชื่อมต่ออุปกรณ์ต่าง ๆ เข้าด้วยกัน อาจเป็นแบบมี

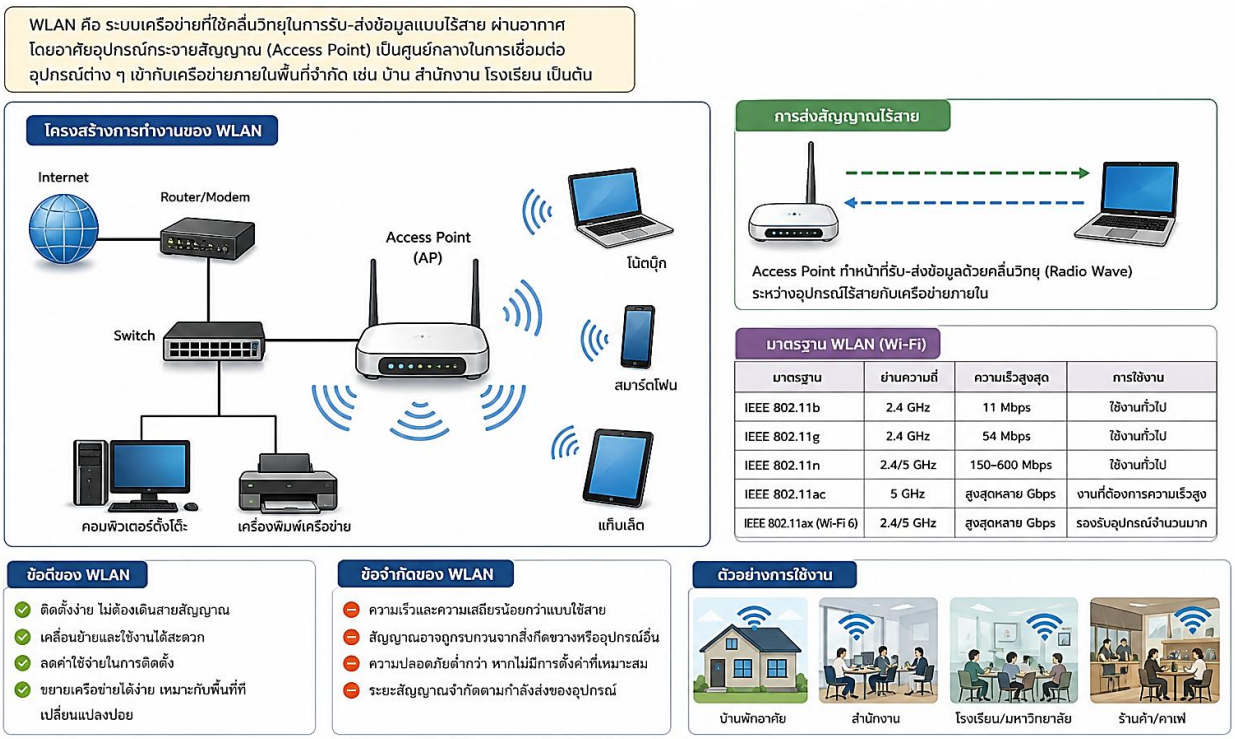
สายหรือไร้สาย ได้แก่ สายคู่บิดเกลียว (Unshielded Twisted Pair: UTP/Shielded Twisted Pair: STP) สายโคแอกเชียล (coaxial) สายใยแก้วนำแสง (fiber optic) และเครือข่ายไร้สาย (Wi-Fi) การเลือกใช้สื่อกลางขึ้นอยู่กับระยะทาง ความเร็ว และสภาพแวดล้อมในการติดตั้ง

2.5) ทรัพยากรและอุปกรณ์ที่ใช้ร่วมกัน (Shared Resources and Peripherals)

ทรัพยากรที่สามารถใช้งานร่วมกันในเครือข่าย ได้แก่ ฮาร์ดดิสก์ เครื่องพิมพ์ เครื่องสแกน หรืออุปกรณ์จัดเก็บข้อมูลต่าง ๆ รวมถึงซอฟต์แวร์และฐานข้อมูล ซึ่งผู้ใช้ในเครือข่ายสามารถเข้าถึงได้ตามสิทธิ์ที่กำหนด ช่วยเพิ่มประสิทธิภาพในการทำงานและลดต้นทุนในการจัดซื้ออุปกรณ์

3) เครือข่ายเฉพาะที่แบบไร้สาย (Wireless Local Area Network: WLAN)

เครือข่ายเฉพาะที่แบบไร้สาย (WLAN) เป็นระบบเครือข่ายที่ใช้การสื่อสารข้อมูลโดยไม่อาศัยสายนำสัญญาณ แต่ใช้คลื่นแม่เหล็กไฟฟ้าในการส่งข้อมูลผ่านอากาศ โดยทั่วไปจะใช้ คลื่นวิทยุ (radio frequency) เป็นหลัก เช่น เทคโนโลยี Wi-Fi ตามมาตรฐาน IEEE 802.11 ส่วนการใช้คลื่นอินฟราเรดพบได้น้อยในปัจจุบัน WLAN ช่วยให้อุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ สมาร์ตโฟน และแท็บเล็ต สามารถเชื่อมต่อและสื่อสารกันได้ภายในพื้นที่จำกัด เช่น บ้าน สำนักงาน หรือสถานศึกษา ดังรูปที่ 3.9



รูปที่ 3.9 โครงสร้างและหลักการทำงานของ WLAN

การทำงานของ WLAN มักอาศัยอุปกรณ์สำคัญคือ จุดกระจายสัญญาณ (Access Point: AP) ซึ่งทำหน้าที่เป็นศูนย์กลางในการรับ-ส่งข้อมูลระหว่างอุปกรณ์ไร้สายกับเครือข่ายแบบมีสาย โดยสัญญาณสามารถครอบคลุมพื้นที่ได้ตามกำลังส่งและสภาพแวดล้อม แม้ว่าคลื่นวิทยุสามารถทะลุผ่านสิ่งกีดขวางบางประเภทได้ แต่ประสิทธิภาพของสัญญาณอาจลดลงจากผนังหรือ

วัสดุที่หนาแน่น ข้อดีของ WLAN คือมีความสะดวกในการติดตั้ง เคลื่อนย้ายอุปกรณ์ได้ง่าย ลดค่าใช้จ่ายด้านการเดินสาย และเหมาะสำหรับพื้นที่ที่ไม่สะดวกในการติดตั้งสายนำสัญญาณ อย่างไรก็ตาม WLAN อาจมีข้อจำกัดด้านความเร็ว ความเสถียร และความปลอดภัยเมื่อเทียบกับระบบ LAN แบบใช้สาย จึงจำเป็นต้องมีการตั้งค่าความปลอดภัย เช่น การเข้ารหัสข้อมูล (WPA2/WPA3) (Kurose & Ross, 2017)

3.1.5 มาตรฐาน Ingress Protection Rating (IP)

มาตรฐาน (Ingress Protection Rating: IP) เป็นมาตรฐานที่ใช้ในการระบุระดับการป้องกันของสิ่งห่อหุ้มอุปกรณ์ไฟฟ้าและอิเล็กทรอนิกส์ จากการแทรกซึมของวัตถุภายนอก เช่น ฝุ่นละออง และของเหลว เช่น น้ำ โดยมาตรฐานนี้มีความสำคัญอย่างยิ่งในการเลือกใช้อุปกรณ์ให้เหมาะสมกับสภาพแวดล้อมในการใช้งาน สำหรับระบบกล้องโทรทัศน์วงจรปิด มาตรฐาน IP ใช้เพื่อบ่งบอกถึงความสามารถของตัวกล้องหรือโครงสร้างภายนอก (housing) ในการป้องกันวงจรและอุปกรณ์ภายในจากสภาพแวดล้อม เช่น ฝุ่น ความชื้น และน้ำ ซึ่งส่งผลโดยตรงต่อความทนทาน อายุการใช้งาน และความน่าเชื่อถือของระบบ มาตรฐาน IP ถูกกำหนดตามมาตรฐานสากล IEC 60529 ซึ่งพัฒนาโดย International Electrotechnical Commission (IEC) โดยบางประเทศหรือองค์กร เช่น European Committee for Electrotechnical Standardization (CENELEC) ยุโรป หรือ National Electrical Manufacturers Association (NEMA) สหรัฐอเมริกา (IEC, 2013; Thai Meister, 2017)

1) โครงสร้างของรหัส IP

รหัส IP ประกอบด้วยตัวอักษร “IP” ตามด้วยตัวเลข 2 หลัก ได้แก่

หลักที่ 1 (first digit) ระดับการป้องกันของแข็ง (solid objects) เช่น ฝุ่น หรือสิ่งแปลกปลอม

หลักที่ 2 (second digit) ระดับการป้องกันของเหลว (liquids) เช่น น้ำหรือความชื้น

ตัวอย่าง เช่น **IP65**

- เลข 6 = ป้องกันฝุ่นได้อย่างสมบูรณ์
- เลข 5 = ป้องกันน้ำฉีดจากทุกทิศทาง

ความสำคัญในการใช้งานกล้องโทรทัศน์วงจรปิด การเลือกกล้องโทรทัศน์วงจรปิดควรพิจารณาค่ามาตรฐาน IP ให้เหมาะสมกับสภาพแวดล้อม เช่น

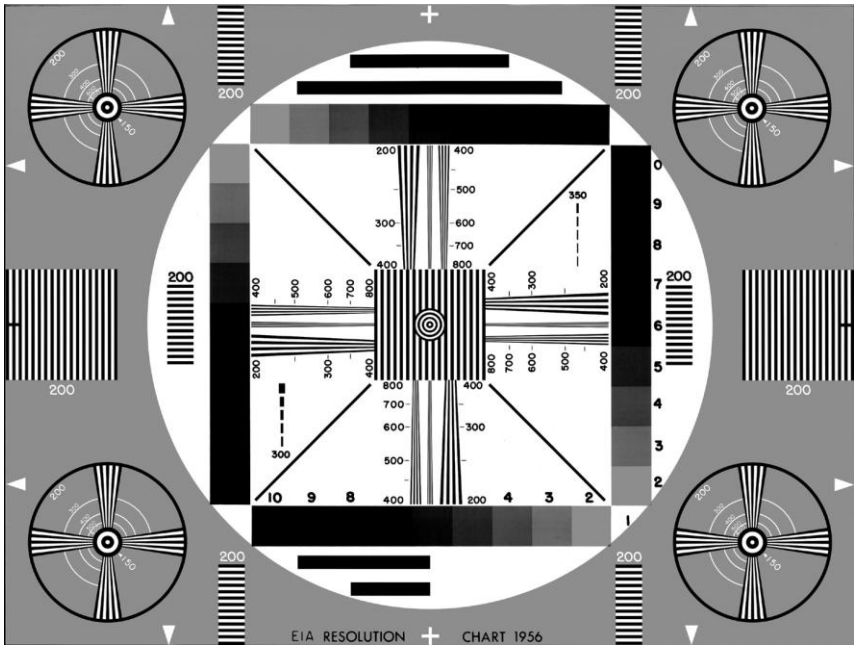
- **IP20 – IP40:** เหมาะสำหรับใช้งานภายในอาคาร
- **IP65 – IP67:** เหมาะสำหรับใช้งานภายนอกอาคาร ทนฝุ่นและฝน
- **IP68:** เหมาะสำหรับพื้นที่ที่มีน้ำหรือความชื้นสูงเป็นพิเศษ

3.1.6 หน่วยวัดความละเอียดภาพ

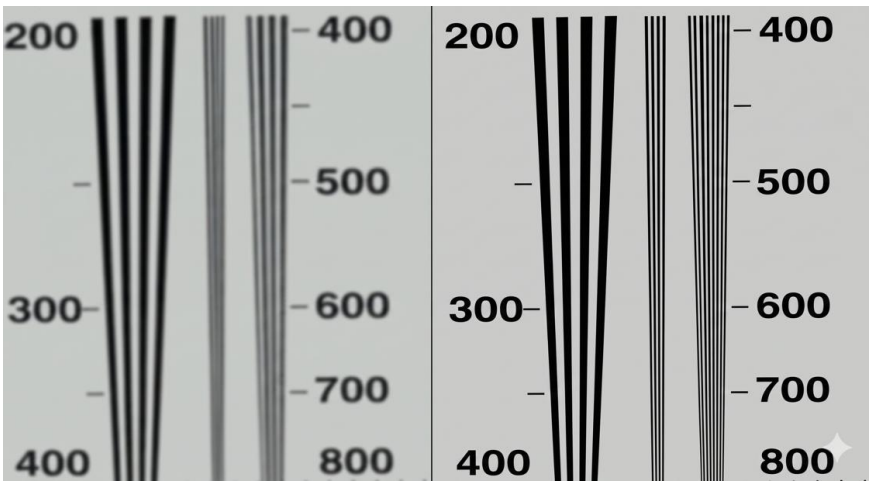
หน่วยวัดความละเอียดภาพ คือความละเอียดของภาพแนวนอน หากยิ่งมีจำนวนเส้นทีวีไลน์สูงภาพที่ได้ก็จะคมชัดยิ่งขึ้นตามไปด้วยโดยปัจจุบันจะเริ่มต้น เช่น กล้องโทรทัศน์วงจรปิด ความคมชัด 700 เส้น จะให้รูปที่ชัดกว่า กล้องโทรทัศน์วงจรปิดที่มีความคมชัด 550 เส้น เป็นต้น กล้องโทรทัศน์วงจรปิดที่มีความคมชัดสูง ๆ ราคาก็จะสูงตามไปด้วย

1) การทดสอบวัดค่า TV line

การเลือกซื้อกล้องโทรทัศน์วงจรปิดที่เป็นแอนะล็อกสิ่งแรกที่ต้องคำนึงถึงคือเรื่องคมชัดของกล้อง ต้องดูที่ค่าของ TV line ดูง่าย ๆ ก็คือค่า TV line หรือ เส้นสแกน ค่ายิ่งมากบอกถึงว่ากล้องตัวนั้นมีความคมชัดสูงนั่นเอง จะต่างจากกล้องที่เป็นระบบดิจิทัลที่ค่าจะบอกเป็นพิกเซล สิ่งแรกที่ต้องเตรียมคือ test TV line chart (รูปที่ 3.10) จะเป็นกระดาษหรือพลาสติกผิวด้านเพื่อลดการสะท้อนแสง นำกล้องที่จะวัดค่า TV line มาจับรูปที่ test TV line chart ปรับเลนส์ให้ชัดภาพที่สุด ดังรูปที่ 3.11



รูปที่ 3.10 แผ่นทดสอบความละเอียดของภาพ (resolution fest chart) (CCTV Thailand, 2011)



รูปที่ 3.11 การเปรียบเทียบความละเอียดของภาพระหว่าง 420 TVL และ 520 TVL (CCTV Thailand, 2011)

จากรูปที่ 3.11 การเปรียบเทียบความละเอียดของภาพ 420 TVL และ 520 TVL โดยสังเกตได้จากบริเวณที่มีเส้นถี่ ซึ่งค่าความละเอียดที่สูงกว่าจะสามารถแยกเส้นที่อยู่ใกล้กันได้ชัดเจนกว่า การประเมินความละเอียดของกล้องจะพิจารณาจากตำแหน่งที่ยังสามารถแยกเส้นออกจากกันได้อย่างชัดเจน หากไม่สามารถแยกเส้นได้แสดงว่าความละเอียดไม่เพียงพอ

ตารางที่ 3.1 ค่าความละเอียดของภาพ

ต่ำสุด	สูงสุด
330 TVL	350 TVL
380 TVL	400 TVL
420 TVL	450 TVL
480 TVL	500 TVL
520 TVL	530 TVL
540 TVL	550 TVL
560 TVL	580 TVL
600 TVL	620 TVL

เมื่อเทียบเป็นพิคเซลดัง ตารางที่ 3.2

ตารางที่ 3.2 ความละเอียดของ TVL เมื่อเทียบเป็นพิคเซล

TV LINE	พิคเซล
420 TVL	270,000
480 TVL	380,000
520 TVL	430,000
550 TVL	480,000

3.2 ประเภทของกล้องโทรทัศน์วงจรปิด (Types of CCTV Cameras)

ระบบกล้องโทรทัศน์วงจรปิดสามารถแบ่งตามเทคโนโลยีการส่งสัญญาณ ได้เป็น 2 ประเภทหลัก ได้แก่ ระบบแอนะล็อกและระบบดิจิทัล ซึ่งมีคุณลักษณะและข้อจำกัดแตกต่างกัน ดังนี้

3.2.1 กล้องโทรทัศน์วงจรปิดระบบแอนะล็อก (Analog CCTV System)

ระบบแอนะล็อกเป็นระบบพื้นฐานที่มีการใช้งานมายาวนาน มีต้นทุนต่ำและติดตั้งได้ง่าย เหมาะสำหรับงานทั่วไปที่ไม่ต้องการความละเอียดสูงมาก ระบบนี้ใช้มาตรฐานสัญญาณวิดีโอระบบ Phase Alternating Line (PAL) และระบบ National Television System Committee (NTSC) ทำให้สามารถใช้งานกล้องจากหลากหลายผู้ผลิตร่วมกันได้ กล้องแอนะล็อกส่วนใหญ่มีอินฟราเรด (infrared) สำหรับการมองเห็นในเวลากลางคืน และมีความเสถียรสูง เนื่องจากเทคโนโลยีมีการ

พัฒนาอย่างต่อเนื่องจนมีความสมบูรณ์ในระดับหนึ่ง อย่างไรก็ตามข้อจำกัดสำคัญคือ ความละเอียดของภาพค่อนข้างต่ำ เมื่อเทียบกับระบบดิจิทัล และได้มีการพัฒนาเป็นระบบ High Definition (HD) over coaxial เพื่อให้ภาพมีความคมชัดมากขึ้น โดยยังคงใช้สายโคแอกเชียลเดิม แต่สามารถส่งภาพความละเอียดสูงได้มากขึ้น

1) มาตรฐานของระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก (Analog CCTV System Standard) แบ่งออกเป็น 4 มาตรฐานหลัก ได้แก่

1.1)Analog High Definition (AHD) รองรับระยะส่งสัญญาณไกลประมาณ 500 m รองรับความละเอียด 720p และ 1080p สามารถใช้งานร่วมกับกล้องแอนะล็อกบางประเภทได้

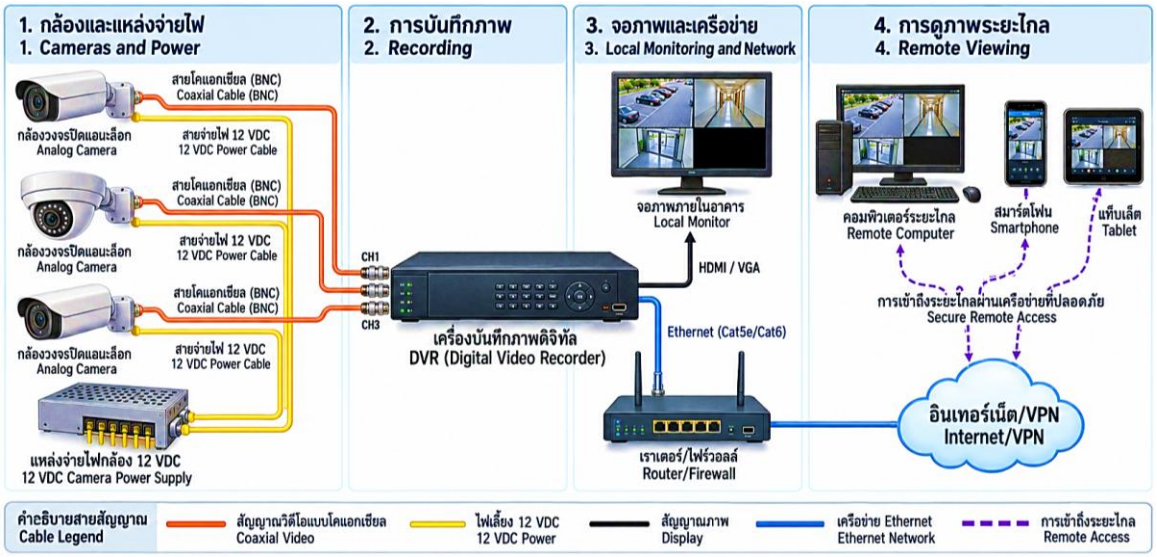
1.2)High-Definition Composite Video Interface (HDCVI) รองรับระยะในการส่งสัญญาณใกล้เคียงกับ AHD ให้ภาพคุณภาพสูง แต่ข้อจำกัดคือ DVR ไม่สามารถบันทึกความละเอียดต่างกันในระบบเดียวกันได้

1.3)High-Definition Serial Digital Interface (HDSDI) ให้ภาพคมชัดสูงและเป็นแบบเรียลไทม์ ไม่มีการหน่วงสัญญาณ แต่มีข้อจำกัดด้านระยะทางประมาณ 100–150 m และต้องใช้สายคุณภาพสูง

1.4)High-Definition Transport Video Interface (HDTVI) รองรับระยะทางไกลสูงสุด 500 m และสามารถบันทึกภาพหลายความละเอียดในระบบเดียวกันได้ จึงมีความยืดหยุ่นสูง เหมาะสำหรับการอัปเกรดจากระบบแอนะล็อกเดิม ไม่ต้องเปลี่ยนโครงสร้างสายสัญญาณทั้งหมด

2) โครงสร้างของระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก

ระบบที่กล้องโทรทัศน์วงจรปิดทำหน้าที่จับภาพและส่งสัญญาณวิดีโอ รูปแบบแอนะล็อกไปยังเครื่องบันทึกภาพชนิด DVR ผ่านสายสัญญาณโคแอกเชียล พร้อมสายไฟเลี้ยงกล้อง เมื่อสัญญาณแอนะล็อกถูกส่งเข้าสู่เครื่อง DVR ระบบจะทำการแปลงสัญญาณให้เป็นข้อมูลดิจิทัลเพื่อใช้ในการบันทึกลงในฮาร์ดดิสก์ และสามารถนำข้อมูลไปประมวลผลต่อได้ ในขณะเดียวกัน DVR จะส่งสัญญาณภาพไปยังจอแสดงผล เพื่อดูภาพแบบเรียลไทม์ (Ideal Quality Solutions Co., Ltd., 2560; CS Odessa, 2025b)

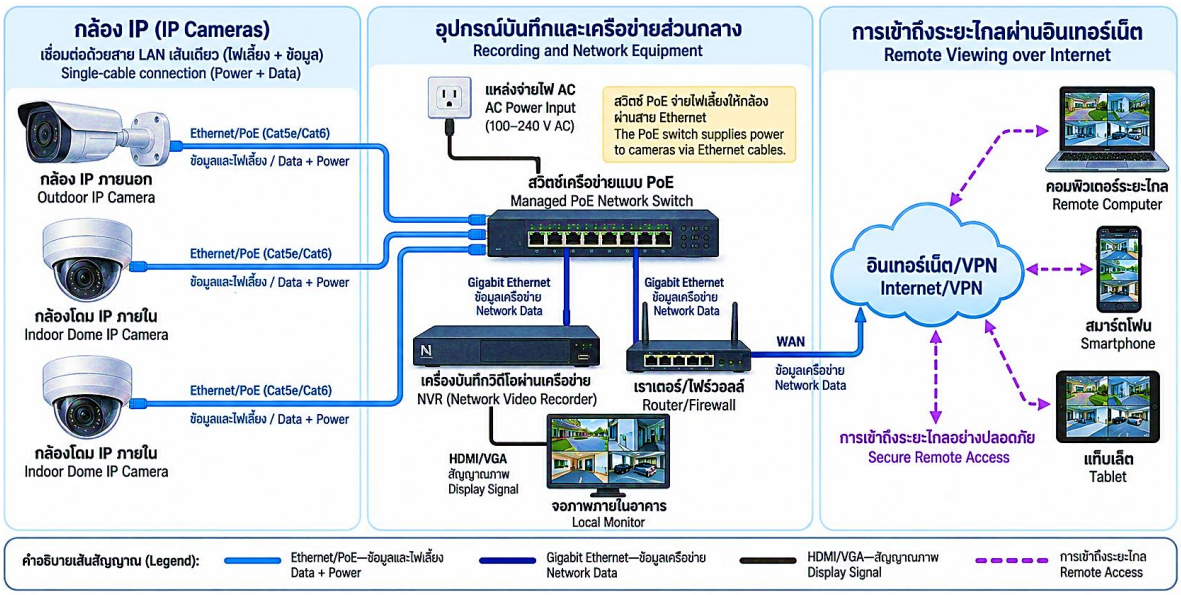


รูปที่ 3.12 โครงสร้างของกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก

3.2.2 กล้องโทรทัศน์วงจรปิดระบบดิจิทัล (Internet Protocol Camera: IP CCTV System)

ระบบดิจิทัลเป็นระบบที่ทันสมัยที่สุด โดยใช้เครือข่ายคอมพิวเตอร์ (network) ในการส่งข้อมูลภาพ ทำให้สามารถรองรับความละเอียดสูง เช่น full HD (1080p), 2MP, และ 4MP หรือสูงกว่า ข้อเด่นของระบบ IP ได้แก่ ความคมชัดของภาพสูงมาก สามารถขยายจำนวนกล้องได้ง่าย ไม่จำกัดจำนวนช่องเหมือน DVR รองรับการเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ต มีฟังก์ชันอัจฉริยะ เช่น ตรวจจับใบหน้า ตรวจจับการเคลื่อนไหว และวิเคราะห์ภาพ (video analytics) สามารถบริหารจัดการผ่านซอฟต์แวร์หรือแอปพลิเคชันได้สะดวก อย่างไรก็ตาม ระบบ IP มีต้นทุนสูงกว่าระบบอื่น และต้องมีความรู้ด้านเครือข่ายในการติดตั้งและดูแลระบบ โครงสร้างของกล้องโทรทัศน์วงจรปิดระบบดิจิทัล

ระบบกล้องโทรทัศน์วงจรปิดแบบดิจิทัลนำมาใช้แทนระบบแอนะล็อก ซึ่งกล้องโทรทัศน์วงจรปิดที่ส่งภาพและวิดีโอออกมาจากกล้องในลักษณะภาพสัญญาณดิจิทัล เข้าสู่เครื่องบันทึก NVR โดยผ่านสายสัญญาณแบบ UTP พร้อมสายไฟเลี้ยงให้กล้องมาที่เครื่องสลับภาพ และในเวลาเดียวกันเครื่อง NVR จะส่งสัญญาณดิจิทัลไปยังหน้าจอภาพ และส่งผ่านข้อมูลไปยังเว็บเน็ตเวิร์ค (Web network) ทำให้สามารถดูวีดีโอของระบบกล้องโทรทัศน์วงจรปิดผ่านเน็ตเวิร์คไปยังคอมพิวเตอร์และมือถือได้พร้อมกันในเวลาเดียวกัน ระบบIP จะส่งสัญญาณในรูปแบบดิจิทัลทำให้รูปที่ได้มีความคมชัด ไม่เกิดการสูญหายของสัญญาณ คือถ้ามีการเดินระบบผิดพลาดภาพก็จะไม่แสดงเลย แต่ถ้าเดินระบบได้ถูกต้องภาพจะมีความชัดตามคุณภาพของกล้องที่ส่งภาพมา ซึ่งต่างกับระบบแอนะล็อกที่ภาพจะมีทั้งภาพชัด ภาพไม่ชัด และภาพหาย (Ideal Quality Solutions Co., Ltd., 2560; CS Odessa, 2025b) ดังรูปที่ 3.13



รูปที่ 3.13 โครงสร้างของกล้องโทรทัศน์วงจรปิดระบบดิจิทัล

3.3 อุปกรณ์ของระบบกล้องโทรทัศน์วงจรปิด (Components of CCTV Systems)

3.3.1 กล้องโทรทัศน์วงจรปิด (CCTV Camera)

กล้องโทรทัศน์วงจรปิด แบ่งออกเป็น 2 ประเภทหลัก ได้แก่ กล้องแบบแอนะล็อก (analog camera) และกล้องแบบดิจิทัล (IP camera) กรณีที่แบ่งตามระบบสัญญาณระบบแอนะล็อก (analog system) มีการส่งสัญญาณผ่านสาย coaxial ใช้เครื่องบันทึก DVR เช่น กล้อง AHD, HDTVI, และ HDCVI กล่าวคือสัญญาณภาพเป็นแอนะล็อกแล้วมาแปลงเป็นดิจิทัลที่ DVR ส่วนระบบดิจิทัล (digital/IP system) จะส่งข้อมูลผ่านเครือข่าย (LAN/internet) ใช้เครื่องบันทึก NVR เช่น IP camera โดยสัญญาณเป็นดิจิทัลตั้งแต่ต้นทาง กรณีจำแนกตามลักษณะการใช้งานและรูปแบบของตัวกล้อง การแบ่งตามลักษณะของตัวกล้อง เช่น dome, bullet, หรือ speed dome (Kruegle, 2011) ซึ่งรูปแบบของตัวกล้องไม่สามารถใช้ระบุได้ว่าเป็นระบบแอนะล็อกหรือดิจิทัล จำเป็นต้องพิจารณาจากรูปแบบการส่งสัญญาณและอุปกรณ์ที่ใช้งานร่วมกัน

1) กล้องมาตรฐาน (Standard Camera/Box Camera)

เป็นกล้องที่มีลักษณะเป็นทรงสี่เหลี่ยมหรือทรงกระบอก สามารถเปลี่ยนเลนส์ได้ตามลักษณะงาน เหมาะสำหรับพื้นที่ที่ต้องการมุมมองระยะไกล เช่น ถนน โรงงาน หรือบริเวณลานจอดรถ มีข้อดี คือปรับเปลี่ยนเลนส์ได้ตามต้องการ ให้รูปที่ยืดหยุ่นในการใช้งาน และข้อจำกัดคือรูปลักษณ์ไม่สวยงามเท่ากล้องโดม และต้องใช้อุปกรณ์เสริมเมื่อติดตั้งภายนอกอาคาร

2) กล้องอินฟราเรด (Infrared Camera)

เป็นกล้องที่สามารถบันทึกภาพในที่มืดได้ โดยใช้หลอด LED อินฟราเรดช่วยส่องสว่าง กล้องที่มีระยะอินฟราเรด 10 m, 20 m, และ 30 m และระยะอื่น ๆ ที่จำเป็นต้องใช้ ข้อดีคือสามารถมองเห็นภาพในที่มืดสนิทได้ แต่มีข้อจำกัดด้านระยะการมองเห็น และเกิดความร้อนจากหลอดอินฟราเรด

3) กล้องโดม (Dome Camera)

มีลักษณะเป็นครึ่งวงกลม ติดตั้งกับเพดาน เหมาะสำหรับพื้นที่ภายในที่ต้องการความเรียบร้อย มีข้อดี คือ สวยงาม กลมกลืนกับสภาพแวดล้อม และป้องกันการรบกวนตัวกล้อง ส่วนข้อจำกัด คือ มุมมองอาจจำกัดเมื่อเทียบกับกล้องบางประเภท

4) กล้องสปีดโดม (Speed Dome Camera)

สามารถหมุน ซูม และควบคุมทิศทางได้ระยะไกล สามารถหมุนส่าย ได้ 360 องศา ก้มเงย ได้ มากกว่า 90 องศา ซูมภาพได้ระยะทางไกลได้มากกว่า 200 m เหมาะสำหรับระบบรักษาความปลอดภัยขนาดใหญ่ ข้อดี คือ ครอบคลุมพื้นที่กว้าง ควบคุมได้แบบเรียลไทม์ ส่วนข้อจำกัด มีราคาสูง และต้องใช้ระบบควบคุมเฉพาะ

5) กล้องเดย์/ไนท์ (Day/Night Camera)

สามารถทำงานได้ทั้งกลางวันและกลางคืน โดยอาศัยแสงน้อยร่วมกับระบบปรับภาพ สามารถดูภาพได้ทั้งที่มีปริมาณแสงมาก ไปจนปริมาณแสงน้อยมาก กล้องเดย์ไนท์ต่างจากกล้องอินฟราเรดตรงที่ต้องอาศัยแสงเข้าช่วย ขณะที่กล้องอินฟราเรดไม่ต้องการแสงเลย ก็สามารถดูภาพได้ ค่าการกินแสงของกล้องแบบนี้จะต่ำมาก เช่น 0.01 lux และ ถ้ายิ่งต่ำมากก็จะยิ่งมองเห็นภาพใน

ที่ที่มีแสงน้อยมากได้ดีขึ้น มีข้อดีคือเหมาะกับพื้นที่แสงน้อยที่ยังมีแสงบางส่วน ข้อจำกัดนั้นไม่สามารถใช้งานในที่มืดสนิทได้เท่ากล้องอินฟราเรด

6) กล้องชดเชยแสง (Backlight Camera)

มีระบบปรับสมดุลแสงอัตโนมัติ จะมีการชดเชยของแสของ Charge-Coupled Device (CCD) หรือตัดแสงที่จ้ามากเกินไปให้ลดลงอัตโนมัติ เหมาะสำหรับพื้นที่ที่มีแสงย้อน เช่น ทางเข้า-ออก ข้อดีสามารถมองเห็นวัตถุได้ชัดแม้มีแสงจ้า ข้อจำกัด ในปัจจุบันถูกแทนที่ด้วยเทคโนโลยีปรับสมดุลแสงในกล้องถ่ายภาพและกล้องโทรทัศน์วงจรปิด (Wide Dynamic Range: WDR)

7) กล้องกล้องทรงกระบอก (Bullet)

กล้องโทรทัศน์วงจรปิด bullet จะมีรูปทรงกระบอกยาว ตัวกล้องมีขนาดเล็ก ถูกออกแบบมาให้สามารถจับภาพในมีแสงน้อยได้ดีพอสมควร แต่ก็ไม่เท่าเทียมเท่ากล้องแบบ day/night เพียงแต่กล้อง bullet จะถูกออกแบบมาให้กินแสงต่ำ เหมาะกับการติดตั้งนอกอาคารที่มีเพียงหลอดไฟฟลูออเรสเซนต์ที่ให้แสงสว่างเพียงจำกัด มีข้อดีทนต่อสภาพอากาศ เหมาะกับงานกลางแจ้ง ส่วนข้อจำกัด คือมองเห็นได้ชัดเจน อาจไม่เหมาะกับงานที่ต้องการความสวยงาม

8) กล้องซ่อน (Hidden Camera)

เป็นกล้องขนาดเล็ก ใช้สำหรับงานที่ต้องการความลับ เช่น การเฝ้าระวังพฤติกรรม มีข้อดีไม่เป็นที่สังเกต ข้อจำกัด มีข้อจำกัดด้านกฎหมายและจริยธรรมในการใช้งาน

9) กล้อง IP Camera

เป็นกล้องที่ทำงานบนระบบเครือข่าย (network) ส่งข้อมูลแบบดิจิทัลผ่านระบบ LAN หรืออินเทอร์เน็ต มีข้อดี คือความคมชัดสูง (HD, Full HD, 4MP ขึ้นไป) รองรับการดูผ่านมือถือและอินเทอร์เน็ต ขยายระบบได้ง่าย ส่วนข้อจำกัด ใช้แบนด์วิดท์สูง มีค่าใช้จ่ายและความซับซ้อนในการติดตั้งมากกว่า

(ก) กล้องแบบมาตรฐาน

(ข) กล้องแบบอินฟราเรด

(ค) กล้องแบบโดม

(ง) กล้องสปีดโดม

(จ) กล้องแบบเดย์ไนท์

(ฉ) กล้องแบบย้อนแสง

(ช) กล้อง CCTV bullet

(ซ) กล้องแบบซ่อน

ฌ) กล้องแบบ IP

รูปที่ 3.14 กล้องโทรทัศน์วงจรปิดชนิดต่าง ๆ

3.3.2 เซ็นเซอร์รับภาพ (Image Sensor)

เซ็นเซอร์รับภาพ (image sensor) เป็นองค์ประกอบสำคัญของกล้อง ทำหน้าที่รับพลังงานแสงที่ผ่านเลนส์เข้ามา แล้วแปลงเป็นสัญญาณไฟฟ้า ก่อนนำไปประมวลผลเป็นสัญญาณภาพดิจิทัล โดยเซ็นเซอร์เปรียบเสมือน “ฉากรับภาพ” ของกล้อง ซึ่งมีผลโดยตรงต่อคุณภาพของภาพ เช่น ความคมชัด ความไวแสง และสัญญาณรบกวน เทคโนโลยีของเซ็นเซอร์รับภาพที่ใช้กันโดยทั่วไปสามารถแบ่งออกเป็น 2 ประเภทหลัก ได้แก่ CCD และ CMOS (Complementary Metal-Oxide-Semiconductor)

1) CCD เป็นเทคโนโลยีที่ถูกพัฒนาขึ้นมาก่อน โดยมีหลักการทำงานคือการแปลงแสงเป็นประจุไฟฟ้า แล้วถ่ายโอนประจุไปยังวงจรอ่านค่าแบบลำดับ ทำให้ได้สัญญาณภาพที่มีความสม่ำเสมอและมีสัญญาณรบกวนน้อย ส่งผลให้ภาพมีคุณภาพสูง เหมาะสำหรับงานที่ต้องการความแม่นยำ เช่น งานด้านวิทยาศาสตร์หรืออุตสาหกรรม อย่างไรก็ตาม CCD มีข้อจำกัดด้านการใช้พลังงานที่สูง ต้นทุนการผลิตสูง และมีความเร็วในการอ่านข้อมูลต่ำกว่า

2) ในขณะที่ CMOS เป็นเทคโนโลยีที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบัน โดยมีการพัฒนาต่อจาก CCD ให้สามารถประมวลผลสัญญาณได้ภายในแต่ละพิกเซล ทำให้สามารถอ่านข้อมูลได้รวดเร็ว ใช้พลังงานต่ำ และสามารถรวมวงจรต่าง ๆ ไว้ในชิปเดียวกันได้ ส่งผลให้ต้นทุนการผลิตต่ำกว่า นอกจากนี้ CMOS ในยุคปัจจุบันยังได้รับการพัฒนาให้มีคุณภาพของภาพสูง สามารถลดสัญญาณรบกวนและเพิ่มความไวแสงได้ดี จนสามารถให้คุณภาพภาพเทียบเท่าหรือดีกว่า CCD ในหลายการใช้งาน

โดยสรุป CCD ให้คุณภาพภาพสูงและสัญญาณรบกวนน้อย แต่มีข้อจำกัดด้านพลังงานและต้นทุน ขณะที่ CMOS มีข้อได้เปรียบด้านความเร็ว การใช้พลังงาน และต้นทุน จึงกลายเป็นเทคโนโลยีหลักที่ใช้ในกล้องดิจิทัล กล้องโทรทัศน์วงจรปิด และอุปกรณ์สมัยใหม่ในปัจจุบัน

3.3.3 เลนส์ของกล้องโทรทัศน์วงจรปิด

1) ข้อต่อที่ใช้ต่อกับกล้องโทรทัศน์วงจรปิด ข้อต่อของเลนส์กับตัวรับภาพกล้องโทรทัศน์วงจรปิด มี 2 ชนิด ดังรูปที่ 3.15 คือ

C-Mount มีความยาวช่วงท้ายเลนส์ ถึงหน้าตัวรับภาพ 17.5 mm

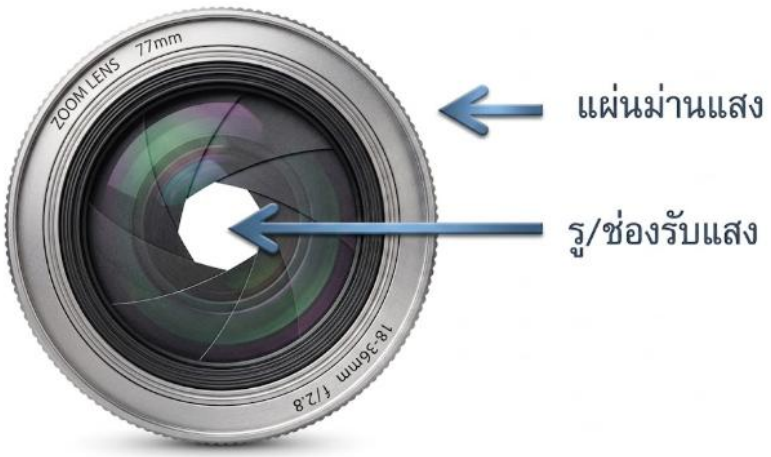
CS-Mount มีความยาวช่วงท้ายเลนส์ ถึงหน้าตัวรับภาพ 12.5 mm

รูปที่ 3.15 ข้อต่อแบบ C-mount และ CS-mount

ดังนั้นการเลือกใช้เลนส์ต้องเลือกให้ถูก คือ กล้องที่มีข้อต่อแบบ CS-mount ก็ควรจะใช้เลนส์ที่มีข้อต่อเป็นแบบ CS-mount กล้องที่มีข้อต่อแบบ C-mount ก็ควรใช้เลนส์ที่มีข้อต่อเป็นแบบ C-mount แต่เลนส์ที่มีข้อต่อเลนส์แบบ C-mount สามารถที่จะใช้กับกล้องที่มีข้อต่อแบบ CS-mount ได้ โดยใช้แหวนข้อต่อ (5 mm adapter ring) ต่อกลางระหว่างเลนส์กับกล้องถ้านำเลนส์ที่มีข้อต่อแบบ C-mount ไปต่อเข้ากับกล้องที่มีข้อต่อแบบ CS-mount โดยตรงโดยไม่ใช้แหวนข้อต่ออาจจะทำให้หน้าตัวรับภาพเกิดความเสียหายได้ เพราะว่าความยาวช่วงท้ายเลนส์ของ เลนส์แบบ C-mount มีความยาวมากกว่าแบบ CS-mount

2) รูรับแสง

รูรับแสง คือจุดที่ให้แสงผ่านเข้าไปในเลนส์ ขนาดของรูรับแสงสามารถเปลี่ยนไปได้ด้วยการ เปิด ปิดม่านรับแสง (iris) การเลือกใช้ขนาดของรูรับแสงจะมีผลต่อความชัดลึกของภาพ (DOF) ความชัดลึกของภาพ หมายถึง ภาพที่เห็นมีความคมชัดของภาพตั้งแต่หน้าเลนส์ ไปจนสุดสายตา มีความคมชัดเท่ากันหมด ในบางภาพจะเห็นว่ามีความคมชัด ความชัดเจนเพียงบางส่วน เช่น ระยะต้นๆ แสดงว่าภาพนั้นไม่มีความชัดลึกของภาพ ความชัดลึกของภาพมีผลต่อภาพที่เห็น เช่น ดูภาพจากกล้องที่ติดตั้ง ที่ทาง เดินหน้าอาคาร ถ้ามีคนเดินมาในระยะไกล เราก็ไม่สามารถจะทราบได้ว่าเป็นใคร



รูปที่ 3.16 รูรับแสง

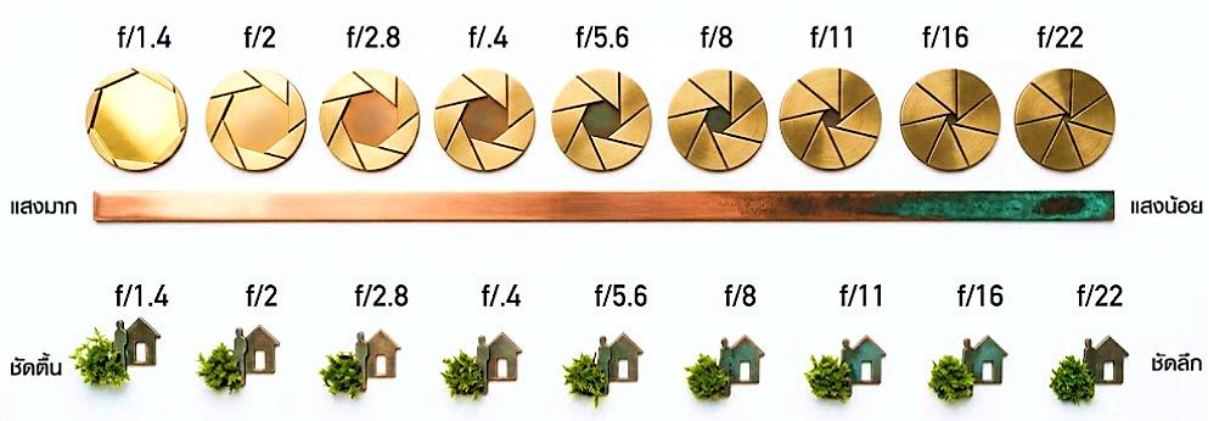
การเปิดปิดม่านรับแสงของเลนส์ คือ ม่านแสงที่จะยอมให้แสงผ่านช่องรับแสงไปยังเซนเซอร์รับภาพช่องรับแสง ช่องรับแสงชนิดที่สามารถปรับขนาดรู้ได้จะช่วยให้รูปที่มืดสว่างขึ้นได้ โดยปรับช่องให้ใหญ่ขึ้นแสงเข้าได้มากขึ้นภาพสว่างขึ้น แสดงดังรูปที่ 3.17 มี 2 ชนิด คือ

2.1) ชนิดเปิด-ปิด ด้วยมือ (manual iris) การปรับขนาดของม่านแสง เพื่อให้ขนาดของรูรับแสง เปลี่ยนแปลง ใช้มือหมุนวงแหวนปรับขนาดม่านแสง (iris ring) ที่ตัวเลนส์ ตัวเลขค่ามาก เช่น 16 ขนาด ของรูจะเล็กปริมาณแสงจะผ่านได้น้อย ตัวเลขค่าน้อย เช่น 1.4 ขนาดของรูจะใหญ่ ปริมาณแสงจะผ่านได้มาก

2.2) ชนิดแบบเปิด-ปิด อัตโนมัติ (auto-iris) การปรับขนาดม่านแสง ทำงานอัตโนมัติร่วมกับการทำงาน ของกล้องจะมีการจ่ายไฟฟ้าให้กับเลนส์มี 2 แบบ

2.2.1) แบบสัญญาณภาพ (video type) ตัวกล้องโทรทัศน์วงจรปิดจะจ่ายไฟฟ้าให้กับเลนส์ในลักษณะของสัญญาณภาพ โดยจะมีความเข้มของสัญญาณรูปที่แตกต่างกันไปตามการเปลี่ยนแปลงของแสง เลนส์ที่จะใช้กับกล้องที่จ่ายไฟฟ้าแบบนี้ จะต้องมีแผงวงจรเพื่อเปลี่ยนความแตกต่างของสัญญาณภาพให้เป็นการเปลี่ยนแปลงทางไฟฟ้า เพื่อให้อุปกรณ์ซึ่งคล้ายกับมอเตอร์มีขนาดเล็กมาก เรียกว่า กัลวานอมิเตอร์ (galvanometer) หลักการทำงานก็เพื่อทำให้ม่านแสงเปิด หรือ ปิดตามการเปลี่ยนแปลงของแสง

2.2.2) แบบไฟตรง (DC type) ตัวกล้องโทรทัศน์วงจรปิดจะมีวงจรจ่ายไฟฟ้าจ่ายไฟกระแสตรงให้กับเลนส์เพื่อให้กัลวานอมิเตอร์ทำงานโดยตรง เพื่อทำให้ม่านแสงเปิด หรือ ปิด ไปตามการเปลี่ยนแปลงของแสง การเลือกใช้เลนส์ที่เปิดปิดม่านแสงอัตโนมัติ เป็นชนิด video type หรือ DC type ต้องดูจากคู่มือของกล้องโทรทัศน์วงจรปิด ถ้าใช้ผิดประเภท ก็จะไม่มีภาพ เพราะว่าเลนส์ไม่เปิดรับแสง เลนส์จะไม่ทำงาน และอาจจะชำรุดได้



รูปที่ 3.17 ตัวอย่างขาดของรูรับแสงขนาดต่าง ๆ (ดัดแปลงจาก Tataisong, 2020)

นอกจากนี้เลนส์บางรุ่น บางผู้ผลิตสามารถใช้งานได้ทั้ง manual-iris และ auto-iris ในเลนส์ตัวเดียวกัน บางรุ่นจะมีสวิตซ์เลือกใช้อย่างใดอย่างหนึ่งจากตัวควบคุม แต่ในบางรุ่นสามารถที่จะสั่งเปิดหรือปิดรูรับแสง ในขณะที่ยังคงทำงานเป็น auto-iris ได้ด้วย

3) เลนส์กล้องโทรทัศน์วงจรปิด

เลนส์กล้องโทรทัศน์วงจรปิดจะทำหน้าที่รวมแสง และปรับระยะภาพให้มีขนาดใหญ่หรือเล็ก ตามความเหมาะสมเลนส์บางรุ่นมีความสามารถในการหรี่รูรับแสงเพื่อเพิ่มความคมชัดของภาพได้ ซึ่งเลนส์ดังกล่าวจะต้องใช้คู่กับตัวกล้องที่สามารถสั่งค่ารูรับแสงได้เท่านั้น โดยทั่วไปเลนส์แบ่งตามการปรับระยะโฟกัสได้ 3 ชนิด มีดังนี้

3.1) เลนส์ที่มีขนาดช่องรับแสงคงที่ (Fix Lens)

เลนส์ที่มีขนาดช่องรับแสงคงที่เป็นเลนส์ที่ไม่สามารถปรับช่องรับแสงได้ ความยาวโฟกัสคงที่ (fixed focal length) โรงงานผู้ผลิตเลนส์จะเป็นผู้กำหนดค่าความยาวโฟกัสของเลนส์ที่จะผลิตออกมาขายจะมีค่าแตกต่างกันไปหลายขนาด เช่น 8.0 mm หรือน้อยกว่า (สำหรับ CCD ขนาด 1/3″) 12 mm (สำหรับ CCD ขนาด 1/2″) 16 mm (สำหรับ CCD ขนาด 2/3″) เป็นต้น การเลือกใช้เลนส์ที่มีความยาวโฟกัสคงที่นี้ ควรเลือกใช้ตามความต้องที่จะได้ขนาดของภาพ ความยาวโฟกัสจะมีความสัมพันธ์กับมุมมองภาพ ความยาวโฟกัสที่มีค่าตัวเลขมาก มุมมองภาพจะแคบ ความยาวโฟกัสที่มีค่าตัวเลขน้อย มุมมองภาพจะกว้าง ควรใช้ในสถานที่ภายในอาคารที่มีแสงสว่างคงที่ตลอดเวลา ดังรูปที่ 3.18

รูปที่ 3.18 เลนส์ที่มีขนาดช่องรับแสงคงที่

3.2) เลนส์ปรับช่องรับแสงได้ (Manual Lens)

เลนส์ปรับช่องรับแสงได้ เป็นเลนส์ที่สามารถปรับช่องรับแสงได้ ความยาวโฟกัสปรับได้ (variable focal length) ใช้มือปรับขนาดภาพ (หมุนวงแหวนขนาดภาพ) และขนาดรูรับแสง (หมุนวงแหวนปรับขนาดม่านแสง) ปรับขนาดภาพด้วยมือแสงอัตโนมัติ (manual zoom & auto-iris) การใช้งานปรับขนาดภาพด้วยมือ แต่การเปิด-ปิดม่านแสงอัตโนมัติ เลนส์ชนิดนี้ส่วนมากจะมีค่าในการปรับขนาดภาพไม่มากนัก โดยทั่วไปประมาณ 2 ถึง 3 เท่า เหมาะสำหรับงานในอาคารที่มีความสว่างในแต่ละห้องไม่เท่ากัน ซึ่งสามารถปรับแสงให้เหมาะสมในแต่ละห้องได้ ดังรูปที่ 3.19

รูปที่ 3.19 ลักษณะของเลนส์ปรับช่องรับแสงได้

3.3) เลนส์ปรับขนาดช่องรับแสงอัตโนมัติ (Auto-Iris Lens)

เลนส์ปรับขนาดช่องรับแสงอัตโนมัติ เป็นเลนส์ที่สามารถปรับช่องรับแสงได้เองโดยอัตโนมัติ ขึ้นอยู่กับความเข้มของแสงที่ตกกระทบเลนส์ ปรับขนาดภาพด้วยมอเตอร์ (motorized zoom) เลนส์ชนิดนี้จะมีมอเตอร์อยู่ภายในตัวเลนส์ ทำหน้าที่ขับให้วงแหวนขนาดภาพเปลี่ยนแปลง (เปลี่ยนค่า ความยาวโฟกัส) ไปตามที่ต้องการ ด้วยตัว ควบคุม เลนส์ชนิดนี้ยังแบ่งได้อีก 2 แบบ คือ เปิด-ปิดม่านแสงด้วยการควบคุม เช่น เดียวกันกับการเปลี่ยนขนาดของภาพ จะมีมอเตอร์ทำหน้าที่ เปิด-ปิดม่านแสง หรือจะเรียกว่าควบคุมด้วยมือก็ได้ และ เปิด-ปิดม่านแสงอัตโนมัติ ซึ่งเหมาะสำหรับการติดตั้งนอกอาคารที่ความสว่างเปลี่ยนแปลงตามสภาพแวดล้อม ดังรูปที่ 3.20

รูปที่ 3.20 ลักษณะของเลนส์ปรับขนาดช่องรับแสงอัตโนมัติ

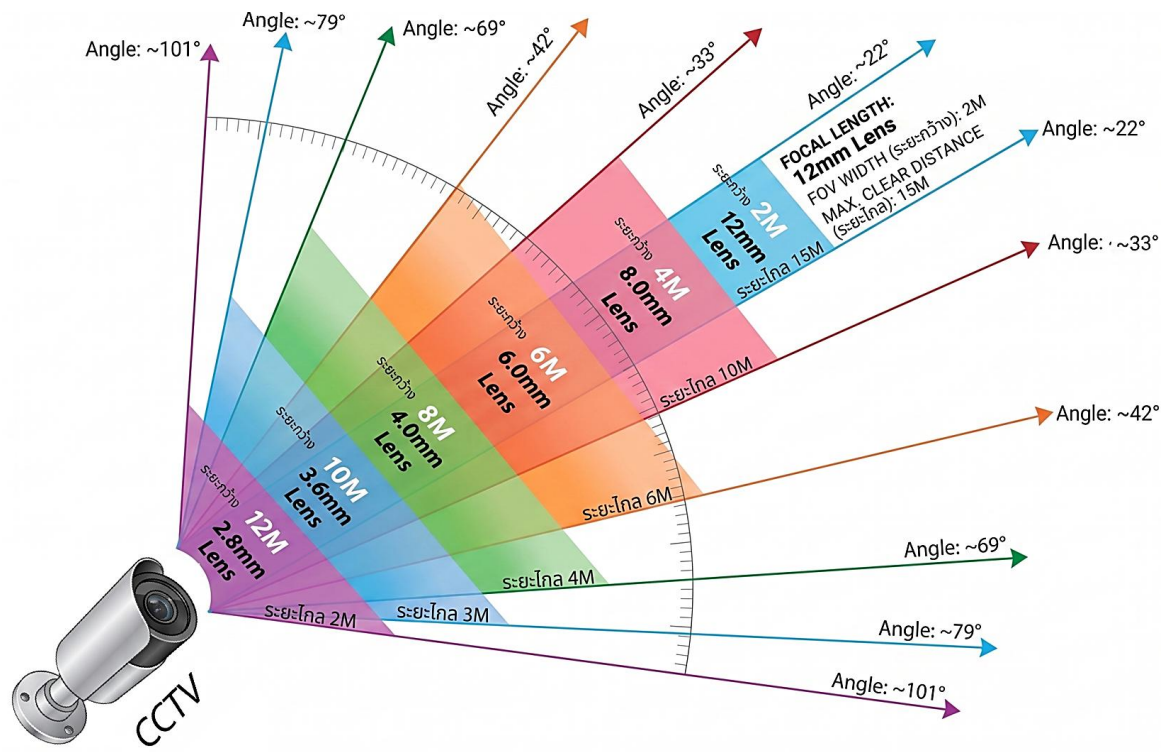
3.4) ระยะโฟกัสของเลนส์หรือความยาวโฟกัส (Focal Length)

ความยาวโฟกัสของเลนส์ คือ ระยะทางระหว่างจุดศูนย์กลางของเลนส์กับเซนเซอร์รับภาพ เมื่อเลนส์สามารถโฟกัสภาพของวัตถุได้อย่างชัดเจน โดยทั่วไปความยาวโฟกัสมีหน่วยเป็นมิลลิเมตร (mm) และเป็นปัจจัยสำคัญที่มีผลต่อมุมมองภาพ (Field of View: FOV) ของกล้องโทรทัศน์วงจรปิด มีหน่วยเป็นองศา โดยเลนส์ที่มีความยาวโฟกัสต่ำจะให้มุมมองภาพที่กว้าง ส่วนเลนส์ที่มีความยาวโฟกัสสูงจะให้มุมมองภาพแคบลง ตัวอย่าง เช่น เลนส์ที่มีค่าความยาวโฟกัส

ต่ำ เช่น 2.8 mm หรือ 3.6 mm จะให้มุมมองภาพกว้าง เหมาะสำหรับการเฝ้าระวังพื้นที่กว้างในระยะใกล้ ส่วนเลนส์ที่มีค่าความยาวโฟกัสสูง เช่น 8 mm หรือ 12 mm จะให้มุมมองภาพแคบกว่า แต่สามารถมองเห็นรายละเอียดของวัตถุในระยะไกลได้ชัดเจนมากขึ้น การเลือกเลนส์จึงต้องพิจารณาให้เหมาะสมกับลักษณะพื้นที่และวัตถุประสงค์ของการใช้งาน หากต้องการทั้งมุมมองที่กว้างและรายละเอียดของภาพที่ชัดเจน อาจจำเป็นต้องเลือกกล้องที่มีความละเอียดสูงขึ้นร่วมด้วย ดังแสดงในตารางที่ 3.3

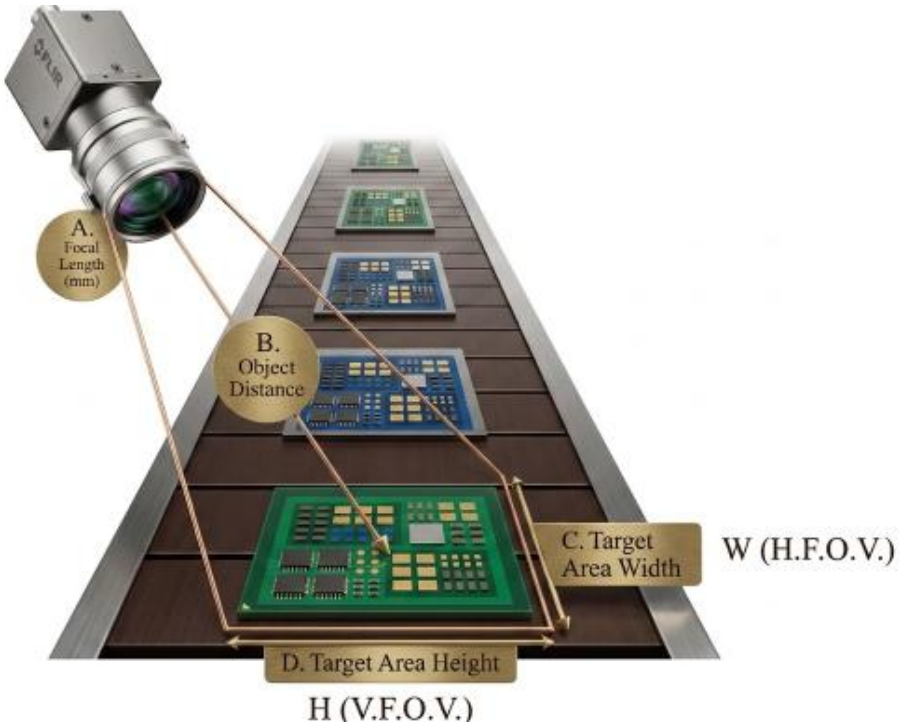
ตารางที่ 3.3 การเลือกขนาดเลนส์ให้เหมาะสมกับลักษณะการใช้งาน

ขนาดเลนส์ (mm)	ระยะมองเห็นแนวกว้าง (m)	ระยะมองเห็นแนวลึก (m)	ลักษณะการใช้งาน
2.8	12	2	เหมาะสำหรับพื้นที่แคบที่ต้องการมุมกว้าง ลิฟต์
3.6	10	3	มุมมองมาตรฐาน เหมาะสำหรับพื้นที่ทั่วไป
4.0	8	4	เหมาะสำหรับบริเวณเคาน์เตอร์ หน้าร้าน
6.0	6	6	เหมาะสำหรับเน้นรายละเอียดมากขึ้น
8.0	4	10	เหมาะสำหรับทางเดินหรือพื้นที่แคบ ระยะไกล
12.0	2	15	เหมาะสำหรับลานจอดรถหรือพื้นที่ระยะไกล



รูปที่ 3.21 ขนาดของความยาวโฟกัสและมุมมองในการเห็นภาพ

ความยาวโฟกัสของเลนส์ ขนาดของเซนเซอร์รับภาพ และระยะห่างระหว่างกล้องกับวัตถุ เป็นปัจจัยสำคัญที่ส่งผลต่อมุมมองภาพของกล้องโทรทัศน์วงจรปิด โดยเซนเซอร์ที่มีขนาดใหญ่จะให้มุมมองภาพที่กว้างขึ้นเมื่อใช้เลนส์ที่มีความยาวโฟกัสเท่ากัน (Holst & Lomheim, 2011) เมื่อใช้ร่วมกับเลนส์ที่มีความยาวโฟกัสเท่ากัน ดังแสดงในรูปที่ 3.22



รูปที่ 3.22 ความสัมพันธ์ระหว่างระยะโฟกัส ระยะทาง และขนาดอุปกรณ์รับภาพ (ดัดแปลงจาก Teledyne Vision Solutions, 2026)

ความสัมพันธ์ระหว่างความยาวโฟกัสของเลนส์ ระยะห่างจากวัตถุ และขนาดของเซนเซอร์รับภาพ มีผลโดยตรงต่อขนาดของพื้นที่ที่กล้องสามารถมองเห็นได้ (FOV) ความสัมพันธ์ระหว่างความยาวโฟกัสและขนาดพื้นที่มองเห็นในการคำนวณ กำหนดให้

หากต้องการคำนวณจากความสูงของวัตถุ; $$f = \frac{S_V \times D}{Y} \quad (3.1)$$

หากต้องการคำนวณจากความกว้างของวัตถุ; $$f = \frac{S_H \times D}{X} \quad (3.2)$$

เมื่อ f คือ ความยาวโฟกัส (มิลลิเมตร)

S_V คือ ความสูงของเซนเซอร์รับภาพ (มิลลิเมตร)

S_H คือ ความกว้างของเซนเซอร์รับภาพ (มิลลิเมตร)

D คือ ระยะห่างจากกล้องถึงวัตถุ (เมตร)

X คือ ความกว้างของวัตถุ หรือความกว้างของพื้นที่ที่ต้องการมองเห็น (เมตร)

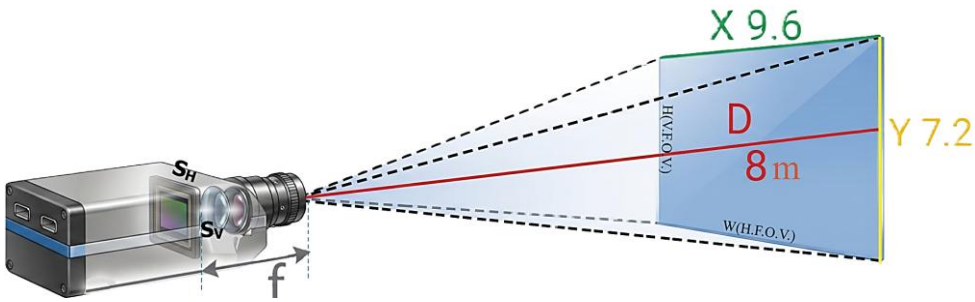
Y คือ ความสูงของวัตถุ หรือความสูงของพื้นที่ที่ต้องการมองเห็น (เมตร)

ตารางที่ 3.4 ขนาดอุปกรณ์รับภาพของ CCD

ขนาดภาพ (Imager Size)	ความกว้าง (H) (mm)	ความสูง (V) (mm)	เส้นทแยงมุม (mm)	หมายเหตุการใช้งาน
1″	12.8	9.6	16.0	งานอุตสาหกรรม/AI/Vision
1/1.8″	7.2	5.3	8.9	กล้องคุณภาพสูง/แสงน้อย
2/3″	8.8	6.6	11.0	กล้องอุตสาหกรรม
1/2″	6.4	4.8	8.0	CCTV คุณภาพสูง
1/2.8″	5.6	3.1	6.9	IP Camera (นิยมใช้งาน)
1/2.7″	5.4	3.0	6.7	กล้อง HD
1/2.5″	5.8	4.3	7.2	กล้องทั่วไป
1/3″	4.8	3.6	6.0	CCTV มาตรฐาน
1/4″	3.6	2.7	4.5	กล้องรุ่นเก่า

ขนาดเซนเซอร์ที่ระบุในรูปแบบ 1/x″ เป็นค่ามาตรฐานเชิงเปรียบเทียบ ไม่ใช่ขนาดจริงของเซนเซอร์ โดยค่าความกว้างและความสูงที่แสดงในตารางเป็นค่าประมาณที่ใช้ในการคำนวณทางวิศวกรรม เช่น การคำนวณมุมมองภาพ (FOV) และความยาวโฟกัสของเลนส์

ตัวอย่างที่ 1 สมมุติว่าต้องการบันทึกภาพพื้นที่ที่มีความกว้าง (X) 9.6 m และสูง (Y) 7.2 m ที่ระยะห่าง (D) 8 m โดยใช้กล้องที่มีเซนเซอร์ขนาด 1/3″ ต้องการคำนวณหาความยาวโฟกัสของเลนส์ ดังรูปที่ 3.23



รูปที่ 3.23 ความสัมพันธ์ระหว่างความยาวโฟกัส ระยะห่างจากวัตถุ และพื้นที่การมองเห็น

แทนค่าในสูตรการความยาวโฟกัสดังนี้ S_V = 3.6 mm, S_H = 4.8 mm, D = 8 m, Y = 7.2 m, และ X = 9.6 m

วิธีทำ

$$f = \frac{S_V \times D}{Y} \quad \text{หรือ} \quad f = \frac{S_H \times D}{X}$$

แทนค่าตามสูตรดังนี้

$$f = \frac{3.6\ \text{mm} \times 8\ \text{m}}{7.2\ \text{m}} = 4\ \text{mm} \quad \text{หรือ} \quad f = \frac{4.8\ \text{mm} \times 8\ \text{m}}{9.6\ \text{m}} = 4\ \text{mm}$$

3.5) ความกว้างของพื้นที่ที่กล้องมองเห็นได้ (Field of View)

มุมมองของ "ปกติ" คล้ายกับสิ่งที่เราเห็นด้วยตาของเราเองและมีความยาวโฟกัสสัมพัมธ์เท่ากับอุปกรณ์รับ ในปัจจุบันจะมีโปรแกรมคิดขนาดของเลนส์ออนไลน์ ซึ่งเป็นอุปกรณ์ที่ใช้ง่ายในการหาความยาวโฟกัสขนาดวัตถุและมุมมอง การคำนวณความยาวโฟกัส ดังนี้

$$x = \frac{S_H \times D}{f} \tag{3.3}$$

เมื่อ f คือ ความยาวโฟกัส

D คือ ระยะห่างของเลนส์ถึงวัตถุ

S_H คือ ความกว้างเซนเซอร์

X คือ ความกว้างของพื้นที่ที่กล้องมองเห็นได้

ตัวอย่างที่ 2 เมื่อใช้กล้องโทรทัศน์วงจรปิดที่มีเซนเซอร์รับภาพขนาด 1/4" ซึ่งมีความกว้างของเซนเซอร์รับภาพ (S_H) เท่ากับ 4.8 mm และใช้เลนส์ที่มีความยาวโฟกัส 4 mm เพื่อจับภาพวัตถุที่ระยะ 10 m ต้องการทราบว่ากล้องสามารถมองเห็นพื้นที่ได้กว้างเท่าใด

วิธีทำ

$$x = \frac{S_H \times D}{f}$$

$$x = \frac{4.8\text{mm} \times 10\text{m}}{4\text{mm}}$$

$$x = 12\ \text{m}$$

ในปัจจุบันมีโปรแกรมคำนวณหาค่าพารามิเตอร์ต่าง ๆ ของเลนส์ในหลายเว็ปไซด์ เพื่อให้เกิดความสะดวกในการติดตั้ง ทั้งในและต่างประเทศ โดยโปรแกรมสามารถใส่ค่าพารามิเตอร์ต่างๆ และสามารถคำนวณค่า คือ มุมมองการมองเห็น (angle) ความกว้าง (width) ความสูง (height) แนวทแยงมุม (diagonal) เช่น โปรแกรม Video Surveillance Design Apps (JVSG.com, 2024) หรือ Calculadora de lentes de visión artificial (Teledyne Vision Solutions, 2026) หรือ Lens Calculator of CCTV Camera (VEC Thai, 2013) มีขั้นตอนหลัก ๆ ดังนี้

ขั้นที่ 1 เข้าเว็บไซต์ http://www.vecthai.com/lens-calculator/index.htm

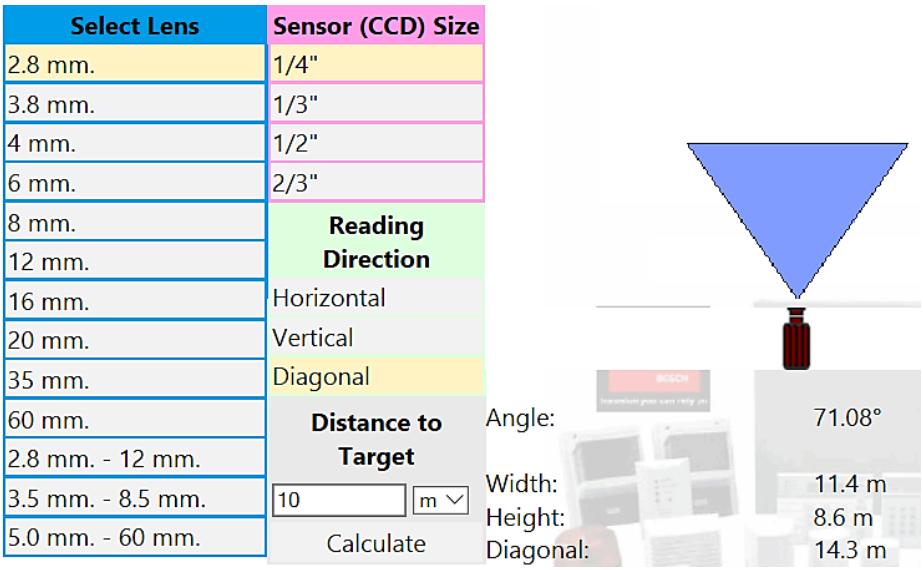
ขั้นที่ 2 เลือกขนาดของ เลนส์ (select lens)

ขั้นที่ 3 เลือกของแผ่นรับภาพ (sensor - CCD)

ขั้นที่ 4 กำหนดทิศทางการอ่าน (reading direction) ตามมุมมอง แนวนอน แนวตั้ง แนวทแยงมุม

ขั้นที่ 5 เลือกกำหนดระยะเป้าหมาย (distance to target)

ขั้นที่ 6 ดูผลของการคำนวณ (calculate) คือ angle, width, height, และ diagonal แสดงดังรูปที่ 3.24



รูปที่ 3.24 โปรแกรมคิดขนาดของเลนส์ออนไลน์ (VEC Thai, 2013)

3.6) ค่ารูรับแสงของเลนส์ (F-Number หรือ F-Stop)

ค่ารูรับแสงของเลนส์ (F-number หรือ F-stop) เป็นค่าที่ใช้แสดงขนาดของช่องรับแสงของเลนส์ ซึ่งมีผลโดยตรงต่อปริมาณแสงที่เข้าสู่เซนเซอร์ โดยค่ารูรับแสงคำนวณจากอัตราส่วนระหว่างความยาวโฟกัสกับขนาดของช่องรับแสง (Holst & Lomheim, 2011) เลนส์จะมีช่วงค่ารูรับแสง เช่น f/1.4, f/2.0, f/2.8, f/4 เป็นต้น โดยสามารถอธิบายได้ดังนี้

- ค่า F ต่ำ (เช่น f/1.4) > ช่องรับแสงกว้าง > แสงเข้ามาก > สำหรับที่แสงน้อย
- ค่า F สูง (เช่น f/8, f/11) > ช่องรับแสงแคบ > แสงเข้าน้อย > สำหรับที่มีแสงมาก

ในระบบกล้องโทรทัศน์วงจรปิด เลนส์แบบ auto iris จะสามารถปรับขนาดรูรับแสงอัตโนมัติตามระดับแสง เพื่อป้องกันภาพสว่างเกิน (overexposure) และช่วยให้ได้ภาพที่เหมาะสมในทุกสภาพแสง นอกจากนี้ ค่า F-stop ยังมีผลโดยตรงต่อความลึกของเขตชัด

3.7) ความลึกของเขตชัด (Depth of Field: DOF)

ความลึกของเขตชัด (DOF) หมายถึง ช่วงระยะของภาพที่ปรากฏชัดเจนในมุมมองของกล้อง ตั้งแต่วัตถุที่อยู่ใกล้ไปจนถึงวัตถุที่อยู่ไกล (Holst & Lomheim, 2011) ความลึกของเขตชัดขึ้นอยู่กับปัจจัยหลัก 3 ประการ ได้แก่

3.7.1) ค่ารูรับแสง (F-stop) F สูง > ชัดลึกมาก แต่ถ้า F ต่ำ > ชัดตื้น

3.7.2) ความยาวโฟกัสของเลนส์ (focal length) เลนส์มุมกว้าง > ชัดลึกมาก ถ้าเลนส์เทเลโฟโต้ > ชัดตื้น

3.7.3) ระยะห่างจากวัตถุ (distance) วัตถุใกล้ > ชัดตื้น แต่วัตถุไกล > ชัดลึก

ในเวลากลางคืน เลนส์จะเปิดรูรับแสงกว้าง (F ต่ำ) เพื่อรับแสงมากขึ้น ส่งผลให้ความลึกของเขตชัดลดลง ทำให้บางวัตถุอาจไม่อยู่ในโฟกัสเมื่อเทียบกับเวลากลางวัน

3.8) หน่วยวัดความสว่าง (Lux)

Lux เป็นหน่วยวัดความสว่างของแสง (illuminance) ซึ่งกำหนดโดยระบบ SI โดย 1 Lux เท่ากับปริมาณแสง 1 ลูเมนต่อตารางเมตร (1 lumen/m²) ในระบบกล้องโทรทัศน์วงจรปิด ค่า Lux ใช้บ่งบอกระดับแสงขั้นต่ำที่กล้องสามารถให้ภาพที่ใช้งานได้ โดยทั่วไป

- ค่า Lux ต่ำ > กล้องทำงานได้ดีในที่มืด
- ค่า Lux สูง > ต้องใช้แสงมากขึ้น

ตัวอย่างเช่น 0.8 Lux (color mode) หมายถึง กล้องสามารถให้ภาพสีได้เมื่อมีแสงอย่างน้อย 0.8 Lux หากแสงต่ำกว่านี้ กล้องจะเปลี่ยนเป็นภาพขาวดำ (black and white mode)

ตารางที่ 3.5 แสดงแสงสว่างโดยประมาณของค่า Lux

ค่าของ Lux	สถานที่
10,000 Lux	แสงแดดในตอนกลางวัน
500 Lux	แสงสว่างภายในอาคาร ห้างสรรพสินค้าขณะเปิดไฟ
100 Lux	ภายในอาคารจอดรถ
10 Lux	แสงไฟถนน
1 Lux	แสงจากการจุดเทียน 1 เล่ม
0.1 Lux	ตอนกลางคืนขณะที่พระจันทร์เต็มดวง
0 Lux	ที่มืดสนิท จะมองเห็นได้กล้องจะต้องทำงานร่วมกับแสงอินฟราเรดเป็นตัวส่อง และยิ่งมีหลอดอินฟราเรดมาก ก็จะยิ่งทำให้ส่องแสงไกลขึ้น แต่รูปที่ได้จะเป็นภาพขาวดำ หมายเหตุ: กล้องที่มีค่า 0 Lux มักเป็นกล้องที่มี Infrared (IR) ช่วยส่องสว่าง ไม่ได้หมายความว่ากล้องมองเห็นได้โดยไม่มีแสงเลย

3.3.4 เครื่องบันทึกภาพ (Video Recorder)

เครื่องบันทึกภาพเป็นอุปกรณ์สำคัญในระบบกล้องโทรทัศน์วงจรปิด ทำหน้าที่รับสัญญาณภาพจากกล้อง บันทึกข้อมูลลงในหน่วยเก็บข้อมูล และแสดงผลหรือส่งต่อข้อมูลไปยังอุปกรณ์อื่น เช่น จอภาพหรือระบบเครือข่าย เครื่องบันทึกภาพสามารถแบ่งออกได้เป็น 2 ประเภทหลัก ได้แก่ DVR และ NVR (SKnBiz. 2020)

รูปที่ 3.25 เครื่องบันทึกภาพ NVR และ DVR

1) เครื่องบันทึกภาพระบบแอนะล็อก (Digital Video Recorder: DVR)

DVR เป็นเครื่องบันทึกภาพที่ใช้กับกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก โดยสัญญาณภาพจากกล้องจะถูกส่งมาในรูปแบบแอนะล็อกผ่านสายโคแอกเชียล จากนั้นเครื่อง DVR จะทำหน้าที่แปลงสัญญาณแอนะล็อกให้เป็นสัญญาณดิจิทัลก่อน จากนั้นทำการบันทึกลงในฮาร์ดดิสก์ องค์ประกอบหลักของ DVR ได้แก่

1.1) ช่องรับสัญญาณภาพและเสียง (video/audio input)

1.2) ช่องส่งสัญญาณออก (HDMI, VGA)

1.3) วงจรแปลงสัญญาณ (Analog to Digital Converter: ADC)

1.4) หน่วยประมวลผลและบีบอัดภาพ (Compression เช่น H.264/H.265)

1.5) หน่วยเก็บข้อมูล (hard disk: HHD)

1.6) ช่องเชื่อมต่อเครือข่าย (LAN)

1.7) ช่องเชื่อมต่ออุปกรณ์ภายนอก เช่น USB

มีข้อดี คือ ราคาประหยัด และเหมาะกับระบบขนาดเล็กถึงกลาง ส่วนข้อจำกัดความละเอียดจำกัดเมื่อเทียบกับระบบ IP ต้องเดินสายเฉพาะโคแอกเชียล

2) เครื่องบันทึกภาพระบบดิจิทัล (Network Video Recorder: NVR)

NVR เป็นเครื่องบันทึกภาพที่ใช้กับกล้องโทรทัศน์วงจรปิดระบบ IP โดยกล้องจะทำการแปลงสัญญาณเป็นดิจิทัลตั้งแต่ต้นทาง และส่งข้อมูลผ่านเครือข่าย LAN มายัง NVR เพื่อบันทึกลักษณะการทำงาน จะรับสัญญาณภาพจากกล้อง IP โดยส่งข้อมูลผ่านเครือข่าย จากนั้น NVR รับข้อมูลและบันทึกลงฮาร์ดดิสก์ มีคุณสมบัติเด่น คือ

2.1) รองรับความละเอียดสูง (HD, full HD, 4K)

2.2) ใช้สายสัญญาณเครือข่าย (UTP) หรือ fiber optic

2.3) รองรับระบบจ่ายไฟผ่านสายสัญญาณเครือข่าย Power over Ethernet (PoE)

2.4) สามารถดูภาพผ่านเครือข่ายหรืออินเทอร์เน็ตได้สะดวก

2.5) รองรับระบบอัจฉริยะ เช่น AI, face detection

ข้อดี คือ ภาพคมชัดสูง มีระบบยืดหยุ่น ขยายง่าย และรองรับเทคโนโลยีใหม่ ในส่วนของข้อจำกัด คือ ราคาสูงกว่า DVR ต้องมีความรู้ด้านเครือข่าย

3.3.5 ฮาร์ดดิสก์สำหรับงานระบบกล้องโทรทัศน์วงจรปิด

ฮาร์ดดิสก์ (HHD) ที่ใช้สำหรับระบบกล้องโทรทัศน์วงจรปิด เป็นอุปกรณ์จัดเก็บข้อมูลที่ถูกออกแบบมาเฉพาะสำหรับการทำงานแบบต่อเนื่องตลอด 24 ชั่วโมง (24/7 operation) โดยมีคุณสมบัติแตกต่างจากฮาร์ดดิสก์ทั่วไป (desktop HDD) อย่างชัดเจน ทั้งในด้านความทนทาน การจัดการข้อมูล และรูปแบบการใช้งาน ฮาร์ดดิสก์สำหรับกล้องโทรทัศน์วงจรปิดถูกออกแบบให้รองรับการทำงานในลักษณะ เขียนข้อมูล (write) ต่อเนื่องเป็นหลัก ซึ่งอาจมีสัดส่วนการเขียนมากกว่า 90% ของการใช้งานทั้งหมด เนื่องจากระบบกล้องต้องบันทึกภาพและวิดีโออย่างต่อเนื่อง นอกจากนี้ยังรองรับการทำงานพร้อมกันจากกล้องหลายตัว (multi-stream recording) และมีความสามารถในการจัดการข้อมูลแบบสตรีมมิ่งได้อย่างมีประสิทธิภาพ

ในด้านโครงสร้างฮาร์ดดิสก์ประเภทนี้ถูกออกแบบให้มีความทนทานต่ออุณหภูมิสูงและการทำงานระยะยาว รวมถึงมีระบบควบคุมพลังงานและการทำงานที่เหมาะสมกับการใช้งานต่อเนื่อง เพื่อลดความเสี่ยงต่อความเสียหายของข้อมูล ตัวอย่างฮาร์ดดิสก์สำหรับระบบกล้องโทรทัศน์วงจรปิด ได้แก่ Seagate SkyHawk ซึ่งพัฒนาเฟิร์มแวร์เฉพาะสำหรับงานวิดีโอ เช่น เทคโนโลยี ImagePerfect™ ที่ช่วยลดการสูญเสียเฟรม (frame loss) และเพิ่มความต่อเนื่องของการบันทึกวิดีโอ รองรับการบันทึกข้อมูลจากกล้องหลายตัวพร้อมกัน โดยในบางรุ่นสามารถรองรับได้สูงสุดประมาณ 64 ช่องสัญญาณ ขึ้นอยู่กับรุ่นและสเปกของอุปกรณ์ นอกจากนี้ยังมีระบบ SkyHawk Health Management (SHM) ซึ่งเป็นระบบตรวจสอบสถานะการทำงานของฮาร์ดดิสก์แบบฝังตัว (embedded monitoring) ที่ช่วยวิเคราะห์และแจ้งเตือนเมื่อพบความผิดปกติ เพื่อป้องกันการสูญเสียข้อมูลและเพิ่มความน่าเชื่อถือของระบบ โดยทั่วไปฮาร์ดดิสก์ประเภทนี้มีหลายความจุให้เลือกใช้งาน เช่น 1TB –10TB หรือมากกว่า รองรับการเชื่อมต่อผ่านอินเทอร์เฟซแบบ SATA III (6 Gb/s) และมีอัตราการรับส่งข้อมูลที่เหมาะสมกับงานบันทึกวิดีโอความละเอียดสูง เช่น HD และ Full HD

รูปที่ 3.26 ฮาร์ดดิสก์สำหรับระบบกล้องโทรทัศน์วงจรปิด

1) คำนวณกับความจุ hard disk จะได้สูตรนี้

จำนวนพื้นที่จัดเก็บจากความละเอียดของกล้อง (pixel) x จำนวนกล้อง ได้ค่าความจุจำนวนกล้องแล้ว นำมาคิดกับจำนวนความจุ hard disk โดยจำนวน hard disk 1 TB = 1000 GB ใช้ได้ 90% จะต้องเลือกใช้ 1000 – 10% = 900 GB

$$\frac{\text{จำนวนความจุ}}{\text{ค่าความจุจำนวนกล้อง}} = \text{จำนวนวันโดยเฉลี่ย} \qquad (3.4)$$

ตัวอย่างที่ 3 กล้องมีความละเอียด 2 ล้านพิกเซล (35 GB) จำนวน 2 ตัว จะได้ 35 x 2 = 70 GB/วัน จากนั้นนำค่า hard disk 1 TB = 1000 GB

$$1000 - 10\% = 900 \text{ GB}$$

$$\frac{900}{70} = 12.8 \ (\sim 12 \text{ วัน})$$

ผลลัพธ์คือ ใช้กล้องความละเอียด 2 ล้านพิกเซล 2 ตัว บันทึกภาพบนความจุ HHD 1 TB จะสามารถบันทึกภาพได้นาน 12 วันโดยเฉลี่ย อัตราการใช้งานพื้นที่บันทึกข้อมูล HDD ดังตารางที่ 3.6

ตารางที่ 3.6 อัตราการใช้งานพื้นที่บันทึกข้อมูล HDD

การเข้ารหัส	อัตราการใช้งานพื้นที่บันทึกข้อมูล HDD			
	1ตัว	4ตัว	8ตัว	16ตัว
CIF	5 GB	20 GB	40 GB	80 GB
D1	20 GB	80 GB	160 GB	320 GB
1.0 MP	15 GB	60 GB	120 GB	240 GB
1.3 MP	25 GB	100 GB	200 GB	400 GB
2.0 MP	40 GB	160 GB	320 GB	640 GB
3.0 MP	30 GB	240 GB	480 GB	960 GB
4.0 MP	80 GB	320 Gb	640 GB	1280 GB

การใช้งานระบบกล้องโทรทัศน์วงจรปิด ระยะเวลาในการบันทึกภาพ (recording time) จะขึ้นอยู่กับปัจจัยหลายประการ เช่น ความละเอียดของภาพ (resolution) อัตราเฟรม (frame rate) รูปแบบการบีบอัด (compression) และความจุของฮาร์ดดิสก์ (HDD) โดยทั่วไป การคำนวณระยะเวลาการบันทึกมักอ้างอิงจากกล้องจำนวน 1 ตัว กับฮาร์ดดิสก์ขนาด 1 TB หากมีการใช้งานกล้องหลายตัว ระยะเวลาการบันทึกจะลดลงตามจำนวนกล้องที่เพิ่มขึ้น กล่าวคือ ต้องนำจำนวนกล้องมาหารระยะเวลาที่ได้จากการคำนวณ อย่างไรก็ตาม สามารถเพิ่มระยะเวลาในการบันทึกได้ด้วยวิธีต่าง ๆ ดังนี้

1) เพิ่มความจุของฮาร์ดดิสก์ (HDD Capacity)

เป็นวิธีที่ตรงไปตรงมาและมีประสิทธิภาพ โดยการเพิ่มขนาดหรือจำนวนฮาร์ดดิสก์ในเครื่องบันทึก เช่น หากเพิ่มฮาร์ดดิสก์จาก 1 TB เป็น 4 TB ระยะเวลาในการบันทึกจะเพิ่มขึ้นประมาณ 4 เท่า ทั้งนี้ เครื่องบันทึกบางรุ่นสามารถติดตั้งฮาร์ดดิสก์ได้มากกว่า 1 ลูก เช่น 2–8 ลูก ซึ่งจะช่วยเพิ่มระยะเวลาในการบันทึกได้อย่างมีนัยสำคัญ

2) ลดอัตราเฟรม (Frame Rate)

อัตราเฟรมเป็นจำนวนภาพต่อวินาที (frames per second: fps) โดยทั่วไปการบันทึกที่ 25–30 fps จะให้ภาพเคลื่อนไหวที่ต่อเนื่อง หากลดอัตราเฟรมลง เช่น เหลือ 12–15 fps จะช่วยลดปริมาณข้อมูล (bitrate) ลงประมาณครึ่งหนึ่ง ส่งผลให้สามารถบันทึกข้อมูลได้นานขึ้น อย่างไรก็ตาม ภาพที่ได้อาจมีความต่อเนื่องลดลง

3) ลดความละเอียดของภาพ (Resolution)

การลดความละเอียดของภาพ เช่น จาก full HD (1080p) เป็น HD (720p) จะช่วยลดขนาดของข้อมูลและเพิ่มระยะเวลาในการบันทึกได้ อย่างไรก็ตาม วิธีนี้จะทำให้รายละเอียดของภาพลดลง จึงควรพิจารณาตั้งค่าตั้งแต่ขั้นตอนการออกแบบระบบ และไม่แนะนำให้ปรับลดลงหากต้องการใช้ศักยภาพของกล้องอย่างเต็มประสิทธิภาพ

4) เพิ่มอุปกรณ์จัดเก็บข้อมูลภายนอก (External Storage)

ในกรณีที่เครื่องบันทึกไม่สามารถเพิ่มฮาร์ดดิสก์ภายในได้ สามารถใช้อุปกรณ์จัดเก็บข้อมูลภายนอก เช่น eSATA หรือ Network Storage (NAS) เพื่อขยายความจุในการบันทึก ทั้งนี้ต้องตรวจสอบความเข้ากันได้กับเครื่องบันทึกก่อนใช้งาน

5) คำนวณหาแบนด์วิธ (Bandwidth)

แบนด์วิธ คือ การวัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต ซึ่งโดยมากมักวัดความเร็วของการส่งข้อมูลเป็น bps (bit per second), Mbp (bps*1000000) เช่น bandwidth ของการใช้สายโทรศัพท์ในประเทศไทย เท่ากับ 14.4 Kbps, bandwidth ของสายส่งข้อมูลที่ใช้ในการเชื่อมต่อกับอเมริกาเท่ากับ 2 Mbps เป็นต้น โดยมีสูตรคำนวณหาแบนด์วิธ ดังนี้

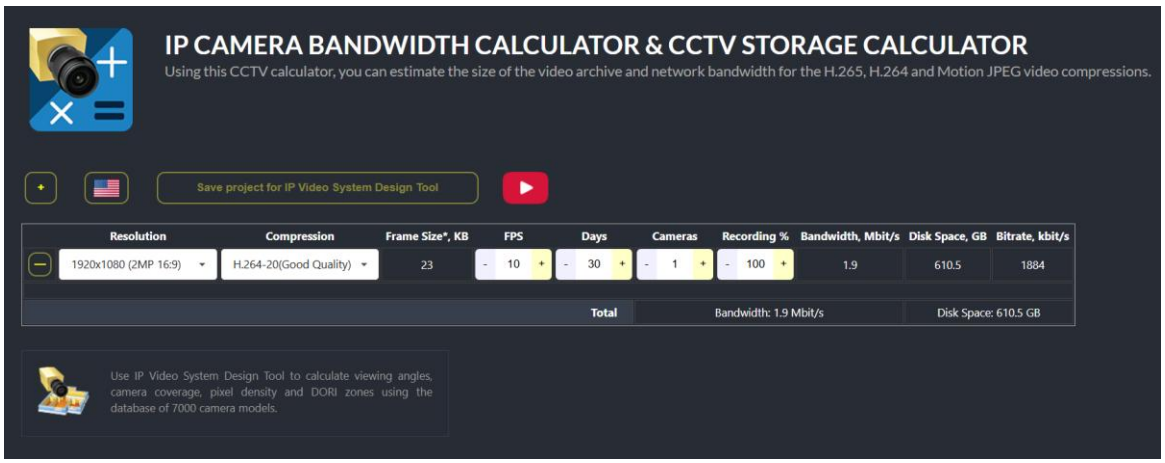
$$\text{พื้นที่แบนด์วิธ} = \text{จำนวนกล้อง} \times \text{อัตราการบันทึก} \qquad (3.5)$$

ตัวอย่างที่ 4 สมมุติว่าในระบบมีกล้องทั้งหมด 500 กล้อง และแต่ละกล้อง ใช้อัตราการบันทึกที่ 512 kbps พื้นที่แบนด์วิธ จากสูตร

$$\begin{aligned} \text{พื้นที่แบนด์วิธ} &= \text{จำนวนกล้อง} \times \text{อัตราการบันทึก} \\ &= 500 \times 512 \\ &= 256 \text{ Mbps} \end{aligned}$$

ในกรณีที่ระบบมีแบนด์วิดท์จำกัด เช่น มีแบนด์วิดท์รวมเพียง 100 Mbps แม้จะสามารถใช้งานระบบกล้องโทรทัศน์วงจรปิดได้ แต่เมื่อปริมาณข้อมูลจากกล้องรวมกันเกินความสามารถของเครือข่าย จะส่งผลให้เกิดความล่าช้าในการส่งข้อมูล (delay) รวมถึงอาจเกิดอาการภาพกระตุกหรือข้อมูลสูญหาย (packet loss) ได้ เพื่อให้เข้าใจง่าย สามารถเปรียบเทียบแบนด์วิดท์กับ “ถนน” และข้อมูลกับ “รถยนต์” ได้ กล่าวคือ แบนด์วิดท์เปรียบเสมือนความกว้างของถนน ส่วนข้อมูลจากกล้องแต่ละตัวเปรียบเสมือนรถยนต์ที่วิ่งบนถนนนั้น หากจำนวนรถมีมากกว่าความสามารถของถนนในการรองรับ จะทำให้เกิดการชะลอตัวและต้องรอคิว ส่งผลให้การเดินทางล่าช้า ในลักษณะเดียวกัน หากระบบกล้องโทรทัศน์วงจรปิดมีอัตราการส่งข้อมูลรวม (total bitrate) เช่น 256 Mbps แต่เครือข่ายรองรับได้เพียง 100 Mbps ข้อมูลจะไม่สามารถส่งผ่านได้ทันทีทั้งหมด จำเป็นต้องมีการรอคิวหรือถูกหน่วงเวลา ทำให้เกิดความล่าช้าในการแสดงผลหรือการควบคุมระบบ ดังนั้น การออกแบบระบบเครือข่ายสำหรับกล้องโทรทัศน์วงจรปิดควรคำนึงถึงความเพียงพอของแบนด์วิดท์ โดยควรเลือกใช้อุปกรณ์เครือข่ายที่สามารถรองรับปริมาณข้อมูลรวมของระบบได้อย่างเหมาะสม เพื่อให้การส่งข้อมูลมีความต่อเนื่องและมีประสิทธิภาพ

ปัจจุบันมีโปรแกรมคำนวณหาคำนวณกับความจุ hard disk มาช่วยในการคำนวณ ดังรูปที่ 3.27 โดยมีขั้นตอนดังนี้ (1) เข้าเว็บไซต์ https://www.jvsg.com/ip-video-system-design-tool/ (2) เลือก Bandwidth and Storage Calculator (3) เลือกกำหนดค่าพารามิเตอร์ของระบบ และ (4) ระบบจะคำนวณค่าความจุของตัวจัดเก็บข้อมูล



รูปที่ 3.27 โปรแกรมคำนวณความจุของฮาร์ดดิสก์ไดร์ฟ (jvsg.com, 2024)

3.3.6 จอภาพ (Monitor)

จอมอนิเตอร์กล้องโทรทัศน์วงจรปิดทำหน้าที่เป็นอุปกรณ์ดูภาพวีดีโอที่ได้รับสด ๆ จากกล้องโทรทัศน์วงจรปิดตัวเดียวหรือหลาย ๆ ตัว ใช้สำหรับเล่นย้อนกลับมาดูภาพวีดีโอที่ถูกบันทึกเก็บไว้โดย เครื่องบันทึกภาพวีดีโอ (DVR/NVR) เพื่อดูเหตุการณ์ที่เกิดขึ้นมาก่อนแล้ว โดยทั่วไปจอภาพที่ใช้ในระบบกล้องโทรทัศน์วงจรปิดสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ได้แก่ จอภาพแบบ CRT, LCD และ LED ซึ่งแต่ละประเภทมีหลักการทำงานและคุณสมบัติที่แตกต่างกัน ดังนี้

1) จอภาพแบบ Cathode Ray Tube (CRT)

จอภาพแบบ CRT เป็นเทคโนโลยีจอภาพรุ่นเก่าที่ใช้หลอดภาพในการแสดงผล โดยอาศัยการยิงลำอิเล็กตรอนไปยังพื้นผิวฟอสฟอรัสบนหน้าจอ เพื่อสร้างภาพผ่านการผสมของแสงสีหลัก ได้แก่ สีแดง สีเขียว และสีน้ำเงิน (RGB) ลักษณะเด่นของจอ CRT คือสามารถแสดงภาพได้ต่อเนื่องและมีการตอบสนองที่รวดเร็ว อย่างไรก็ตาม จอ CRT มีข้อจำกัดหลายประการ เช่น ขนาดใหญ่ น้ำหนักมาก ใช้พลังงานสูง และเกิดความร้อนขณะใช้งาน นอกจากนี้ยังมีการแผ่รังสีในระดับหนึ่ง ทำให้ในปัจจุบันจอภาพประเภทนี้ได้ถูกยกเลิกการผลิตและแทนที่ด้วยเทคโนโลยีสมัยใหม่

2) จอภาพแบบ Liquid Crystal Display (LCD)

จอภาพแบบ LCD ใช้หลักการของผลึกเหลว (liquid crystal) ในการควบคุมการผ่านของแสง โดยมีแหล่งกำเนิดแสงพื้นหลัง (backlight) ซึ่งในอดีตมักใช้หลอดฟลูออเรสเซนต์ (Cold Cathode Fluorescent Lamp: CCFL) เป็นตัวให้แสง จอ LCD มีข้อดีคือมีขนาดบาง น้ำหนักเบา ใช้พลังงานน้อยกว่าจอ CRT และไม่เกิดการสั่นไหวของภาพเหมือนจอ CRT อย่างไรก็ตาม ข้อจำกัดของจอ LCD ได้แก่ มุมมองภาพที่อาจแคบ และการตอบสนองของภาพอาจช้ากว่าในบางรุ่น ส่งผลให้ภาพเคลื่อนไหวเร็วอาจเกิดอาการเบลอได้

3) จอภาพแบบ Light Emitting Diode (LED)

จอภาพแบบ LED เป็นการพัฒนาต่อยอดจากเทคโนโลยี LCD โดยยังคงใช้หลักการของผลึกเหลวเช่นเดียวกัน แต่เปลี่ยนแหล่งกำเนิดแสงพื้นหลังจากหลอด CCFL มาเป็นหลอด LED ซึ่งมีขนาดเล็กและประหยัดพลังงานมากกว่า ข้อดีของจอ LED ได้แก่ ความสว่างสูง ประหยัดพลังงาน ให้สีสันคมชัด และมีความร้อนต่ำ รวมถึงสามารถออกแบบให้มีความบางได้มากขึ้น จึงเป็นจอภาพที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบัน โดยเฉพาะในระบบกล้องโทรทัศน์วงจรปิดที่ต้องการความคมชัดและความเสถียรในการแสดงผล

ก) จอ CRT ข) จอ LCD ค) จอ LED

รูปที่ 3.28 จอภาพ

3.3.7 สายนำสัญญาณ (Transmission Medium)

สายนำสัญญาณ (transmission medium) เป็นอุปกรณ์สำคัญในระบบกล้องโทรทัศน์วงจรปิด ทำหน้าที่เป็นตัวกลางในการนำและถ่ายทอดสัญญาณภาพจากกล้องไปยังอุปกรณ์ปลายทาง เช่น เครื่องบันทึกภาพ (DVR/NVR) หรือจอแสดงผล แม้ว่าปัจจุบันกล้องโทรทัศน์วงจรปิดจะมีการพัฒนาในด้านความละเอียดของภาพ ความสามารถในการประมวลผล และฟังก์ชันอัจฉริยะต่าง ๆ อย่างต่อเนื่อง แต่หากสื่อกลางในการส่งข้อมูลไม่มีประสิทธิภาพ ก็จะส่งผลให้คุณภาพของระบบโดยรวมลดลง โดยเฉพาะในระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก คุณภาพของสายสัญญาณมีผลโดยตรงต่อความคมชัดของภาพและระดับสัญญาณรบกวน หากใช้สายที่มีคุณภาพต่ำหรือไม่ได้มาตรฐาน อาจทำให้เกิดสัญญาณรบกวน (noise) การลดทอนสัญญาณ (attenuation) และภาพไม่ชัดเจนได้ การเลือกใช้สายสัญญาณที่มีคุณภาพและเหมาะสมกับระยะทางจึงเป็นสิ่งสำคัญอย่างยิ่ง

1) สายโคแอกเชียล (Coaxial Cable)

สายโคแอกเชียลเป็นสายสัญญาณที่นิยมใช้ในระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก โดยมีโครงสร้างประกอบด้วย (1) แกนตัวนำ (center conductor) ทำจากทองแดง ใช้สำหรับส่งสัญญาณ (2) ชั้นฉนวน (dielectric insulator) (3) ชั้นป้องกันสัญญาณรบกวน (shielding) ซึ่งอาจเป็นฟอยล์หรือสายถักโลหะ และ (4) เปลือกหุ้มภายนอก (outer jacket) ชั้น shielding มีหน้าที่ป้องกันสัญญาณรบกวนจากภายนอก และช่วยรักษาคุณภาพของสัญญาณ โดยแกนกลางและชั้น Shield จะต้องไม่สัมผัสกัน เพื่อป้องกันการลัดวงจร

1.1) โครงสร้างภายในสายโคแอกเชียล

1.1.1) ตัวนำสัญญาณ (Conductor)

ส่วนใหญ่แล้วจะเป็นเหล็กหุ้มด้วยทองแดง ถ้าหุ้มด้วยทองแดง Copper Covered Steel (CCS) จะบอกเป็นเปอร์เซนต์ของทองแดงหุ้มหรือบางครั้งจะใช้เป็นทองแดงล้วนไปเลย สาเหตุที่ส่วนใหญ่ไม่ใช้เป็นแกนทองแดงล้วนเพราะ ราคาทองแดงราคาสูง และกระแสไฟฟ้าส่วนใหญ่จะไหลผ่านตัวนำที่บริเวณพื้นที่ผิวของวัตถุ

1.1.2) ฉนวนหุ้ม (Insulator)

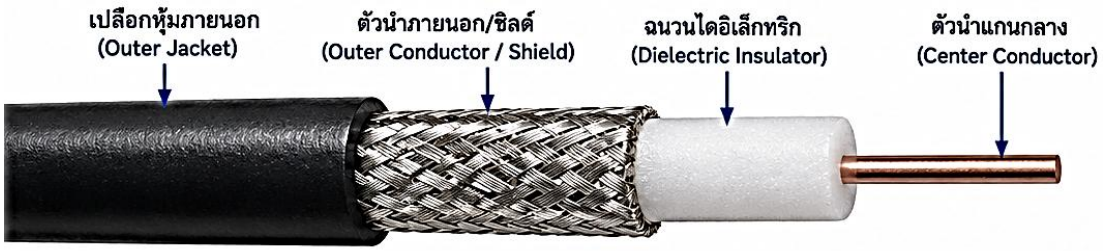
ทำหน้าที่ป้องกันสัญญาณรบกวน จะใช้เป็นโฟม หรือ Polyethylene Foam (PE) แล้วหุ้มทับด้วยเทปอลูมิเนียม

1.1.3) ชิลด์หรือเส้นถัก (Wire Braid Shield)

ส่วนใหญ่ทำจากอลูมิเนียมและทองแดง ป้องกันการแพร่กระจายของสัญญาณรบกวน และการกระจายของสัญญาณออกมาภายนอก จะบอกเป็นเปอร์เซนต์คือพื้นที่ความหนาแน่นที่ในการถัก เช่น 60% 90% 95% สูงสุดอยู่ที่ 95% หรือจำนวนของเส้นที่ใช้ในการถัก เช่น 112, 120, 124, 144 เส้นยิ่งมากก็ยิ่งช่วยในการนำสัญญาณได้ดี และป้องกันสัญญาณรบกวนจากภายนอก ทำให้เดินสายในระยะไกลขึ้น และป้องกันการกวนของสัญญาณจากภายนอกดี

1.1.4) เปลือกหุ้มสาย (Plastic Jacket)

ทำหน้าที่หุ้มสายทั้งหมดถ้าใช้ภายในจะทำด้วย Polyvinylchloride (PVC) ส่วนภายนอกจะใช้วัสดุที่เป็น PE ซึ่งมีคุณสมบัติสามารถป้องกันน้ำและทนแดด สามารถใช้ภายนอกได้ ดังรูปที่ 3.29



รูปที่ 3.29 โครงสร้างของโคแอกเชียล

1.2) ประเภทของสายโคแอกเชียลที่นิยมใช้ในระบบ CCTV ได้แก่ สาย RG6 สาย RG59 และสาย RG11

1.2.1) สาย RG59

สาย RG59 มีขนาดเล็กกว่า RG6 มีความยืดหยุ่นสูง เหมาะสำหรับงานติดตั้งภายในอาคารหรือพื้นที่ที่ต้องการความคล่องตัว เช่น ภายในลิฟต์หรือพื้นที่จำกัด อย่างไรก็ตาม RG59 มีค่าการลดทอนสัญญาณสูงกว่า จึงเหมาะกับการใช้งานในระยะทางสั้น โดยทั่วไปไม่ควรเกินประมาณ 200–300 m (ขึ้นอยู่กับคุณภาพสายและระบบที่ใช้งาน)

1.2.2) สาย RG6

สาย RG6 เป็นสายที่นิยมใช้งานในระบบส่งสัญญาณภาพ เช่น โทรทัศน์ เคเบิล และกล้องโทรทัศน์วงจรปิด มีขนาดใหญ่กว่าสาย RG59 และมีค่าการลดทอนสัญญาณต่ำกว่า จึง

สามารถส่งสัญญาณได้ในระยะไกลกว่าในการใช้งานระบบ CCTV ควรเลือกสาย RG6 ที่มีค่าการป้องกันสัญญาณรบกวน (shielding) สูง เช่น 90–95% เพื่อให้ได้คุณภาพของภาพที่คมชัดและลดสัญญาณรบกวน ใช้ในการเดินสายกล้องโทรทัศน์วงจรปิดในระยะ 0-700 m

1.2.3) สาย RG11

สาย RG11 เป็นสายโคแอกเชียลที่มีขนาดใหญ่ที่สุดในกลุ่มนี้ มีค่าการลดทอนสัญญาณต่ำมาก จึงสามารถส่งสัญญาณได้ในระยะไกล เช่น หลายร้อยเมตร อยู่ที่ประมาณระยะทาง 700-1000 m สายประเภทนี้เหมาะสำหรับงานติดตั้งภายนอกหรือระบบที่ต้องการเดินสายระยะไกล แต่มีข้อจำกัดคือมีขนาดใหญ่ แข็ง และติดตั้งได้ยากกว่าสายชนิดอื่น ใช้ในการเดินสายกล้องโทรทัศน์วงจรปิดใน

ตารางที่ 3.7 คุณลักษณะของสายโคแอกเชียลเบอร์ต่าง ๆ

เบอร์สาย (n)	โครงสร้าง (mm)	เส้นผ่านศูนย์กลางของฉนวน (mm)	อัตราการครอบคลุมของฉนวนถัก (%)	ขนาดเส้นผ่าศูนย์กลาง (mm)
RG58	19/0.18	2.95	-	4.95
RG59	1/0.81	3.70	60%	6.10
RG59message	1/0.81+1/1.30	3.70	60%	6.10
RG6	1/1.02	4.57	60%	7.00
RG6message	1/1.02+1/1.30	4.57	60%	7.00
RG7	1/1.29	5.72	60%	8.10
RG7message	1/1.29+1/1.83	5.72	60%	8.10
RG11	1/1.63	7.11	60%	10.1
RG11message	1/1.63+1/1.83	7.11	60%	10.1
RG174	7/0.16	1.50	95%	2.80
RG179	1/0.31	1.42	95%	2.54
RG213	7/0.75	7.25	-	10.1
QR500	1/2.77	11.5	-	14.7
QR540	1/3.15	13.0	-	15.4

ลักษณะของสายและคุณสมบัติของสายสายโคแอกเชียลเบอร์ต่าง ๆ สรุปดังรูปที่ 3.30 (Ningbo Holden Cable Co., Ltd., 1998)

รุ่นสาย (Type)	RG-178	RG-174	RG-316	RG-141	RG-59	RG-6	RG-8	RG-213	RG-214	LMR-195
อิมพีแดนซ์ (Ω)	50	50	50	50	75	75	50	50	50	50
เส้นผ่านศูนย์กลางภายนอก (ประมาณ, mm)	1.8	2.8	2.5	4.1	6.0	6.9	10.3	10.3	10.8	4.9
การใช้งานทั่วไป	อุปกรณ์ RF ขนาดเล็ก	อุปกรณ์ RF ทั่วไป	งานความถี่สูง	งานการบิน และอวกาศ	ระบบวิดีโอ และ CCTV	ทีวีและ ระบบกระจายสัญญาณ	งานสื่อสาร และ RF กำลังสูง	งานสื่อสาร และ RF กำลังสูง	งานสื่อสารที่ต้องการ ชิลด์สุนทานเป็นพิเศษ	งาน RF ความสูญเสียน้อย

รูปที่ 3.30 ลักษณะของสาย RG ชนิดต่าง ๆ

2) สายคู่บิดเกลียว (Twisted Pair Cable)

สายคู่บิดเกลียวเป็นสื่อนำสัญญาณที่ประกอบด้วยสายทองแดง 2 เส้นบิดเกลียวเข้าด้วยกัน เพื่อลดการรบกวนทางแม่เหล็กไฟฟ้า (Electromagnetic Interference: EMI) และลดการรบกวนระหว่างคู่สาย (crosstalk) การบิดเกลียวช่วยให้สัญญาณมีความเสถียรมากขึ้นและสามารถส่งข้อมูลได้อย่างมีประสิทธิภาพ สายประเภทนี้นิยมใช้อย่างแพร่หลายในระบบเครือข่ายคอมพิวเตอร์และระบบกล้องโทรทัศน์วงจรปิดแบบ IP เนื่องจากมีราคาประหยัด ติดตั้งง่าย น้ำหนักเบา และรองรับการส่งข้อมูลความเร็วสูง อย่างไรก็ตาม ระยะทางในการใช้งานของสายคู่บิดเกลียวมาตรฐาน (เช่น Cat5e, Cat6) โดยทั่วไปไม่ควรเกิน 100 m/segment ตามมาตรฐานเครือข่าย สายคู่บิดเกลียวสามารถแบ่งออกได้เป็น 2 ประเภทหลัก (Richard, 2022)

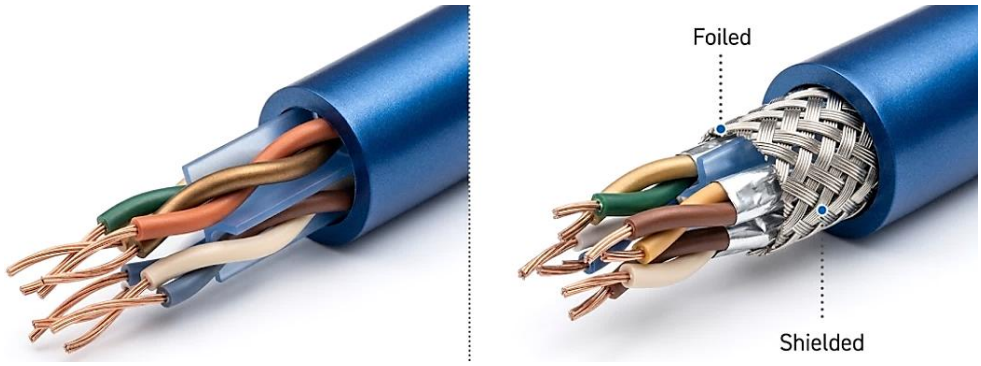
2.1) ชนิดของสายคู่บิดเกลียว

2.1.1) สายคู่บิดเกลียวมีฉนวนป้องกัน (Shielded Twisted Pair: STP)

สาย STP เป็นสายที่มีชั้นป้องกันสัญญาณรบกวนเพิ่มเติม (shielding) ซึ่งอาจเป็นฟอยล์โลหะหรือสายถักโลหะ (braided shield) ห่อหุ้มสายคู่บิดเกลียวไว้ วัตถุประสงค์เพื่อป้องกันการรบกวนจากคลื่นแม่เหล็กไฟฟ้าภายนอก เช่น คลื่นวิทยุ หรืออุปกรณ์ไฟฟ้ากำลังสูง สาย STP เหมาะสำหรับใช้งานในสภาพแวดล้อมที่มีสัญญาณรบกวนสูง เช่น โรงงานอุตสาหกรรม หรือบริเวณที่มีอุปกรณ์ไฟฟ้าขนาดใหญ่ อย่างไรก็ตาม สายชนิดนี้มีราคาสูงกว่าและติดตั้งได้ยากกว่าสาย UTP

2.1.2) สายคู่บิดเกลียวไม่มีฉนวนป้องกัน (Unshielded Twisted Pair: UTP)

สาย UTP เป็นสายคู่บิดเกลียวที่ไม่มีชั้นป้องกันสัญญาณรบกวนเพิ่มเติม โดยมีเพียงฉนวนพลาสติกหุ้มสายเท่านั้น สายชนิดนี้เป็นที่นิยมใช้อย่างแพร่หลายในระบบเครือข่าย LAN และระบบกล้องโทรทัศน์วงจรปิดแบบ IP เนื่องจากมีราคาประหยัด ติดตั้งง่าย และรองรับการใช้งานทั่วไปได้ดี อย่างไรก็ตาม สาย UTP มีข้อจำกัดในด้านการป้องกันสัญญาณรบกวน จึงไม่เหมาะสำหรับการติดตั้งในบริเวณที่มีแหล่งกำเนิดคลื่นแม่เหล็กไฟฟ้าสูง เช่น ใกล้มอเตอร์ เครื่องกำเนิดไฟฟ้า หรือสายไฟแรงสูง (Gcabling, 2023)



ก) สาย UTP ข) สาย STP

รูปที่ 3.31 สายคู่เกลียวบิด

สายคู่บิดเกลียวเป็นสื่อนำสัญญาณที่สำคัญในระบบเครือข่ายและกล้องโทรทัศน์วงจรปิด โดยเฉพาะระบบ IP ซึ่งควรเลือกใช้สายให้เหมาะสมกับสภาพแวดล้อม เช่น ใช้ UTP สำหรับงานทั่วไป และใช้ STP ในพื้นที่ที่มีสัญญาณรบกวนสูง เพื่อให้ระบบมีประสิทธิภาพและเสถียรภาพในการส่งข้อมูล ในปัจจุบันแบ่งออกเป็นระดับต่างๆ โดยเรียกเป็น category ต่างๆ ได้ดังตารางที่ 3.8

ตารางที่ 3.8 สายคู่บิดเกลียว Category ต่าง ๆ

ประเภท	แบนด์วิธ (MHz)	ความเร็วสูงสุด	หมายเหตุ
CAT1	–	ใช้โทรศัพท์	ไม่ใช้ในเครือข่ายข้อมูล
CAT2	4 MHz	4 Mbps	เลิกใช้งานแล้ว
CAT3	16 MHz	10 Mbps	ใช้กับ Ethernet รุ่นเก่า (10BASE-T)
CAT4	20 MHz	16 Mbps	ใช้กับ Token Ring (เลิกใช้แล้ว)
CAT5	100 MHz	100 Mbps	ปัจจุบันแทบไม่ใช้แล้ว
CAT5e	100 MHz	1Gbps	ใช้แพร่หลาย (Gigabit Ethernet)
CAT6	250 MHz	1Gbps-10Gbps(ระยะสั้น)	คุณภาพสูงกว่า CAT5e
CAT6a	500 MHz	10Gbps (100 เมตร)	ใช้ในระบบ CCTV/IP
CAT7*	600 MHz	10 Gbps	ใช้มาตรฐาน ISO ไม่ใช่ TIA
CAT8	2000 MHz	25–40 Gbps	ใช้ใน Data Center

2.2) โครงสร้างสายคู่บิดเกลียว (Twisted Pair Cable Structure)

สายคู่บิดเกลียวเป็นสื่อนำสัญญาณที่ออกแบบมาเพื่อลดการรบกวนทางแม่เหล็กไฟฟ้า (EMI) และการรบกวนระหว่างคู่สาย (crosstalk) โดยใช้หลักการบิดเกลียวของสายตัวนำแต่ละคู่ ซึ่งเป็นไปตามมาตรฐาน เช่น ISO/IEC 11801 และ ANSI/TIA-568 โครงสร้างของสายคู่บิดเกลียวประกอบด้วยชั้นต่าง ๆ ดังนี้

2.2.1) เปลือกหุ้มภายนอก (Outer Jacket)

เป็นชั้นนอกสุดของสาย ทำหน้าที่ปกป้องโครงสร้างภายในจากสภาพแวดล้อม

เช่น ความชื้น แสงแดด ความร้อน และแรงกระแทก วัสดุที่ใช้มักเป็น Polyvinyl Chloride (PVC) หรือ Low Smoke Zero Halogen (LSZH) ซึ่งเหมาะกับการใช้งานภายในอาคาร

2.2.2) ชั้นป้องกันสัญญาณรบกวน (Shielding Layer)

ชั้นนี้มีหน้าที่ลดการรบกวนจากภายนอก และสัญญาณรบกวนระหว่างสาย โดยอาจมีรูปแบบแตกต่างกัน เช่น

- Foil Shield (F/UTP) ใช้แผ่นฟอยล์หุ้มสายทั้งหมด
- Braided Shield (S/UTP) ใช้ลวดถักโลหะหุ้ม
- Individual Pair Shield (U/FTP หรือ S/FTP) หุ้มแต่ละคู่สาย

สายที่มี Shield จะมีประสิทธิภาพสูงในการป้องกันสัญญาณรบกวน เหมาะสำหรับพื้นที่ที่มีคลื่นแม่เหล็กไฟฟ้าสูง เช่น โรงงานอุตสาหกรรม

2.2.3) คู่สายบิดเกลียว (Twisted Pair Conductors)

เป็นส่วนสำคัญของสาย ประกอบด้วยสายทองแดง 2 เส้นบิดเกลียวเข้าด้วยกัน การบิดเกลียวช่วยลด crosstalk และเพิ่มความเสถียรของสัญญาณ โดยในสายสัญญาณเครือข่ายมาตรฐานจะมีทั้งหมด 4 คู่สาย (รวม 8 เส้น)

2.2.4) ฉนวนหุ้มตัวนำ (Insulation)

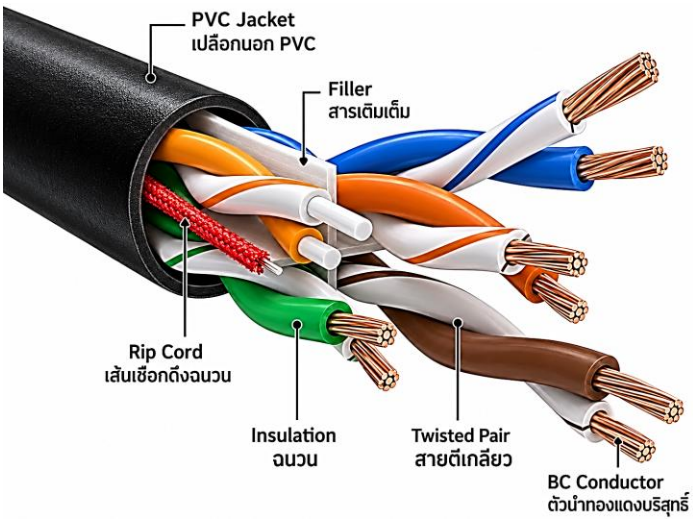
เป็นชั้นพลาสติกที่หุ้มตัวนำแต่ละเส้น ทำหน้าที่ป้องกันการลัดวงจร และควบคุมคุณสมบัติทางไฟฟ้าของสาย โดยมักใช้วัสดุประเภท PE

2.2.5) รหัสสีของสาย (Color Coding)

สายแต่ละคู่จะมีการกำหนดสีเพื่อให้ง่ายต่อการติดตั้งและเชื่อมต่อ เช่น

- ขาว/ส้ม – ส้ม
- ขาว/เขียว – เขียว
- ขาว/น้ำเงิน – น้ำเงิน
- ขาว/น้ำตาล – น้ำตาล

รหัสสีนี้เป็นไปตามมาตรฐาน TIA/EIA-568 ซึ่งช่วยลดความผิดพลาดในการเข้าหัวสาย (RJ-45)



รูปที่ 3.32 โครงสร้างของสายสายคู่เกลียวบิด

โครงสร้างของสายคู่บิดเกลียวถูกออกแบบมาเพื่อลดสัญญาณรบกวน และเพิ่มประสิทธิภาพในการส่งข้อมูล โดยประกอบด้วยชั้นเปลือกหุ้ม ฉนวน ตัวนำ และชั้นป้องกันสัญญาณรบกวน ซึ่งการเลือกใช้สายที่เหมาะสมจะช่วยให้ระบบเครือข่ายและกล้องโทรทัศน์วงจรปิดทำงานได้อย่างมีประสิทธิภาพ (Zi, 2022)

2.3) สายใยแก้วนำแสง (Fiber Optic Cable)

สายใยแก้วนำแสง (fiber optic cable) เป็นสื่อนำสัญญาณที่ใช้แสงในการส่งข้อมูล โดยผลิตจากแก้วหรือพลาสติกที่มีความบริสุทธิ์สูง ลักษณะเป็นเส้นใยขนาดเล็กมาก ใกล้เคียงกับเส้นผมมนุษย์ สามารถนำสัญญาณแสงจากจุดหนึ่งไปยังอีกจุดหนึ่งได้ด้วยการสูญเสียสัญญาณต่ำ ในระบบกล้องโทรทัศน์วงจรปิด สายใยแก้วนำแสงถูกนำมาใช้ในงานที่ต้องการส่งข้อมูลระยะไกล หรือในสภาพแวดล้อมที่มีสัญญาณรบกวนสูง เนื่องจากมีความเสถียรและรองรับความเร็วในการส่งข้อมูลได้สูงกว่าสายทองแดง

2.3.1) คุณสมบัติของสายใยแก้วนำแสง

2.3.1.1) ความสามารถในการรับส่งข้อมูลสูง (High Bandwidth)

สายใยแก้วนำแสงสามารถรองรับอัตราการส่งข้อมูลได้สูงมาก ตั้งแต่ระดับกิกะบิตต่อวินาที (Gbps) ไปจนถึงเทราบิตต่อวินาที (Tbps) ขึ้นอยู่กับประเภทของสายและอุปกรณ์ที่ใช้งาน เช่น single-mode และ multi-mode

2.3.1.2) รองรับระยะทางไกล (Long Distance Transmission)

สายใยแก้วนำแสงสามารถส่งข้อมูลได้ไกลหลายกิโลเมตร โดยมีการสูญเสียสัญญาณต่ำ เช่น multi-mode ระยะทางประมาณ 300–550 m และ single-mode ระยะทางหลายกิโลเมตร (10–40 km หรือมากกว่า)

2.3.1.3) น้ำหนักเบาและขนาดเล็ก

สายใยแก้วนำแสงมีขนาดเล็กและน้ำหนักเบากว่าสายทองแดง ทำให้สะดวกต่อการติดตั้ง โดยเฉพาะในพื้นที่ที่มีข้อจำกัดด้านพื้นที่

2.3.1.4) ทนต่อสัญญาณรบกวน (EMI Immunity)

เนื่องจากใช้แสงเป็นตัวนำสัญญาณ จึงไม่ถูรบกวนทางแม่เหล็กไฟฟ้า หรือสัญญาณรบกวนจากอุปกรณ์ไฟฟ้า ทำให้ได้สัญญาณที่มีคุณภาพสูงและมีสัญญาณรบกวนต่ำ

2.3.1.5) ความปลอดภัยสูง (High Security)

การดักฟังข้อมูลในสายใยแก้วนำแสงทำได้ยากกว่าสายทองแดง เนื่องจากไม่มีการแผ่คลื่นแม่เหล็กไฟฟ้าออกมา จึงเหมาะสำหรับระบบที่ต้องการความปลอดภัยของข้อมูล

2.3.1.6) การสูญเสียสัญญาณต่ำ (Low Attenuation)

สายใยแก้วนำแสงมีค่าการลดทอนสัญญาณต่ำมากเมื่อเทียบกับสายทองแดง ทำให้สามารถส่งข้อมูลได้ในระยะไกลโดยไม่ต้องใช้ตัวขยายสัญญาณบ่อย

2.3.1.7) ไม่นำไฟฟ้า (Electrical Isolation)

สายใยแก้วนำแสงไม่เป็นตัวนำไฟฟ้า จึงไม่มีความเสี่ยงจากไฟฟ้าลัดวงจรหรือไฟฟ้ารั่ว ทำให้มีความปลอดภัยต่อผู้ใช้งาน

2.3.2) ข้อจำกัดของสายใยแก้วนำแสง

2.3.2.1) การติดตั้งต้องใช้เครื่องมือเฉพาะ เช่น fusion splicer

2.3.2.2) ต้องใช้ตัวแปลงสัญญาณ (media converter หรือ SFP module)

2.3.2.3) ค่าใช้จ่ายด้านอุปกรณ์เริ่มต้นสูงกว่าสายทองแดง

2.3.2.4) ต้องใช้ผู้ติดตั้งที่มีความชำนาญ

2.3.3) โครงสร้างของสายใยแก้วนำแสง (Fiber Optic Cable Structure)

สายใยแก้วนำแสงประกอบด้วยส่วนสำคัญหลายชั้น ซึ่งแต่ละชั้นมีหน้าที่แตกต่างกัน เพื่อให้สามารถนำสัญญาณแสงได้อย่างมีประสิทธิภาพและป้องกันความเสียหายจากสภาพแวดล้อม โครงสร้างหลักประกอบด้วย แกน (core) ชั้นห่อหุ้ม (cladding) และชั้นป้องกัน (coating/buffer) รวมถึงส่วนเสริมความแข็งแรง

2.3.3.1) แกน (Core)

แกนเป็นส่วนที่อยู่ตรงกลางของเส้นใยแก้วนำแสง ทำหน้าที่เป็นตัวนำสัญญาณแสง โดยผลิตจากแก้วหรือพลาสติกที่มีความบริสุทธิ์สูง แกนจะมีค่าดัชนีหักเห (refractive index) สูงกว่าชั้นห่อหุ้ม (cladding) เพื่อให้แสงสามารถสะท้อนกลับภายในแกนได้ การส่งผ่านสัญญาณแสงในแกนเกิดจากหลักการ การสะท้อนกลับหมดภายใน (total internal reflection) ทำให้แสงสามารถเดินทางไปตามเส้นใยจนถึงปลายทางโดยมีการสูญเสียต่ำ

2.3.3.2) ชั้นห่อหุ้ม (Cladding)

Cladding เป็นชั้นที่ห่อหุ้มแกนไว้โดยรอบ ทำหน้าที่ควบคุมทิศทางของแสงให้สะท้อนกลับเข้าสู่แกน โดยมีค่าดัชนีหักเหน้อยกว่าแกนเล็กน้อย ความแตกต่างของค่าดัชนีหักเหระหว่าง core และ cladding เป็นปัจจัยสำคัญที่ทำให้เกิดการสะท้อนกลับหมดภายใน ซึ่งช่วยให้สัญญาณแสงไม่รั่วออกนอกแกน

2.3.3.3) ชั้นเคลือบป้องกัน (Coating/Buffer)

เป็นชั้นพลาสติกที่เคลือบอยู่รอบ cladding ทำหน้าที่ป้องกันเส้นใยแก้วจากความเสียหายทางกายภาพ เช่น แรงกระแทก ความชื้น และรอยขีดข่วน ชั้นนี้ไม่ได้มีหน้าที่ควบคุมแสงโดยตรง แต่มีบทบาทสำคัญในการเพิ่มความทนทานและอายุการใช้งานของสายใยแก้วนำแสง

2.3.3.4) ส่วนเสริมความแข็งแรง (Strength Member)

เป็นส่วนประกอบที่ทำหน้าที่เพิ่มความแข็งแรงเชิงกลให้กับสายใยแก้วนำแสง โดยทั่วไปผลิตจากเส้นใยอะรามิด (aramid fiber หรือ Kevlar) ซึ่งมีคุณสมบัติทนต่อแรงดึงสูง ทำหน้าที่รองรับแรงดึงและป้องกันความเสียหายของเส้นใยแก้วนำแสงภายในระหว่างการติดตั้งและการใช้งาน

2.3.3.5) เปลือกหุ้มภายนอก (Outer Jacket)

เป็นชั้นนอกสุดของสาย ทำหน้าที่ป้องกันสภาพแวดล้อมภายนอก เช่น ความร้อน ความชื้น แสงแดด และสารเคมี

2.3.3) หลักการส่งสัญญาณของแสงในสายใยแก้วนำแสง

การส่งสัญญาณในสายใยแก้วนำแสงอาศัยหลักการของ การสะท้อนกลับหมดภายใน โดยแสงจะถูกส่งเข้าสู่แกน (core) และสะท้อนกลับไปมาระหว่างผิวของ core และ cladding เนื่องจากค่าดัชนีหักเหของทั้งสองส่วนแตกต่างกัน ทำให้แสงสามารถเดินทางภายในแกนไปยังปลายทางได้อย่างมีประสิทธิภาพ โดยมีการสูญเสียพลังงานต่ำและไม่ถูกรบกวนจากคลื่น

แม่เหล็กไฟฟ้าภายนอก โดยทั่วไปค่าดัชนีหักเหของ core จะอยู่ประมาณ 1.46–1.48 และ cladding จะมีค่าต่ำกว่าเล็กน้อย (ประมาณ 1.44–1.46) ซึ่งเพียงพอให้เกิดการสะท้อนกลับหมดภายใน มีข้อดีของระบบ คือ การสูญเสียพลังงานต่ำ เนื่องจากเป็นการสะท้อนภายในที่สมบูรณ์ แสงจึงเดินทางได้ไกลโดยมีการลดทอน (attenuation) น้อยกว่าสายทองแดงมากปราศจากการรบกวน (EMI immunity) เนื่องจากแสงเป็นคลื่นแม่เหล็กไฟฟ้าที่มีความถี่สูงมากและเดินทางในตัวนำที่เป็นฉนวน (แก้ว/พลาสติก) จึงไม่ถูกรบกวนจากคลื่นวิทยุหรือสนามแม่เหล็กไฟฟ้าภายนอก (Senior, 2009)

2.4) สายไฟฟ้าในงานระบบกล้องโทรทัศน์วงจรปิด

สายไฟฟ้าเป็นอุปกรณ์ที่ใช้ในการส่งพลังงานไฟฟ้าจากแหล่งจ่ายไปยังอุปกรณ์ไฟฟ้า โดยอาศัยการไหลของกระแสไฟฟ้าผ่านตัวนำไฟฟ้า (conductor) ซึ่งมักทำจากโลหะ เช่น ทองแดง หรืออะลูมิเนียม เนื่องจากมีคุณสมบัติในการนำไฟฟ้าสูง ความสามารถในการนำไฟฟ้าของตัวนำขึ้นอยู่กับค่าความต้านทานไฟฟ้า (electrical resistance) โดยตัวนำที่มีความต้านทานต่ำจะสามารถนำกระแสไฟฟ้าได้ดีและสูญเสียพลังงานน้อย ในทางตรงกันข้าม ตัวนำที่มีความต้านทานสูงจะทำให้กระแสไฟฟ้าไหลผ่านได้น้อยและเกิดการสูญเสียพลังงานมากขึ้น ในระบบกล้องโทรทัศน์วงจรปิด สายไฟฟ้ามีบทบาทสำคัญในการจ่ายพลังงานให้กับอุปกรณ์ต่าง ๆ เช่น กล้อง เครื่องบันทึก และอุปกรณ์เครือข่าย ดังนั้นการเลือกใช้สายไฟที่เหมาะสมจึงมีความสำคัญต่อความปลอดภัยและประสิทธิภาพของระบบ

2.4.1) สายไฟ VCT (Vinyl Insulated Cabtyre Cable)

สายไฟ VCT เป็นสายไฟชนิดอ่อน (flexible cable) ที่ออกแบบมาสำหรับใช้งานที่ต้องการความยืดหยุ่นสูง โดยมีโครงสร้างเป็นสายกลม ภายในประกอบด้วยตัวนำทองแดงแบบฝอย (stranded copper) หลายเส้นรวมกัน หุ้มด้วยฉนวนและเปลือกนอกทำจากวัสดุพีวีซี (PVC) สายไฟชนิดนี้สามารถทนแรงดันไฟฟ้าได้ประมาณ 450/750 V ตามมาตรฐาน และมีจำนวนแกนตั้งแต่ 1 แกนขึ้นไป (โดยทั่วไป 2–4 แกน) ซึ่งคุณสมบัติ คือ มีความยืดหยุ่นสูง สามารถโค้งงอได้ง่าย ทนต่อแรงกระแทกและการสั่นสะเทือน เหมาะสำหรับงานที่มีการเคลื่อนย้ายอุปกรณ์ และฉนวนและเปลือกหุ้มช่วยป้องกันความชื้นและสภาพแวดล้อมภายนอก (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม, ม.ป.ป.)

ลักษณะการใช้งาน สายไฟ VCT นิยมใช้ในงานที่ต้องการความยืดหยุ่น เช่น จ่ายไฟให้กล้องโทรทัศน์วงจรปิดภายนอกอาคาร งานติดตั้งที่มีการเคลื่อนย้ายอุปกรณ์ และเดินสายบนรางเคเบิล หรือในท่อร้อยสาย โดยทั่วไป ไม่แนะนำให้ฝังดินโดยตรง เว้นแต่เป็นสายที่ออกแบบสำหรับงานฝังดินโดยเฉพาะ หรือมีท่อป้องกันเพิ่มเติม

2.4.2) สายไฟ VAF (Vinyl Flat Cable)

สายไฟ VAF มีลักษณะ (1) สายแบน มี 2–3 แกน (2) ตัวนำทองแดงแบบแข็ง (solid) และ (3) หุ้มฉนวน PVC โดยใช้งานเดินลอยภายในอาคาร ใช้กับงานติดตั้งแบบถาวร เช่น เดินตามผนัง มีข้อดี คือ ราคาประหยัด ติดตั้งง่าย ส่วนข้อจำกัด คือ ไม่เหมาะกับภายนอก ไม่ทนความชื้นและแสงแดด

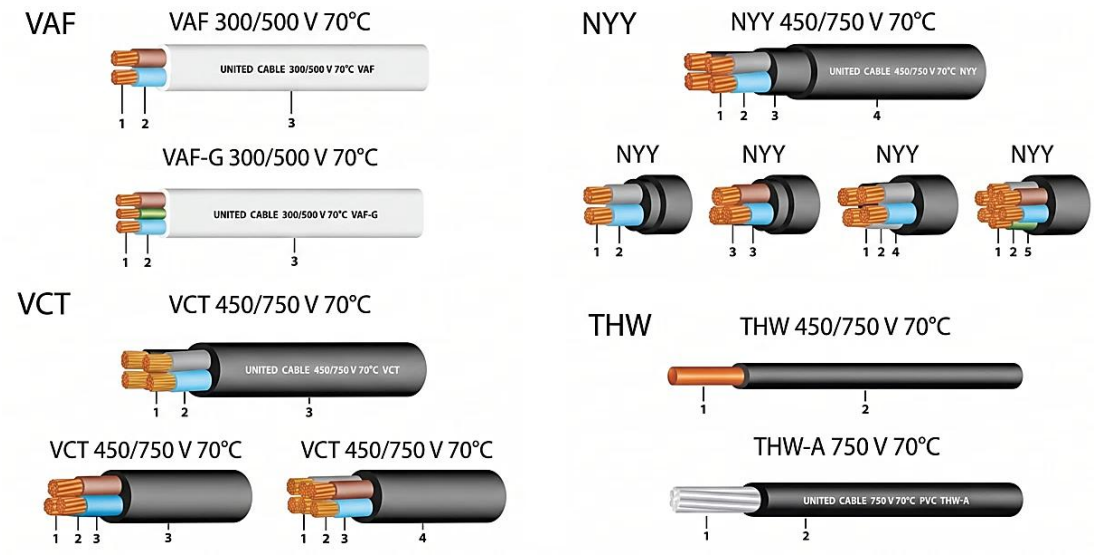
2.4.3) สายไฟ NYY (NYY Cable)

สายไฟ NYY เป็นสายกลม มีเปลือกหุ้มหนา มีตัวนำทองแดง ฉนวนเป็น PVC 2 ชั้น ใช้งานภายนอกอาคาร สามารถฝังดินได้โดยตรง โดยเหมาะกับงาน CCTV กลางแจ้ง ข้อดีของสายประเภทนี้คือ ทนแดด ทนฝน ทนความชื้นสูง อายุการใช้งานยาว

2.4.4) สายไฟ THW (Thermoplastic Heat and Water Resistant)

สายไฟ THW ลักษณะเป็นสายแกนเดี่ยว ใช้งานต้องเดินในท่อร้อยสาย ใช้ในอาคาร มีข้อดี คือ ทนความร้อน นิยมใช้ในระบบไฟฟ้าทั่วไป

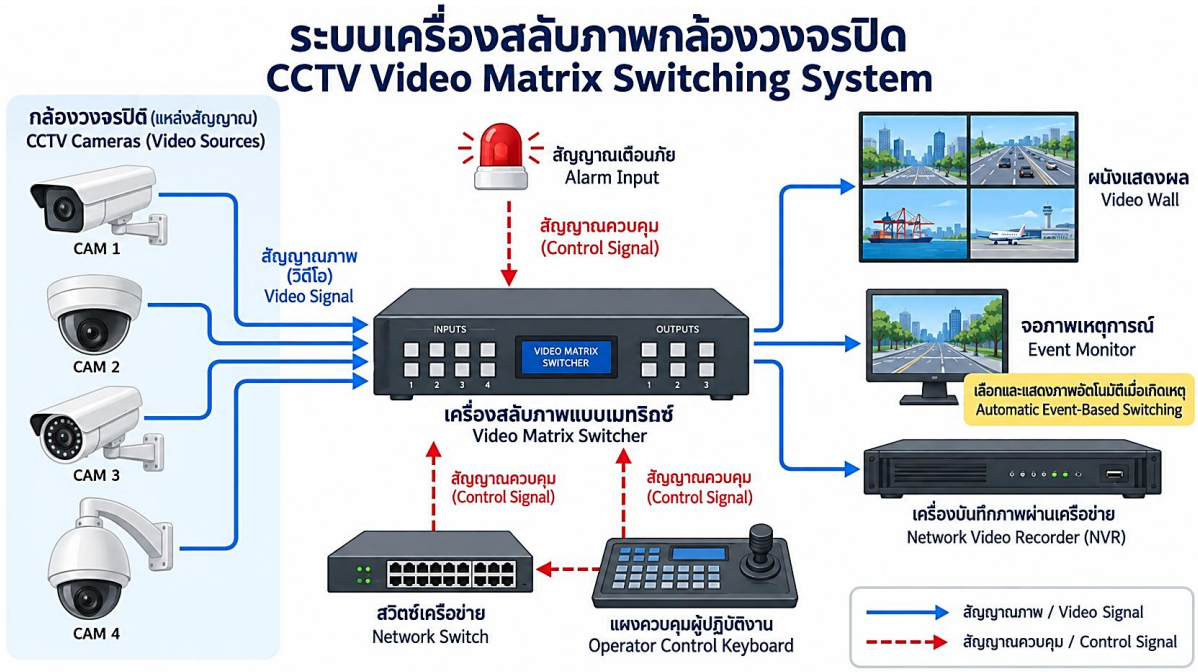
การเลือกสายไฟฟ้าในระบบกล้องโทรทัศน์วงจรปิดควรพิจารณาจากลักษณะการติดตั้ง สภาพแวดล้อม และความปลอดภัย โดยสายแต่ละประเภทมีคุณสมบัติแตกต่างกัน เช่น สาย VAF เหมาะกับงานภายในอาคาร สาย NYY เหมาะกับงานภายนอกและฝังดิน ส่วนสาย VCT เหมาะกับงานที่ต้องการความยืดหยุ่น



รูปที่ 3.33 สายไฟฟ้าในงานระบบกล้องโทรทัศน์วงจรปิด

3.3.8 เครื่องสลับภาพ (Switcher)

เครื่องสลับภาพ เป็นอุปกรณ์ที่ใช้ในระบบกล้องโทรทัศน์วงจรปิด ทำหน้าที่เป็นตัวกลางในการรับสัญญาณภาพจากกล้องหลายตัว แล้วทำการสลับสัญญาณภาพเพื่อนำไปแสดงผลยังจอภาพ โดยจะแสดงภาพจากกล้องแต่ละตัวทีละภาพตามลำดับเวลา (sequential switching) ผู้ใช้งานสามารถกำหนดระยะเวลาในการแสดงผลของแต่ละกล้องได้ เช่น 1–30 วินาทีต่อภาพ ทั้งนี้ขึ้นอยู่กับคุณสมบัติของอุปกรณ์ที่ใช้งาน เครื่องสลับภาพมีให้เลือกใช้งานหลายขนาดตามจำนวนช่องสัญญาณ (channels) เช่น 4, 8, 12, และ 16 ช่อง เพื่อรองรับจำนวนกล้องที่แตกต่างกันในแต่ละระบบ ในปัจจุบัน เครื่องสลับภาพแบบเดิมถูกลดบทบาทลง เนื่องจากเครื่องบันทึกภาพสมัยใหม่ เช่น DVR และ NVR มีฟังก์ชันการแสดงผลหลายภาพ (multi-view) และการสลับภาพในตัว ทำให้ไม่จำเป็นต้องใช้อุปกรณ์ switcher แยกต่างหากในระบบทั่วไป (MacroCare Co., Ltd., ม.ป.ป.)



รูปที่ 3.34 การใช้งานเครื่องสลับภาพ

3.3.9 เครื่องแบ่งสัญญาณภาพ

เครื่องแบ่งสัญญาณภาพเป็นอุปกรณ์ที่ใช้ในระบบกล้องโทรทัศน์วงจรปิด ทำหน้าที่รับสัญญาณภาพจากกล้องหลายตัว และแสดงผลภาพหลายภาพพร้อมกันบนหน้าจอเดียว โดยไม่มีช่วงเวลาขาดหายของภาพ (no switching delay) ซึ่งแตกต่างจากเครื่องสลับภาพ (switcher) ที่จะแสดงภาพทีละกล้องตามลำดับเวลา

1) เครื่องแบ่งสัญญาณภาพแบบควอด (Quad Splitter)

เครื่องแบ่งสัญญาณภาพแบบควอด (quad) เป็นอุปกรณ์ที่ใช้แบ่งหน้าจอออกเป็น 4 ส่วนเท่า ๆ กัน เพื่อแสดงภาพจากกล้อง 4 ตัวพร้อมกันในเวลาเดียวกัน มีคุณสมบัติ (1) แสดงภาพพร้อมกัน 4 ช่อง (4 channel) (2) ไม่มีการสลับภาพ จึงไม่เกิดช่วงเวลาที่ภาพหาย และ (3) เหมาะสำหรับระบบขนาดเล็ก ซึ่งในบางรุ่นอาจรองรับมากกว่า 4 ช่อง เช่น 8 ช่อง โดยใช้วิธีสลับหน้า (dual page) แต่ยังคงแสดงได้ครั้งละ 4 ภาพ

2) เครื่องแบ่งสัญญาณภาพแบบมัลติเพล็กเซอร์ (Multiplexer)

Multiplexer เป็นอุปกรณ์ที่มีความสามารถสูงกว่า quad โดยสามารถรวมและจัดการสัญญาณภาพจากกล้องหลายตัว และแสดงผลได้หลายรูปแบบ เช่น 4, 9, หรือ 16 ช่องบนหน้าจอเดียว ซึ่งมีคุณสมบัติ (1) รองรับจำนวนกล้องได้มาก (เช่น 9, 16 ช่อง หรือมากกว่า) (2) สามารถแสดงภาพหลายรูปแบบ (multi-screen display) (3) รองรับการบันทึกภาพจากหลายกล้องในเวลาเดียวกัน และ (4) บางรุ่นสามารถเลือกดูภาพย้อนหลังเฉพาะกล้องได้

ในระบบกล้องโทรทัศน์วงจรปิดสมัยใหม่ อุปกรณ์ประเภท quad และ multiplexer มักถูกรวมอยู่ในเครื่องบันทึกภาพ เช่น DVR และ NVR ซึ่งสามารถแสดงภาพหลายกล้อง (multi-view) และบันทึกภาพได้พร้อมกันโดยไม่ต้องใช้อุปกรณ์แยก

(ก) เครื่องแบ่งสัญญาณภาพแบบมัลติเพล็กเซอร์ (ข) เครื่องแบ่งสัญญาณภาพแบบควอด

รูปที่ 3.35 เครื่องแบ่งสัญญาณภาพ

3.3.10 อุปกรณ์แปลงสัญญาณภาพ (Balanced–Unbalanced: Balun)

บาลันเป็นอุปกรณ์อิเล็กทรอนิกส์ที่ใช้สำหรับแปลงสัญญาณระหว่างระบบสัญญาณแบบไม่สมดุล (unbalanced) และระบบสัญญาณแบบสมดุล (balanced) ในระบบกล้องโทรทัศน์วงจรปิด บาลันทำหน้าที่แปลงสัญญาณวิดีโอจากสายโคแอกเชียล (coaxial cable) ซึ่งเป็นสื่อส่งสัญญาณแบบไม่สมดุล ให้สามารถส่งผ่านสายคู่บิดเกลียว (twisted pair cable) เช่น สาย UTP หรือ STP ซึ่งเป็นสื่อส่งสัญญาณแบบสมดุลได้ และสามารถแปลงสัญญาณกลับเป็นรูปแบบเดิมที่ปลายทาง เพื่อให้การส่งสัญญาณภาพมีประสิทธิภาพและรองรับระยะทางที่ไกลขึ้น

1) หลักการทำงาน

ในระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก สัญญาณวิดีโอจากกล้องจะเป็นแบบ unbalanced (ในสายนำสัญญาณโคแอกเชียล) บาลันตัวแรกจะทำหน้าที่แปลงสัญญาณให้เป็นแบบ balanced (ในสายนำสัญญาณ UTP) เพื่อส่งผ่านสายสัญญาณเครือข่าย เมื่อถึงปลายทาง บาลันอีกตัวจะทำการแปลงสัญญาณกลับเป็น Unbalanced เพื่อส่งเข้าสู่เครื่องบันทึก DVR ซึ่งบาลันไม่ได้ทำหน้าที่แปลงสัญญาณแอนะล็อกเป็นดิจิทัล และ ไม่ได้เป็นอุปกรณ์ขยายสัญญาณโดยตรง แต่เป็นอุปกรณ์สำหรับ “แปลงรูปแบบการส่งสัญญาณ” เท่านั้น

2) คุณสมบัติและข้อดี

2.1) ช่วยให้สามารถใช้สาย UTP (เช่น CAT5e, CAT6) แทนสาย coaxial ได้

2.2) ลดสัญญาณรบกวน (noise) และสัญญาณรบกวนข้ามสาย (crosstalk)

2.3) ลดต้นทุนการติดตั้งเมื่อเทียบกับการใช้สาย coaxial ระยะไกล

2.4) รองรับการเดินสายได้ไกล 300–500 m (ขึ้นอยู่กับคุณภาพอุปกรณ์)

2.5) ติดตั้งง่ายและสะดวก

3) การใช้งานในระบบ CCTV

บาลันนิยมใช้ในระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก โดยเฉพาะในกรณีที่ต้องเดินสายระยะไกล หรือมีข้อจำกัดด้านการเดินสายโคแอกเชียล

บาลันเป็นอุปกรณ์ที่ใช้แปลงสัญญาณระหว่างระบบสายแบบ unbalanced และ balanced เพื่อให้สามารถใช้สาย UTP ในการส่งสัญญาณภาพจากกล้องโทรทัศน์วงจรปิดได้อย่างมีประสิทธิภาพ โดยไม่ได้ทำหน้าที่แปลงสัญญาณเป็นดิจิทัลหรือขยายสัญญาณโดยตรง

รูปที่ 3.36 อุปกรณ์ขยายสัญญาณภาพบาลัน

3.3.11 อุปกรณ์เชื่อมต่อระบบเครือข่าย

เราเตอร์ (router) เป็นอุปกรณ์เครือข่ายที่ทำหน้าที่เชื่อมต่อเครือข่ายตั้งแต่สองเครือข่ายขึ้นไปเข้าด้วยกัน และทำหน้าที่ส่งต่อข้อมูลระหว่างเครือข่าย (network-to-network communication) โดยอาศัยกระบวนการกำหนดเส้นทาง (routing) (บริษัท มีเดีย เสิร์ช จำกัด, 2021)

1) หลักการทำงานของ Router

Router ทำงานในระดับ layer 3 (network layer) ของแบบจำลอง OSI โดยใช้หมายเลข IP address ในการตัดสินใจเลือกเส้นทางที่เหมาะสมที่สุดในการส่งข้อมูลไปยังปลายทาง เมื่อ router ได้รับข้อมูล จะดำเนินการดังนี้

1.1) ตรวจสอบข้อมูลส่วนหัว (header) ของแพ็กเกต เพื่อระบุที่อยู่ปลายทาง (destination IP address)

1.2) ตรวจสอบตารางเส้นทาง (routing table) เพื่อค้นหาเส้นทางที่เหมาะสม

1.3) เลือกเส้นทางที่ดีที่สุดตามอัลกอริทึมการกำหนดเส้นทาง (routing algorithm)

1.4) ส่งต่อข้อมูลไปยังเครือข่ายปลายทางผ่านอินเทอร์เฟซ (interface) ที่เหมาะสม

2) คุณสมบัติของ router

2.1) สามารถเชื่อมต่อเครือข่ายหลายประเภท เช่น Ethernet fiber optic

2.2) รองรับการสื่อสารระหว่างเครือข่ายที่มีโครงสร้างต่างกัน

2.3) สามารถจัดการทราฟฟิกเครือข่าย และควบคุมการไหลของข้อมูล

2.4) รองรับฟังก์ชันเพิ่มเติม เช่น Network Address Translation (NAT), firewall, และ DHCP

3) ส่วนประกอบสำคัญของ router

3.1) interface (port) คือ ช่องเชื่อมต่อเครือข่าย เช่น LAN และ WAN

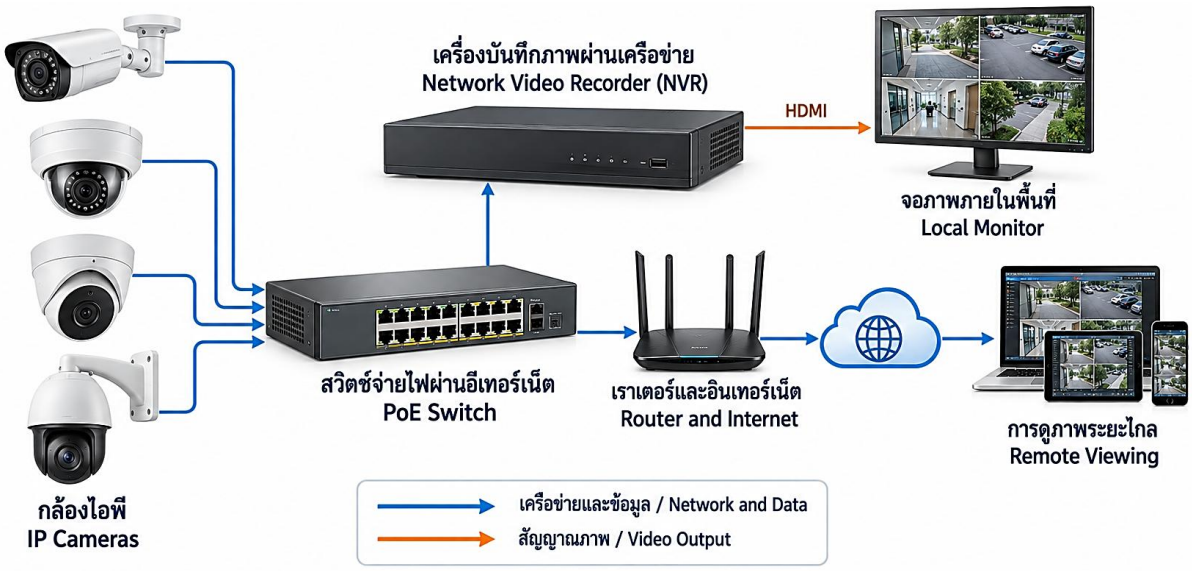
3.2) routing table คือ ตารางเส้นทางที่ใช้ในการตัดสินใจส่งข้อมูล

3.3) operating system เช่น Cisco IOS หรือระบบปฏิบัติการของผู้ผลิต

3.4) processor และ memory ใช้ประมวลผลและจัดเก็บข้อมูลเส้นทาง

Router ไม่ได้ทำหน้าที่เพียงเชื่อมต่อคอมพิวเตอร์หลายเครื่องเท่านั้น แต่ทำหน้าที่หลักในการ “กำหนดเส้นทางข้อมูลระหว่างเครือข่าย” ซึ่งแตกต่างจาก switch ทำงานในระดับ layer 2

สรุป router เป็นอุปกรณ์สำคัญในระบบเครือข่าย ทำหน้าที่เชื่อมต่อและกำหนดเส้นทางการส่งข้อมูลระหว่างเครือข่าย โดยใช้ IP address และ routing table เพื่อให้ข้อมูลไปถึงปลายทางอย่างมีประสิทธิภาพ



รูปที่ 3.37 การใช้งาน router ในระบบ CCTV

3.3.12 ขั้วต่อสายสัญญาณในงานกล้องโทรทัศน์วงจรปิด

ขั้วต่อสายนำสัญญาณ (connector) เป็นอุปกรณ์ที่ใช้เชื่อมต่อสัญญาณไฟฟ้าและสัญญาณภาพระหว่างอุปกรณ์ในระบบกล้องโทรทัศน์วงจรปิด เช่น กล้อง เครื่องบันทึก (DVR/NVR) และจอแสดงผล การเลือกใช้ขั้วต่อที่เหมาะสมมีผลต่อคุณภาพของสัญญาณและความเสถียรของระบบ ลักษณะหัวต่อต่าง ๆ ดังนี้

1) หัวต่อ DC (DC Power Connector)

หัวต่อ DC ตัวผู้ (male) และตัวเมีย (female) ใช้สำหรับจ่ายไฟเลี้ยงให้กับกล้องโทรทัศน์ วงจรปิด แรงดันไฟฟ้า 12 VDC โดยตัวผู้ต่อออกจากแหล่งจ่ายไฟ และตัวเมียต่อเข้ากับตัวกล้อง

2) หัวต่อชนิด F-Type

เป็นหัวต่อที่ใช้กับสายโคแอกเชียล นิยมในงานในระบบโทรทัศน์และบางระบบ CCTV มีทั้งแบบหมุน (twist-on) และแบบย้ำ (crimp/compression) แบบหมุนจะติดตั้งง่าย แต่ความแน่นและคุณภาพต่ำกว่า ส่วนแบบย้ำ (crimp/compression) ซึ่งจะแข็งแรงและคุณภาพสัญญาณดีกว่า

3) หัวต่อชนิด BNC (Bayonet Neill–Concelman)

เป็นหัวต่อมาตรฐานที่นิยมใช้ในระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อกใช้กับสาย Coaxial เช่น RG59 หรือ RG6 ประเภทการติดตั้งมีทั้งแบบบีบ (crimp) แบบบิดเกลียว (twist-on) และแบบ compression ซึ่งมีคุณภาพสูง ที่สำคัญควรเลือกหัว BNC ให้เหมาะกับชนิดสาย เช่น RG59 หรือ RG6 เพื่อป้องกันการสูญเสียสัญญาณ

4) หัวต่อชนิด RCA (Radio Corporation of America)

หัวต่อ RCA ใช้สำหรับสัญญาณภาพและเสียงแบบแอนะล็อก (composite video/audio) ปัจจุบันใช้น้อยลง เนื่องจากถูกแทนที่ด้วย HDMI หรือ Video Graphics Array (VGA) ที่ให้คุณภาพสูงกว่า อย่างไรก็ตามยังพบได้ในเครื่อง DVR รุ่นเก่า

5) หัวแปลงสัญญาณ (Adapter)

BNC to RCA และ RCA to BNC ใช้สำหรับแปลงรูปแบบขั้วต่อให้สามารถใช้งานร่วมกันได้ เช่น ต่อ DVR (ใช้หัวต่อ RCA) กับกล้อง (ใช้หัวต่อ BNC) ใช้ในงานติดตั้งหรือซ่อมบำรุง

6) หัวเชื่อมต่อแบบ RJ-45

เป็นหัวเชื่อมต่อสำหรับสายคู่บิดเกลียว (UTP/STP) ใช้ในระบบเครือข่าย นิยมใช้กับกล้องโทรทัศน์วงจรปิดระบบ IP มีคุณสมบัติ รองรับสาย 4 คู่ (8 เส้น) ใช้กับมาตรฐาน Ethernet (สายเคเบิลเครือข่ายประเภท Cat 5e หรือ Cat 6)

(ก) ขั้วต่อ DC ตัวเมีย

(ข) ขั้วต่อ DC ตัวเมีย

(ค) ขั้วต่อ DC ตัวเมีย

(ง) ขั้วต่อชนิด BNC

(จ) ขั้วต่อชนิด RCA

(ฉ) ขั้วต่อชนิด RCA to BNC

(ช) ขั้วต่อแบบ RJ-45

รูปที่ 3.38 ขั้วต่อสายสัญญาณในงานระบบกล้องโทรทัศน์วงจรปิด

3.3.13 อุปกรณ์เสริมในงานกล้องโทรทัศน์วงจรปิด

1) ขายึดกล้องโทรทัศน์วงจรปิด (Bracket)

เป็นอุปกรณ์ที่ใช้สำหรับรองรับและยึดติดตัวกล้องโทรทัศน์วงจรปิดให้อยู่ในตำแหน่งที่เหมาะสม โดยต้องพิจารณาให้สอดคล้องกับน้ำหนักของกล้องและลักษณะการติดตั้ง เพื่อให้มีความมั่นคงและปลอดภัยในการใช้งาน ขายึดกล้องมีหลายรูปแบบ ขึ้นอยู่กับลักษณะพื้นที่ติดตั้ง เช่น แบบติดผนัง (wall mount) เหมาะสำหรับติดตั้งบริเวณผนังอาคาร และแบบติดเพดาน (ceiling mount) เหมาะสำหรับติดตั้งบนเพดาน นอกจากนี้ ยังมีการออกแบบให้สามารถปรับมุมมองของกล้องได้ เพื่อให้ครอบคลุมพื้นที่ที่ต้องการเฝ้าระวังได้อย่างมีประสิทธิภาพ

รูปที่ 3.39 ขายึดกล้องโทรทัศน์วงจรปิด

2) กล่องครอบกล้องโทรทัศน์วงจรปิด (Camera Housing)

กล่องครอบกล้องโทรทัศน์วงจรปิด (camera housing) เป็นอุปกรณ์ที่ใช้ป้องกันตัวกล้องจากสภาพแวดล้อมภายนอก เช่น ฝุ่นละออง ความชื้น ความร้อน แสงแดด และน้ำฝน เพื่อช่วยยืดอายุการใช้งานและรักษาประสิทธิภาพของกล้องให้ทำงานได้อย่างต่อเนื่อง กล่องครอบกล้องมีหลายรูปแบบและคุณสมบัติ เช่น มีพัดลมระบายอากาศ (cooling fan) สำหรับลดความร้อน มีฮีตเตอร์ (heater) สำหรับป้องกันความชื้นหรือไอน้ำในสภาพอากาศเย็น มีซีลป้องกันฝุ่นและน้ำ (sealed enclosure) ตามมาตรฐาน IP และผลิตจากวัสดุที่ทนต่อการกัดกร่อน เช่น อะลูมิเนียมหรือสเตนเลส

2.1) ประเภทของกล่องครอบกล้องโทรทัศน์วงจรปิด

2.1.1) กล่องครอบกล้องแบบภายในอาคาร (indoor housing) ใช้สำหรับติดตั้งภายในอาคาร มีหน้าที่ป้องกันฝุ่นละอองและสิ่งสกปรก เหมาะสำหรับพื้นที่ที่มีสภาพแวดล้อมปกติ เช่น สำนักงาน โรงเรียน หรืออาคารทั่วไป ในพื้นที่ที่มีสภาพแวดล้อมควบคุม เช่น ห้องปรับอากาศ อาจไม่จำเป็นต้องใช้ housing เพิ่มเติม

2.12) กล่องครอบกล้องแบบภายนอกอาคาร (outdoor housing) ออกแบบให้ทนต่อสภาพแวดล้อมภายนอก เช่น ฝน แดด ความชื้น และอุณหภูมิที่เปลี่ยนแปลง มักมีคุณสมบัติกันน้ำและกันฝุ่นตามมาตรฐาน (เช่น IP66 หรือ IP67) เหมาะสำหรับการติดตั้งในพื้นที่กลางแจ้ง เช่น ลานจอดรถ ถนน เสาไฟฟ้า พื้นที่ภายนอกอาคาร

กล่องครอบกล้องโทรทัศน์วงจรปิดเป็นอุปกรณ์ที่ช่วยปกป้องกล้องจากสภาพแวดล้อมและเพิ่มความทนทานในการใช้งาน โดยควรเลือกใช้ให้เหมาะสมกับลักษณะพื้นที่ติดตั้ง เช่น ภายในหรือภายนอกอาคาร

รูปที่ 3.40 กล่องครอบกล้องโทรทัศน์วงจรปิด

3) หม้อแปลงไฟฟ้า (Adapter)

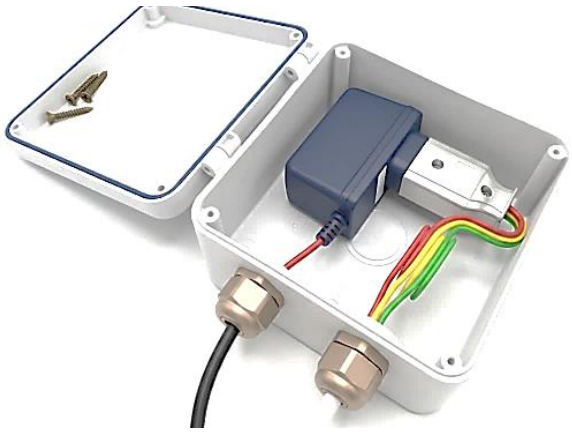
หม้อแปลงไฟฟ้าหรืออะแดปเตอร์เป็นอุปกรณ์ที่ทำหน้าที่แปลงพลังงานไฟฟ้าจากกระแสสลับ (AC) ที่ใช้ตามอาคารทั่วไป (220 V) ให้เป็นกระแสตรง (DC) ที่มีแรงดันไฟฟ้าต่ำลงเพื่อใช้จ่ายไฟให้กับอุปกรณ์อิเล็กทรอนิกส์ เช่น กล้องโทรทัศน์วงจรปิด ในระบบกล้องโทรทัศน์วงจรปิด โดยทั่วไปกล้องจะใช้แรงดันไฟฟ้า 12 VDC ดังนั้นการเลือกใช้อะแดปเตอร์จึงต้องพิจารณาค่าทางไฟฟ้าให้เหมาะสมกับอุปกรณ์ หลักเกณฑ์ในการเลือกใช้อะแดปเตอร์

3.1) แรงดันไฟฟ้า (voltage) ต้องตรงกับค่าที่อุปกรณ์กำหนด เช่น 12 VDC โดยทั่วไปอุปกรณ์สามารถยอมรับความคลาดเคลื่อนได้ประมาณ ±10% ค่าสูงสุดประมาณ 13.2 V และค่าต่ำสุดประมาณ 10.8 V

3.2) กระแสไฟฟ้า (current) ต้องเพียงพอต่อความต้องการของอุปกรณ์ เช่น 1A, 2A เป็นต้นโดยควรเลือกอะแดปเตอร์ที่มีกระแสสูงกว่าที่อุปกรณ์ต้องการเล็กน้อย เพื่อความเสถียรในการทำงาน

3.3) คุณภาพของแหล่งจ่ายไฟ (power quality) ควรมีแรงดันไฟฟ้าคงที่ (stable output) และมีระบบป้องกัน เช่น ป้องกันไฟเกิน (overvoltage protection) ป้องกันกระแสเกิน (overcurrent protection) และป้องกันไฟฟ้าลัดวงจร (short circuit protection)

กล่าวโดยสรุป อะแดปเตอร์เป็นอุปกรณ์สำคัญในระบบกล้องโทรทัศน์วงจรปิด ทำหน้าที่แปลงและจ่ายพลังงานไฟฟ้าให้กับอุปกรณ์ ต้องเลือกใช้อย่างเหมาะสมทั้งในด้านแรงดัน กระแส และคุณภาพของแหล่งจ่ายไฟ เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและปลอดภัย



รูปที่ 3.41 อะแดปเตอร์ในระบบกล้องโทรทัศน์วงจรปิด

4) เบรกเกอร์ (Circuit Breaker)

เบรกเกอร์ เป็นอุปกรณ์ไฟฟ้าที่ทำหน้าที่เป็นทั้ง สวิตช์เปิด–ปิดวงจรไฟฟ้า และอุปกรณ์ป้องกัน (protective device) ในระบบไฟฟ้า โดยใช้สำหรับตัดกระแสไฟฟ้าโดยอัตโนมัติเมื่อเกิดความผิดปกติในวงจร เช่น กระแสไฟฟ้าเกิน (overcurrent) หรือการลัดวงจร (short circuit)

4.1) หลักการทำงาน

เบรกเกอร์ทำงานโดยอาศัยกลไกหลัก 2 รูปแบบ ได้แก่

4.1.1) กลไกความร้อน (thermal protection) ใช้แผ่นไบเมทัล (bimetallic strip) ที่จะโค้งงอเมื่อเกิดความร้อนจากกระแสไฟฟ้าเกิน ทำให้วงจรถูกตัด

4.1.2) กลไกแม่เหล็กไฟฟ้า (magnetic protection) ใช้แรงแม่เหล็ก ไฟฟ้าในการตัดวงจรทันทีเมื่อเกิดกระแสลัดวงจร เมื่อเบรกเกอร์ตัดวงจรแล้ว สามารถรีเซต (reset) และนำกลับมาใช้งานได้ใหม่ โดยไม่จำเป็นต้องเปลี่ยนอุปกรณ์เหมือนฟิวส์

4.2) ความสำคัญในการใช้งาน

4.2.1) ป้องกันความเสียหายของอุปกรณ์ไฟฟ้า

4.2.2) ลดความเสี่ยงการเกิดไฟฟ้าลัดวงจรและอัคคีภัย

4.2.3) เพิ่มความปลอดภัยในการใช้งานระบบไฟฟ้า

4.2.4) ใช้ควบคุมการเปิด–ปิดระบบไฟฟ้าในงานติดตั้ง

4.3) การใช้งานในระบบกล้องโทรทัศน์วงจรปิด เบรกเกอร์ถูกนำมาใช้ในระบบกล้องโทรทัศน์วงจรปิดเพื่อ ป้องกันอุปกรณ์ เช่น กล้อง DVR/NVR และ Power Supply และควบคุมวงจรไฟฟ้าของระบบให้สามารถตัด ต่อได้อย่างปลอดภัย

เบรกเกอร์เป็นอุปกรณ์สำคัญในระบบไฟฟ้าที่ทำหน้าที่ทั้งควบคุมและป้องกันวงจร โดยสามารถตัดกระแสไฟฟ้าเมื่อเกิดความผิดปกติ และสามารถใช้งานซ้ำได้ ช่วยเพิ่มความปลอดภัยให้กับระบบกล้องโทรทัศน์วงจรปิดและอุปกรณ์ไฟฟ้า (บริษัท มีเดีย เสิร์ช จำกัด., 2025)

รูปที่ 3.42 เบรกเกอร์

3.4 การออกแบบและติดตั้งระบบกล้องโทรทัศน์วงจรปิด

การปฏิบัติงานในการติดตั้งระบบไฟฟ้าและการติดตั้งอุปกรณ์ไฟฟ้า เช่นกล้องโทรทัศน์วงจรปิดตามบ้านพักอาศัยหรือตามอาคาร ช่างไฟฟ้าจะต้องมีความรู้ความสามารถเกี่ยวกับทางด้านไฟฟ้าแล้วจะต้องมีความรู้และมีทักษะในด้านการใช้เครื่องมือช่างทั่วไปให้ถูกต้องตามประเภทของงาน

3.4.1 เครื่องมือพื้นฐานสำหรับงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด

เครื่องมือช่างเป็นอุปกรณ์สำคัญในการติดตั้งและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด โดยเครื่องมือแต่ละชนิดถูกออกแบบมาให้เหมาะสมกับลักษณะงานเฉพาะด้าน เช่น งานตัด งานย้ำสาย งานเจาะ และงานวัดระยะ ซึ่งช่วยให้การติดตั้งมีความปลอดภัย ถูกต้อง และมีประสิทธิภาพ

1) คีมย้ำหัวต่อกล้อง (Crimp Tool for BNC Connector)

คีมย้ำหัวต่อกล้องเป็นเครื่องมือที่ใช้สำหรับย้ำหัวต่อ BNC เข้ากับสายโคแอกเชียล เช่น สาย RG59 หรือ RG6 เพื่อให้การเชื่อมต่อสัญญาณมีความแน่นหนาและลดการสูญเสียสัญญาณ

2) คีมตัดปากเฉียง (Diagonal Cutting Pliers)

คีมตัดปากเฉียงเป็นเครื่องมือสำหรับตัดสายไฟ ลวด หรือวัสดุโลหะขนาดเล็ก โดยคมตัดจะอยู่ในลักษณะเฉียง ช่วยให้สามารถตัดในพื้นที่แคบได้สะดวก ด้ามจับมักหุ้มฉนวนเพื่อเพิ่มความปลอดภัยในการใช้งาน

3) คีมปากแหลม (Long Nose Pliers)

คีมปากแหลมใช้สำหรับจับ ดัด หรือดึงชิ้นงานขนาดเล็ก รวมถึงงานในพื้นที่แคบที่เครื่องมือทั่วไปเข้าถึงได้ยาก นอกจากนี้ยังใช้ในการดัดสายไฟหรือจัดตำแหน่งอุปกรณ์ขนาดเล็กได้

4) คีมปากจิ้งจก (Combination Pliers)

คีมปากจิ้งจกเป็นเครื่องมืออเนกประสงค์ ใช้สำหรับจับ บีบ ดัด และตัดสายไฟหรือวัสดุโลหะขนาดเล็ก โดยบริเวณปากคีมมีร่องฟันช่วยเพิ่มแรงยึดเกาะ และมีคมตัดอยู่ใกล้จุดหมุนของคีม

5) ไขควง (Screwdriver)

ไขควงเป็นเครื่องมือสำหรับขันหรือคลายสกรู มีหลายรูปแบบ เช่น ไขควงปากแบน และไขควงแฉก ซึ่งเลือกใช้งานตามลักษณะของหัวสกรู

6) คีมย้ำหัวแลน (RJ-45 Crimping Tool)

คีมย้ำหัวแลนใช้สำหรับย้ำหัวเชื่อมต่อ RJ-45 กับสาย UTP/STP ในระบบเครือข่าย รวมถึงสามารถใช้กับหัว RJ-11 และ RJ-12 สำหรับงานโทรศัพท์ได้ในบางรุ่น

7) มีดปลอกสาย (Cable Stripper)

มีดปลอกสายใช้สำหรับปอกฉนวนหุ้มสายไฟหรือสายนำสัญญาณ โดยช่วยลดความเสียหายต่อแกนตัวนำและเพิ่มความสะดวกในการเข้าหวสาย

8) สว่านไฟฟ้า (Electric Drill)

สว่านไฟฟ้าเป็นเครื่องมือสำหรับเจาะรูบนวัสดุต่าง ๆ เช่น ไม้ โลหะ หรือผนังคอนกรีต โดยใช้งานร่วมกับดอกสว่านชนิดต่าง ๆ ตามประเภทวัสดุ

9) กรรไกรตัดท่อพีวีซี (PVC Pipe Cutter)

กรรไกรตัดท่อ PVC ใช้สำหรับตัดท่อร้อยสายไฟหรือท่อพีวีซีให้ได้ขนาดตามต้องการ โดยช่วยให้รอยตัดเรียบและลดความเสียหายของท่อ

10) ตลับเมตร (Tape Measure)

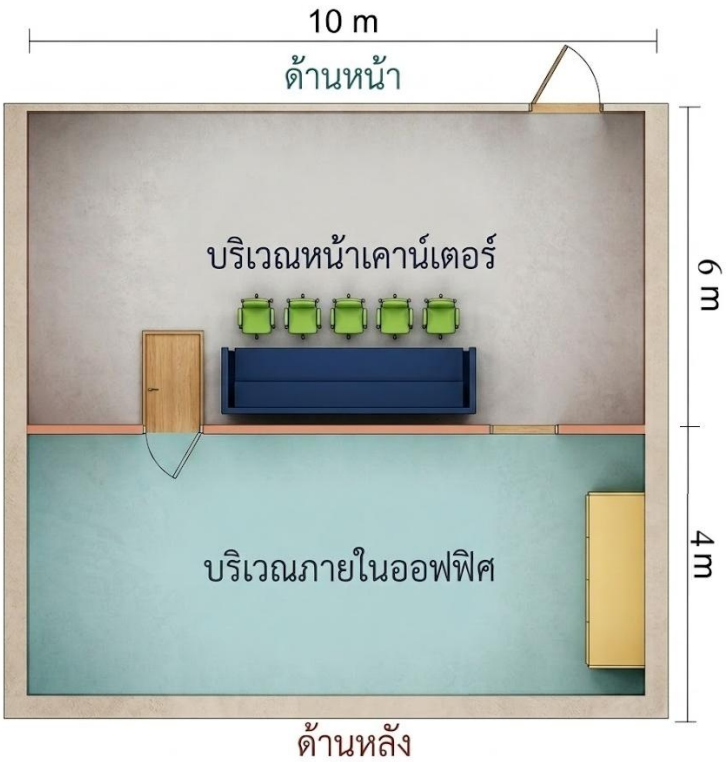
ตลับเมตรเป็นเครื่องมือวัดระยะ ใช้สำหรับวัดขนาดพื้นที่ ระยะเดินสาย หรือกำหนดตำแหน่งติดตั้งอุปกรณ์ต่าง ๆ ในงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด

รูปที่ 3.43 เครื่องมือพื้นฐานสำหรับงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด (ชลดา ปานสง และคณะ, 2561; ชลดา ปานสง และคณะ, 2566)

ก่อนดำเนินการติดตั้งระบบกล้องโทรทัศน์วงจรปิด จำเป็นต้องมีการสำรวจพื้นที่ติดตั้ง (site survey) เพื่อศึกษาสภาพแวดล้อมและวิเคราะห์ความต้องการของผู้ใช้งาน ทั้งนี้เพื่อกำหนดตำแหน่งติดตั้งกล้องให้เหมาะสม ครอบคลุมพื้นที่เฝ้าระวัง และช่วยในการเลือกใช้อุปกรณ์ต่าง ๆ ให้สอดคล้องกับลักษณะงานและงบประมาณ การออกแบบระบบที่เหมาะสมจะช่วยเพิ่มประสิทธิภาพในการเฝ้าระวัง ลดจุดอับของภาพ และทำให้ระบบสามารถทำงานได้อย่างมีเสถียรภาพและปลอดภัย ปัจจัยที่ควรพิจารณาในการออกแบบระบบ ได้แก่ พื้นที่และสภาพแวดล้อมในการติดตั้ง ระยะการมองเห็นและมุมมองของกล้อง สภาพแสงในเวลากลางวันและกลางคืน ประเภทของกล้องและอุปกรณ์บันทึกภาพ ระบบเครือข่ายและแหล่งจ่ายไฟ และ ความต้องการของผู้ใช้งานและงบประมาณ การออกแบบการติดตั้งระบบกล้องโทรทัศน์วงจรปิด มีขั้นตอนดังต่อไปนี้ (ชลดา ปานสง และคณะ, 2566)

3.4.2 การสำรวจพื้นที่การติดตั้งระบบกล้องโทรทัศน์วงจรปิด

การสำรวจพื้นที่ติดตั้งเป็นขั้นตอนสำคัญในการออกแบบระบบกล้องโทรทัศน์วงจรปิด เนื่องจากช่วยให้สามารถกำหนดตำแหน่งติดตั้งได้อย่างเหมาะสม ขั้นตอนถัดไปคือการกำหนดตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดให้เหมาะสมกับลักษณะพื้นที่และวัตถุประสงค์ในการเฝ้าระวัง โดยต้องพิจารณามุมมองของกล้อง ระยะการมองเห็น จุดอับสายตา สภาพแสง และความปลอดภัยของอุปกรณ์ จากนั้นจึงดำเนินการวัดระยะสำหรับการเดินสายนำสัญญาณ สายไฟฟ้า หรือสายเครือข่าย เพื่อใช้ในการคำนวณปริมาณวัสดุอุปกรณ์ และวางแผนการติดตั้งให้มีความเหมาะสมและประหยัดค่าใช้จ่าย



รูปที่ 3.44 ตัวอย่างการสำรวจพื้นที่และกำหนดตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดภายในอาคารสำนักงาน (ชลดา ปานสง และคณะ, 2566)

จากตัวอย่างแปลนพื้นที่ในรูปที่ 3.44 เป็นอาคารขนาด 10 × 10 m ซึ่งแบ่งพื้นที่ใช้งานออกเป็นบริเวณหน้าเคาน์เตอร์และพื้นที่ภายในออฟฟิศ การออกแบบตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดควรคำนึงถึงการครอบคลุมพื้นที่สำคัญ การลดจุดอับของภาพ และความเหมาะสมของมุมมองกล้อง บริเวณด้านหน้าของอาคารควรติดตั้งกล้องเพื่อเฝ้าระวังทางเข้าออก และสามารถบันทึกภาพบุคคลที่เข้ามาใช้งานภายในอาคารได้อย่างชัดเจน ส่วนบริเวณภายในออฟฟิศควรติดตั้งกล้องเพิ่มเติมเพื่อเฝ้าระวังพื้นที่ทำงานและทรัพย์สินภายใน โดยเลือกตำแหน่งที่สามารถมองเห็นพื้นที่ได้ครอบคลุมและลดการบดบังของภาพจากผนังหรือเฟอร์นิเจอร์ นอกจากนี้ควรพิจารณาตำแหน่งติดตั้งอุปกรณ์ประกอบ เช่น เครื่องบันทึกภาพ (DVR/NVR) แหล่งจ่ายไฟ และเส้นทางเดินสายนำสัญญาณ เพื่อให้สามารถติดตั้งและบำรุงรักษาระบบได้สะดวก รวมทั้งช่วยลดความเสียหายของสายสัญญาณและเพิ่มความปลอดภัยให้กับระบบโดยรวม จากรูปจะเห็นได้ว่าการกำหนดตำแหน่งกล้องถูกออกแบบให้สามารถมองเห็นพื้นที่ใช้งานหลักทั้งบริเวณหน้าเคาน์เตอร์และพื้นที่ภายในออฟฟิศได้อย่างเหมาะสม ซึ่งเป็นหลักการสำคัญในการออกแบบระบบกล้องโทรทัศน์วงจรปิดให้มีประสิทธิภาพ (ชลดา ปานสง และคณะ, 2566) ปัจจุบันมีแอปพลิเคชันบนสมาร์ตโฟนที่สามารถใช้วัดระยะหรือขนาดของวัตถุและพื้นที่ต่าง ๆ ได้ เพิ่มความสะดวกและรวดเร็วในการสำรวจพื้นที่ติดตั้งระบบกล้องโทรทัศน์วงจรปิด ลดข้อจำกัดในการใช้เครื่องมือวัด เช่น ตลับเมตร และช่วยให้การวางแผนติดตั้งมีความคล่องตัวมากยิ่งขึ้น

รูปที่ 3.45 ตัวอย่างการใช้แอปพลิเคชั่น AR Plan: Room & Floor Measure

3.4.3 การเขียนแบบงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด

ก่อนดำเนินการติดตั้งระบบกล้องโทรทัศน์วงจรปิด เช่น การเจาะผนัง การติดตั้งอุปกรณ์ และการเดินสายนำสัญญาณ จำเป็นต้องมีการเขียนแบบงานติดตั้ง (installation layout) เพื่อใช้ในการวางแผนและกำหนดตำแหน่งอุปกรณ์ต่าง ๆ ให้เหมาะสมกับพื้นที่ใช้งาน การเขียนแบบติดตั้งมีวัตถุประสงค์เพื่อช่วยให้สามารถกำหนดมุมมองของกล้องได้อย่างมีประสิทธิภาพ ลดจุดอับของภาพ และเลือกใช้อุปกรณ์ให้เหมาะสมกับความต้องการของผู้ใช้งาน รวมถึงช่วยให้การติดตั้งเป็นไปอย่าง

ถูกต้องและสะดวกต่อการบำรุงรักษาในอนาคต ในการจัดทำแบบติดตั้ง ผู้ติดตั้งสามารถเขียนแบบจากการสำรวจสถานที่จริง หรือใช้แบบแปลนอาคารที่มีอยู่แล้วมาปรับปรุงเพิ่มเติม โดยแบบติดตั้งควรแสดงรายละเอียดที่สำคัญ เช่น ขนาดและลักษณะของพื้นที่ ตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิด ตำแหน่งเครื่องบันทึกภาพ (DVR/NVR) เส้นทางเดินสายสัญญาณและสายไฟฟ้า ตำแหน่งอุปกรณ์เครือข่ายและแหล่งจ่ายไฟ และชนิดและขนาดของสายสัญญาณที่ใช้งาน

ปัจจุบันมีโปรแกรมช่วยออกแบบระบบกล้องโทรทัศน์วงจรปิดหลายประเภท เช่น โปรแกรม Video Surveillance Design Apps สามารถดาวน์โหลดได้ที่เว็บไซต์ http://www.jvsg.com/ip-video-system-design-tool/ ซึ่งสามารถใช้ฟรีไม่มีค่าใช้จ่ายในกรณีที่ระบบไม่ใหญ่มาก ในกรณีระบบที่ใหญ่จำเป็นต้องมีค่าใช้จ่ายในการใช้งาน (ชลดา ปานสง และคณะ, 2566) ดังรูปที่ 3.46

รูปที่ 3.46 ตัวอย่าง Video Surveillance Design Apps (.jvsg.com, 2024)

ตัวอย่างความต้องการของลูกค้าในการติดตั้งระบบกล้องโทรทัศน์วงจรปิด มีดังนี้

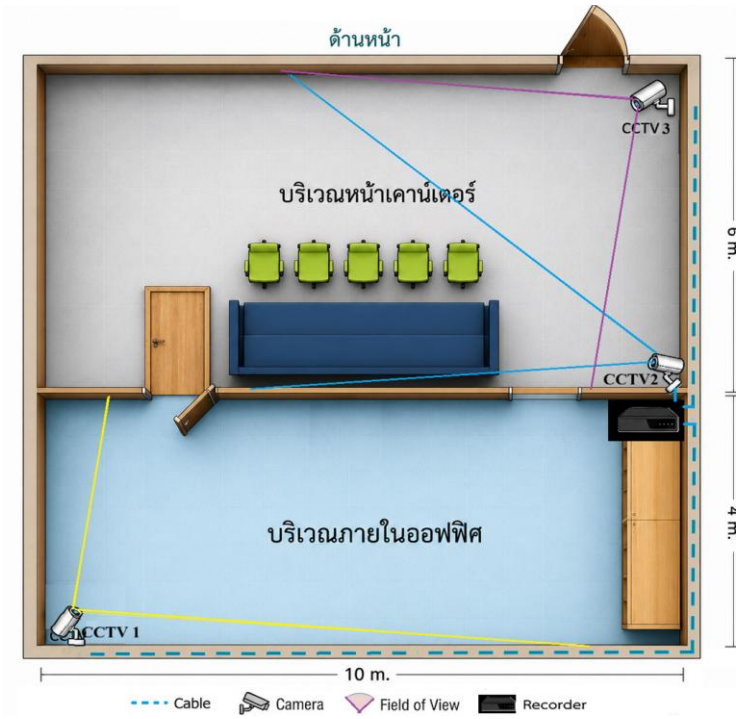
2.1) ต้องการบันทึกภาพภายในห้องทำงานสำนักงาน

2.2) ต้องการบันทึกภาพบริเวณเคาน์เตอร์รับลูกค้า

2.3) ต้องการบันทึกภาพบริเวณประตูทางเข้าออกบริษัท

2.4) มีงบประมาณสำหรับติดตั้งระบบประมาณ 25,000 บาท

จากความต้องการดังกล่าว ผู้ออกแบบระบบจึงสามารถกำหนดตำแหน่งติดตั้งกล้องให้ครอบคลุมพื้นที่สำคัญ พร้อมเลือกอุปกรณ์ที่เหมาะสมกับงบประมาณและลักษณะการใช้งาน เพื่อให้ระบบมีประสิทธิภาพในการเฝ้าระวังและสามารถใช้งานได้อย่างคุ้มค่า ดังตัวอย่างในรูปที่ 3.47

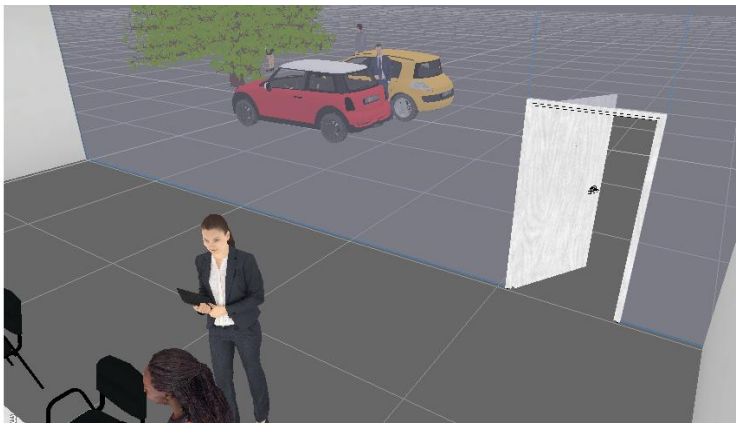


รูปที่ 3.47 ตัวอย่างการเขียนแบบติดตั้งระบบกล้องโทรทัศน์วงจรปิดภายในสำนักงาน (ชลดา ปานสง และคณะ, 2566)

ตัวอย่างมุมมอง 3D ของกล้องโทรทัศน์วงจรปิดที่ใช้ภายในออฟฟิต ดังรูปที่ 3.48

ก) มุมมองจากภาพกล้องตัวที่ 1

ข) มุมมองจากภาพกล้องตัวที่ 2



ค) มุมมองจากภาพกล้องตัวที่ 3

รูปที่ 3.48 ตัวอย่างมุมมองภาพสามมิติของกล้องโทรทัศน์วงจรปิดแต่ละตำแหน่งติดตั้ง จาก Video Surveillance Design Apps (ชลดา ปานสง และคณะ, 2566)

3.5.4 การคำนวณระยะเลนส์ของกล้องโทรทัศน์วงจรปิด

1) กล้องตัวที่ 1 ใช้สำหรับบันทึกภาพภายในสำนักงาน

พื้นที่ที่ต้องการมองเห็นมีความกว้าง 4 m สูง 3 m และตำแหน่งติดตั้งกล้องอยู่ห่างจากวัตถุประมาณ 8 m ใช้กล้องที่มีเซนเซอร์ขนาด 1/4″ ซึ่งมีขนาดเซนเซอร์แนวนอน 3.6 mm และแนวตั้ง 2.7 mm การคำนวณระยะเลนส์สามารถคำนวณได้ดังนี้

$$f = \frac{S_V \times D}{Y}$$

$$f = \frac{2.7\text{mm} \times 8\text{m}}{3\text{m}}$$

$$f = 7.2\ \text{mm}$$

หรือคำนวณจากแนวนอน

$$f = \frac{S_H \times D}{X}$$

$$f = \frac{3.6\text{mm} \times 8\text{m}}{4\text{m}}$$

$$f = 7.2\ \text{mm}$$

ดังนั้นควรเลือกใช้เลนส์ขนาดประมาณ 8 mm ซึ่งใกล้เคียงกับค่าที่คำนวณได้ และเหมาะสมกับระยะการมองเห็นของพื้นที่ดังกล่าว (ชลดา ปานสง และคณะ, 2566)

2) กล้องตัวที่ 2 ใช้สำหรับจับภาพหน้าเคาน์เตอร์

พื้นที่ที่ต้องการมองเห็นมีความกว้าง 6 m สูง 3 m และตำแหน่งติดตั้งกล้องอยู่ห่างจากวัตถุประมาณ 6 m ใช้กล้องที่มีเซนเซอร์ขนาด 1/4″ ซึ่งมีขนาดเซนเซอร์แนวนอน 3.6 mm และแนวตั้ง 2.7 mm การคำนวณระยะเลนส์สามารถคำนวณได้ดังนี้

$$f = \frac{S_V \times D}{Y}$$
$$f = \frac{2.7\ mm \times 6\ m}{3m}$$
$$f = 5.4\ mm$$

หรือคำนวณจากแนวนอน

$$f = \frac{S_H \times D}{X}$$
$$f = \frac{3.6\ mm \times 6\ m}{6m}$$
$$f = 3.6\ mm$$

สรุปจากการคำนวณระยะเลนส์กล้องโทรทัศน์วงจรปิดจากแนวตั้งได้ 5.4 mm และการคำนวณจากแนวนอน ได้ 3.6 mm ดังนั้นจะเลือกค่าที่ “แคบกว่า” เพื่อให้เห็นภาพครบตามต้องการ ดังนั้นกรณีนี้ควรใช้ประมาณ 5–6 mm และในงาน CCTV จริง มักเลือกเลนส์มาตรฐานใกล้เคียง เช่น 4 mm จะมีมุมกว้างกว่า ส่วน 6 mm ภาพแคบลง เห็นรายละเอียดมากขึ้น ดังนั้นถ้าต้องการให้ “เห็นพื้นที่สูง 3 m ครบ” ค่า 6 mm จึงจะเหมาะสมที่สุด (ชลดา ปานสง และคณะ, 2566)

3) กล้องตัวที่ 3 ใช้สำหรับจับภาพหน้าเคาน์เตอร์

พื้นที่ที่ต้องการมองเห็นมีความกว้าง 10 m และสูง 3 m โดยตำแหน่งติดตั้งกล้องอยู่ห่างจากวัตถุประมาณ 12 m เลือกใช้กล้องที่มีเซนเซอร์ขนาด 1/4″ ซึ่งมีขนาดเซนเซอร์แนวนอน (S_H) เท่ากับ 3.6 mm และขนาดเซนเซอร์แนวตั้ง (S_V) เท่ากับ 2.7 mm สามารถคำนวณระยะเลนส์ที่เหมาะสมได้ดังนี้ (ชลดา ปานสง และคณะ, 2566)

$$f = \frac{S_V \times D}{Y}$$
$$f = \frac{2.7mm \times 12m}{3m}$$
$$f = 10.8\ mm$$

หรือคำนวณจากแนวนอน

$$f = \frac{S_H \times D}{X}$$
$$f = \frac{3.6mm \times 12m}{10m}$$
$$f = 4.32\ mm$$

จากการคำนวณพบว่า การคำนวณจากแนวตั้ง ได้ค่าความยาวโฟกัสประมาณ 10.8 mm และการคำนวณจากแนวนอน ได้ค่าความยาวโฟกัสประมาณ 4.32 mm เนื่องจากพื้นที่ที่ต้องการเฝ้าระวังบริเวณหน้าเคาน์เตอร์จำเป็นต้องมองเห็นภาพในแนวนอนให้ครอบคลุมพื้นที่กว้าง

ประมาณ 10 m จึงควรอ้างอิงค่าที่คำนวณจากแนวนอนเป็นหลัก ดังนั้นในการออกแบบจึงเลือกใช้เลนส์ขนาดประมาณ 4–6 mm

ในกรณีนี้เลือกใช้เลนส์ขนาด 6 mm เนื่องจากสามารถมองเห็นพื้นที่ได้ครอบคลุมพร้อมทั้งให้รายละเอียดของภาพชัดเจนมากกว่าเลนส์ขนาด 4 mm เหมาะสำหรับการเฝ้าระวังบริเวณหน้าเคาน์เตอร์และพื้นที่ภายในอาคาร (ชลดา ปานสง และคณะ, 2566)

3.4.5 การคำนวณความกว้างของพื้นที่ที่กล้องมองเห็นได้ (Field Width)

1) ความกว้างของพื้นที่ที่กล้องมองเห็นของกล้อง CCTV 1

สำหรับห้องที่ 1 ขนาด 4 × 10 m ควรเลือกใช้กล้องโทรทัศน์วงจรปิดที่มีเซนเซอร์รับภาพขนาด 1/4″ ร่วมกับเลนส์มุมกว้างประมาณ 4 mm จำนวน 2 ตัว แต่เนื่องจากมีงบประมาณจำกัด จากแบบเราทำการติดตั้งได้เพียง 1 ตัว จะครอบคลุมพื้นที่โดนประมาณ 4 × 5 m (เนื่องห้องมีทางเข้าออกเพียงทางเดียว จึงเลือกติดฝั่งที่สามารถมองเห็นการเข้าออกได้)

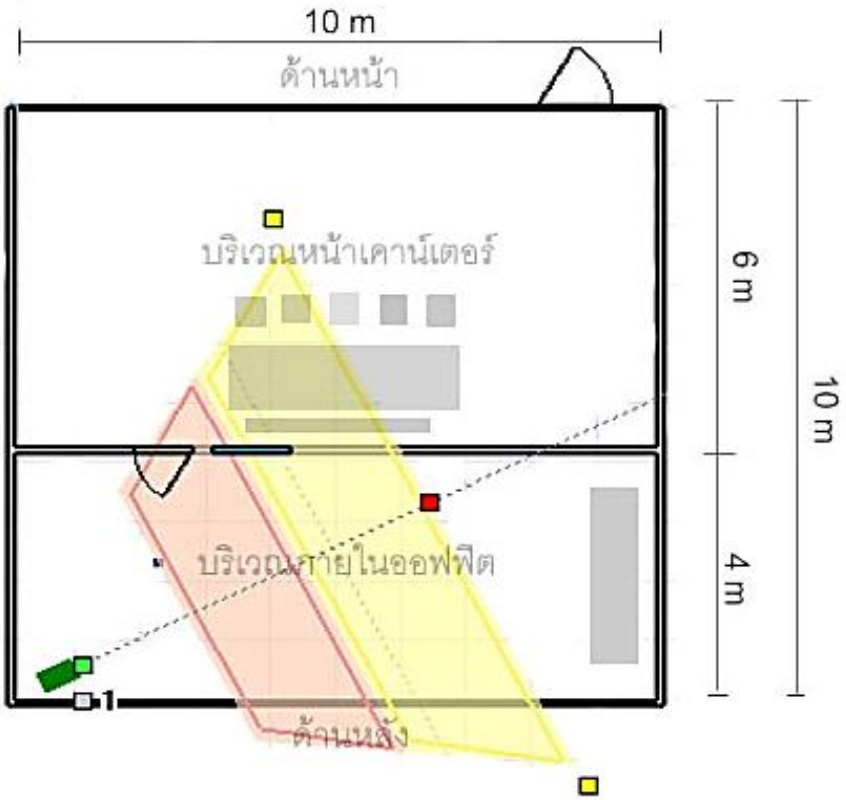
เพื่อให้สามารถมองเห็นพื้นที่ภายในห้องได้อย่างครอบคลุมและลดจุดอับของภาพสำหรับกล้อง CCTV 1 เลือกใช้เลนส์ขนาดประมาณ 8 mm และเซนเซอร์ 1/4″ ซึ่งสามารถคำนวณเหมาะสมกับระยะการมองเห็นของพื้นที่ดังกล่าว เมื่อกำหนดระยะห่างของเลนส์ถึงวัตถุ (D) ประมาณ 5 m ความกว้างเซนเซอร์ (S_H) คือ 3.6 ดังนั้นสามารถคำนวณหาความกว้างของพื้นที่ที่กล้องมองเห็นได้ (X) ดังนี้

$$x = \frac{S_H \times D}{f}$$

$$x = \frac{3.6 \times 5}{4}$$

$$x = 4.5 \text{ m}$$

ดังนั้นกล้อง CCTV1 สามารถมองเห็นพื้นที่ได้กว้างที่สุดประมาณ 4.5 m ดังรูปที่ 3.49 ซึ่งเป็นตัวอย่างการจำลองการทำงานจากโปรแกรม Video Surveillance Design Apps



รูปที่ 3.49 แสดงตัวอย่างงความสามารถมองเห็นพื้นที่ด้านกว้างของกล้อง CCTV 1 (ชลดา ปานสง และคณะ, 2566)

2) ความกว้างของพื้นที่ที่กล้องมองเห็นของกล้อง CCTV 2

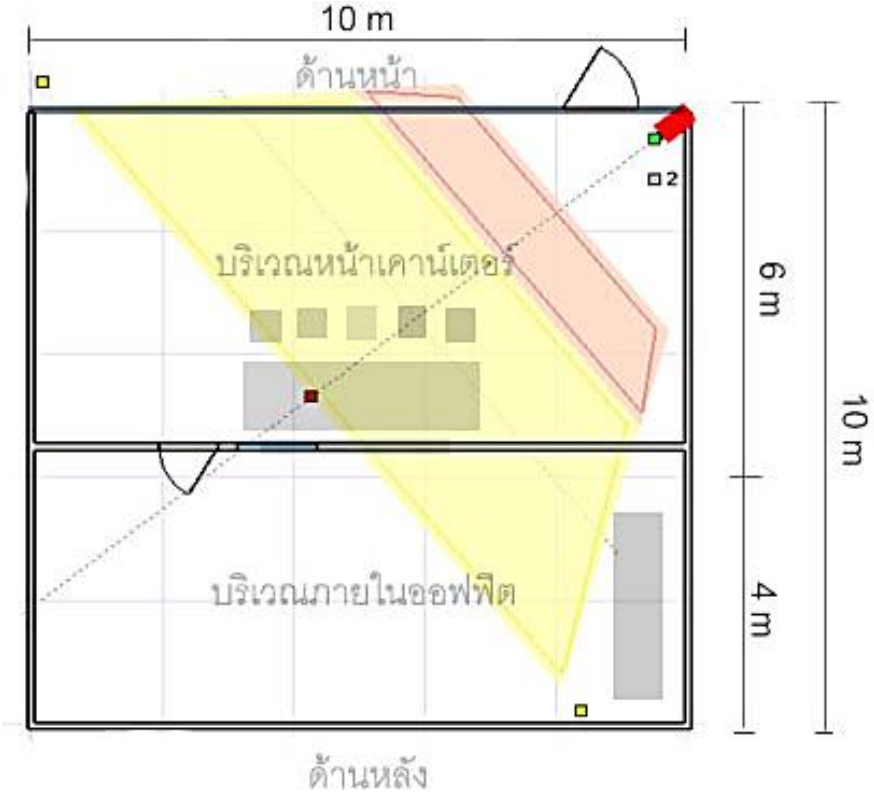
สำหรับกล้อง CCTV 2 เลือกใช้เลนส์ขนาด 6 mm ร่วมกับเซนเซอร์ขนาด 1/4″ โดยกำหนดระยะห่างจากกล้องถึงวัตถุ (D) เท่ากับ 10 m และความกว้างเซนเซอร์ S_H เท่ากับ 3.6 mm สามารถคำนวณความกว้างของพื้นที่ที่กล้องมองเห็นได้ (X) ดังนี้ ดังนี้

$$x = \frac{S_H \times D}{f}$$

$$x = \frac{3.6 \times 10}{6}$$

$$x = 6 \text{ m}$$

ดังนั้นกล้อง CCTV 2 สามารถมองเห็นพื้นที่ได้กว้างที่สุดประมาณ 6 m เพื่อให้ครอบคลุมห้องกว้าง 10 m ควรใช้กล้อง 2 ตัว ถือว่าเพียงพอในเชิงความกว้าง แต่ควรเผื่อมุมซ้อนทับและจุดอับด้วย เป็นตัวอย่างการจำลองการทำงานจากโปรแกรม Video Surveillance Design Apps ดังรูปที่ 3.50



รูปที่ 3.50 แสดงตัวอย่างงความสามารถมองเห็นพื้นที่ด้านกว้างของกล้อง CCTV 2 (ชลดา ปานสง และคณะ, 2566)

3) ความกว้างของพื้นที่ที่กล้องมองเห็นของกล้อง CCTV 3

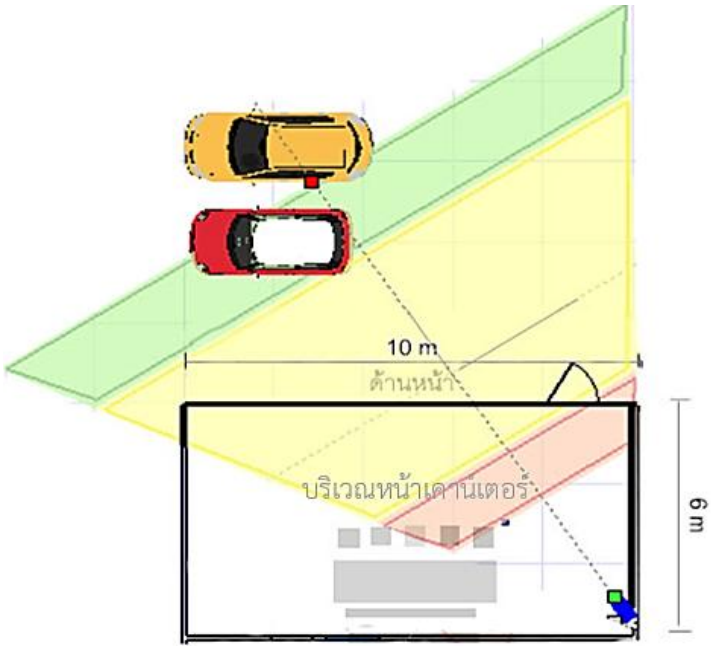
สำหรับกล้อง CCTV 3 เลือกใช้เลนส์ขนาด 6 mm ร่วมกับเซนเซอร์ขนาด 1/2.8″ เพื่อให้สามารถมองเห็นบริเวณด้านหน้าอาคารและพื้นที่ภายนอกได้ชัดเจน โดยกำหนดระยะห่างจากกล้องถึงวัตถุ (D) ประมาณ 10 m และความกว้างเซนเซอร์ (S_H) เท่ากับ 5.37 mm สามารถคำนวณความกว้างของพื้นที่ที่กล้องมองเห็นได้ (X) (ชลดา ปานสง และคณะ, 2566) ดังนี้

$$x = \frac{S_H \times D}{f}$$

$$x = \frac{5.37 \times 10}{6}$$

$$x = 8.95 \text{ m}$$

ดังนั้น กล้องจะมองเห็นพื้นที่ได้กว้างประมาณ 9 m ซึ่งถือว่าเหมาะสำหรับการมองครอบคลุมบริเวณด้านหน้าอาคาร ทางเข้าออก และลานจอดรถขนาดเล็กถึงปานกลาง



รูปที่ 3.51 แสดงตัวอย่างงความสามารถมองเห็นพื้นที่ด้านกว้างของกล้อง CCTV 3 (ชลดา ปานสง และคณะ, 2566)

3.4.6 การคำนวณความจุฮาร์ดดิสก์และแบนด์วิดท์ของระบบกล้องโทรทัศน์วงจรปิด

1) การคำนวณความจุฮาร์ดดิสก์ของระบบกล้องโทรทัศน์วงจรปิด

ในการออกแบบระบบกล้องโทรทัศน์วงจรปิด จำเป็นต้องคำนวณความจุของฮาร์ดดิสก์ (hard disk capacity) เพื่อให้เพียงพอต่อการบันทึกข้อมูลภาพจากกล้องโทรทัศน์วงจรปิด โดยในการติดตั้งครั้งนี้เลือกใช้กล้องโทรทัศน์วงจรปิดจำนวน 3 ตัว ความละเอียด 2 ล้านพิกเซล (2 MP) พร้อมเลนส์ขนาด 6 mm และเซนเซอร์ขนาด 1/2.8″ ซึ่งทำการบันทึกภาพแบบต่อเนื่องตลอด 24 ชั่วโมง โดยประมาณ กล้องโทรทัศน์วงจรปิดความละเอียด 2 MP จะใช้พื้นที่จัดเก็บข้อมูลประมาณ 70 GB ต่อวันต่อกล้อง เมื่อใช้การบีบอัดข้อมูลแบบ H.264 หรือ H.265 มีวิธีคำนวณดังนี้ (ชลดา ปานสง และคณะ, 2566)

พื้นที่จัดเก็บข้อมูลต่อวันของกล้องทั้งหมด $= 70\ \text{GB} \times 3$ ตัว

$= 210\ \text{GB/ วัน}$

เลือกใช้ฮาร์ดดิสก์ขนาด 2 TB ซึ่งมีพื้นที่ใช้งานจริงประมาณ 90% ของความจุทั้งหมด เท่ากับ 1800 GB ดังนั้น ระยะเวลาที่สามารถบันทึกข้อมูลได้ คือ

$$\frac{1800}{210} = 8.57 \text{ วัน}$$

2) การคำนวณแบนด์วิดท์ของระบบกล้องโทรทัศน์วงจรปิด

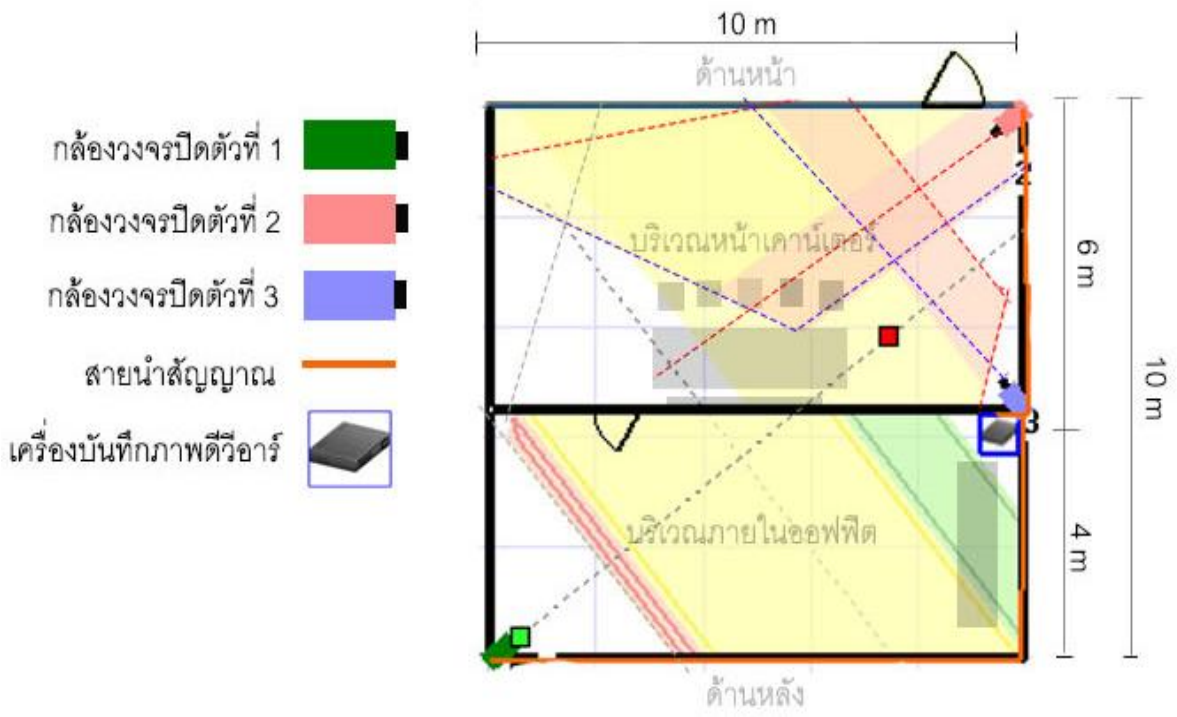
ในการออกแบบระบบกล้องโทรทัศน์วงจรปิด จำเป็นต้องคำนวณค่าแบนด์วิดท์ (bandwidth) เพื่อประเมินปริมาณการรับส่งข้อมูลของระบบเครือข่าย โดยในการติดตั้งครั้งนี้เลือกใช้กล้องโทรทัศน์วงจรปิดจำนวน 3 ตัว และกำหนดอัตราการส่งข้อมูล (bitrate) ของแต่ละกล้องไว้ที่ 2 Mbps ดังนั้น สามารถคำนวณปริมาณแบนด์วิดท์รวมของระบบได้ดังนี้ (ชลดา ปานสง และคณะ, 2566)

$$\text{ปริมาณแบนด์วิดท์รวมของระบบ} = 3\ \text{ตัว} \times 2\text{Mbp}$$

$$= 6\ \text{Mbp}$$

ดังนั้น ระบบกล้องโทรทัศน์วงจรปิดนี้จะใช้แบนด์วิดท์รวมประมาณ 6 Mbps สำหรับการรับส่งข้อมูลภาพจากกล้องทั้งหมดเข้าสู่เครื่องบันทึกภาพ ค่าดังกล่าวช่วยในการเลือกใช้อุปกรณ์เครือข่าย เช่น สวิตช์เครือข่าย (network switch) เราเตอร์ (router) และสายนำสัญญาณ ให้เหมาะสมกับการทำงานของระบบกล้องโทรทัศน์วงจรปิด เพื่อให้สามารถรับส่งข้อมูลได้อย่างมีประสิทธิภาพและลดปัญหาความล่าช้าของสัญญาณภาพ

เมื่อเลือกอุปกรณ์และคำนวณระยะเลนส์ของระบบกล้องโทรทัศน์วงจรปิดเรียบร้อยจะแสดงดังรูปที่ 3.52



รูปที่ 3.52 แผนผังระบบกล้องโทรทัศน์วงจรปิดภายในอาคาร (ชลดา ปานสง และคณะ, 2566)

3.4.7 สรุปการเลือกอุปกรณ์สำหรับการติดระบบกล้องโทรทัศน์วงจรปิด

1) การเลือกใช้กล้องโทรทัศน์วงจรปิด

จากตัวอย่างการออกแบบในรูปที่ 3.47 และ 3.48 พื้นที่ติดตั้งเป็นลักษณะสำนักงานภายในอาคาร ซึ่งประกอบด้วยบริเวณหน้าเคาน์เตอร์รับลูกค้า พื้นที่ทำงานภายในออฟฟิศ และบริเวณทางเข้าออกอาคาร ดังนั้นการเลือกใช้กล้องโทรทัศน์วงจรปิดควรคำนึงถึงลักษณะพื้นที่ใช้งาน มุมมองการเฝ้าระวัง สภาพแสง และความเหมาะสมในการติดตั้ง จากภาพตัวอย่าง ตำแหน่งติดตั้งกล้องถูกกำหนดให้ครอบคลุมพื้นที่สำคัญ ได้แก่ (1) บริเวณหน้าเคาน์เตอร์รับลูกค้า เพื่อบันทึกภาพการติดต่อและการให้บริการ (2) พื้นที่ภายในสำนักงาน เพื่อเฝ้าระวังการปฏิบัติงานและทรัพย์สินภายใน และบริเวณประตูทางเข้าออก เพื่อบันทึกภาพบุคคลที่เข้าใช้งานอาคาร

การเลือกกล้องโทรทัศน์วงจรปิดสำหรับลักษณะงานดังกล่าว ควรเลือกกล้องที่มีความละเอียดเหมาะสม เช่น full HD หรือสูงกว่า มีเลนส์ที่รองรับมุมมองครอบคลุมพื้นที่ และรองรับการทำงานในสภาพแสงน้อย เพื่อให้สามารถบันทึกภาพได้อย่างชัดเจนและมีประสิทธิภาพ (ชลดา ปานสง และคณะ, 2566) สรุปพื้นที่ติดตั้งเพื่อให้ได้มุมมองที่ชัดเจนและครอบคลุมพื้นที่ใช้งาน ดังตารางที่ 3.9

ตารางที่ 3.9 สรุปจำนวนกล้องโทรทัศน์วงจรปิดและมุมมองที่ชัดเจนและครอบคลุมพื้นที่ใช้งาน

ห้อง/พื้นที่	จำนวนกล้อง	จุดติดตั้งที่แนะนำ	วัตถุประสงค์และพื้นที่ครอบคลุม
1. ห้องด้านหน้า (บริเวณหน้าเคาน์เตอร์)	2 ตัว	**กล้อง CCTV 2:** ติดตั้งบริเวณมุมซ้ายด้านหน้าของห้อง **กล้อง CCTV 3:** ติดตั้งบริเวณมุมขวาด้านหน้าของห้องเหนือเคาน์เตอร์	**กล้อง CCTV 2:** ใช้สำหรับตรวจสอบภาพรวมของห้องการติดต่อของลูกค้า และลดจุดอับของภาพ **กล้อง CCTV 3:** ใช้สำหรับตรวจสอบพื้นที่หน้าเคาน์เตอร์ ทางเข้าออก และบริเวณด้านหน้าอาคาร
2. ห้องด้านหลัง (บริเวณภายในออฟฟิศ)	1 ตัว	**กล้อง CCTV 1:** ติดตั้งบริเวณมุมซ้ายด้านหลังของห้อง ใกล้ประตูภายใน	**กล้อง CCTV 1:** ใช้สำหรับตรวจสอบพื้นที่ภายในออฟฟิศ การเข้า–ออกภายในห้องและพื้นที่จัดเก็บอุปกรณ์

2) การเลือกเลนส์

ในการเลือกเลนส์ จำเป็นต้องคำนวณระยะเลนส์กล้องและความยาวโฟกัส เพื่อให้ตอบสนองกับความต้องการของลูกค้า

กล้องตัวที่ 1 เลือกเลนส์ จับภาพภายในออฟฟิต จึงเลือกใช้เลนส์ขนาด 8 mm

กล้องตัวที่ 2 จับภาพหน้าเคาน์เตอร์ จึงเลือกใช้เลนส์ขนาด 6 mm

กล้องตัวที่ 3 จับภาพบุคคลภายนอกที่สามารถเข้าและออกประตู จึงเลือกใช้เลนส์ขนาด 6 mm

3) เลือกใช้เครื่องบันทึกภาพและจอแสดงผล

เครื่องบันทึกภาพใช้เครื่องบันทึกภาพ DVR แบบ 4 ช่อง จอแสดงผลใช้ LED TV 19 นิ้ว

4) การเลือกสายนำสัญญาณ

การเลือกสายสัญญาณเป็นการติดตั้งกล้องแบบแอนะล็อก ใช้สายสัญญาณโคแอคเชียลชนิด RG59 เนื่องจากเหมาะสมกับระยะในการเดินสาย 0-200 m

ตารางที่ 3.10 ตารางประมาณการค่าใช้จ่ายในการติดตั้งระบบกล้องโทรทัศน์วงจรปิด

รายการอุปกรณ์และค่าแรง	ราคาประมาณการ (บาท)
1. ชุดกล้องโทรทัศน์วงจรปิดระบบ IP จำนวน 3 ตัว ความละเอียด 2 ล้านพิกเซล (2 MP) พร้อมเลนส์ขนาด 4–6 mm	9,000 – 12,000
2. เครื่องบันทึกภาพเครือข่าย (NVR) ขนาด 4 ช่อง พร้อมฮาร์ดดิสก์สำหรับบันทึกข้อมูลขนาด 1–2 TB	5,000 – 7,000
3. สวิตช์เครือข่ายแบบ PoE (Power over Ethernet) พร้อมสายนำสัญญาณ LAN CAT6	2,000 – 3,000
4. ค่าแรงติดตั้ง เดินสาย และตั้งค่าระบบกล้องโทรทัศน์วงจรปิด จำนวน 3 จุด	5,000 – 6,000
5. อุปกรณ์เสริมสำหรับงานติดตั้ง เช่น ท่อร้อยสาย กล่องกันน้ำ ขายึดกล้อง และอุปกรณ์เชื่อมต่อ	1,000 – 2,000
รวมประมาณการงบประมาณ	**22,000 – 25,000**

จากการประมาณค่าใช้จ่ายในการติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบ IP Camera จำนวน 3 จุดติดตั้ง พบว่าใช้งบประมาณโดยรวมประมาณ 22,000–25,000 บาท ซึ่งสอดคล้องกับงบประมาณที่กำหนดไว้ โดยระบบดังกล่าวสามารถรองรับการเฝ้าระวังพื้นที่ภายในอาคารและบริเวณหน้าอาคารได้อย่างมีประสิทธิภาพ

3.5 โปรแกรมบริหารจัดการระบบกล้องโทรทัศน์วงจรปิด

3.5.1 ความหมายของโปรแกรมบริหารจัดการ

โปรแกรมบริหารจัดการ คือ ซอฟต์แวร์ที่ใช้สำหรับควบคุมและจัดการระบบคอมพิวเตอร์รวมถึงอุปกรณ์ในระบบกล้องโทรทัศน์วงจรปิด เช่น กล้องโทรทัศน์วงจรปิดและเครื่องบันทึกภาพ โดยสามารถแสดงผลภาพบนจอภาพ จัดเก็บข้อมูลเป็นแฟ้ม เรียกค้นข้อมูล และสื่อสารข้อมูลภายในระบบได้ นอกจากนี้ยังช่วยดูแลและควบคุมอุปกรณ์ต่าง ๆ ในระบบกล้องโทรทัศน์วงจรปิด เช่น การดูภาพกล้องโทรทัศน์วงจรปิดผ่านอินเทอร์เน็ต การดูภาพย้อนหลัง การตั้งค่าพารามิเตอร์ต่าง ๆ ของเครื่องบันทึกภาพ ซึ่งผู้ใช้งานสามารถดำเนินการได้อย่างสะดวกและมีประสิทธิภาพ

3.5.2 ซอฟแวร์ Central Management System (CMS)

CMS เป็นโปรแกรมที่ใช้สำหรับดูกล้องโทรทัศน์วงจรปิดผ่านคอมพิวเตอร์ และช่วยในการบริหารจัดการระบบกล้องโทรทัศน์วงจรปิด ผู้ใช้งานจะได้รับความสะดวกสบาย พร้อมทั้งสามารถใช้งานฟังก์ชันต่าง ๆ ได้อย่างหลากหลาย เช่น การดูกล้องโทรทัศน์วงจรปิดผ่านอินเทอร์เน็ต การดูภาพย้อนหลัง และการตั้งค่าพารามิเตอร์ต่าง ๆ ของเครื่องบันทึกภาพ ซึ่งทั้งหมดสามารถดำเนินการได้ผ่านโปรแกรม CMS โปรแกรม CMS ทำหน้าที่เป็นระบบจัดการและควบคุมภาพจากศูนย์กลาง เหมาะสำหรับการติดตั้งกล้องโทรทัศน์วงจรปิดหลายสถานที่ในเวลาเดียวกัน โดยปกติหากไม่มีโปรแกรม CMS ผู้ใช้งานจำเป็นต้องเปิด Browser หลายหน้าต่างเพื่อดูภาพจากแต่ละสถานที่ แต่ซอฟต์แวร์ CMS ถูกออกแบบมาเพื่อรวบรวมภาพจากทุกหน้างานมาแสดงไว้ในระบบเดียว ทำให้สะดวกต่อการตรวจสอบและบริหารจัดการมากยิ่งขึ้น ทั้งนี้ แต่ละหน้างานจำเป็นต้องมีการเชื่อมต่ออินเทอร์เน็ตเพื่อส่งสัญญาณภาพมายังศูนย์กลาง หรือหากเป็นการใช้งานภายในสถานที่เดียวกัน ก็สามารถเชื่อมต่อผ่านระบบเครือข่ายภายใน (network) ได้ ปัจจุบันซอฟต์แวร์บริหารจัดการระบบกล้องโทรทัศน์วงจรปิดของ PEOPLE FU มีจำนวน 3 โปรแกรม ดังแสดงในตารางที่ 3.11

ตารางที่ 3.11 Software CMS ของ PEOPLE FU สำหรับการดูกล้องโทรทัศน์วงจรปิด

ซอฟต์แวร์ CMS	ใช้งานสำหรับ
Software CMS	TOD AHD 40xxB
Software CMS Client	DVR 9108
Software CMS Client 2.0.0.47	DVR 50xxHV

ข้อดีของการใช้ซอฟต์แวร์ CMS

1) โปรแกรมใช้งานง่าย สามารถใช้งานได้ทั้งภายในระบบเครือข่าย LAN และผ่านทางอินเทอร์เน็ต ทำให้ผู้ใช้งานสามารถตรวจสอบภาพจากกล้องโทรทัศน์วงจรปิดได้จากทุกสถานที่

2) ซอฟต์แวร์เป็นโปรแกรมฟรีสำหรับเวอร์ชัน Standard โดยไม่มีค่าใช้จ่ายเพิ่มเติมในการใช้งาน

3) สามารถบริหารจัดการระบบกล้องโทรทัศน์วงจรปิดได้อย่างมีประสิทธิภาพมากขึ้นด้วยระบบ E-Map ซึ่งช่วยแสดงตำแหน่งของกล้องโทรทัศน์วงจรปิดบนแผนผังพื้นที่

4) สามารถบันทึกภาพสดจากกล้องโทรทัศน์วงจรปิดลงในเครื่องคอมพิวเตอร์ เพื่อใช้ในการจัดเก็บข้อมูลและตรวจสอบย้อนหลังได้

5) สามารถปรับคุณสมบัติของวิดีโอได้ เช่น อัตราส่วนภาพ ความสว่าง ความคมชัด และยังสามารถควบคุมการซูมเข้า–ออกของกล้อง Speed Dome ได้อีกด้วย

สำหรับ Software CMS สำหรับการดูกล้องโทรทัศน์วงจรปิดผ่านแอปพลิเคชั่นบนโทรศัพท์มือถือ ผู้ใช้งานจะสามารถดูผ่านแอปพลิเคชั่นบนโทรศัพท์ได้เนื่องจากกล้องโทรทัศน์วงจรปิดบางรุ่นอาจจะรองรับการใช้งานผ่านแอปพลิเคชั่นผ่านโทรศัพท์เฉพาะตัว ทั้งนี้ขึ้นอยู่กับการเลือกใช้งานตามความต้องการ ข้อดีของการใช้ Software CMS สำหรับการดูกล้องโทรทัศน์วงจรปิด

บนโทรศัพท์มือถือ โดย (1) โปรแกรมใช้งานง่ายสามารถดูภาพสดได้ทุกที่ ทุกเวลา (2) ตัวซอฟแวร์ฟรี ไม่มีค่าใช้จ่ายใดๆ และ (3) สามารถบันทึกภาพสดกล้องโทรทัศน์วงจรปิดลงในตัวแอปพลิเคชั่นได้

3.5.3 การติดตั้งโปรแกรมบริหารจัดการ

โปรแกรมบริหารจัดการที่ใช้งานบนคอมพิวเตอร์ หรือ โปรแกรม CMS ซึ่งใช้สำหรับควบคุมและบริหารจัดการเครื่องบันทึกภาพดิจิทัล (DVR) หลายเครื่องให้อยู่ในระบบเดียวกัน ผู้ใช้งานสามารถดูภาพสด ตั้งค่าการทำงานของอุปกรณ์ และดูภาพย้อนหลังได้จากศูนย์กลาง โปรแกรม CMS เป็นซอฟต์แวร์ฟรีที่มาพร้อมกับเครื่องบันทึกภาพ ในการติดตั้งโปรแกรม CMS จำเป็นต้องคำนึงถึงความพร้อมของทั้งซอฟต์แวร์และฮาร์ดแวร์ของเครื่องคอมพิวเตอร์ เพื่อให้โปรแกรมสามารถทำงานได้อย่างมีประสิทธิภาพ (Evolveo, 2021) โดยมีรายละเอียดดังนี้

1) ความต้องการด้านซอฟต์แวร์

โปรแกรม CMS สามารถทำงานบนระบบปฏิบัติการ Windows ก่อนทำการติดตั้งโปรแกรม ควรปิดโปรแกรมป้องกันไวรัสและไฟร์วอลล์ชั่วคราว เพื่อป้องกันปัญหาที่อาจเกิดขึ้นระหว่างการติดตั้ง และเพื่อให้โปรแกรมสามารถติดตั้งได้อย่างสมบูรณ์

2) ความต้องการด้านฮาร์ดแวร์

2.1) หน่วยประมวลผล (CPU) ระดับ Pentium 4 ความเร็ว 2.0 GHz ขึ้นไป

2.2) การ์ดแสดงผล (graphic card) ที่รองรับการประมวลผลแบบ hardware acceleration เช่น ATI, TNT2 และ PRO โดยแนะนำให้ใช้ ATI9800 หรือสูงกว่า

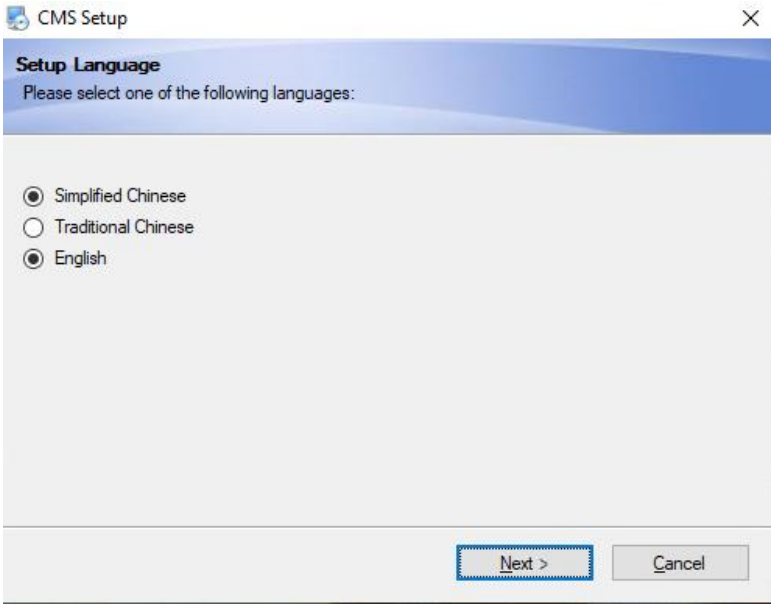
2.3) หน่วยความจำการ์ดจอ (graphic memory) ขนาดไม่น้อยกว่า 128 MB และรองรับ 128-bit

2.4) การ์ดเครือข่าย (network card) รองรับความเร็ว 100/1000 Mbps

ควรเลือกใช้เครื่องคอมพิวเตอร์ที่มีประสิทธิภาพด้าน CPU และหน่วยความจำการ์ดจอในระดับที่เหมาะสม โดยเฉพาะกรณีที่ต้องแสดงผลหลายหน้าจอพร้อมกัน เนื่องจากระบบจะมีการบีบอัดและรับส่งข้อมูลผ่านเครือข่ายจำนวนมาก

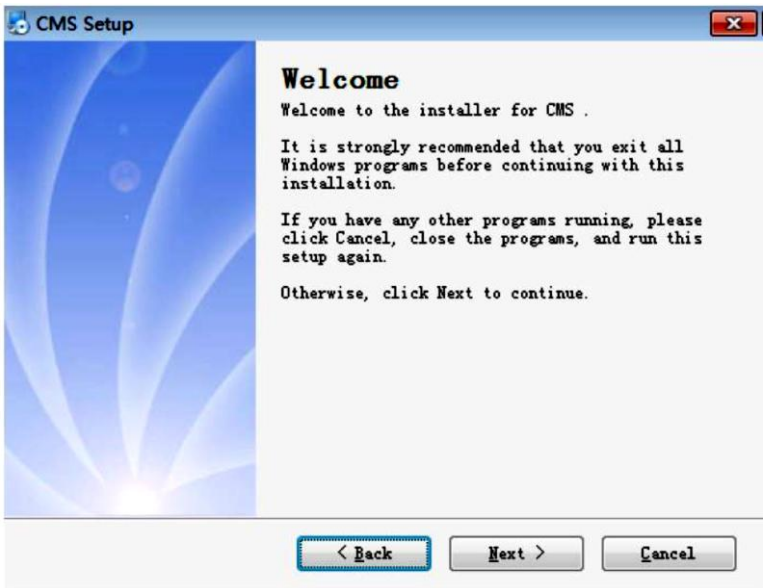
3) ขั้นตอนการติดตั้งโปรแกรม CMS

3.1) ค้นหาไฟล์ “Setup” ภายในแผ่นซีดีติดตั้งโปรแกรม จากนั้นคลิก Run เพื่อเริ่มต้นการติดตั้ง โปรแกรมจะแสดงหน้าต่างติดตั้งขึ้นมา ให้เลือกภาษา English แล้วคลิก “Next” ดังรูปที่ 3.53



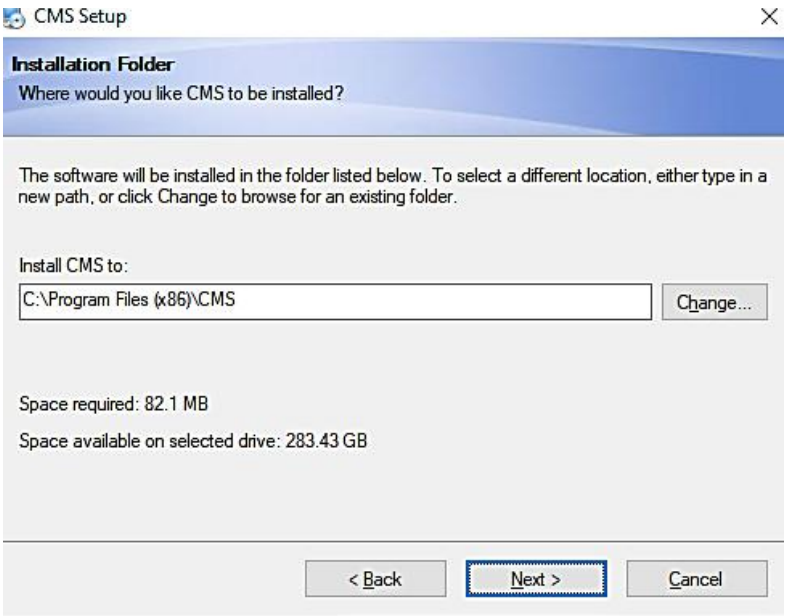
รูปที่ 3.53 การ Download โปรแกรม CMS

2) คลิก "Next" เพื่อทำการติดตั้งการติดตั้ง ดังรูปที่ 3.54



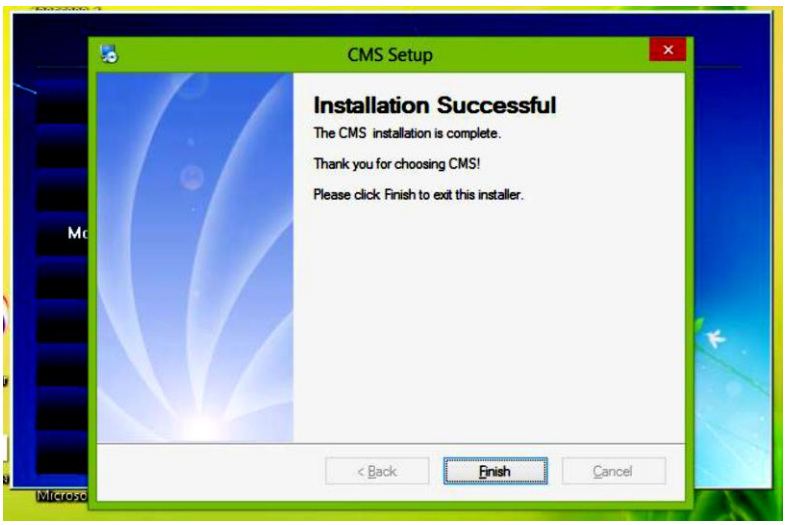
รูปที่ 3.54 ขั้นตอนการคลิก "Next" สำหรับการติดตั้งโปรแกรม CMS

3) คลิก "Browser" เพื่อเลือกเส้นทางการติดตั้ง (เส้นทางเริ่มต้น "C: \Program Files") จากนั้นคลิก "Next" เพื่อเริ่มการติดตั้ง ดังรูปที่ 3.55



รูปที่ 3.55 การเลือกเส้นทางการติดตั้ง

4) คลิก "Finish" เพื่อสิ้นสุดการติดตั้ง ดังรูปที่ 3.56



รูปที่ 3.56 ขั้นตอนการลงโปรแกรมสำเร็จ

5) หลังจากติดตั้งเสร็จแล้วจะปรากฏไอคอนบทหน้าเดสก์ท็อป ดังรูปที่ 3.57

รูปที่ 3.57 ไอคอนโปรแกรม CMS

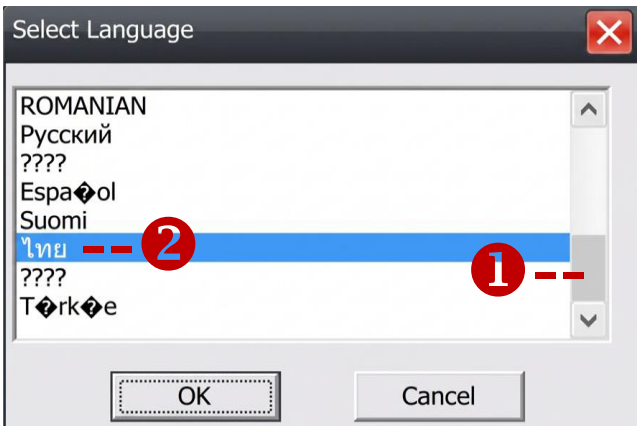
3.5.4 การทดสอบการใช้งานโปรแกรมบริหารจัดการ

โปรแกรมอาจสามารถติดตั้งได้สำเร็จโดยไม่มีการแจ้งข้อผิดพลาดใด ๆ แต่เมื่อนำโปรแกรมไปใช้งานจริง อาจพบว่าผลลัพธ์ที่ได้ไม่ถูกต้องหรือไม่ตรงตามความเป็นจริง ทั้งนี้อาจเกิดจากข้อผิดพลาดของระบบหรือการตั้งค่าการทำงานของโปรแกรม ดังนั้นจึงจำเป็นต้องมีการทดสอบการทำงานของโปรแกรมอีกครั้ง เพื่อให้มั่นใจว่าโปรแกรมสามารถทำงานได้อย่างถูกต้องและมีประสิทธิภาพ การทดสอบความถูกต้องของข้อมูลและการทำงานของโปรแกรมสามารถดำเนินการได้หลายวิธี ดังต่อไปนี้

1) การตั้งค่าโปรแกรมบริหารจัดการ

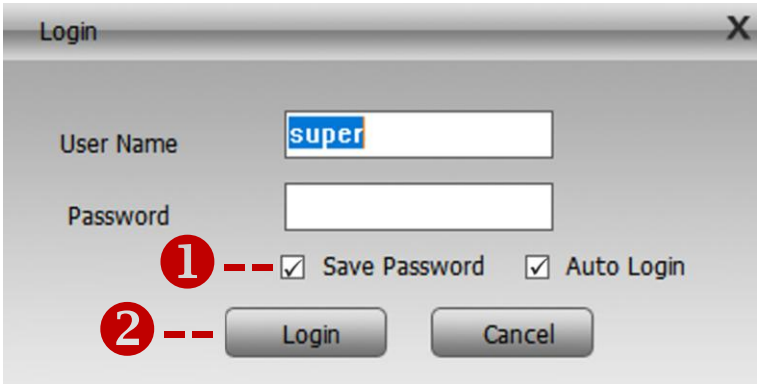
กรณีต้องการดูภาพย้อนหลัง มีขั้นตอนการตั้งค่าดังนี้

1.1) หลังจากติดตั้งโปรแกรมเสร็จเรียบร้อย โปรแกรมจะแสดงหน้าต่างสำหรับเลือกภาษาในการใช้งาน ให้เลื่อนเลือกภาษาไทยหรือภาษาอังกฤษ จากนั้นคลิกปุ่ม “OK” ดังรูปที่ 3.58



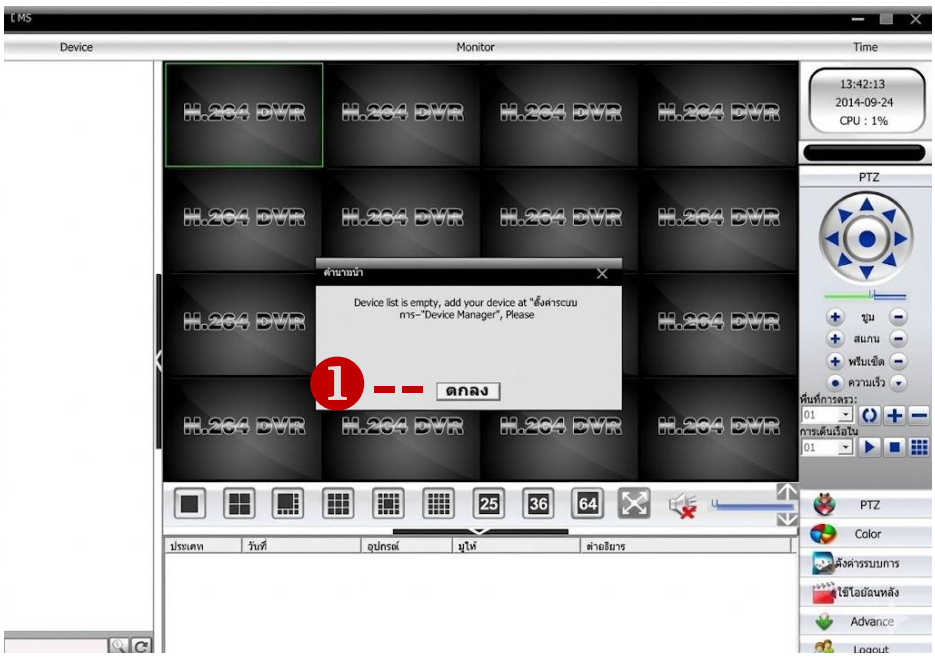
รูปที่ 3.58 การเลือกภาษาสำหรับตัวโปรแกรมบริหารจัดการ

1.2) กดคลิกถูกที่ [บันทึกรหัสผ่าน] และ [Auto Login] แล้วกด [ล็อคอิน] ดังรูปที่ 3.59



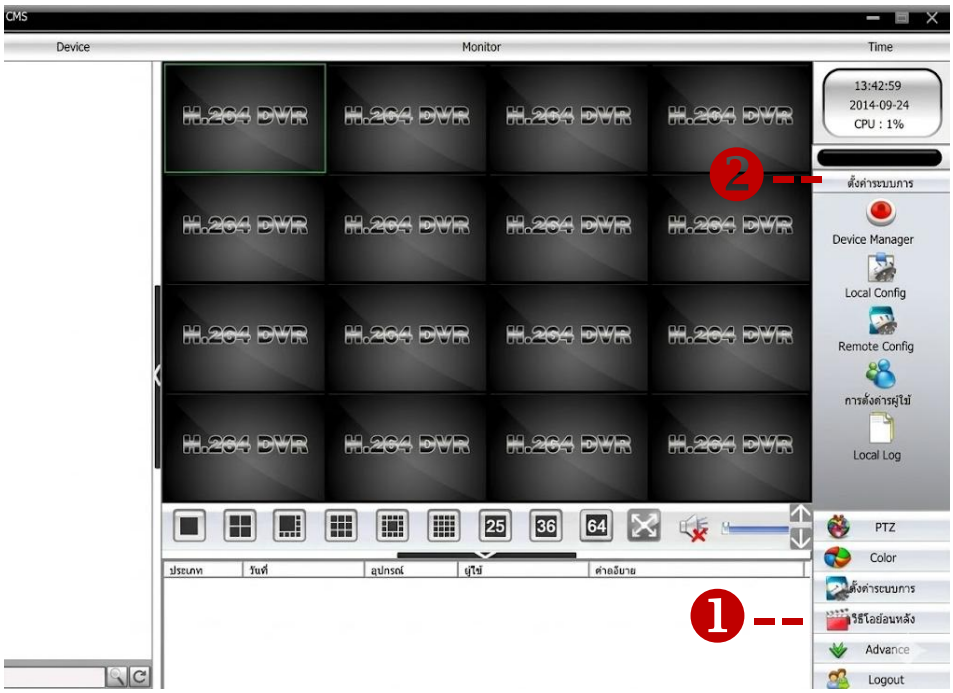
รูปที่ 3.59 หน้าต่างล็อคอินโปรแกรมบริหารจัดการ

1.3) การติดตั้งเสร็จสมบูรณ์ ระบบจะแจ้งว่าเรายังไม่มี Device กด [ตกลง] ดังรูปที่ 3.60



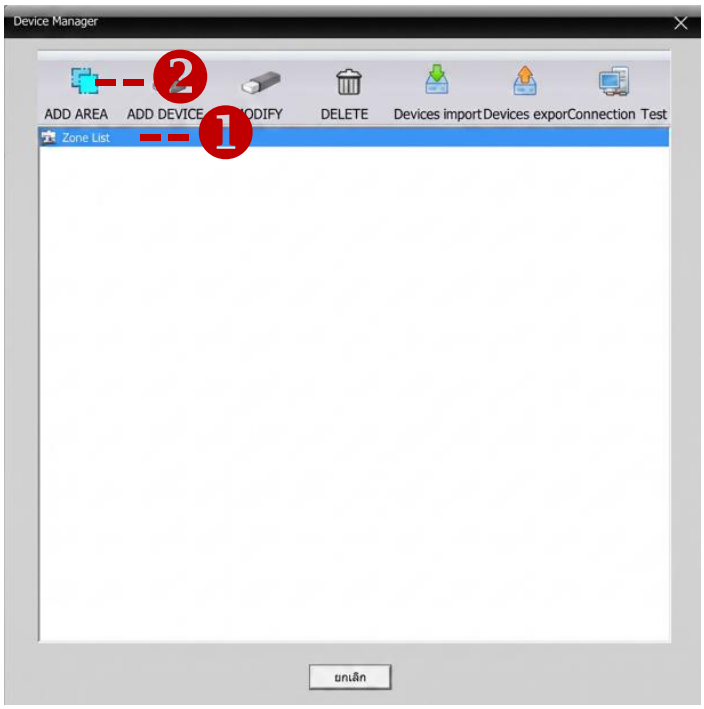
รูปที่ 3.60 หน้าต่างแสดงตัวโปรแกรมแสดงการติดตั้งเสร็จสมบูรณ์

1.4) เลือกช่วงเวลาที่ต้องการดูภาพ ดังรูปที่ 3.61



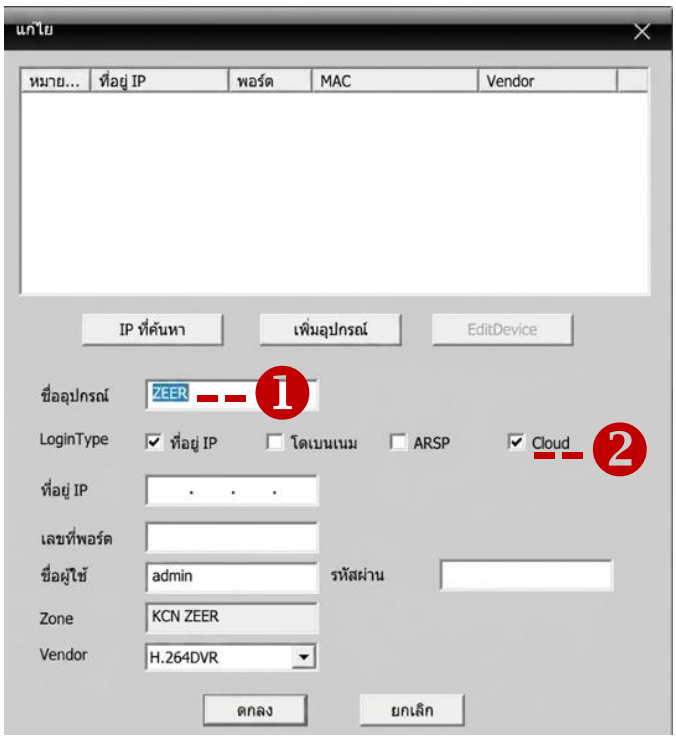
รูปที่ 3.61 หน้าต่างแสดงตัวโปรแกรมแสดงช่วงเวลาที่ต้องการดูภาพ

1.5) กด [Zone List] และ [ADD Area] ดังรูปที่ 3.62



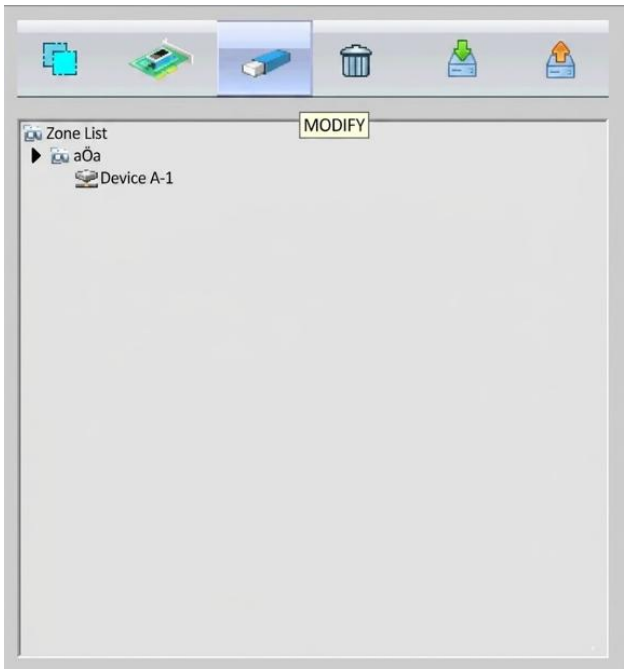
รูปที่ 3.62 หน้าต่างแสดงตัวโปรแกรมแสดงการเพิ่ม Zone List และ ADD Area

1.6) กด [ADD DEVICE] เพื่อทำการตั้งค่าอุปกรณ์ ดังรูปที่ 3.63



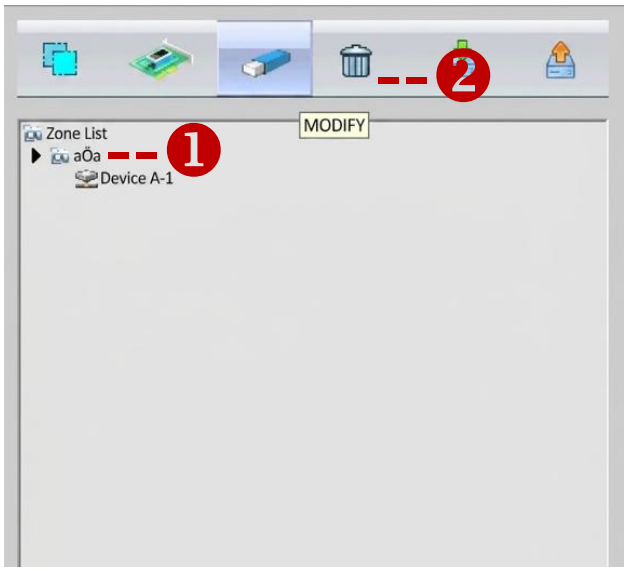
รูปที่ 3.63 หน้าต่างแสดงการตั้งค่าอุปกรณ์

1.7) คลิก MODIFY เพื่อปรับเปลี่ยนการตั้งค่าอุปกรณ์หลังจากเสร็จสิ้นการปรับเปลี่ยนทั้งหมดคลิก "OK" ดังรูปที่ 3.64



รูปที่ 3.64 หน้าต่างแสดงการปรับเปลี่ยนการตั้งค่าอุปกรณ์

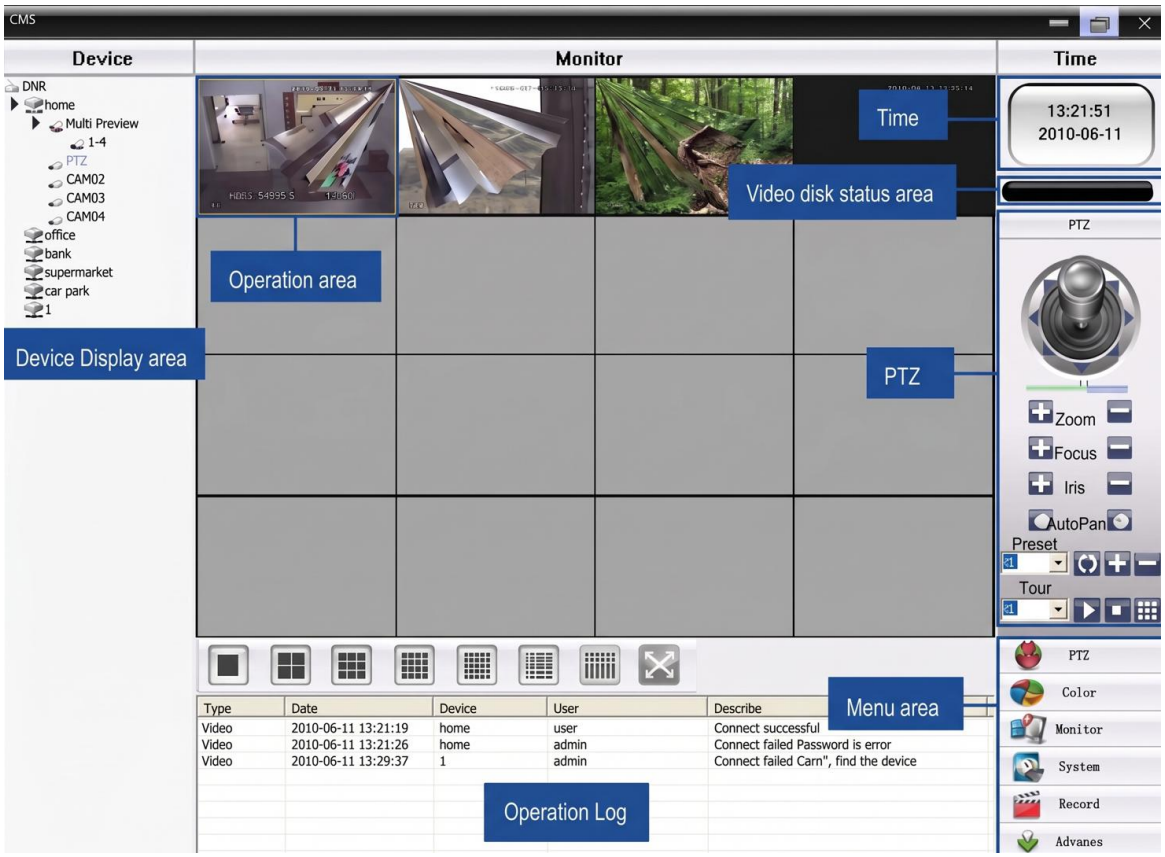
1.8) เมื่อต้องการลบอุปกรณ์หรือปรับเปลี่ยนอุปกรณ์ คลิก DELETE เพื่อลบออก ดังรูปที่ 3.65



รูปที่ 3.65 หน้าต่างแสดงการลบอุปกรณ์

3.5.5 เมนูหลักของโปรแกรม CMS

ก่อนเริ่มต้นใช้งานโปรแกรม CMS เพื่อใช้ดูกล้องโทรทัศน์วงจรปิดบนคอมพิวเตอร์และช่วยในการบริหารการจัดการระบบกล้องโทรทัศน์วงจรปิด เราจำเป็นต้องรู้เมนูที่ใช้งานของตัวโปรแกรมที่ถูกต้อง เพื่อให้ใช้โปรแกรมได้อย่างมีประสิทธิภาพ ดังรูปที่ 3.66



รูปที่ 3.66 เมนูหลักของโปรแกรม CMS

จากรูปที่ 3.66 การเรียกใช้งานโปรแกรม CMS มีเมนูดังนี้

1) พื้นที่แสดงผลอุปกรณ์ (device display area) ทำหน้าที่ในบริเวณนี้คุณสามารถดูตัวอย่างหน้าจอสดโดยการตั้งค่าของอุปกรณ์และผู้ดูแลระบบบัญชีซุปเปอร์คลิกที่ชื่ออุปกรณ์หรือกลุ่มช่องทางในการเปลี่ยน channels

2) การดำเนินงานในพื้นที่ (operation area) ทำหน้าที่คุณสามารถดูตัวอย่างหน้าจอสดและการตั้งค่าพารามิเตอร์เมื่อตั้งค่าระบบและวิดีโอค้นหาในบริเวณนี้

3) เวลา (time) ทำหน้าที่แสดงเวลา วัน เดือน ปี

4) วิดีโอพื้นที่แสดงสถานะดิสก์ (video disk status area) ทำหน้าที่สามารถแสดงพื้นที่ดิสก์ที่เหลือที่เก็บไฟล์วิดีโอ

5) การดำเนินการเข้าสู่ระบบ (operation log) ทำหน้าที่จะแสดงข้อมูลการดำเนินการต่างๆ เมื่อการติดตั้งและการดำเนินงาน

6) พื้นที่เมนู (menu area) ทำหน้าที่ผู้ใช้สามารถตั้งค่าเมนูเดียวและเมนูย่อยในพื้นที่นี้ เลือกเมนูที่เกี่ยวข้องกับการทำงานการเฝ้าระวังวิดีโอ

7) PTZ (PAN TILT ZOOM) ทำหน้าที่ผู้ใช้สามารถตั้งค่าเมนู PAN ทำหน้าที่ หมุน ส่าย ส่วน TILT ทำหน้าที่ ก้ม เงย และซูม ทำหน้าที่ขยายภาพลดภาพ

3.6 การแก้ไขปัญหาและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด

ระบบกล้องโทรทัศน์วงจรปิดอาจเกิดปัญหาจากการใช้งานหรือการเสื่อมสภาพของอุปกรณ์ (Samsung CCTV Thai, 2024; Olivia, 2025; DTIQ, 2025) ซึ่งส่งผลต่อประสิทธิภาพในการทำงานของระบบ ดังนั้น การตรวจสอบ แก้ไขปัญหา และบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ จึงเป็นสิ่งสำคัญที่จะช่วยให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพและยืดอายุการใช้งานของอุปกรณ์ได้ยาวนานขึ้น

3.6.1 อาการภาพดับหรือไม่เกิดภาพ

1) สาเหตุของอาการภาพดับหรือไม่เกิดภาพ

อาการภาพดับ หรือไม่ปรากฏภาพจากกล้องโทรทัศน์วงจรปิด อาจเกิดขึ้นได้ทั้งบางกล้องหรือทุกกล้องในระบบ ซึ่งปัญหาดังกล่าวสามารถเกิดได้จากหลายสาเหตุ เช่น การเชื่อมต่อของอุปกรณ์ไม่แน่น สายสัญญาณหลวม สายไฟขาด หรืออุปกรณ์บางส่วนเกิดความเสียหาย ส่งผลให้ระบบไม่สามารถส่งสัญญาณภาพมายังเครื่องบันทึกได้อย่างสมบูรณ์ ดังรูปที่ 3.67

รูปที่ 3.67 แสดงอาการภาพดับหรือไม่เกิดภาพในระบบกล้องโทรทัศน์วงจรปิด

ในการตรวจสอบเบื้องต้น ควรตรวจสอบจุดเชื่อมต่อต่าง ๆ ของระบบกล้องโทรทัศน์วงจรปิด ได้แก่ สายสัญญาณ สายไฟ อะแดปเตอร์ และพอร์ตเชื่อมต่อของเครื่องบันทึกภาพ ว่ามีการหลุด หลวม หรือชำรุดหรือไม่ นอกจากนี้ สามารถตรวจสอบอุปกรณ์ที่มีปัญหาได้โดยการสลับอุปกรณ์กับกล้องโทรทัศน์วงจรปิดที่ใช้งานได้ตามปกติ เพื่อวิเคราะห์หาสาเหตุที่แท้จริงของปัญหา เช่น สลับสายสัญญาณ สลับช่องต่อ หรือสลับตัวกล้อง หากเมื่อสลับแล้วภาพกลับมาใช้งานได้ แสดงว่าอุปกรณ์เดิมอาจเกิดความเสียหาย

2) การแก้ไขภาพดับหรือไม่เกิดภาพ วิธีการตรวจสอบดังต่อไปนี้

2.1) การสลับช่องต่อที่เครื่องบันทึกภาพ

ทำการย้ายช่องสัญญาณของกล้องโทรทัศน์วงจรปิดที่ด้านหลังเครื่องบันทึกภาพ โดยย้ายพร้อมชุดบาลัน (balun) เดิมทั้งหมด ไปยังช่องอื่นที่สามารถใช้งานได้ตามปกติ หากเมื่อสลับช่องแล้วภาพกลับมาแสดงผลได้ แสดงว่าปัญหาอาจเกิดจากช่องรับสัญญาณของเครื่องบันทึกภาพบางช่องเกิดความเสียหาย จากนั้นควรทดลองนำกล้องที่ใช้งานได้ปกติ มาเชื่อมต่อกับช่องที่เดิมมีปัญหาอีกครั้ง เพื่อตรวจสอบว่าเครื่องบันทึกภาพเป็นสาเหตุของปัญหาหรือไม่ ทั้งนี้ควรย้ายอุปกรณ์พร้อมชุดบาลันเดิมทุกครั้ง เพื่อให้ผลการตรวจสอบมีความถูกต้อง

2.2) การสลับสายสัญญาณด้านหลังเครื่องบันทึกภาพ

ทำการสลับสายสัญญาณของกล้องโทรทัศน์วงจรปิดที่มีปัญหา ไปเชื่อมต่อกับบาลันของช่องที่สามารถแสดงภาพได้ตามปกติ เพื่อตรวจสอบว่าระบบสามารถแสดงภาพได้หรือไม่ หากเมื่อสลับแล้วภาพกลับมาใช้งานได้ตามปกติ อาจสันนิษฐานได้ว่าบาลันด้านหลังเครื่องบันทึกภาพเกิดความเสียหาย

2.3) การสลับบาลันด้านกล้องโทรทัศน์วงจรปิด

ทำการถอดบาลันของกล้องโทรทัศน์วงจรปิดที่มีปัญหาออก แล้วนำบาลันจากกล้องโทรทัศน์วงจรปิดที่สามารถใช้งานได้ตามปกติมาทดลองเชื่อมต่อแทน จากนั้นตรวจสอบว่าภาพสามารถแสดงผลได้หรือไม่ หากภาพกลับมาใช้งานได้ตามปกติ แสดงว่าบาลันตัวเดิมอาจเกิดความเสียหายและควรเปลี่ยนอุปกรณ์ใหม่เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพ

3.6.2 อาการภาพเป็นคลื่น

1) สาเหตุของการเกิดภาพเป็นคลื่น

โดยปกติ อาการภาพเป็นคลื่นของกล้องโทรทัศน์วงจรปิด มักเกิดจากปัญหาของอุปกรณ์จ่ายไฟ เช่น แหล่งจ่ายไฟ (power supply) หรืออะแดปเตอร์ (adapter) ที่ใช้จ่ายไฟให้กับกล้องโทรทัศน์วงจรปิดเกิดความผิดปกติ ส่งผลให้กระแสไฟฟ้าที่จ่ายไปยังกล้องไม่สม่ำเสมอหรือไม่เพียงพอ

ทั้งนี้ กล้องโทรทัศน์วงจรปิดจำเป็นต้องได้รับกำลังไฟฟ้าที่เหมาะสมและคงที่ในการทำงาน หากอุปกรณ์จ่ายไฟมีการเสื่อมสภาพจากการใช้งานเป็นเวลานาน อาจทำให้ประสิทธิภาพในการจ่ายไฟลดลง ส่งผลให้ภาพที่แสดงออกมามีลักษณะเป็นคลื่น สั่นไหว หรือเกิดสัญญาณรบกวน (Olivia, 2025) ดังรูปที่ 3.68

รูปที่ 3.68 อาการภาพเป็นคลื่น

2) การแก้ไขอาการภาพเป็นคลื่น

การตรวจสอบและแก้ไขปัญหาอาการภาพเป็นคลื่น สามารถดำเนินการได้ดังนี้

2.1) ตรวจสอบอุปกรณ์จ่ายไฟให้กับกล้องโทรทัศน์วงจรปิด ว่ายังสามารถทำงานได้ตามปกติหรือไม่

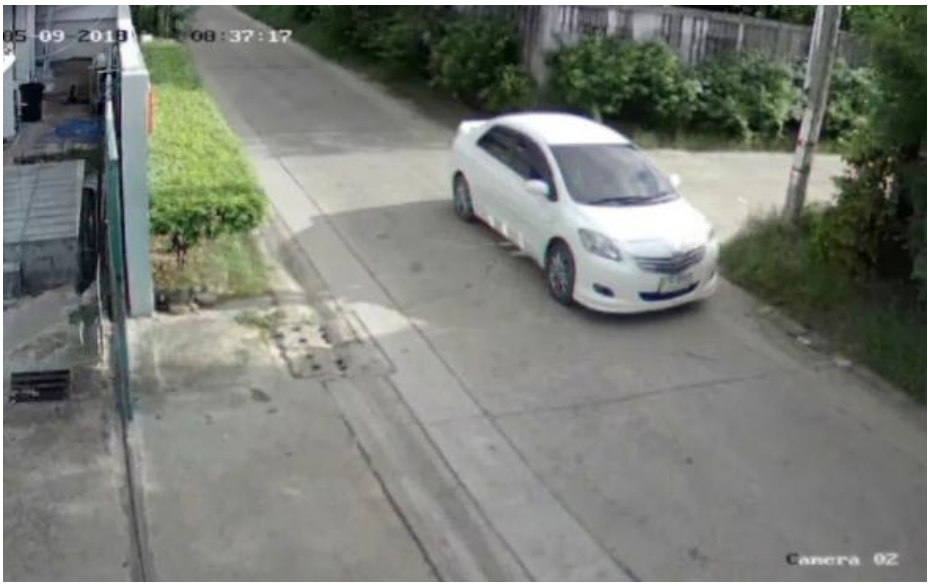
2.2) ตรวจสอบสายไฟของอุปกรณ์จ่ายไฟ ว่ามีการชำรุด หลวม หรือเกิดการเสื่อมสภาพหรือไม่

2.3) หากพบว่าอุปกรณ์จ่ายไฟ หรือสายไฟบางส่วนเกิดความเสียหาย ควรรีบดำเนินการเปลี่ยนอุปกรณ์ใหม่ทันที เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบกล้องโทรทัศน์วงจรปิดในระยะยาว

3.6.3 อาการภาพเบลอ

1) สาเหตุของอาการภาพเบลอ

อาการภาพเบลออาจเกิดจากเลนส์ของกล้องโทรทัศน์วงจรปิดเกิดการคลายตัว หรือระบบล็อกโฟกัสไม่แน่น ทำให้ตำแหน่งโฟกัสเปลี่ยนแปลง ส่งผลให้ภาพที่แสดงผลมีความไม่คมชัด (Olivia, 2025) ดังรูปที่ 3.69



รูปที่ 3.69 อาการภาพเบลอ

2) การแก้ไขอาการภาพเบลอ

2.1) ทำการปรับโฟกัสของหน้ากล้องโทรทัศน์วงจรปิด โดยหมุนเลนส์เพื่อหาตำแหน่งที่ให้ภาพคมชัดที่สุด

2.2) เมื่อได้ตำแหน่งที่ภาพชัดเจนแล้ว ให้ค่อย ๆ หมุนน็อตยึดเลนส์ให้แน่น เพื่อป้องกันการเคลื่อนตัวของเลนส์ในภายหลัง ทั้งนี้ หากเป็นกล้องโทรทัศน์วงจรปิดระบบอินฟราเรด (infrared camera) จำเป็นต้องถอดฝาครอบกระจกด้านหน้ากล้องออกก่อน จึงจะสามารถปรับโฟกัสของเลนส์ได้

2.3) หลังจากทำการปรับโฟกัสของเลนส์เรียบร้อยแล้ว ให้ประกอบฝาครอบเลนส์กลับเข้าที่เดิม เพื่อให้กล้องสามารถทำงานได้ตามปกติและป้องกันฝุ่นหรือความชื้นเข้าสู่ตัวกล้อง

3.6.4 การบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด

ระบบกล้องโทรทัศน์วงจรปิดประกอบด้วยองค์ประกอบสำคัญหลายส่วน ได้แก่ ระบบจ่ายไฟ ระบบแปลงไฟ กล้องจับภาพ และระบบบันทึกภาพ ซึ่งทุกส่วนล้วนมีความสำคัญต่อการทำงานของระบบ หากส่วนใดส่วนหนึ่งเกิดความเสียหาย อาจส่งผลให้ระบบกล้องโทรทัศน์วงจรปิดไม่สามารถทำงานได้อย่างมีประสิทธิภาพ นอกจากนี้ ระบบกล้องโทรทัศน์วงจรปิดส่วนใหญ่มักติดตั้งอยู่ภายนอกอาคารและต้องเผชิญกับสภาพแวดล้อมต่าง ๆ เช่น แสงแดด ฝน และความชื้น ซึ่งอาจทำให้อุปกรณ์เกิดการเสื่อมสภาพได้ง่าย ดังนั้น การบำรุงรักษาและตรวจสอบระบบกล้องโทรทัศน์วงจรปิดอย่างสม่ำเสมอจึงเป็นสิ่งสำคัญ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น และช่วยยืดอายุการใช้งานของระบบให้ยาวนานมากยิ่งขึ้น (Samsung CCTV Thai, 2024)

1) การตรวจสอบความสะอาดของหน้าเลนส์กล้องโทรทัศน์วงจรปิด

ควรตรวจสอบความคมชัดของภาพจากกล้องโทรทัศน์วงจรปิด รวมถึงตรวจสอบว่ามีวัตถุใดบดบังมุมมองของกล้องหรือไม่ หากพบว่าหน้าเลนส์มีฝุ่นหรือคราบสกปรก ควรใช้ผ้านุ่มหรือผ้า

ไมโครไฟเบอร์เช็ดทำความสะอาดบริเวณหน้าเลนส์อย่างระมัดระวัง นอกจากนี้สามารถใช้น้ำยาเช็ดกระจกในการทำความสะอาดกระจกหน้ากล้อง เพื่อให้ภาพที่บันทึกมีความคมชัดมากยิ่งขึ้น ทั้งนี้ควรตรวจสอบภาพจากกล้องเป็นประจำ หากทำความสะอาดหน้าเลนส์แล้วภาพยังไม่ชัดเจน ควรติดต่อศูนย์บริการหรือช่างผู้เชี่ยวชาญ เนื่องจากอาจเกิดปัญหาที่ตัวกล้องหรือเลนส์ภายใน

2) การตรวจสอบการทำงานของเครื่องบันทึกภาพและกล้องโทรทัศน์วงจรปิด

ควรตรวจสอบการทำงานของเครื่องบันทึกภาพและกล้องโทรทัศน์วงจรปิดอย่างสม่ำเสมอ โดยเปิดดูภาพจากกล้องทุกตัวเพื่อตรวจสอบความผิดปกติ เช่น ภาพขาดหาย สัญญาณภาพไม่ต่อเนื่อง หรือมีข้อความแจ้งเตือนบนหน้าจอ เช่น ไม่พบฮาร์ดดิสก์ (hard disk) เป็นต้น วิธีการป้องกันและดูแลระบบ มีดังนี้

2.1) ควรตรวจสอบภาพย้อนหลังอย่างน้อยสัปดาห์ละ 1 ครั้ง เพื่อให้มั่นใจว่าเครื่องบันทึกภาพยังสามารถทำงานได้ตามปกติ

2.2) ควรติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อช่วยป้องกันปัญหาไฟตกหรือไฟกระชาก ซึ่งอาจส่งผลให้ฮาร์ดดิสก์เกิดความเสียหาย

2.3) ควรแยกปลั๊กไฟสำหรับระบบกล้องโทรทัศน์วงจรปิดโดยเฉพาะ และตรวจสอบขั้วต่อปลั๊กไฟให้แน่นหนาอยู่เสมอ หากพบว่าปลั๊กไฟหรือปลั๊กพ่วงมีสภาพชำรุด ควรเปลี่ยนใหม่ทันที เพื่อป้องกันปัญหาระบบติด ๆ ดับ ๆ

3) การตรวจสอบสายสัญญาณที่เชื่อมต่อกับกล้องโทรทัศน์วงจรปิด

ควรตรวจสอบสายสัญญาณและสายไฟที่เชื่อมต่อกับตัวกล้องโทรทัศน์วงจรปิด ว่ายังคงอยู่ในสภาพพร้อมใช้งานหรือไม่ หากพบว่าสายเกิดการชำรุด แตกร้าว หรือเปื่อยจากสภาพอากาศ ควรรีบดำเนินการเปลี่ยนใหม่ทันที เพื่อป้องกันปัญหาการสูญเสียสัญญาณภาพ

4) การตรวจสอบแหล่งจ่ายไฟ

ควรตรวจสอบแหล่งจ่ายไฟหรืออะแดปเตอร์ของกล้องโทรทัศน์วงจรปิด ว่ายังคงสามารถจ่ายกระแสไฟฟ้าได้อย่างเพียงพอและสม่ำเสมอ เนื่องจากกล้องโทรทัศน์วงจรปิดจำเป็นต้องได้รับกำลังไฟที่เหมาะสมในการทำงาน หากอุปกรณ์จ่ายไฟเกิดการเสื่อมสภาพ อาจส่งผลให้กระแสไฟฟ้าที่จ่ายให้กล้องไม่เพียงพอ และทำให้เกิดปัญหาในการใช้งานได้ นอกจากนี้ อะแดปเตอร์และแหล่งจ่ายไฟถือเป็นอุปกรณ์ที่มีอายุการใช้งานค่อนข้างสั้น โดยเฉพาะในกรณีที่ไม่ได้ติดตั้งระบบป้องกันไฟกระชากหรือเครื่องสำรองไฟฟ้า (UPS) จะอาจทำให้อุปกรณ์ดังกล่าวเสียหายได้ง่าย

อีกปัญหาที่พบได้บ่อย คือ สายไฟหรือสายสัญญาณที่เชื่อมต่อกับตัวกล้องเกิดการกรอบหรือชำรุดจากการถูกแสงแดดเป็นเวลานาน ซึ่งมักเกิดจากการติดตั้งที่ไม่เหมาะสม ดังนั้นจึงควรติดตั้งอุปกรณ์ป้องกันสาย เช่น ท่อร้อยสายหรือกล่อง PVC เพื่อช่วยป้องกันความร้อนและยืดอายุการใช้งานของสายสัญญาณ ทั้งนี้ การติดตั้งระบบที่ถูกต้องและเหมาะสมจะช่วยเพิ่มประสิทธิภาพและยืดอายุการใช้งานของระบบกล้องโทรทัศน์วงจรปิดได้มากยิ่งขึ้น

บรรณานุกรมบทที่ 3

กิตติศักดิ์ เฮงสว่าง. (2553). *การจัดการระบบเครือข่ายกล้องโทรทัศน์วงจรปิดเอซิต*. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีมหานคร.

ชลดา ปานสง, เกียรติศักดิ์ สมฤทธิ์, จิรพงษ์ จิตตะโคตร์, พัชราวรรณ พูลใจ, ศิวกร รัตนวราหะ, และธนพล แก้วคำแจ้ง. (2566). การพัฒนาสื่อบทเรียนออนไลน์มูเดิลคลาวด์ สำหรับการฝึกอบรมการติดตั้งและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด ตามมาตรฐานกรมพัฒนาฝีมือแรงงาน. *วารสารวิจัยและนวัตกรรมการอาชีวศึกษา*, 7(2), 66-75.

ชลดา ปานสง, ปรียานุช จันหนู, และวัฒนา ภูสูง. (2561). การพัฒนาชุดฝึกอบรมการติดตั้งและบำรุงรักษากล้องโทรทัศน์วงจรปิด ตามสมรรถนะของกรมพัฒนาฝีมือแรงงาน. ใน: *การประชุมวิชาการครุศาสตร์อุตสาหกรรมระดับนานาชาติและระดับชาติ (The 6th International Conference on Learning Innovation in Science and Technology (ICLIST 2018) and the 2nd National Conference on Learning Innovation in Science and Technology (NCLIST 2018): ICLIST & NCLIST 2018*. วันที่ 21-24 มีนาคม 2561, 710-723.

บริษัท มีเดีย เสิร์ช จำกัด. (2021). *กล้องโทรทัศน์วงจรปิดระบบ WiFi กับการออกแบบระบบเครือข่าย*. https://www.cctvbangkok.com/cctv-wifi-system/.

บริษัท มีเดีย เสิร์ช จำกัด. (2025). *กล้องโดม และ Circuit Breaker และ Fuse สำหรับ CCTV ใช้ในงานเดินสายไฟกล้องโทรทัศน์วงจรปิด*. https://www.cctvbangkok.com/dome-camera/.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม. (ม.ป.ป.). *ข้อมูลผู้ได้รับใบอนุญาตมาตรฐานผลิตภัณฑ์อุตสาหกรรม*. สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม. https://appdb.tisi.go.th/Q/i.php?d=3224880409.

Ideal Quality Solutions Co., Ltd. (2560). *ระบบกล้องโทรทัศน์วงจรปิด*. https://www.ideal-solutions.co.th/products/cctv-closed-circuit-television-system/.

MacroCare Co., Ltd. (ม.ป.ป.). *KVM Switch สำหรับศูนย์รักษาความปลอดภัย (Security Center) หรือ SOC (Security Operation Center) ศูนย์กลางการดูแลความปลอดภัยขององค์กร*. https://www.mc.co.th/eshop/content/194-kvm-for-nvr-dvr-cctv-security-center

Samsung CCTV Thai. (2024). *การดูแลและบำรุงรักษากล้องโทรทัศน์วงจรปิด CCTV*. https://www.samsungcctvthai.com/การดูแลและบำรุงรักษา/.

Tataisong, S. (2020). *เรื่องควรรู้เกี่ยวกับรูรับแสง (Aperture)*. Fotoinfo Magazine. https://fotoinfo.online/เรื่องควรรู้เกี่ยวกับรู/.

Thai Meister. (2017). *คู่มือฝึกอบรม Thai Meister สาขา Mechatronics*. มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

CCTV Thailand. (2011). *TV line*. https://www.cctvthailand.com/index.php?mo=3&art=41938757.

CS Odessa. (2025a). *Computer network diagrams*. https://www.conceptdraw.com/solution-park/computer-and-networks.

CS Odessa. (2025b). *CCTV network example*. https://www.conceptdraw.com/How-To-Guide/cctv-network-example.

DTIQ. (2025). *How to resolve CCTV camera video loss*. https://www.dtiq.com/blog/video-surveillance/how-to-resolve-cctv-camera-video-loss-a-step-by-step-guide.

Evolveo. (2021). *Fast manual instruction of network video CMS V*. https://ftp.evolveo.com/monitoring_system/Detective-S4CIH7D/software/CMS/CMS%20instruction.pdf.

Forouzan, B. A. (2013). *Data communications and networking* (5th ed.). McGraw-Hill.

Gcabling. (2023). *Twisted pair cable: Types, shielding, and applications (2026 guide).* https://www.gcabling.com/ar/what-is-twisted-pair-cable-and-types/.

Holst, G. C., & Lomheim, T. S. (2011). *CMOS/CCD sensors and camera systems*. SPIE Press.

International Electrotechnical Commission (IEC). (2013). *IEC 60529: Degrees of protection provided by enclosures (IP Code)*. https://www.iec.ch/ip-ratings.

JVSG.com. (2024). *Video surveillance design apps*. https://www.jvsg.com/.

Kruegle, H. (2011). *CCTV surveillance: Video practices and technology*. Butterworth-Heinemann.

Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7th ed.). Pearson.

Ningbo Holden Cable Co., Ltd. (1998). *Best price 75ohm coaxial cable RG11 copper RG6 RG58 coaxial cable price*. GoldSupplier. https://www.goldsupplier.com/provide/p167033101.html.

Olivia. (2025). *What causes video loss in security cameras?* https://reolink.com/blog/video-loss-on-security-camera/.

Richard. (2022). *Twisted pair cable: 6 fantastic tips about its quality*. https://zwcables.com/twisted-pair-cable/.

Senior, J. M. (2009). *Optical fiber communications: Principles and practice*. Pearson.

SKnBiz. (2020). *CCTV 저장장치 NVR 과 DVR - 차이점은 무엇일까?* https://m.blog.naver.com/dreamxpeed/222116222142.

Teledyne Vision Solutions. (2026). *Calculadora de lentes de visión artificial*. https://www.teledynevisionsolutions.com/es-mx/support/support-center/technical-guidance/lens-calculator/.

VEC Thai. (2013). *Lens calculator of CCTV camera*. https://www.vecthai.com/lens-calculator/index.htm.

Zi, R. (2022). *Twisted pair cable: 6 fantastic tips about its quality*. https://zwcables.com/twisted-pair-cable/.

สรุปสาระสำคัญของบทที่ 3
ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

ความหมาย ความเป็นมา และระบบกล้องโทรทัศน์วงจรปิด

กล้องโทรทัศน์วงจรปิด หรือ CCTV (Closed Circuit Television) คือ ระบบบันทึกภาพและส่งสัญญาณภาพเพื่อใช้ในการเฝ้าระวังและรักษาความปลอดภัย โดยระบบจะส่งสัญญาณภาพไปยังอุปกรณ์ที่กำหนด เช่น จอภาพหรือเครื่องบันทึกภาพ ต่างจากการแพร่ภาพโทรทัศน์ทั่วไปที่ส่งสัญญาณสู่สาธารณะ ระบบ CCTV ถูกออกแบบมาเพื่อใช้ในพื้นที่เฉพาะ เช่น บ้าน อาคารสำนักงาน โรงงานห้างสรรพสินค้า และสถานที่ราชการ

จุดเริ่มต้นของกล้องโทรทัศน์วงจรปิดเกิดขึ้นในช่วงสงครามโลกครั้งที่ 2 โดยถูกพัฒนาขึ้นเพื่อใช้สังเกตการณ์การยิงจรวดของประเทศเยอรมนี ต่อมาระบบกล้องโทรทัศน์วงจรปิดได้ถูกนำมาใช้ในด้านความปลอดภัย การจราจร และการเฝ้าระวังทั่วไป จนกลายเป็นเทคโนโลยีสำคัญที่ใช้ในชีวิตประจำวัน

ระบบกล้องโทรทัศน์วงจรปิดสามารถแบ่งตามพัฒนาการได้หลายยุค ได้แก่

1) ระบบดูภาพอย่างเดียว (monitoring system)
2) ระบบบันทึกภาพด้วยเครื่อง VCR
3) ระบบ DVR แบบดิจิทัล
4) ระบบ IP camera ที่เชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ต

องค์ประกอบหลักของระบบกล้องโทรทัศน์วงจรปิดประกอบด้วย

1) กล้องโทรทัศน์วงจรปิด (camera)
2) เครื่องบันทึกภาพ (DVR/NVR)
3) จอแสดงผล (monitor)
4) สายสัญญาณและอุปกรณ์เชื่อมต่อ
5) ระบบเครือข่ายและแหล่งจ่ายไฟ

กล้องโทรทัศน์วงจรปิดมีบทบาทสำคัญในการช่วยลดอาชญากรรม ตรวจสอบเหตุการณ์ย้อนหลัง และช่วยในการบริหารจัดการพื้นที่ นอกจากนี้ยังช่วยเพิ่มความมั่นใจและความปลอดภัยให้แก่ผู้ใช้งาน

อุปกรณ์และหลักการทำงานของระบบกล้องโทรทัศน์วงจรปิด

อุปกรณ์ของระบบกล้องโทรทัศน์วงจรปิดมีหลายชนิด โดยแต่ละอุปกรณ์มีหน้าที่เฉพาะที่ช่วยให้ระบบทำงานได้อย่างสมบูรณ์ เริ่มจากตัวกล้องซึ่งทำหน้าที่รับภาพและแปลงเป็นสัญญาณ จากนั้นจึงส่งข้อมูลไปยังเครื่องบันทึกภาพและจอแสดงผล ประเภทของกล้องโทรทัศน์วงจรปิด ได้แก่

1) กล้องแบบแอนะล็อก (analog camera)
2) กล้อง IP camera
3) กล้องอินฟราเรด (IR camera)

4) กล้องโดม (dome camera)

5) กล้องกระบอก (bullet camera)

6) กล้องสปีดโดม (PTZ camera)

เลนส์ของกล้องมีผลต่อมุมมองภาพ โดยความยาวโฟกัส (focal length) จะกำหนดระยะและมุมมองของภาพ เลนส์มุมกว้างเหมาะสำหรับพื้นที่กว้าง ส่วนเลนส์ระยะไกลเหมาะสำหรับการซูมดูรายละเอียด นอกจากนี้ยังมีค่าที่สำคัญ เช่น

1) ค่า Lux เป็นค่าความไวแสงของกล้อง ยิ่งค่าต่ำยิ่งทำงานในที่มืดได้ดี

2) Resolution หรือความละเอียดภาพ ยิ่งสูงภาพยิ่งคมชัด

3) Frame rate คือจำนวนภาพต่อวินาที

4) Field of View (FOV) คือพื้นที่ที่กล้องสามารถมองเห็นได้

สายสัญญาณที่ใช้ในระบบกล้องโทรทัศน์วงจรปิดมีทั้งสาย coaxial และสาย UTP โดยสาย Coaxial นิยมใช้กับระบบแอนะล็อก ส่วนสาย UTP ใช้กับระบบ IP camera ขั้วต่อที่ใช้ในงาน CCTV ได้แก่

1) BNC connector

2) RJ-45

3) DC connector

การเลือกใช้อุปกรณ์ต้องพิจารณาจากพื้นที่ติดตั้ง ระยะทาง ความละเอียดที่ต้องการ และงบประมาณ เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพ

การติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก

ระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อกเป็นระบบที่ใช้สัญญาณภาพแบบ analog โดยส่งสัญญาณผ่านสาย coaxial ไปยังเครื่อง DVR การติดตั้งระบบประเภทนี้ต้องอาศัยความรู้ด้านการเดินสายไฟและการอ่านแบบติดตั้ง

ขั้นตอนแรกของการติดตั้งคือการอ่านแบบงานติดตั้ง เพื่อกำหนดตำแหน่งของกล้อง มุมมอง และแนวเดินสายให้เหมาะสม ตำแหน่งติดตั้งควรลดจุดอับของภาพและสามารถมองเห็นพื้นที่ได้ครอบคลุม อุปกรณ์ที่ใช้ในการติดตั้งประกอบด้วย

1) กล้องโทรทัศน์วงจรปิด

2) เครื่อง DVR

3) สาย RG59 หรือ RG6

4) Adapter จ่ายไฟ

5) จอภาพ

6) อุปกรณ์ยึดและกล่องพักสาย

ขั้นตอนการติดตั้งประกอบด้วย

1) เตรียมเครื่องมือและอุปกรณ์

2) กำหนดตำแหน่งติดตั้งกล้อง

3) เจาะผนังและติดตั้งกล่องพักสาย

4) เดินสายสัญญาณและสายไฟ

5) ต่อสายเข้ากับ DVR

6) ทดสอบระบบและปรับมุมกล้อง

ข้อดีของระบบแอนะล็อกคือราคาประหยัด ติดตั้งง่าย และเหมาะกับงานขนาดเล็กถึงกลาง แต่มีข้อจำกัดเรื่องความละเอียดและระยะทางของสัญญาณ การติดตั้งที่ถูกต้องจะช่วยลดปัญหาสัญญาณรบกวน ภาพไม่ชัด หรือสายชำรุดจากสภาพอากาศ จึงควรมีการเก็บสายอย่างเป็นระเบียบและใช้ท่อร้อยสายเพื่อป้องกันความเสียหาย

การติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบ IP/Network

ระบบกล้องโทรทัศน์วงจรปิดแบบ IP หรือ network เป็นระบบที่ใช้สัญญาณดิจิทัลผ่านเครือข่ายอินเทอร์เน็ต ทำให้สามารถดูภาพผ่านคอมพิวเตอร์ โทรศัพท์มือถือ หรืออินเทอร์เน็ตได้สะดวก ระบบนี้ประกอบด้วย

1) IP camera

2) NVR (Network Video Recorder)

3) Switch hub

4) Router

5) สายสัญญาณเครือข่าย หรือ fiber optic

ข้อดีของระบบ IP ได้แก่

1) รองรับความละเอียดสูง เช่น full HD และ 4k

2) ดูภาพออนไลน์ได้

3) รองรับระบบ PoE จ่ายไฟผ่านสายสัญญาณเครือข่าย

4) ขยายระบบได้ง่าย

5) รองรับ AI และระบบอัจฉริยะ

ขั้นตอนการติดตั้งเริ่มจากการวางแผนตำแหน่งติดตั้งกล้องและเดินสายสัญญาณเครือข่าย ไปยัง switch หรือ NVR จากนั้นจึงตั้งค่า IP address และเชื่อมต่อระบบเข้ากับเครือข่าย การตั้งค่าเครือข่ายถือเป็นขั้นตอนสำคัญ เช่น

1) การกำหนด IP address

2) การตั้งค่า port

3) การเชื่อมต่ออินเทอร์เน็ต

4) การดูภาพผ่าน Web browser หรือ application

นอกจากนี้ยังมีโปรแกรม CMS สำหรับบริหารจัดการระบบกล้องหลายตัวพร้อมกัน โดยคอมพิวเตอร์ที่ใช้ควรมีประสิทธิภาพเพียงพอทั้งด้าน CPU และ graphic card เพื่อรองรับการประมวลผลภาพจำนวนมาก ระบบ IP เหมาะกับองค์กรหรือพื้นที่ขนาดใหญ่ที่ต้องการความละเอียดสูงและการควบคุมผ่านเครือข่าย

เครื่องบันทึกภาพและระบบจัดเก็บข้อมูล

เครื่องบันทึกภาพเป็นอุปกรณ์สำคัญที่ใช้เก็บข้อมูลภาพจากกล้องโทรทัศน์วงจรปิด โดยแบ่งออกเป็น 2 ประเภทหลัก คือ DVR และ NVR

DVR ใช้กับระบบแอนะล็อก ทำหน้าที่แปลงสัญญาณ analog เป็น digital ก่อนบันทึกลง hard disk ส่วน NVR ใช้กับระบบ IP โดยรับข้อมูลดิจิทัลผ่านเครือข่ายโดยตรง องค์ประกอบของเครื่องบันทึกภาพ ได้แก่

1) ช่องรับสัญญาณภาพ
2) ช่องส่งสัญญาณ HDMI/VGA
3) ระบบบีบอัดภาพ H.264 หรือ H.265
4) Hard disk
5) ช่องเชื่อมต่อเครือข่าย

Hard disk ที่ใช้ในงาน CCTV ควรเป็นชนิด surveillance hard disk ซึ่งออกแบบให้ทำงานตลอด 24 ชั่วโมง และรองรับการเขียนข้อมูลต่อเนื่อง การเลือกขนาดพื้นที่จัดเก็บต้องคำนึงถึง

1) จำนวนกล้อง
2) ความละเอียดของภาพ
3) ระยะเวลาการบันทึก
4) Frame rate

ระบบบันทึกภาพสมัยใหม่ยังสามารถรองรับการดูย้อนหลัง การสำรองข้อมูล และการแจ้งเตือนอัตโนมัติได้อีกด้วย

การแก้ไขปัญหาและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด

ระบบกล้องโทรทัศน์วงจรปิดอาจเกิดปัญหาได้จากการใช้งานเป็นเวลานาน สภาพอากาศ หรืออุปกรณ์เสื่อมสภาพ ดังนั้นจึงจำเป็นต้องมีการตรวจสอบและบำรุงรักษาอย่างสม่ำเสมอ ปัญหาที่พบบ่อย ได้แก่

1) ภาพดับหรือไม่มีภาพ
2) ภาพมีสัญญาณรบกวน
3) ภาพไม่ชัด
4) ระบบบันทึกไม่ทำงาน
5) กล้องไม่สามารถเชื่อมต่อเครือข่ายได้

วิธีการตรวจสอบเบื้องต้น เช่น

1) ตรวจสอบสายไฟและสายสัญญาณ
2) ตรวจสอบ adapter และแหล่งจ่ายไฟ
3) ตรวจสอบพอร์ตเชื่อมต่อ
4) สลับอุปกรณ์เพื่อหาสาเหตุของปัญหา

การบำรุงรักษาควรดำเนินการดังนี้

1) ทำความสะอาดเลนส์กล้อง

2) ตรวจสอบสายสัญญาณ

3) ตรวจสอบพื้นที่จัดเก็บข้อมูล

4) สำรองข้อมูลสำคัญ

5) อัปเดตซอฟต์แวร์และเฟิร์มแวร์

นอกจากนี้ควรติดตั้งอุปกรณ์ป้องกัน เช่น ท่อร้อยสายหรือกล่อง PVC เพื่อป้องกันความร้อน ความชื้น และแสงแดด ซึ่งจะช่วยยืดอายุการใช้งานของระบบ การดูแลรักษาระบบอย่างถูกต้องจะช่วยให้กล้องโทรทัศน์วงจรปิดทำงานได้อย่างมีประสิทธิภาพ ลดความเสียหาย และเพิ่มความปลอดภัยในการใช้งานระยะยาว

แบบฝึกหัดท้ายบทที่ 3
ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

<u>คำชี้แจง</u> จงตอบคำถามโดยเติมคำในช่องว่างให้สมบูรณ์

1. ความปลอดภัย หมายถึง

.....

.....

.....

.....

2. กล้องโทรทัศน์วงจรปิดมีระบบหลัก ๆ 3 ระบบ ประกอบด้วย อะไรบ้าง จงอธิบายมาพอเข้าใจ

.....

.....

.....

.....

3. โปรแกรมบริหารจัดการ หมายถึง

.....

.....

.....

.....

.....

.....

.....

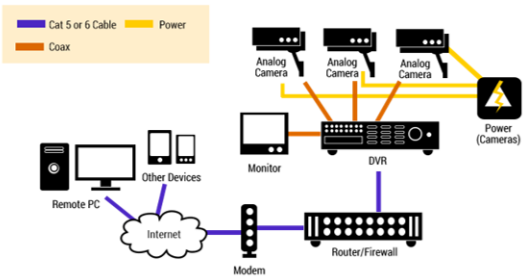
.....

<u>คำชี้แจง</u> จงพิจารณาข้อความต่อไปนี้ และทำเครื่องหมาย √ หน้าข้อความที่ถูก

1. ไม่ควรยิงนกที่เกาะสายไฟฟ้า หรือใช้ไฟฟ้าจับปลา เพราะอาจได้รับอันตรายจากไฟฟ้าดูด

   ☐ ถูก ☐ ผิด

2. จากภาพคือโครงสร้างของระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก



☐ ถูก ☐ ผิด

3. ข้อต่อ C- Mount มีความยาวท้ายเลนส์ ถึงตัวรับภาพ 12.5 มิลลิเมตร

☐ ถูก ☐ ผิด

4. จากรูปเป็น Jack DC ตัวเมีย

☐ ถูก ☐ ผิด

5. ข้อดีของการใช้ซอฟแวร์ CMS

1) โปรแกรมใช้งานง่ายสามารถใช้ดูได้ทั้งวงแลนภายใน และผ่านทางอินเตอร์เน็ต

2) ตัวซอฟแวร์มีค่าใช้จ่ายูง สำหรับเวอร์ชัน Standard

3) สามารถบริหารจัดการกล้องโทรทัศน์วงจรปิดได้ง่ายขึ้น ด้วย E-Map

4) สามารถบันทึกภาพสดกล้องโทรทัศน์วงจรปิดลงในเครื่อง Computer ได้

5) สามารถสามารถปรับคุณสมบัติของวีดีโอได้ เช่น อัตราส่วนภาพ, ความสว่าง หรือความเข้ม รวมถึงการ Control Zoom เข้า-ออก ของกล้อง Speed Dome

☐ ถูก ☐ ผิด

6. ข้อดีของการใช้ Software CMS บนโทรศัพท์มือถือ คือสามารถดูกล้องโทรทัศน์วงจรปิดได้ทุกที่ทุกเวลาโดยไม่จำเป็นต้องใช้อินเตอร์เน็ต

☐ ถูก ☐ ผิด

6. การติดตั้งกล้องแบบดิจิทัล ต้องใช้สายสัญญาณ RG-11

☐ ถูก ☐ ผิด

7. การทดสอบและตรวจสอบระบบจำเป็นสิ่งสำคัญอีกหนึ่งที่ควรทำหลังจากการติดตั้งกล้องโทรทัศน์วงจรปิด

☐ ถูก ☐ ผิด

8. ต่ออุปกรณ์ให้เรียบร้อยและเช็คIPของเครื่องบันทึกภาพเป็นขั้นตอนการตั้งค่าโปรแกรมบริหารเพื่อทดสอบสัญญาณภาพที่ถูกต้อง

☐ ถูก ☐ ผิด

9. สาเหตุของภาพดับหรือไม่เกิดภาพเกิดขึ้นจากสภาพอากาศ

☐ ถูก ☐ ผิด

<u>คำชี้แจง</u> ให้นักเรียนจับคู่ข้อความที่มีความสัมพันธ์กัน โดยนำตัวอักษรมาใส่หน้าข้อที่ถูกต้อง

1. กล้องโทรทัศน์วงจรปิดถูกแบ่งตามเทคโนโลยีออกเป็นกี่ยุค

..... 1.1 Ear Protection — a. หมวกป้องกันศีรษะ

..... 1.2 Eye Protection — b. แว่นนิรภัย

..... 1.3 Head Protection Devices — c. อุปกรณ์ป้องกันหู

..... 1.4 Reflective Clothing — d. เสื้อสะท้อนแสง

2. ระบบกล้องโทรทัศน์วงจรปิด

.....2.1

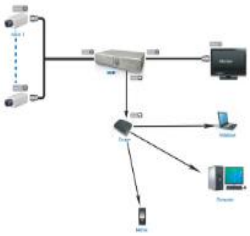
a. เป็นการต่อกล้องโทรทัศน์วงจรปิดไปยังจอเพื่อดูภาพเท่านั้น

..... 2.2

b. เป็นต่อกล้องส่งการบันทึกภาพเก็บเอาไว้ดูในภายหลังผ่านเครื่องวีซีอาร์ (Video Cassette Recorder : VCR) แสดงภาพบนจอมอนิเตอร์

..... 2.3

c. เป็นการบันทึกภาพ และต่อกล้องวงจรปิดมากกว่า 1 ตัว โดยใช้อุปกรณ์รวมสัญญาณเข้ามา

..... 2.4 

d. เป็นต่อกล้องวงจรปิดมากกว่า 1 ตัว ทำการบันทึกภาพด้วยดีวีอาร์ (Digital Video Recorder : DVR) ซึ่งเป็นยุคปัจจุบัน และสามารถเชื่อมต่ออินเทอร์เน็ต

3. เครื่องมือพื้นฐานที่ใช้ในการติดตั้งระบบกล้องโทรทัศน์วงจรปิด

..... 3.1 — a. คีมย้ำหัวแลน

..... 3.2 — b. กรรไกรตัดท่อ

..... 3.3 — c. คีมตัดสายไฟ

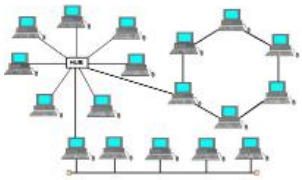
..... 3.4 — d. คีมย้ำหัว BNC

4. ระบบเครือข่ายคอมพิวเตอร์ในงานติดตั้งกล้องโทรทัศน์วงจรปิด

..... 4.1 a. แบบบัส (Bus Topology)

..... 4.2 b. แบบดาว (Star Topology)

..... 4.3 c. แบบวงแหวน (Ring Topology)

..... 4.4  d. แบบผสมผสาน (Hybrid Topology)

5. มาตรฐาน IP

..... 5.1 สามารถป้องกันของแข็งที่มีขนาดไม่เกิน 12 มิลลิเมตร ได้ a. 2

..... 5.2 สามารถป้องกันฝนได้ b. 6

6. สายโคแอคเชียล

.....6.1 ใช้ในการเดินสายกล้องโทรทัศน์วงจรปิดในระยะ 0 - 200 เมตร a. RG-59

..... 6.2 ใช้ในการเดินสายกล้องโทรทัศน์วงจรปิดในระยะ 0 - 700 เมตร b. RG-6

..... 6.3 ใช้ในการเดินสายกล้องโทรทัศน์วงจรปิดในระยะ 700 - 1000 เมตร c. RG-11

7. การติดตั้งระบบกล้องโทรทัศน์วงจรปิด

..... 7.1 กำหนดจุดติดตั้งกล้องโทรทัศน์วงจรปิดบนฝากล่องเก็บสาย a. การตรวจสอบกล้อง CCTV

..... 7.2 ใช้คีมบีบ ย้ำหัวสายให้แน่นเป็น 6 เหลี่ยม b. ขั้นตอนการเข้าหัว

..... 7.3 เก็บสายสัญญาณภาพและสายไฟเลี้ยงกล้องให้เรียบร้อย c. การเชื่อต่อระบบกล้องโทรทัศน์วงจรปิด

..... 7.4 ตรวจดูสัญญาณภาพถ้าภาพสั่นให้ขยับสายสัญญาณ d. การติดตั้งกล้องโทรทัศน์วงจรปิด

8. เรียงลำดับขั้นตอนการติดตั้งโปรแกรม CMS

..... 8.1 a. ขั้นตอนที่ 1

.....8.2 b. ขั้นตอนที่ 2

.....8.3 c. ขั้นตอนที่ 3

..... 8.4 d. ขั้นตอนที่ 4

9. โปรแกรมบริหารจัดการ

..... 9.1 CMS ย่อมาจาก a. สำหรับ DVR 9108

..... 9.2 Software CMS b. สำหรับ TOD AHD 40xxB

..... 9.3 Software CMS Client c. สำหรับ DVR 50xxHV

..... 9.4 Software CMS Client 2.0.0.47 d. Central Management System

10. โปรแกรมบริหารจัดการ

..... 10.1 ตรวจสอบการเชื่อมต่อระบบกล้องโทรทัศน์วงจรปิด a. ทดสอบระบบฮาร์ดแวร์ของกล้องโทรทัศน์วงจรปิด

..... 10.2 การตั้งค่าวันและเวลา

..... 10.3 ตรวจสอบIPของเครื่องบันทึกภาพ b. ทดสอบระบบซอฟแวร์ของกล้อง

..... 10.4 ตั้งค่าโปรแกรมบริหารเพื่อทดสอบสัญญาณภาพ

11. การวิเคราะห์ปัญหาและบำรุงรักษา

.....11.1 a. ภาพดับหรือไม่เกิดภาพ

..... 11.2 b. ภาพเป็นคลื่น

..... 11.3 c. ภาพเบลอ

<u>คำสั่ง</u> จงเลือกคำตอบที่ถูกต้องที่สุดเพียงคำตอบเดียวแล้วทำเครื่องหมาย × ลงในแบบทดสอบ

1. จากรูปเป็นกล้องโทรทัศน์วงจรปิดแบบใด

ก. กล้องโดม

ข. กล้องมาตรฐาน

ค. กล้องสปีดโดม

ง. กล้องแอบซ่อน

2. กล้องณทรทัศน์วงจรปิดใดมีคุณสมบัติสามารถให้ดูภาพเคลื่อนไหวตามวัตถุที่ต้องการ และสามารถซูมดูรายละเอียดต่าง ๆ ได้

ก. กล้องชนิด Dome

ข. กล้องมาตรฐาน

ค. กล้อง PTZ

ง. กล้องสปีดโดม

3. โปรแกรมที่ใช้ในตัวอย่างงานติดตั้งกล้องโทรทัศน์วงจรปิดเขียนแบบ มีชื่อว่าอะไร

ก. โปรแกรม Analog Video System Design Tool version 9.2

ข. โปรแกรม IP Video System Design Tool version 9.2

ค. โปรแกรม IP System Design Tool version 9.2

ง. โปรแกรม IP and Analog Video System Design Tool version 9.2

4. ก่อนที่จะทำการวัดระยะการเดินสายติดตั้งกล้องโทรทัศน์วงจรปิด ควรคำนึงถึงสิ่งใดก่อน

ก. เตรียมอุปกรณ์

ข. เขียนแบบ

ค. ออกแบบ

ง. สำรวจพื้นที่

5. ข้อใดคือกล่าวถึงตรวจสอบสัญญาณภาพจากกล้องโทรทัศน์วงจรปิดที่ถูกต้อง

ก. ดูที่จอว่ามีสัญญาณภาพเข้ามาครบตามจำนวนกล้องที่ได้ติดตั้งไป ถ้าสัญญาณเข้ามาจะปรากฏภาพ

ข. ดูที่จอว่ามีสัญญาณภาพตามจำนวนกล้อง 1 ตัว ถ้าสัญญาณเข้ามาจะไม่ปรากฏภาพ

ค. ที่เครื่องบันทึกว่ามีสัญญาณภาพเข้ามาครบตามจำนวนกล้องที่ได้ติดตั้งไป ถ้าสัญญาณเข้ามาจะปรากฏภาพ

ง. ถูกทุกข้อ

6. ข้อใดเป็นวิธีการตรวจสอบ IP ของเครื่องบันทึกภาพที่ถูกต้อง

ก. ต่ออุปกรณ์ให้เรียบร้อยและเช็คIPของเครื่องบันทึกภาพ ให้ค่าไม่ตรงกัน โดยคลิกขวาเมนูหลักระบบเครือข่าย

ข. ต่ออุปกรณ์ให้เรียบร้อยและเช็คIPของเครื่องบันทึกภาพ ให้ค่าตรงกัน โดยคลิกขวาเมนูหลักระบบเครือข่าย

ค. ต่ออุปกรณ์ให้เรียบร้อยและเช็คIPของจอมอนิเตอร์ ให้ค่าตรงกัน โดยคลิกขวาเมนูหลักระบบเครือข่าย

ง. ถูกทุกข้อ

7. วิธีการแก้ไขภาพดับหรือไม่เกิดภาพเกิดมีวิธีใดบ้าง

ก. ย้ายช่องที่ใช้ต่อกล้องโทรทัศน์วงจรปิดด้านหลังเครื่องบันทึกภาพโดยย้ายพร้อมกับบาลัน

ข. สลับสายแลนหลังเครื่องบันทึกภาพ โดยการนำสายแลนของช่องที่มีปัญหาย้ายไปเสียบกับบาลัน ตัวอื่นของช่องที่มีภาพปกติว่าภาพติดหรือไม่

ค. สลับบาลันด้านที่ติดกล้องโทรทัศน์วงจรปิด โดยการนำบาลันของกล้องโทรทัศน์วงจรปิดที่ภาพติดปกติ ไปลองเปลี่ยน

ง. ถูกทุกข้อ

8. ข้อใดไม่ใช่ขั้นตอนการแก้ไขภาพเบลอ

ก. ปรับเปลี่ยนเลนส์ใหม่

ข. เมื่อทำการปรับโฟกัสของเลนส์แล้ว ก็ใส่ฝาครอบเลนส์กลับคืนไปที่เดิม

ค. ทำการปรับโฟกัสหน้ากล้องโทรทัศน์วงจรปิด โดยการหาจุดที่ชัดที่สุด

ง. ค่อย ๆ หมุนน็อตให้แน่น ถอดฝากระจากด้านหน้าก่อน ค่อยทำการปรับโฟกัสของเลนส์

9. สิ่งที่ผิดปกติของสายที่ต่อเข้ากับตัวกล้องโทรทัศน์วงจรปิดมีอะไรบ้าง

ก. ผิดทุกข้อ

ข. ไม่พบฮาร์ดดิสก์

ค. สายสัญญาณภาพขาดหาย

ง. สายขาดหรือสายเปื่อย

10. การบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด ขอใดถูกต้อง

ก. ทำความสะอาดเลนส์กล้อง และตรวจสอบสายสัญญาณ

ข. ตรวจสอบพื้นที่จัดเก็บข้อมูล และสำรองข้อมูลสำคัญ

ค. อัปเดตซอฟต์แวร์และเฟิร์มแวร์

ง. ถูกทุกข้อ

4 ระบบควบคุมการเข้าออก

41

ความรู้พื้นฐานของระบบควบคุมการเข้าออก

4.1.1 ความหมายของระบบควบคุมการเข้าออก
4.1.2 ความสำคัญของระบบควบคุมการเข้าออก
4.1.3 หลักการทำงานของระบบควบคุมการเข้าออก
4.1.4 องค์ประกอบพื้นฐานของระบบควบคุมการเข้าออก
4.1.5 ความแตกต่างระหว่าง Authentication, Authorization และ Access Control
4.1.6 คุณลักษณะของระบบควบคุมการเข้าออกสมัยใหม่

42

ระบบอาร์เอฟไอดี

4.2.1 ความหมายของ RFID
4.2.2 องค์ประกอบของ RFID
4.2.3 ประเภทของระบบ RFID
4.2.4 มาตรฐาน RFID
4.2.5 หลักการทำงานของระบบ RFID
4.2.6 หลักการทำงานของ RFID มาตรฐาน ISO14443 Type A
4.2.7 โครงสร้างของโมดูล RFID รุ่น RC522

43

เทคโนโลยีการสื่อสารระยะใกล้

4.3.1 ความหมายของระบบ NFC
4.3.2 ความรู้พื้นฐานของเทคโนโลยี NFC
4.3.3 หลักการทำงานของ NFC
4.3.4 โครงสร้างระบบของ NFC
4.3.5 โหมดการทำงานของ NFC
4.3.6 ประเภทของอุปกรณ์ NFC และลักษณะการใช้งาน

44

ระบบล็อกประตูด้วยคิวอาร์โค้ด

4.4.1 หลักการพื้นฐานของ QR Code

4.4.2 สถาปัตยกรรมของระบบ QR Code Door Lock

4.4.3 หลักการทำงานของระบบ QR Code Door Lock

4.4.4 แบบจำลองการตรวจสอบสิทธิ์

4.4.5 กลไกการทำงานของระบบล็อกประตูไฟฟ้า

4.4.6 การบันทึกและติดตามการเข้าออก

4.4.7 ความมั่นคงปลอดภัยของระบบ QR Code Door Lock

บทที่ 4 ระบบควบคุมการเข้าออก

Access Control Systems

4.1 ความรู้พื้นฐานของระบบควบคุมการเข้าออก (Fundamentals of Access Control Systems)

4.1.1 ความหมายของระบบควบคุมการเข้าออก

ระบบควบคุมการเข้าออก (Access Control System: ACS) เป็นระบบที่ใช้กำหนด ตรวจสอบ และควบคุมสิทธิ์ในการเข้าถึงพื้นที่ อาคาร ห้อง หรือทรัพยากรสารสนเทศ โดยอนุญาตให้เฉพาะผู้ที่ได้รับสิทธิ์เท่านั้นสามารถเข้าถึงทรัพยากรได้ตามเงื่อนไขที่กำหนด ขณะที่ผู้ที่ไม่ได้รับอนุญาตจะถูกปฏิเสธการเข้าถึง ทั้งนี้ ระบบควบคุมการเข้าออกถือเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยทั้งด้านกายภาพ (physical security) และด้านสารสนเทศ (information security) เนื่องจากช่วยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ลดความเสี่ยงจากการรั่วไหลของข้อมูล และสนับสนุนการบริหารจัดการสิทธิ์ของผู้ใช้งานอย่างเป็นระบบ (Farhadighalati et al., 2025; Rahul et al et al., 2022) ระบบควบคุมการเข้าออกมีบทบาทสำคัญในการรักษาความลับของข้อมูล (confidentiality) การคงความถูกต้องของข้อมูล (integrity) และการรับรองความพร้อมใช้งานของระบบ (availability) ซึ่งเป็นหลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ (Confidentiality, Integrity, Availability: CIA triad) นอกจากนี้ยังช่วยให้องค์กรสามารถตรวจสอบและติดตามเหตุการณ์การเข้าใช้งานย้อนหลังได้อย่างมีประสิทธิภาพ (Farhadighalati et al., 2025)

4.1.2 ความสำคัญของระบบควบคุมการเข้าออก

ในยุคดิจิทัลที่องค์กรต้องเผชิญกับภัยคุกคามทั้งทางกายภาพและทางไซเบอร์ ระบบควบคุมการเข้าออกได้กลายเป็นโครงสร้างพื้นฐานด้านความปลอดภัยที่สำคัญ เนื่องจากสามารถกำหนดสิทธิ์การเข้าใช้งานตามบุคคล กลุ่มผู้ใช้งาน บทบาท หรือช่วงเวลาได้อย่างยืดหยุ่น อีกทั้งยังสามารถบันทึกข้อมูลการเข้าออก (access log) เพื่อใช้ในการตรวจสอบเหตุการณ์ย้อนหลัง การสืบสวนเหตุการณ์ และการตรวจประเมินด้านความปลอดภัย (audit) ได้อย่างมีประสิทธิภาพ (Mohamed et al., 2022) นอกจากนี้ ระบบควบคุมการเข้าออกยังสามารถเชื่อมโยงกับระบบรักษาความปลอดภัยอื่น เช่น ระบบกล้องวงจรปิด (CCTV) ระบบแจ้งเหตุบุกรุก (intrusion detection system) ระบบแจ้งเหตุเพลิงไหม้ (fire alarm system) ระบบบริหารอาคารอัจฉริยะ (Building Management System: BMS) และระบบ Internet of Things (IoT) เพื่อสร้างระบบรักษาความปลอดภัยแบบบูรณาการ (integrated security system) ที่สามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและแม่นยำ (Farhadighalati et al., 2025)

4.1.3 หลักการทำงานของระบบควบคุมการเข้าออก

หลักการทำงานของระบบควบคุมการเข้าออกเริ่มต้นจากการที่ผู้ใช้งานร้องขอการเข้าถึงทรัพยากรหรือพื้นที่ จากนั้นระบบจะดำเนินการตรวจสอบข้อมูลประจำตัว เปรียบเทียบกับนโยบาย

การเข้าถึง (access policy) และตัดสินใจว่าจะอนุญาตหรือปฏิเสธการเข้าถึง ก่อนส่งคำสั่งไปยังอุปกรณ์ควบคุม เช่น กลอนไฟฟ้า (electric lock) หรือประตูอัตโนมัติ (Mohamed et al., 2022) กระบวนการทำงานของระบบสามารถแบ่งออกเป็น 5 ขั้นตอน ดังนี้

1) ผู้ใช้งานยืนยันตัวตน เช่น บัตร RFID ลายนิ้วมือ ใบหน้า หรือรหัสผ่าน

2) เครื่องอ่านข้อมูล (reader) ส่งข้อมูลไปยังชุดควบคุม (access controller)

3) ชุดควบคุมตรวจสอบข้อมูลกับฐานข้อมูลและนโยบายการเข้าถึง

4) ระบบตัดสินใจอนุญาต (allow) หรือปฏิเสธ (deny)

5) หากได้รับอนุญาต ระบบจะปลดล็อกประตู พร้อมบันทึกข้อมูลการเข้าออกลงในฐานข้อมูล (Atlam et al., 2020)

4.1.4 องค์ประกอบพื้นฐานของระบบควบคุมการเข้าออก

ระบบควบคุมการเข้าออกประกอบด้วยองค์ประกอบพื้นฐาน 5 ส่วน ได้แก่ ผู้ใช้งาน (subject) ทรัพยากร (object) การดำเนินการ (action) สิทธิ์การเข้าถึง (permission) และนโยบายการเข้าถึง (access policy) ซึ่งองค์ประกอบทั้งหมดทำงานร่วมกันเพื่อให้ระบบสามารถตัดสินใจได้อย่างถูกต้องว่าควรอนุญาตหรือปฏิเสธการเข้าถึง (Atlam et al., 2020; Mohamed et al., 2022)

1) ผู้ใช้งาน (Subject)

บุคคล อุปกรณ์ หรือโปรแกรมที่ร้องขอการเข้าถึงทรัพยากร เช่น พนักงาน นักศึกษา ผู้มาติดต่อ หรือผู้ดูแลระบบ ซึ่งเป็นผู้ส่งคำร้องขอเข้าสู่ระบบ (Atlam et al., 2020)

2) ทรัพยากร (Object)

สิ่งที่ต้องการป้องกัน เช่น อาคาร ห้องปฏิบัติการ ห้องเซิร์ฟเวอร์ ตู้ควบคุม ระบบคอมพิวเตอร์ หรือฐานข้อมูล โดยแต่ละทรัพยากรสามารถกำหนดระดับสิทธิ์ที่แตกต่างกันได้ (Farhadighalati et al., 2025)

3) การดำเนินการ (Action)

การกระทำที่ผู้ใช้งานต้องการดำเนินการกับทรัพยากร เช่น การเปิดประตู การอ่านข้อมูล การเขียนข้อมูล หรือการแก้ไขข้อมูล (Mohamed et al., 2022)

4) สิทธิ์การเข้าถึง (Permission)

เป็นสิทธิ์ที่กำหนดให้ผู้ใช้งานสามารถดำเนินการกับทรัพยากรได้ เช่น อนุญาตเฉพาะวันทำงาน อนุญาตเฉพาะเวลา หรืออนุญาตเฉพาะผู้บริหาร (Farhadighalati et al., 2025)

5) นโยบายการเข้าถึง (Access Policy)

ชุดของกฎหรือเงื่อนไขที่ใช้กำหนดว่าใครสามารถเข้าถึงทรัพยากรใด ภายใต้เงื่อนไขใด เช่น เวลา สถานที่ ระดับตำแหน่งงาน หรือสถานะของระบบ ซึ่งถือเป็นหัวใจสำคัญของระบบควบคุมการเข้าออก (Atlam et al., 2020)

รูปที่ 4.1 องค์ประกอบพื้นฐานของระบบควบคุมการเข้าออก

4.1.5 ความแตกต่างระหว่าง Authentication, Authorization และ Access Control

แม้ว่าคำว่า authentication, authorization และ access control มักถูกใช้ร่วมกัน แต่ทั้งสามกระบวนการมีหน้าที่แตกต่างกันอย่างชัดเจน โดย authentication คือ การพิสูจน์ตัวตนของผู้ใช้งาน authorization คือ การตรวจสอบสิทธิ์ของผู้ใช้งานหลังจากยืนยันตัวตนแล้ว และ access control คือ กระบวนการบังคับใช้นโยบายเพื่ออนุญาตหรือปฏิเสธการเข้าถึงทรัพยากรตามสิทธิ์ที่กำหนด (Atlam et al., 2020; Mohamed et al., 2022) กล่าวคือ ระบบจะพิสูจน์ตัวตนของผู้ใช้งานก่อน จากนั้นจึงตรวจสอบสิทธิ์ และสุดท้ายจึงบังคับใช้นโยบายผ่านอุปกรณ์ควบคุม เช่น ชุดควบคุมประตู หรือระบบควบคุมอาคาร เพื่อกำหนดผลการเข้าใช้งานอย่างเหมาะสม (Mohamed et al., 2022) แม้ว่าทั้งสามคำนี้มักถูกใช้ร่วมกัน กล่าวคือ ระบบจะพิสูจน์ตัวตนก่อน (authentication) จากนั้นตรวจสอบสิทธิ์ (authorization) และสุดท้ายบังคับใช้นโยบายการเข้าถึง (access control) ผ่านอุปกรณ์ควบคุมต่าง ๆ

ตารางที่ 4.1 ความหมายแตกต่างระหว่าง Authentication, Authorization และ Access control

กระบวนการ	ความหมาย	ตัวอย่าง
Authentication	การพิสูจน์ตัวตน	สแกนลายนิ้วมือ หรือแตะบัตร RFID
Authorization	การตรวจสอบสิทธิ์	ตรวจสอบว่าผู้ใช้งานมีสิทธิ์เข้าห้องหรือไม่
Access Control	การบังคับใช้นโยบาย	สั่งปลดล็อกหรือปฏิเสธการเปิดประตู

4.1.6 คุณลักษณะของระบบควบคุมการเข้าออกสมัยใหม่

ระบบควบคุมการเข้าออกในปัจจุบันได้รับการพัฒนาให้รองรับการทำงานในสภาพแวดล้อม ที่มีความซับซ้อนและเปลี่ยนแปลงตลอดเวลา ดังนี้

1) สามารถรองรับการพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)
2) การกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control: RBAC)
3) การกำหนดสิทธิ์ตามคุณลักษณะ (Attribute-Based Access Control: ABAC)
4) และการตัดสินใจบนพื้นฐานของบริบท (Context-Aware Access Control)

รวมทั้งสามารถเชื่อมโยงกับระบบคลาวด์ ระบบ IoT และระบบวิเคราะห์ความเสี่ยงแบบเรียลไทม์ได้ (Farhadighalati et al., 2025; Atlam et al., 2020) แนวโน้มของระบบควบคุมการเข้าออกในอนาคตมุ่งเน้นไปที่การประเมินความเสี่ยงแบบพลวัต (risk-based access control) การใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) และการวิเคราะห์พฤติกรรมผู้ใช้งาน (behavior analytics) เพื่อให้การตัดสินใจด้านความปลอดภัยมีความแม่นยำ ยืดหยุ่น และเหมาะสมกับสถานการณ์มากยิ่งขึ้น (Farhadighalati et al., 2025)

4.2 ระบบอาร์เอฟไอดี (Radio Frequency Identification: RFID)

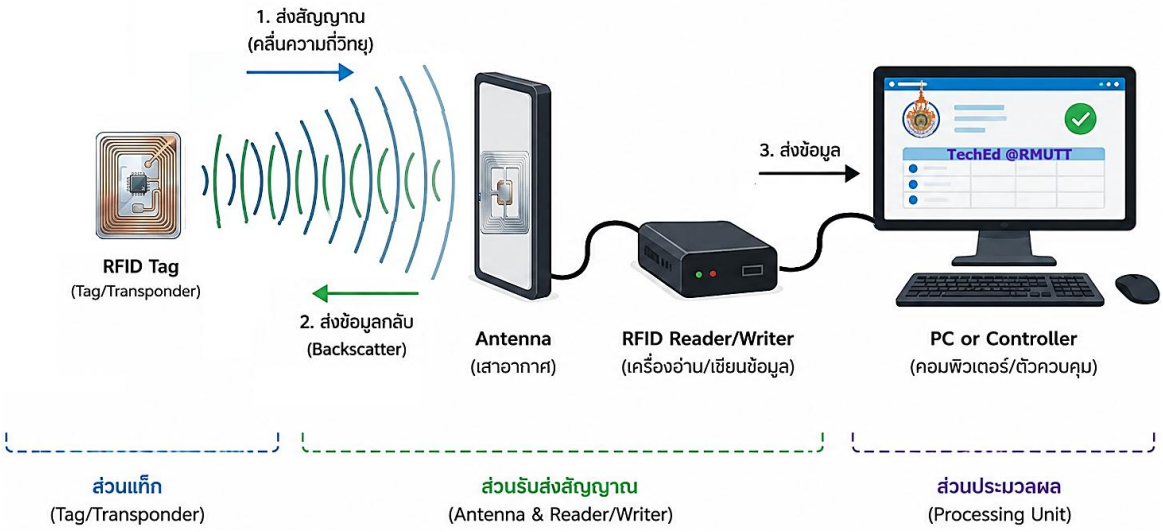
เทคโนโลยี RFID ได้รับการพัฒนามาตั้งแต่ช่วงปี ค.ศ. 1980 โดยมีวัตถุประสงค์หลักเพื่อใช้ทดแทนระบบบาร์โค้ด (barcode) เนื่องจากมีความสามารถในการอ่านข้อมูลได้รวดเร็วและมีประสิทธิภาพมากกว่า ทั้งยังสามารถอ่านข้อมูลจากแท็ก (tag) ได้หลายแท็กพร้อมกัน และสามารถทำงานได้แม้ในสภาพแวดล้อมที่มีข้อจำกัดด้านทัศนวิสัย เช่น บริเวณที่มีฝุ่น ความชื้น หรือแสงสว่างไม่เพียงพอ ข้อมูลของระบบ RFID จะถูกจัดเก็บไว้ภายในไมโครชิป (microchip) ที่ติดตั้งอยู่ภายในแท็ก โดยแท็กจะทำหน้าที่รับและส่งข้อมูลผ่านคลื่นวิทยุไปยังเครื่องอ่านข้อมูล จากนั้นเครื่องอ่านจะส่งข้อมูลต่อไปยังระบบคอมพิวเตอร์เพื่อประมวลผลและนำไปใช้งานต่อไป ปัจจุบัน RFID ถูกนำมาประยุกต์ใช้งานอย่างแพร่หลายในหลายด้าน เช่น ระบบคลังสินค้า ระบบควบคุมการเข้า–ออกอาคาร ระบบเก็บค่าผ่านทางอัตโนมัติ ระบบบัตรจอดรถ ระบบชำระเงินอัตโนมัติ รวมถึงระบบป้องกันการสูญหายของสินค้าในร้านค้า นอกจากนี้ RFID ยังสามารถผลิตในรูปแบบที่มีขนาดเล็กมาก จนสามารถฝังไว้ในบัตร พลาสติก ฉลากสินค้า หรือแม้แต่ใช้ฝังในสัตว์เพื่อบันทึกข้อมูลประจำตัวและประวัติการรักษาได้อีกด้วย

4.2.1 ความหมายของ RFID

RFID ย่อมาจาก Radio Frequency Identification คือ เทคโนโลยีสำหรับการระบุและตรวจสอบข้อมูลของวัตถุ บุคคล หรือสิ่งของต่าง ๆ โดยใช้คลื่นความถี่วิทยุในการรับส่งข้อมูลระหว่างแท็ก (tag) และเครื่องอ่านข้อมูล (reader) ซึ่งสามารถทำงานได้โดยไม่จำเป็นต้องสัมผัสหรือมองเห็นกันโดยตรง

4.2.2 องค์ประกอบของ RFID

สำหรับการอ่านข้อมูลที่ถูกบันทึกไว้บนแท็ก จะต้องนำแท็กซึ่งมีลักษณะเป็นป้ายอิเล็กทรอนิกส์เข้าไปอยู่ใกล้กับเครื่องอ่านข้อมูล โดยไม่จำเป็นต้องอยู่ในแนวสายตาเดียวกันกับเครื่องอ่าน เมื่อเครื่องอ่านสร้างสนามแม่เหล็กไฟฟ้าขึ้น จะทำให้อิเล็กตรอนเคลื่อนที่ผ่านสายอากาศของแท็ก และส่งพลังงานไปยังไมโครชิปภายในแท็ก หลังจากได้รับพลังงานแล้ว ไมโครชิปภายในแท็กจะตอบสนองโดยการส่งข้อมูลที่จัดเก็บไว้กลับไปยังเครื่องอ่านในรูปของสัญญาณวิทยุอีกชุดหนึ่ง กระบวนการนี้เรียกว่า “backscatter” ซึ่งหมายถึงการสะท้อนกลับของคลื่นแม่เหล็กไฟฟ้าหรือคลื่นความถี่วิทยุ (RF wave) จากนั้น เครื่องอ่านจะตรวจจับและแปลผลสัญญาณที่สะท้อนกลับมา ก่อนส่งข้อมูลต่อไปยังคอมพิวเตอร์หรือไมโครคอนโทรลเลอร์เพื่อประมวลผลและใช้งานต่อไป ดังรูปที่ 4.2



รูปที่ 4.2 องค์ประกอบของ RFID

จากรูปที่ 4.2 องค์ประกอบของระบบ RFID ประกอบด้วยองค์ประกอบหลัก 3 ส่วนหลัก ได้แก่ (1) แท็กหรือทรานสปอนเดอร์ (tag/transponder) ติดอยู่กับวัตถุสำหรับใช้ระบุข้อมูล (2) ตัวรับส่งสัญญาณหรือเครื่องอ่านข้อมูล (transceiver) เรียกอีกชื่อหนึ่งว่า interrogator หรือ reader และ (3) ซอฟต์แวร์ตัวกลางเชื่อมโยงระหว่างแอปพลิเคชัน (middleware) มีหน้าที่ส่งคำสั่งรับข้อมูลจากเครื่องอ่านบัตร (Finkenzeller, 2010; ปิยะ โควินท์ทวีวัฒน์ และคณะ, 2551; Duroc, 2022; ทวีศักดิ์ สุขเจริญทรัพย์ และคณะ, 2565) รายละเอียดดังต่อไปนี้

1) แท็ก RFID

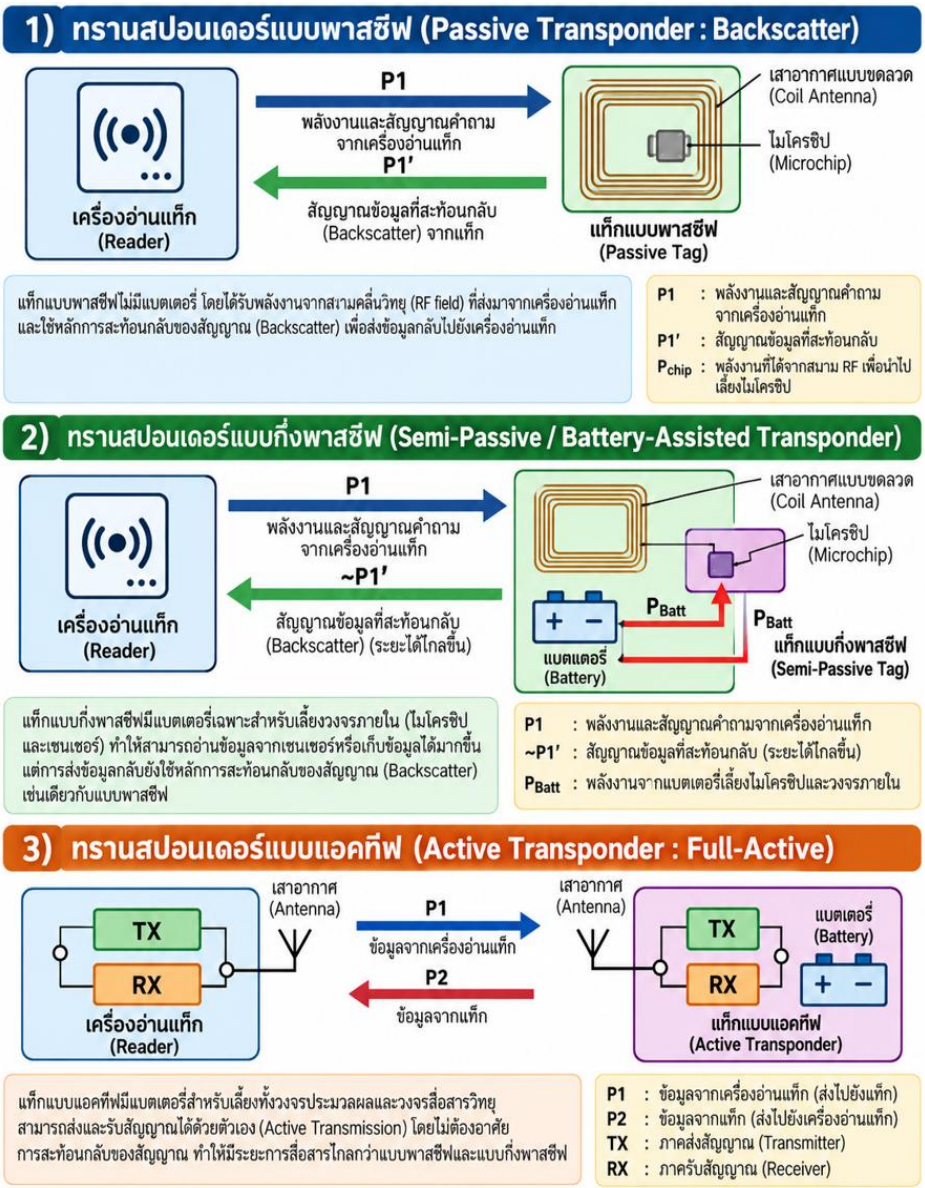
แท็ก RFID ประกอบด้วย สายอากาศ (antenna) สำหรับรับและส่งสัญญาณ และไมโครชิปหรือวงจรรวม (microchip) สำหรับจัดเก็บข้อมูล ประเภทของแท็ก RFID ดังนี้

1.1) Active RFID tag มีแบตเตอรี่ในตัว สามารถส่งสัญญาณได้เองอย่างต่อเนื่อง

1.2) Passive RFID tag ไม่มีแหล่งพลังงานภายใน ต้องอาศัยพลังงานจากคลื่นของเครื่องอ่าน

1.3) Semi-passive RFID tag มีลักษณะคล้าย passive แต่จะส่งสัญญาณเมื่อถูกกระตุ้นโดยเครื่องอ่าน

แท็ก active สามารถอ่านได้ไกลถึงประมาณ 200 m ส่วนแท็ก passive อ่านได้ประมาณ 25 m ราคาของแท็ก RFID แตกต่างกันตามประเภทและคุณสมบัติ โดยทั่วไป passive RFID มีราคาถูกกว่า active RFID หลักการทำงานและความแตกต่างระหว่างแท็ก RFID แบบ passive, active, และ semi-passive โดยเปรียบเทียบแหล่งพลังงาน การส่งสัญญาณ และการสื่อสารข้อมูลระหว่างเครื่องอ่านและแท็ก RFID (Hunt et al., 2007; Finkenzeller, 2010; ปิยะ โควินท์ทวีวัฒน์ และคณะ, 2551; Duroc, 2022)



รูปที่ 4.3 โครงสร้างและหลักการทำงานของแท็ก RFID แบบ passive และ active (ดัดแปลงจาก Finkenzeller, 2010)

สำหรับความถี่ของ RFID ที่ใช้งานในหลายช่วงความถี่ ได้แก่ (1) Low Frequency (LF) ใช้รับ-ส่งสัญญาณระยะใกล้ ราคาถูก (2) High Frequency (HF) อ่านได้เร็วและไกลกว่า LF (3) Ultra High Frequency (UHF) และ (4) Super High Frequency (SHF) ซึ่งระยะการอ่านได้ไกลที่สุดและได้รับความนิยมสูงในงานติดตามสินค้า (Duroc, 2022) หน่วยความจำของแท็ก RFID แท็ก RFID สามารถแบ่งตามลักษณะการใช้งานหน่วยความจำได้ดังนี้ (1) read-only (2) read-write และ (3) Write-Once Read-Many (WORM)

รูปที่ 4.4 แสดงแท็ก RFID ชนิดต่าง ๆ

2) เครื่องอ่าน RFID

สำหรับเครื่องอ่านข้อมูล (reader) ประกอบด้วยโมดูลคลื่นความถี่วิทยุ (radio frequency module) และสายอากาศ (antenna) ซึ่งทำหน้าที่อ่านข้อมูลจากแท็กและส่งข้อมูลไปยังระบบ middleware โดยสามารถเป็นได้ทั้งแบบมือถือ แบบติดตั้งประจำที่ หรือแบบเคลื่อนที่ บางรุ่นยังรองรับระบบป้องกันการชนกันของสัญญาณ (anti-collision) การเข้ารหัส และการยืนยันตัวตน ประเภทของ RFID reader ได้ดังนี้

2.1) แบ่งตามลักษณะการเคลื่อนที่ (Mobility)

2.1.1) แบบพกพา (handheld reader) เน้นความคล่องตัว ใช้ตรวจนับสินค้าหรือสินทรัพย์ได้ทุกที่

2.1.2) แบบติดตั้งประจำที่ (fixed reader) เน้นการทำงานอัตโนมัติ ติดตั้งตามประตูหรือสายพานเพื่ออ่านข้อมูลทันทีที่วัตถุผ่านจุดที่กำหนด

2.2) แบ่งตามรูปแบบการใช้งานพิเศษ

2.2.1) แบบติดยานพาหนะ (vehicle-mounted) ทนทานต่อแรงสั่นสะเทือน ติดตั้งบนรถโฟล์กลิฟต์เพื่ออ่านแท็กขณะขนย้าย

2.2.2) แบบ desktop มีขนาดกะทัดรัด การสื่อสารจะเชื่อมต่อผ่าน USB เพื่อลงทะเบียนหรืออ่านข้อมูลแท็กบนโต๊ะทำงาน

2.3) แบ่งตามคลื่นความถี่ (Frequency)

2.3.1) LF (125/134 kHz) ระยะใกล้มาก ความปลอดภัยสูง เช่น ฝังไมโครชิปสัตว์

2.3.2) HF (13.56 MHz) ระยะใกล้-ระยะกลาง เช่น บัตร smart card หรือการชำระเงิน

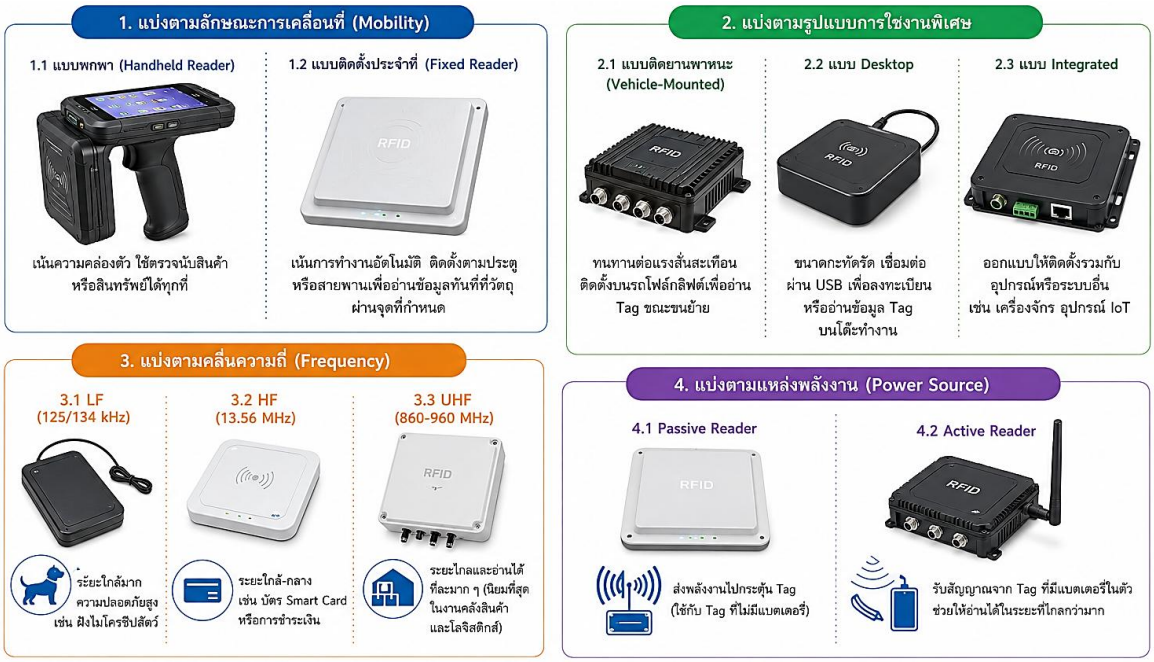
2.3.3) UHF (860-960 MHz) ระยะไกลและอ่านได้ทีละมาก ๆ นิยมที่สุดในงานคลังสินค้าและโลจิสติกส์

2.3.4) SHF (2.45 and 5.8 GHz) เป็นช่วงความถี่ที่ไม่ต้องขอใบอนุญาต ทำให้สามารถใช้ระบบเหล่านี้ได้ทั่วโลก อย่างไรก็ตามแถบความถี่เหล่านี้มีความหนาแน่นและอาจเกิดการรบกวนได้ง่าย

2.4) แบ่งตามแหล่งพลังงาน

2.4.1) Passive reader จะส่งพลังงานไปกระตุ้นแท็ก (ใช้กับแท็กที่ไม่มีแบตเตอรี่)

2.4.2) Active reader ทำการรับสัญญาณจากแท็กที่มีแบตเตอรี่ในตัว ช่วยให้อ่านได้ในระยะที่ไกลกว่ามาก



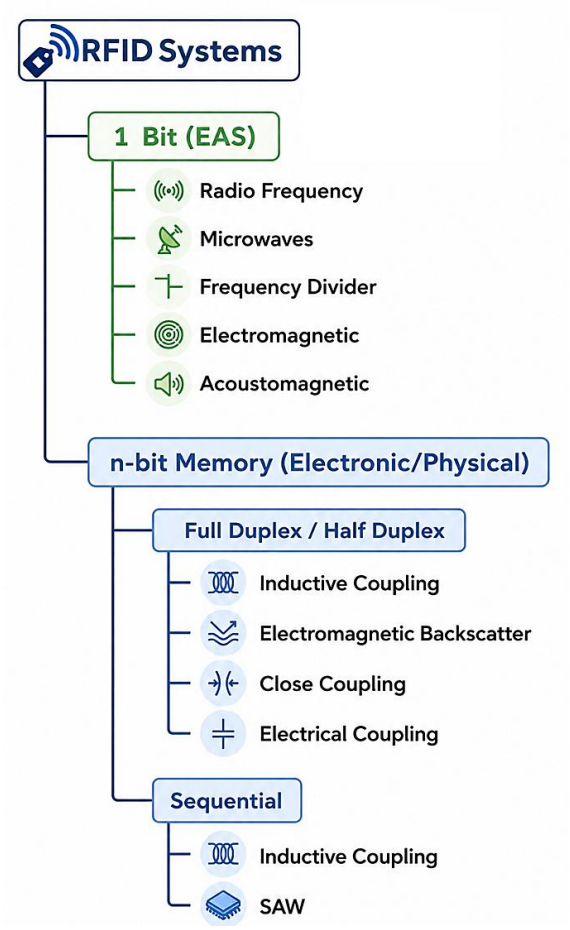
รูปที่ 4.5 แสดงเครื่องอ่าน RFID ประเภทต่าง ๆ

3) ซอฟต์แวร์ตัวกลางเชื่อมโยงระหว่างแอปพลิเคชัน (Middleware)

Middleware เป็นซอฟต์แวร์ตัวกลางที่เชื่อมต่อข้อมูลจากเครื่องอ่าน RFID เข้ากับฐานข้อมูลหรือระบบสารสนเทศ ทำหน้าที่กรอง จัดรูปแบบ และประมวลผลข้อมูล

4.2.3 ประเภทของระบบ RFID (RFID Systems Classification)

ปัจจุบัน RFID ได้รับการพัฒนาให้มีความหลากหลายเพื่อตอบสนองต่อลักษณะงานที่แตกต่างกัน ตั้งแต่ระบบรักษาความปลอดภัยพื้นฐานในร้านค้า ไปจนถึงระบบการจัดการโลจิสติกส์อัจฉริยะและระบบเซนเซอร์ขั้นสูง การจัดจำแนกประเภทของ RFID จึงขึ้นอยู่กับเกณฑ์สำคัญหลายประการ เช่น โครงสร้างการเก็บข้อมูล (จำนวนbit) สถาปัตยกรรมหน่วยความจำ ลักษณะการจับคู่ของคลื่นวิทยุ (coupling) และรูปแบบการรับส่งข้อมูล (transmission)



รูปที่ 4.6 การจำแนกประเภทของระบบ RFID

การจำแนกประเภทของระบบ RFID หากพิจารณาตามโครงสร้างทางสถาปัตยกรรมและเทคโนโลยีทางไฟฟ้า ระบบ RFID สามารถจำแนกประเภทได้อย่างละเอียดตามแผนผังโครงสร้างเทคโนโลยี (Hunt et al., 2007; Finkenzeller, 2010; ปิยะ โควินท์ทวีวัฒน์ และคณะ, 2551) ดังนี้

1) ระบบแบบ 1 bit (1 Bit Systems)

ระบบ 1 bit หรือเรียกว่า Electronic Article Surveillance (EAS) ประเภทนี้ไม่มีหน่วยความจำสำหรับเก็บรหัสสินค้าหรือข้อมูลเฉพาะตัวใด ๆ แท็กจะทำหน้าที่ส่งสัญญาณตอบกลับเพียงแค่ “1” (มี) หรือ “0” (ไม่มี) เท่านั้น นิยมใช้ในระบบ EAS หรือระบบตรวจจับสิ่งของ

สูญหายตามห้างสรรพสินค้าและห้องสมุด โดยแบ่งออกตามเทคโนโลยีสารกึ่งตัวนำและคลื่นความถี่ที่ใช้ดังนี้

1.1) คลื่นความถี่วิทยุ (Radio Frequency)ใช้หลักการเรโซแนนซ์ของวงจร L-C (inductor-capacitor) ที่ความถี่เฉพาะ (มักจะเป็น 8.2 MHz) เมื่อแท็กที่ยังไม่ถูกทำลายสิทธิ์เดินผ่านเครื่องอ่าน ประตูสัญญาณจะแจ้งเตือนทันที

1.2) ไมโครเวฟ (microwaves) ทำงานที่ความถี่สูงมากในย่านกิกะเฮิรตซ์ (GHz) ข้อดีคือตัวแท็กมีขนาดเล็กและตอบสนองได้รวดเร็ว

1.3) ระบบหารความถี่ (frequency divider) แท็กจะรับสัญญาณความถี่หลักจากเครื่องอ่าน แล้วส่งสัญญาณตอบกลับที่มีความถี่ลดลงครึ่งหนึ่ง (f/2) ทำให้เครื่องอ่านแยกแยะสัญญาณรบกวนรอบข้างออกจากสัญญาณแท็กได้อย่างแม่นยำ

1.4) คลื่นแม่เหล็กไฟฟ้า (electromagnetic) ใช้แถบโลหะที่มีค่าความอิ่มตัวทางแม่เหล็กต่ำ (low coercivity) เมื่อผ่านสนามแม่เหล็กสลับของเครื่องอ่าน จะเกิดการเปลี่ยนแปลงของคลื่นแม่เหล็กไฟฟ้าที่ตรวจจับได้

1.5) หลักการคลื่นแม่เหล็กไฟฟ้าและคลื่นเสียงร่วมกัน (acoustomagnetic) ทำงานโดยใช้แถบโลหะสองชนิดที่ตอบสนองต่อสนามแม่เหล็ก เมื่อถูกกระตุ้นด้วยความถี่ที่เหมาะสม แถบโลหะจะเกิดการสั่นสะเทือนเชิงกลและสร้างสนามแม่เหล็กจำเพาะออกมา

2) ระบบหน่วยความจำหลายbit (n-bit Memory Systems)

เป็นระบบ RFID ที่แท็กมีหน่วยความจำ (ทั้งในรูปแบบชิปอิเล็กทรอนิกส์หรือโครงสร้างทางฟิสิกส์) ทำให้สามารถบันทึกรหัสเฉพาะ หรือข้อมูลรายละเอียดของวัตถุนั้น ๆ ได้ ระบบประเภทนี้จะจำแนกตาม กระบวนการรับส่งข้อมูลและวิธีการจ่ายพลังงาน (powering and transmission) เป็นหลัก

2.1) กลุ่ม Full Duplex (FDX) และ Half Duplex (HDX)

เป็นระบบที่มีการแลกเปลี่ยนข้อมูลแบบสองทิศทาง โดย FDX คือเครื่องอ่านและแท็กสามารถส่งข้อมูลสวนทางกันได้ในเวลาเดียวกัน ส่วน HDX คือสลับกันรับและส่ง ซึ่งกลุ่มนี้จะใช้กลไกการจับคู่ทางไฟฟ้าและแม่เหล็ก (coupling) ในรูปแบบต่าง ๆ

2.1.1) การจับคู่เหนี่ยวนำ (inductive coupling) เครื่องอ่านจะสร้างสนามแม่เหล็กไฟฟ้าผ่านขดลวดเสาอากาศ เมื่อแท็กเข้ามาอยู่ในระยะ สนามแม่เหล็กจะเหนี่ยวนำให้เกิดกระแสไฟฟ้าในขดลวดของแท็ก เพื่อเลี้ยงวงจรและส่งข้อมูลกลับด้วยวิธี load modulation ทำงานระยะใกล้ถึงปานกลาง (มักใช้ในย่านความถี่ LF และ HF เช่น บัตรคีย์การ์ด เทคโนโลยีสื่อสารไร้สายระยะสั้น (Near Field Communication: NFC)

2.1.2) การสะท้อนกลับแม่เหล็กไฟฟ้า(electromagnetic backscatter) เครื่องอ่านส่งคลื่นแม่เหล็กไฟฟ้าความถี่สูงออกไปในอากาศ เมื่อกระทบเสาอากาศของแท็ก แท็กจะสะท้อนคลื่นนั้นกลับมาพร้อมกับปรับเปลี่ยนรูปแบบสัญญาณ (modulation) ตามข้อมูลในหน่วยความจำ ทำงานระยะไกล นิยมใช้ในย่านความถี่ UHF เช่น ระบบทางด่วนอัตโนมัติ การจัดการคลังสินค้า

2.1.3) การจับคู่ระยะประชิด (close coupling) ใช้ทั้งสนามแม่เหล็กหรือสนามไฟฟ้าในการเชื่อมต่อ แต่ต้องการให้อยู่ใกล้กันมากๆ ในระดับมิลลิเมตร (แท็กแทบจะต้องแตะหรือเสียบเข้ากับเครื่องอ่าน) มีความปลอดภัยสูงมาก

2.1.4) การจับคู่ทางไฟฟ้า/ความจุไฟฟ้า (electrical coupling) ใช้หลักการของตัวเก็บประจุ (capacitive coupling) โดยแผ่นตัวนำของเครื่องอ่านและแท็กจะสร้างสนามไฟฟ้าต่อกัน เหมาะสำหรับการส่งสัญญาณในระยะที่สั้นมากและแท็กมักมีราคาถูกเนื่องจากพิมพ์ขึ้นรูปง่าย

2.2) กลุ่ม Sequential (SEQ)

ระบบที่ทำงานเป็นลำดับขั้นตอน โดยเครื่องอ่านจะส่งพลังงานผ่านคลื่นวิทยุออกไปช่วงเวลาหนึ่งเพื่อให้แท็กเก็บสะสมพลังงานลงในตัวเก็บประจุ จากนั้นเครื่องอ่านจะ “หยุดส่งคลื่น” เพื่อเปิดช่องสัญญาณให้แท็กส่งข้อมูลกลับมาเพียวๆ ทำให้ลดสัญญาณรบกวนระหว่างการส่งพลังงานและการรับข้อมูลได้อย่างดีเยี่ยม แบ่งออกเป็น

2.2.1) การจับคู่เหนี่ยวนำแบบ (inductive coupling sequential) ทำงานด้วยการเหนี่ยวนำแม่เหล็กไฟฟ้าเหมือนระบบข้างต้น โดยแบ่งเวลา (time slot) ชัดเจนระหว่างช่วง “ชาร์จไฟ” และช่วง “ส่งข้อมูล”

2.2.2) Surface Acoustic Wave (SAW) เป็นระบบ RFID แบบพิเศษที่ไม่ต้องใช้ชิปซิลิคอน (silicon chip) เมื่อแท็กได้รับคลื่นความถี่วิทยุจากเครื่องอ่าน ตัวแปลงสัญญาณบนแท็กจะเปลี่ยนคลื่นวิทยุเป็นคลื่นเสียงเดินทางไปบนผิวของผลึกคริสตัล คลื่นเสียงจะสะท้อนผ่านโครงสร้างฟิสิกส์ที่ถูกสลักรหัสเอาไว้ (reflectors) แล้วเปลี่ยนกลับเป็นคลื่นวิทยุสะท้อนกลับไปหาเครื่องอ่าน ทนทานต่อความร้อนสูง รังสี และสภาพแวดล้อมที่โหดร้ายได้ดีเยี่ยม เนื่องจากไม่มีวงจรอิเล็กทรอนิกส์อยู่ภายใน

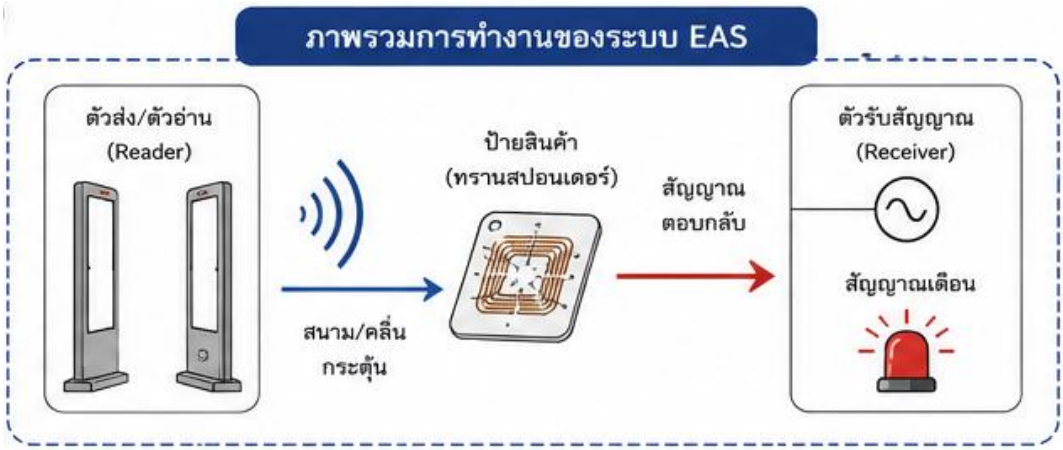
ตารางที่ 4.2 สรุปเปรียบเทียบการใช้งาน RFID แต่ละประเภท

ประเภท RFID	ระยะการอ่านข้อมูล	จุดเด่น	ตัวอย่างการใช้งาน
1 Bit EAS	ใกล้ - ปานกลาง (0.5 - 2 m)	ราคาถูกมาก ตรวจจับเร็ว	ระบบป้องกันขโมยสินค้าในห้างสรรพสินค้า
n-bit (Inductive)	ใกล้ (ไม่เกิน 1 m)	ทำงานได้ดีใกล้ของเหลวและโลหะ	บัตรพนักงาน บัตรโดยสารรถไฟฟ้า แปะชิปสุนัข
n-bit (Backscatter)	ไกล (3 - 10+ m)	อ่านได้พร้อมกันทีละหลายแท็ก ความเร็วสูง	แท็กติดกระจกรถผ่านทางด่วน นับสต็อกสินค้าคงคลัง
n-bit (SAW)	ปานกลาง (1 – 5 m)	ไม่ใช้ชิป ทนความร้อนและสภาวะรุนแรงได้ดี	ติดตามชิ้นงานในไลน์ผลิตที่มีอุณหภูมิสูง อุตสาหกรรมหนัก

การจำแนกระบบ RFID ตามขนาดหน่วยความจำของแท็กและ ความสามารถในการทำงานของระบบ (Finkenzeller, 2010; ปิยะ โควินท์ทวีวัฒน์ และคณะ, 2551) รายละเอียดดังนี้

1) EAS

EAS มีความสามารถต่ำที่สุด ใช้สำหรับระบบป้องกันการขโมยสินค้า โดยทำงานเพียงระดับตรวจจับว่ามีแท็กอยู่หรือไม่ และมีหน่วยความจำน้อยมาก ส่วนเครื่องส่งสัญญาณทดสอบแบบรหัสคงที่ (fixed code transponder) เป็นแท็กที่มีรหัสประจำตัวคงที่ ใช้อ่านข้อมูลได้อย่างเดียว มีหน่วยความจำมากกว่า EAS เล็กน้อย แต่ยังไม่สามารถเขียนข้อมูลใหม่ได้



รูปที่ 4.7 หลักการทำงานของ RFID ชนิด EAS

2) แท็กแบบพาสซีฟ (Passive Transponder)

เป็นกลุ่มที่มีแท็กแบบพาสซีฟ ซึ่งกลุ่มที่มีขนาดใหญ่ที่สุด จะไม่มีแบตเตอรี่ในตัว ใช้พลังงานจากคลื่นวิทยุของเครื่องอ่าน รองรับหลายความถี่ เช่น 135 kHz, 13.56 MHz, 868/915 MHz, และ 2.45 GHz รวมถึงมาตรฐาน ISO 15693, ISO 18000, และ ISO 14223 แท็กกลุ่มนี้มีความสามารถตั้งแต่การอ่าน–เขียนข้อมูล การป้องกันการชนกันของสัญญาณ ไปจนถึงการยืนยันตัวตนและการเข้ารหัสบางรูปแบบ

3) แท็กแบบแอคทีฟ (Active Transponder)

เป็นแท็กที่มีแหล่งพลังงานภายใน เช่น แบตเตอรี่ จึงสามารถส่งสัญญาณได้ไกลกว่าแท็กพาสซีฟ นิยมใช้ในระบบติดตามทรัพย์สิน ยานพาหนะ หรือระบบโลจิสติกส์ ใช้ความถี่ 868/915 MHz, และ 2.45 GHz ตามมาตรฐาน ISO 18000 โดยมีขนาดหน่วยความจำค่อนข้างมากและมีความสามารถสูงกว่าแท็กพื้นฐาน

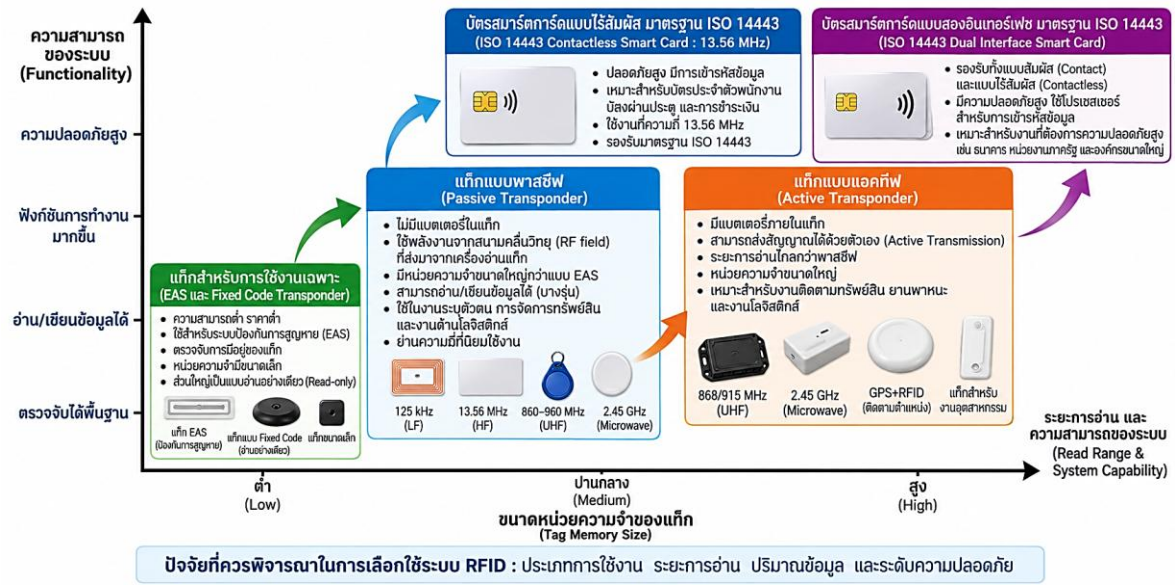
4) กลุ่มมาตรฐาน ISO 14443 (Contactless Smart Card)

เป็นสมาร์ตการ์ดแบบไร้สัมผัสที่ใช้ความถี่ 13.56 MHz มีความสามารถด้านการยืนยันตัวตนและการเข้ารหัสข้อมูล เหมาะสำหรับงานที่ต้องการความปลอดภัย เช่น บัตรประชาชนอิเล็กทรอนิกส์ บัตรพนักงาน บัตรโดยสาร และระบบชำระเงิน

5) มาตรฐาน ISO 14443 (Dual Interface Smart Card)

เป็นกลุ่มที่มีความสามารถสูงที่สุดคือ มาตรฐานISO 14443 เป็นสมาร์ตการ์ดที่รองรับทั้งการทำงานแบบสัมผัสและไร้สัมผัส มีระบบปฏิบัติการของสมาร์ตการ์ด และอาจมีหน่วยประมวลผลเข้ารหัส จึงเหมาะกับงานที่ต้องการความปลอดภัยสูง เช่น ระบบธนาคาร การยืนยันตัวตน และบัตรประจำตัวอิเล็กทรอนิกส์

กล่าวโดยสรุปขนาดหน่วยความจำของแท็ก (memory size) และ ความสามารถในการทำงานของระบบ (functionality) โดยขนาดหน่วยความจำมีหน่วยเป็นไบต์ ตั้งแต่ 1 byte ไปจนถึง 128 kbyte ส่วนระดับความสามารถในการทำงาน เริ่มตั้งแต่การอ่านอย่างเดียว การอ่าน–เขียนข้อมูล การป้องกันการชนกันของสัญญาณ การยืนยันตัวตน การเข้ารหัสข้อมูล ไปจนถึงระบบปฏิบัติการของบัตรสมาร์ตการ์ดและหน่วยประมวลผลเข้ารหัส สามารถแสดง ดังรูปที่ 4.8



รูปที่ 4.8 สรุปประเภทของระบบ RFID

4.2.4 มาตรฐาน RFID

ในช่วงหลายปีที่ผ่านมา ได้มีการพัฒนามาตรฐาน RFID สำหรับความถี่และลักษณะการใช้งานที่แตกต่างกัน โดยมาตรฐานเหล่านี้ครอบคลุมทั้งด้านโปรโตคอลการสื่อสารระหว่างแท็กและเครื่องอ่าน (air interface protocol) รูปแบบการจัดเก็บข้อมูล (data content) การทดสอบความสอดคล้องของอุปกรณ์ตามมาตรฐาน (conformance testing) และรูปแบบการนำไปประยุกต์ใช้งานจริง องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) ได้กำหนดมาตรฐาน RFID สำหรับงานหลายประเภท เช่น ระบบติดตามสัตว์ โดยมาตรฐาน ISO 11784 กำหนดโครงสร้างข้อมูลภายในแท็ก และ ISO 11785 ใช้กำหนดโปรโตคอลการสื่อสารระหว่างแท็กกับเครื่องอ่าน นอกจากนี้ ISO ยังได้กำหนดมาตรฐานสำหรับบัตรสมาร์ตการ์ดแบบไร้สัมผัสและระบบชำระเงินอิเล็กทรอนิกส์ ได้แก่ มาตรฐาน ISO 14443

และมาตรฐานสำหรับบัตรระยะใกล้ (vicinity card) ได้แก่ มาตรฐาน ISO 15693 รวมถึงมาตรฐานสำหรับการทดสอบประสิทธิภาพและความสอดคล้องของอุปกรณ์ RFID เช่น มาตรฐาน ISO 18046 และ มาตรฐาน ISO 18047

การนำ RFID มาใช้ในระบบติดตามสินค้าในห่วงโซ่อุปทานยังถือเป็นเทคโนโลยีที่ค่อนข้างใหม่ ทำให้มาตรฐานหลายส่วนยังอยู่ระหว่างการพัฒนา โดย ISO ได้เสนอแนวทางมาตรฐานสำหรับการติดตามตู้คอนเทนเนอร์ พาเลต หน่วยขนส่ง และสินค้าเฉพาะรายการ ซึ่งอยู่ในกระบวนการพิจารณาอนุมัติ ศูนย์วิจัย Auto-ID Center ซึ่งเป็นผู้พัฒนาเทคโนโลยี Electronic Product Code (EPC) ได้พัฒนาโปรโตคอลการสื่อสารของตนเองสำหรับใช้ในระบบติดตามสินค้าในห่วงโซ่อุปทานระดับโลก โดยมีวัตถุประสงค์เพื่อสร้างระบบ RFID ที่มีต้นทุนต่ำ สามารถใช้งานได้ทั่วโลก และใช้มาตรฐานแบบเปิด (open standards) (Violino, 2005; Zhang, et al., 2019; U.S. Department of Transportation, Federal Highway Administration, 2022) Auto-ID Center ได้ออกแบบระบบให้สามารถทำงานในย่านความถี่สูงพิเศษ (Ultra-High Frequency: UHF) เนื่องจากสามารถอ่านข้อมูลได้ในระยะไกล เหมาะสำหรับการติดตามพาเลตสินค้าและสินค้าในคลังสินค้า โดยมีการพัฒนามาตรฐานแท็ก RFID หลายระดับ ได้แก่

1) มาตรฐานแท็กของ RFID แต่ละระดับ

1.1) Class 1 แท็กแบบพาสซีฟ อ่านข้อมูลได้อย่างเดียว

1.2) Class 2 แท็กแบบพาสซีฟที่สามารถอ่านและเขียนข้อมูลได้

1.3) Class 3 แท็กกึ่งพาสซีฟที่มีแบตเตอรี่ในตัวเพื่อเพิ่มระยะการอ่าน

1.4) Class 4 แท็กแบบแอ็กทีฟที่มีตัวส่งสัญญาณในตัว

1.5) Class 5 แท็กแบบแอ็กทีฟที่สามารถสื่อสารกับแท็กอื่นได้

2) มาตรฐานชุด ISO 18000

ต่อมาได้มีการพัฒนามาตรฐาน EPCglobal Gen 2 หรือ Generation 2 ซึ่งได้รับการอนุมัติในปี ค.ศ. 2004 โดยมีเป้าหมายเพื่อสร้างมาตรฐาน RFID ระดับสากลที่สามารถใช้งานร่วมกันได้ทั่วโลก และมีความสอดคล้องกับมาตรฐาน ISO มากยิ่งขึ้น นอกจากนี้ ISO ยังได้พัฒนามาตรฐานชุด ISO 18000 สำหรับระบบระบุข้อมูลอัตโนมัติและการจัดการสินค้า ซึ่งครอบคลุมโปรโตคอลการสื่อสารในระบบ RFID สำหรับความถี่ต่าง ๆ (Violino, 2005; ISO, 2018) ดังนี้

2.1) ISO 18000-1 เป็นพารามิเตอร์ทั่วไปของระบบ RFID

2.2) ISO 18000-2 ใช้งานความถี่ 135 kHz

2.3) ISO 18000-3 ใช้งานความถี่ 13.56 MHz

2.4) ISO 18000-4 ใช้งานความถี่ 2.45 GHz

2.5) ISO 18000-5 ใช้งานความถี่ 5.8 GHz

2.6) ISO 18000-6 ใช้งานความถี่ 860–930 MHz

2.7) ISO 18000-7 ใช้งานความถี่ 433.92 MHz

4.2.5 หลักการทำงานของระบบ RFID (Operating Principles of RFID)

หลักการสำคัญของระบบ RFID คือการส่งพลังงานและข้อมูลผ่านสนามแม่เหล็กหรือสนามแม่เหล็กไฟฟ้า ซึ่งทำให้แท็กสามารถรับพลังงาน ประมวลผลข้อมูล และตอบกลับมายังเครื่องอ่านได้ หลักการทำงานของ RFID จึงเป็นการผสมผสานองค์ความรู้ด้านคลื่นแม่เหล็กไฟฟ้า การเหนี่ยวนำไฟฟ้า การมอดูเลตสัญญาณ การประมวลผลข้อมูลดิจิทัล และทฤษฎีสายอากาศเข้าไว้ด้วยกัน โดยลักษณะการทำงานจะแตกต่างกันตามชนิดของแท็ก ย่านความถี่ และวิธีการเชื่อมต่อระหว่างแท็กกับเครื่องอ่าน

การเชื่อมต่อระหว่างเครื่องอ่านและแท็ก (coupling methods) เป็นกลไกพื้นฐานที่สำคัญที่สุดของระบบ RFID เนื่องจากเป็นกระบวนการที่ใช้ทั้งในการ ส่งพลังงาน และ แลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ทั้งสอง การเลือกวิธี coupling จะส่งผลโดยตรงต่อระยะอ่าน ความเร็วในการสื่อสาร ความเสถียรของระบบ ต้นทุน และลักษณะการประยุกต์ใช้งาน ระบบ RFID สามารถแบ่งวิธีการเชื่อมต่อหลักได้ 4 รูปแบบ ได้แก่ (1) การเชื่อมต่อแบบเหนี่ยวนำแม่เหล็ก (inductive coupling) (2)การเชื่อมต่อแบบสะท้อนกลับแม่เหล็กไฟฟ้า (electromagnetic backscatter coupling) (3) การเชื่อมต่อระยะประชิด (close coupling) และ (4) การเชื่อมต่อแบบสนามไฟฟ้า (capacitive/electrical coupling)

1) การเชื่อมต่อแบบเหนี่ยวนำแม่เหล็ก (Inductive Coupling)

Inductive coupling เป็นวิธีการเชื่อมต่อที่ใช้แพร่หลายมากที่สุดในระบบ RFID ระยะใกล้ โดยเฉพาะในย่านความถี่ต่ำ (LF) และย่านความถี่สูง (HF) เช่น125–135 kHz และ 13.56 MHz ระบบนี้อาศัยหลักการเหนี่ยวนำแม่เหล็กไฟฟ้าตามกฎของฟาราเดย์ (Faraday's Law of electromagnetic induction) ซึ่งมีลักษณะการทำงานคล้ายหม้อแปลงไฟฟ้า (transformer) ที่ไม่มีแกนเหล็ก

1.1) หลักการทำงานพื้นฐานในระบบการเชื่อมต่อแบบเหนี่ยวนำแม่เหล็ก

เครื่องอ่านจะสร้างกระแสไฟฟ้าสลับความถี่สูงไหลผ่านขดลวดของสายอากาศ ทำให้เกิดสนามแม่เหล็กสลับ (alternating magnetic field) รอบขดลวด เมื่อแท็กเข้าสู่บริเวณสนามแม่เหล็กดังกล่าว สนามแม่เหล็กจะตัดผ่านขดลวดของแท็กและเหนี่ยวนำให้เกิดแรงดันไฟฟ้าขึ้นภายในขดลวด ตามสมการของฟาราเดย์

$$e = -N \frac{d\Phi}{dt} \tag{4.1}$$

โดยที่ e คือ แรงดันไฟฟ้าเหนี่ยวนำ, N คือ จำนวนรอบของขดลวด, และ Φ คือ ฟลักซ์แม่เหล็ก

แรงดันไฟฟ้าที่เหนี่ยวนำได้จะถูกส่งเข้าสู่วงจรเรียงกระแส (rectifier circuit) และวงจรควบคุมแรงดัน (voltage regulator) เพื่อแปลงเป็นไฟฟ้ากระแสตรงสำหรับจ่ายให้กับวงจรภายในแท็ก ดังนั้น ในระบบ passive RFID พลังงานทั้งหมดที่ใช้ในการทำงานของแท็กจึงมาจากสนามแม่เหล็กของเครื่องอ่านโดยตรง หลักการของ inductive coupling ทำงานอยู่ในบริเวณพื้นที่รอบ ๆ สายอากาศ เรียกว่า near field region of antenna ซึ่งเป็นบริเวณใกล้สายอากาศที่พลังงานยังคงอยู่ในรูปสนามแม่เหล็กเป็นหลัก ขอบเขตของ near field of antenna ประมาณ

$$r < \frac{\lambda}{2\pi} \quad (4.2)$$

เมื่อ r คือ ระยะห่างจากสายอากาศ และ λ คือ ความยาวคลื่น

ตัวอย่างเช่น ที่ความถี่ 13.56 MHz จะมีความยาวคลื่นประมาณ 22 m ดังนั้น บริเวณ near field of antenna จะอยู่ประมาณไม่เกิน 3.5 m แต่ในทางปฏิบัติ RFID แบบเหนี่ยวนำแม่เหล็กมักมีระยะอ่านประมาณไม่กี่เซนติเมตรถึงประมาณ 1 m เท่านั้น เนื่องจากประสิทธิภาพการเหนี่ยวนำลดลงอย่างรวดเร็วตามระยะทาง

1.2) โครงสร้างของสายอากาศ

สายอากาศในระบบ Inductive Coupling มักอยู่ในรูปของ loop antenna หรือ coil antenna โดยขดลวดของเครื่องอ่านทำหน้าที่เป็น primary coil และ ขดลวดของแท็กทำหน้าที่เป็น secondary coil การส่งพลังงานจะมีประสิทธิภาพสูงเมื่อ แนวแกนของขดลวดทั้งสองอยู่ในทิศทางเดียวกัน จะมีค่า coupling coefficient สูง และความถี่ของวงจรทั้งสองตรงกัน

1.3) การสั่นพ้องของวงจร (Resonance)

ทั้งเครื่องอ่านและแท็กมักออกแบบให้ขดลวดทำงานร่วมกับตัวเก็บประจุ เพื่อสร้างวงจรเรโซแนนซ์แบบ LC ความถี่เรโซแนนซ์คำนวณได้จาก

$$f_0 = \frac{1}{2\pi\sqrt{LC}} \quad (4.3)$$

เมื่อ L คือ ค่าความเหนี่ยวนำของขดลวด, C คือ ค่าความจุของตัวเก็บประจุ เมื่อวงจรทำงานที่ความถี่เรโซแนนซ์ จะทำให้รับพลังงานได้สูงสุด เพิ่มแรงดันเหนี่ยวนำ เพิ่มระยะอ่าน และลดการสูญเสียพลังงาน

1.4) การส่งข้อมูลกลับจากแท็ก

ในระบบ inductive coupling แท็กจะไม่ส่งคลื่นวิทยุกำลังสูงกลับไปโดยตรง แต่ใช้วิธีที่เรียกว่า load modulation แท็กจะเปลี่ยนโหลดไฟฟ้าภายใน เช่น เปิด–ปิดตัวต้านทานหรือทรานซิสเตอร์ ทำให้กระแสในขดลวดของแท็กเปลี่ยนแปลง ซึ่งจะส่งผลย้อนกลับไปยังขดลวดของเครื่องอ่าน เครื่องอ่านสามารถตรวจจับการเปลี่ยนแปลงของ แรงดัน กระแส หรือ อิมพีแดนซ์ แล้วถอดรหัสกลับเป็นข้อมูลดิจิทัลได้

1.5) คุณลักษณะสำคัญของ inductive coupling

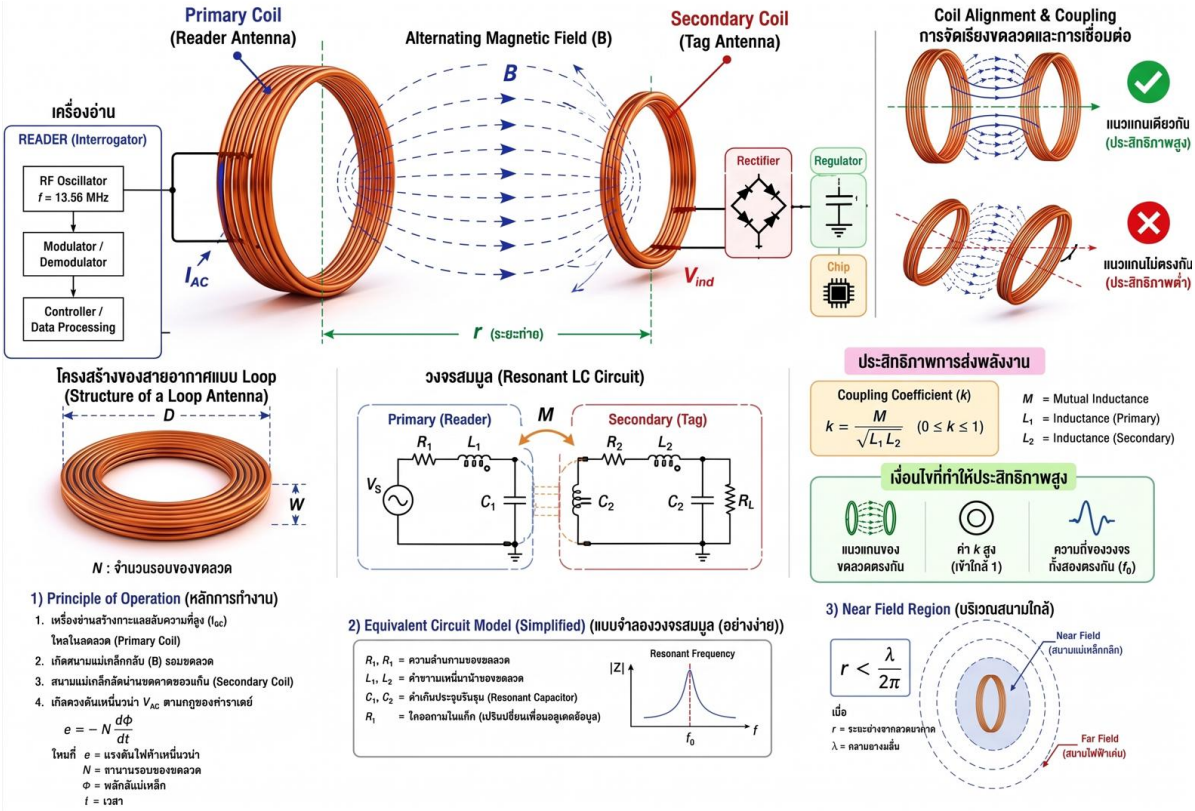
1.5.1) ใช้สนามแม่เหล็กระยะใกล้ (near field) เหมาะสำหรับการสื่อสารระยะใกล้ที่ต้องการความเสถียรสูง

1.5.2) ใช้พลังงานต่ำ เหมาะกับ passive tag ที่ไม่มีแบตเตอรี่

1.5.3) มีความปลอดภัยสูง เนื่องจากระยะอ่านสั้น จึงลดโอกาสการดักฟังข้อมูล

1.5.4) ทนต่อสภาพแวดล้อม ได้รับผลกระทบจากน้ำ ฝุ่น และสิ่งกีดขวางน้อยกว่าระบบ UHF

1.5.5) รองรับการทำงานใกล้โลหะได้ดีกว่า UHF แม้โลหะยังส่งผลต่อสนามแม่เหล็ก แต่ผลกระทบจะน้อยกว่าระบบคลื่นระยะไกล



รูปที่ 4.9 หลักการเชื่อมต่อแบบเหนี่ยวนำแม่เหล็ก

1.6) ข้อจำกัดของระบบ inductive coupling แม้ว่าระบบนี้จะมีความเสถียรสูง แต่ก็มีข้อจำกัดสำคัญ ได้แก่

1.6.1) ระยะอ่านสั้น พลังงานสนามแม่เหล็กจะลดลงอย่างรวดเร็วตามระยะทาง

1.6.2) อัตราการส่งข้อมูลต่ำกว่า UHF เนื่องจากใช้ความถี่ต่ำกว่า

1.6.3) ต้องจัดแนวขดลวดให้เหมาะสม หากแนวของแท็กกับเครื่องอ่านไม่สัมพันธ์กัน ประสิทธิภาพจะลดลง

1.6.4) การอ่านหลายแท็กพร้อมกันทำได้จำกัด เมื่อเทียบกับระบบ UHF RFID

1.7) การประยุกต์ใช้งาน

Inductive coupling ถูกใช้อย่างแพร่หลายในระบบที่ต้องการความปลอดภัย ความเสถียร และระยะอ่านใกล้ เช่น บัตรผ่านเข้า–ออก (access control) สมาร์ตการ์ด (smart card) บัตรโดยสารอัตโนมัติ ระบบ e-payment ระบบ NFC การระบุสัตว์ (animal identification) ระบบห้องสมุด หรือระบบติดตามทรัพย์สินระยะใกล้ ตัวอย่างมาตรฐานที่ใช้ inductive coupling ดังตารางที่ 4.3

ตารางที่ 4.3 ตัวอย่างมาตรฐานที่ใช้ Inductive Coupling

มาตรฐาน	ความถี่	ลักษณะการใช้งาน
ISO 11784/11785	125–134 kHz	ระบุสัตว์
ISO/IEC 14443	13.56 MHz	Smart Card / MIFARE
ISO/IEC 15693	13.56 MHz	Vicinity Card
NFC	13.56 MHz	Near Field Communication

2) การเชื่อมต่อแบบสะท้อนกลับแม่เหล็กไฟฟ้า (Electromagnetic Backscatter Coupling)

Electromagnetic backscatter coupling เป็นวิธีการเชื่อมต่อที่ใช้ในระบบ RFID ระยะไกล โดยเฉพาะในย่านความถี่สูงและไมโครเวฟ เช่น 860–960 MHz (UHF RFID), 2.45 GHz, และ 5.8 GHz (Sami et al., 2025) ระบบนี้แตกต่างจาก inductive coupling อย่างชัดเจน เนื่องจากไม่ได้ใช้สนามแม่เหล็กระยะใกล้ (near field) แต่ใช้การแพร่กระจายของคลื่นแม่เหล็กไฟฟ้าในเขตสนามไกล (far field region) หลักการทำงานของ backscatter coupling คล้ายกับระบบเรดาร์ (radar principle) กล่าวคือ เครื่องอ่านจะส่งคลื่นแม่เหล็กไฟฟ้าออกไปยังแท็ก และแท็กจะสะท้อนคลื่นกลับมายังเครื่องอ่านโดยมีข้อมูลดิจิทัลปะปนอยู่ในสัญญาณสะท้อนนั้น

2.1) หลักการทำงานพื้นฐานของระบบ backscatter RFID

ในระบบ backscatter RFID เครื่องอ่านจะสร้างคลื่นพาหะความถี่สูง (Continuous Wave: CW) และส่งผ่านสายอากาศออกไปยังพื้นที่อ่าน เมื่อแท็กเข้าสู่บริเวณสนามแม่เหล็กไฟฟ้า สายอากาศของแท็กจะรับพลังงานจากคลื่นดังกล่าว และเปลี่ยนพลังงาน RF เป็นไฟฟ้ากระแสตรงผ่านวงจร rectifier เพื่อจ่ายให้กับชิปภายในแท็ก หลังจากแท็กเริ่มทำงานแล้ว แท็กจะไม่สร้างคลื่น RF กำลังสูงส่งกลับไปเอง แต่จะใช้วิธีเปลี่ยนค่าอิมพีแดนซ์ (impedance) ของสายอากาศอย่างรวดเร็ว ทำให้ปริมาณคลื่นที่สะท้อนกลับเปลี่ยนแปลงตามข้อมูลดิจิทัล กระบวนการนี้เรียกว่า modulated backscatter ซึ่งหมายถึง การสะท้อนคลื่นแบบมอดูเลต

2.2) หลักการทางฟิสิกส์ของการสะท้อนคลื่น

คลื่นแม่เหล็กไฟฟ้าตกกระทบสายอากาศของแท็ก จะเกิดพลังงาน 3 ส่วน คือ

$$P_i = P_r + P_a + P_t \tag{4.4}$$

โดยที่ Pi คือ พลังงานตกกระทบ (incident power), Pr คือ พลังงานสะท้อนกลับ (reflected power), Pa คือ พลังงานที่ดูดกลืนโดยแท็ก และ Pt คือ พลังงานสูญเสียอื่น ๆ

หากแท็กเปลี่ยนค่าโหลดที่ปลายสายอากาศ ค่า reflection coefficient จะเปลี่ยนตาม ส่งผลให้ปริมาณคลื่นสะท้อนกลับแตกต่างกัน ดังนั้น เครื่องอ่านจึงสามารถตรวจจับรูปแบบของคลื่นสะท้อน และถอดรหัสข้อมูลได้

2.3) ค่าการสะท้อนของสายอากาศ

ค่าการสะท้อนของสายอากาศ (reflection coefficient) สามารถอธิบายได้ด้วยสมการที่ 4.5

$$\Gamma = \frac{Z_L - Z_A}{Z_L + Z_A} \quad (4.5)$$

เมื่อ Γ คือ Reflection Coefficient, Z_L คือ โหลดของแท็ก, Z_A คือ อิมพีแดนซ์ของสายอากาศ

เมื่อแท็กสลับโหลดระหว่างสองค่า เช่น matched load หรือ mismatched load ค่าการสะท้อนจะเปลี่ยน ทำให้คลื่นสะท้อนกลับมีรูปแบบต่างกัน ซึ่งใช้แทนข้อมูล logic 0 และ logic 1

2.4) เขตสนามไกล (Far Field Region)

Backscatter coupling ทำงานในบริเวณ far field ซึ่งเป็นบริเวณที่สนามไฟฟ้าและสนามแม่เหล็กมีอัตราส่วนคงที่และแพร่กระจายเป็นคลื่นแม่เหล็กไฟฟ้าเต็มรูปแบบ ขอบเขตของ far field ดังสมการที่ 4.2 ตัวอย่างเช่น ที่ความถี่ 915 MHz สามารถคำนวณได้ดังนี้

$$\lambda = \frac{3\times10^8}{915\times10^6}$$
$$\approx 0.328 \text{ m}$$

ดังนั้น Near Field จะอยู่ประมาณ 5 cm และไกลกว่านั้น นั้นจะเป็น far field จึงทำให้ UHF RFID สามารถอ่านได้ไกลหลายเมตร

2.5) โครงสร้างสายอากาศในระบบ backscatter

โครงสร้างสายอากาศในระบบ backscatter ต่างจากระบบ HF ที่ใช้ coil antenna ระบบ UHF และ microwave มักใช้สายอากาศแบบ dipole antenna, folded dipole, patch antenna, และ microstrip antenna เนื่องจากสายอากาศเหล่านี้เหมาะกับการแผ่คลื่นแม่เหล็กไฟฟ้าในเขต far field ขั้นตอนการทำงานของ backscatter RFID

2.5.1) เครื่องอ่านส่งคลื่นพาหะ reader สร้างคลื่น RF อย่างต่อเนื่อง เช่น 915 MHz ผ่านสายอากาศ

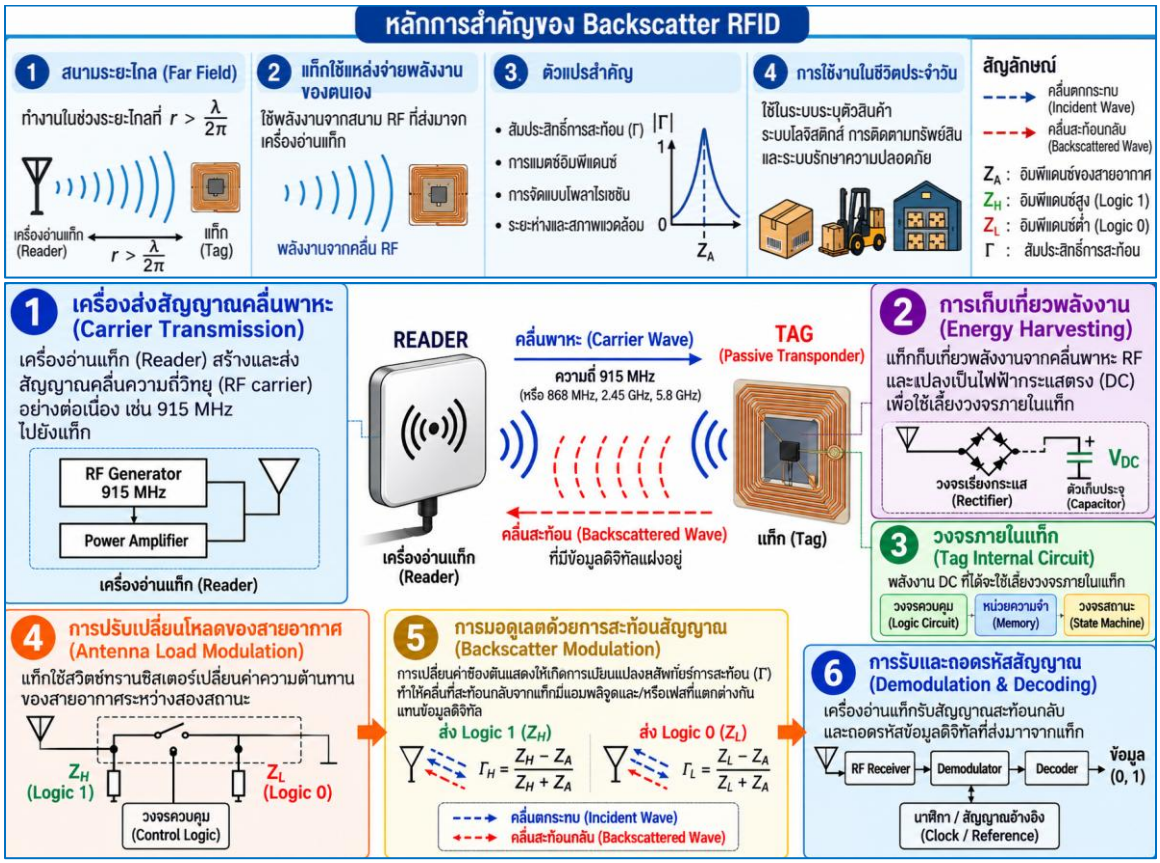
2.5.2) แท็กรับพลังงาน สายอากาศของแท็กรับพลังงาน RF และส่งเข้าสู่วงจร rectifier

2.5.3) วงจรภายในเริ่มทำงาน พลังงาน DC ถูกใช้เลี้ยง logic circuit, memory, และ state machine

2.5.4) แท็กเปลี่ยนโหลดสายอากาศ วงจรภายในจะควบคุม transistor switch เพื่อเปลี่ยนค่าโหลดของสายอากาศ

2.5.5) คลื่นสะท้อนถูกมอดูเลต การเปลี่ยนโหลดทำให้ reflection coefficient เปลี่ยน และคลื่นสะท้อนกลับมีข้อมูลดิจิทัลแฝงอยู่

2.5.6) เครื่องอ่านถอดรหัส reader ตรวจจับสัญญาณสะท้อนกลับ และใช้วงจร demodulator แปลงกลับเป็นข้อมูลดิจิทัล



รูปที่ 4.10 หลักการเชื่อมต่อแบบสะท้อนกลับแม่เหล็กไฟฟ้า

2.6) การมอดูเลตในระบบ RFID (Modulation Techniques in RFID Systems)

ในระบบ RFID แบบ backscatter การส่งข้อมูลจากแท็กกลับไปยังเครื่องอ่านไม่ได้เกิดจากการสร้างคลื่นวิทยุกำลังสูงใหม่เหมือนระบบสื่อสารทั่วไป แต่แท็กจะใช้วิธี “เปลี่ยนคุณสมบัติการสะท้อนของสายอากาศ” เพื่อมอดูเลตคลื่นพาหะ (carrier wave) ที่ส่งมาจากเครื่องอ่าน กระบวนการนี้เรียกว่า backscatter modulation โดยแท็กจะควบคุมการเปลี่ยนแปลงของค่าอิมพีแดนซ์ (impedance) ของสายอากาศ ส่งผลให้ กำลังสะท้อนกลับ ความถี่ของสัญญาณสะท้อน หรือเฟสของคลื่นสะท้อน เปลี่ยนแปลงตามข้อมูลดิจิทัลที่ต้องการส่ง เทคนิคการมอดูเลตที่ใช้ในระบบ backscatter RFID มีหลายรูปแบบ แต่ที่สำคัญที่สุด ได้แก่ Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), และ Phase Shift Keying (PSK)

2.6.1) ASK

ASK เป็นเทคนิคที่นิยมใช้มากที่สุดในระบบ RFID โดยเฉพาะ UHF RFID เนื่องจากวงจรถอดมอดูเลตทำได้ง่ายและใช้พลังงานต่ำ หลักการคือ แท็กจะเปลี่ยนระดับกำลังของคลื่นสะท้อนกลับ โดยเปลี่ยนค่าโหลดของสายอากาศระหว่างสองสถานะ เช่น โหลดแมตช์ (matched load) และ โหลดไม่แมตช์ (mismatched load) มื่อโหลดเปลี่ยน ปริมาณพลังงานที่สะท้อนกลับจะเปลี่ยนตาม ทำให้แอมปลิจูดของคลื่นสะท้อนมีค่าแตกต่างกัน การแทนข้อมูลดิจิทัล ตัวอย่างเช่น logic 1 แทนการมีคลื่น และ logic 0 แทนการไม่มีคลื่น เรียกว่า On-Off Keying (OOK) ลักษณะของสัญญาณ ASK ความถี่ของคลื่นคงที่ เฟสของคลื่นคงที่ เปลี่ยนเฉพาะขนาดหรือแอมปลิจูดเท่านั้น ดังนั้นคลื่น RF จะมีความสูงของคลื่นต่างกันตามข้อมูล ข้อดีของ ASK คือ (1)

วงจรดีมอดูเลตง่าย สามารถใช้ envelope detector ได้ (2) ใช้พลังงานต่ำ เหมาะกับ passive tag (3) ต้นทุนต่ำ โครงสร้างวงจรไม่ซับซ้อน และ (4) นิยมใช้ใน EPC Gen2 RFID ซึ่งเป็นมาตรฐาน UHF RFID หลักในปัจจุบัน ส่วนข้อจำกัดของ ASK ได้แก่ (1) ไวต่อสัญญาณรบกวน โดยเฉพาะ noise ที่มีผลต่อแอมปลิจูด (2) ประสิทธิภาพต่ำกว่าระบบที่ใช้เฟสหรือความถี่ ในสภาพแวดล้อม RF ที่ซับซ้อน

2.6.2) FSK

FSK เป็นเทคนิคที่ใช้การเปลี่ยน "ความถี่" ของคลื่นสะท้อนเพื่อแทนข้อมูลดิจิทัล แท็กจะสร้างการสะท้อนกลับที่มีความถี่ต่างกันสองค่า เช่น f_1 คือ logic 1 และ f_2 คือ logic 0 โดยทั่วไปแท็กจะใช้ Subcarrier Frequency เพื่อสร้างความถี่ทั้งสองค่า หลักการในระบบ backscatter แท็กจะสลับโหลดด้วยความเร็วต่างกัน เช่น โหลดสลับที่ 40 kHz แทน logic 0 และโหลดสลับที่ 80 kHz แทน logic 1 ผลลัพธ์คือคลื่นสะท้อนกลับมี sideband frequency แตกต่างกัน เครื่องอ่านจึงสามารถตรวจจับความถี่ที่เปลี่ยนไปได้ ลักษณะสัญญาณ ใน FSK แอมปลิจูดและเฟสคงที่ เปลี่ยนเฉพาะความถี่ ข้อดี FSK ได้แก่ (1) ทนต่อสัญญาณรบกวนด้านแอมปลิจูดได้ดีเพราะข้อมูลอยู่ในรูปความถี่ (2) มีความเสถียรสูง ในสภาพแวดล้อม RF ที่มี noise และ (3) ตรวจจับข้อมูลได้แม่นยำกว่า ASK ในบางสภาวะ ข้อจำกัด FSK ได้แก่ (1) วงจรถอดมอดูเลตซับซ้อนกว่า ASK (2) ใช้แบนด์วิดท์มากกว่า ASK และ (3) ใช้พลังงานสูงกว่า ASK เล็กน้อย

2.6.3) PSK

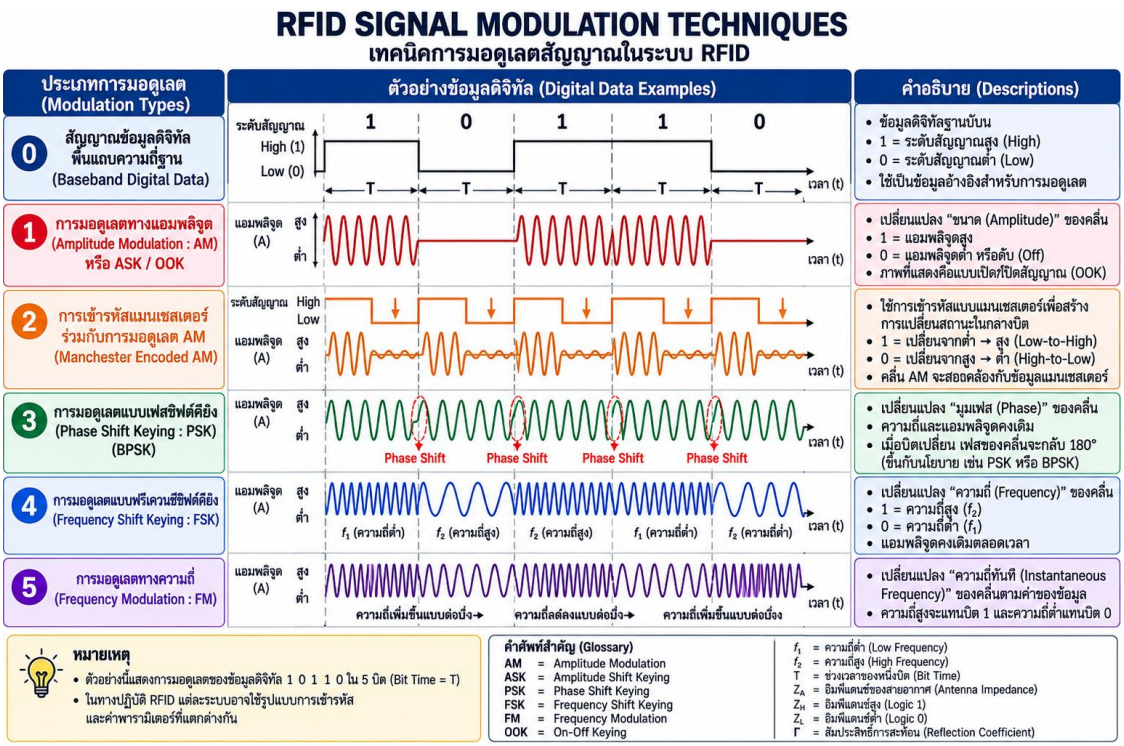
PSK ใช้การเปลี่ยน "เฟส" ของคลื่นสะท้อนเพื่อแทนข้อมูลดิจิทัล แท็กจะเปลี่ยนลักษณะการสะท้อนของสายอากาศ ทำให้เฟสของคลื่นสะท้อนเปลี่ยนไป เช่น 0° แทนlogic 0 และ180° แทน logic 1 นิยมเรียกว่า Binary Phase Shift Keying (BPSK) ลักษณะของสัญญาณใน PSK แอมปลิจูดคงที่ ความถี่คงที่ เปลี่ยนเฉพาะ "เฟส" ข้อดีของ PSK ได้แก่ (1) ทนต่อ Noise สูงมาก โดยเฉพาะสัญญาณรบกวนด้านแอมปลิจูด (2) ประสิทธิภาพการส่งข้อมูลสูง bit error Rate ต่ำกว่า ASK และ (3) ใช้แบนด์วิดท์อย่างมีประสิทธิภาพ ข้อจำกัดของ PSK คือ (1) วงจรซับซ้อนต้องมี phase detector (2) ต้องมีการ synchronization ที่แม่นยำ และ (3) ใช้พลังงานมากกว่า ASK

ตารางที่ 4.4 เปรียบเทียบคุณลักษณะของ ASK, FSK, และ PSK

คุณสมบัติ	ASK	FSK	PSK
สิ่งที่เปลี่ยน	แอมปลิจูด	ความถี่	เฟส
ความซับซ้อน	ต่ำ	ปานกลาง	สูง
การใช้พลังงาน	ต่ำมาก	ปานกลาง	สูงกว่า
ความทน Noise	ต่ำ	ดี	ดีมาก
แบนด์วิดท์	ต่ำ	สูง	ปานกลาง
นิยมใช้	RFID ทั่วไป	บางระบบ	ระบบประสิทธิภาพสูง

การใช้งานของระบบมอดูเลตจริงในระบบ RFID ASK นิยมใช้มากที่สุดใน EPC Gen2 UHF RFID, passive RFID, ระบบต้นทุนต่ำ ส่วน FSK ใช้ในระบบที่ต้องการความทนต่อ

Noise สูง และ PSK ใช้ในระบบ RFID ความเร็วสูงและระบบที่ต้องการ BER ต่ำ กล่าวโดยสรุปการมอดูเลตในระบบ Backscatter RFID เป็นกระบวนการที่แท็กเปลี่ยนคุณสมบัติของคลื่นสะท้อนกลับเพื่อส่งข้อมูลดิจิทัลไปยังเครื่องอ่าน โดยเทคนิคหลักประกอบด้วย ASK, FSK, และ PSK ซึ่งแตกต่างกันที่พารามิเตอร์ของคลื่นที่ถูกเปลี่ยน ได้แก่ แอมปลิจูด ความถี่ และเฟส ตามลำดับ ASK เป็นเทคนิคที่นิยมมากที่สุด เนื่องจากวงจรง่าย ใช้พลังงานต่ำ และเหมาะกับ passive RFID ส่วน FSK และ PSK มีความทนต่อสัญญาณรบกวนสูงกว่า แต่มีความซับซ้อนของวงจรมากขึ้น การเลือกใช้เทคนิคใดขึ้นอยู่กับข้อกำหนดด้านระยะอ่าน ความเร็ว ความน่าเชื่อถือ และต้นทุนของระบบ RFID แต่ละประเภท



รูปที่ 4.11 สรุปเทคนิคการมอดูเลตในระบบ RFID

2.7) การประยุกต์ใช้งาน backscatter RFID

Backscatter RFID ถูกใช้อย่างแพร่หลายในงานที่ต้องการระยะอ่านไกล เช่น ระบบโลจิสติกส์ คลังสินค้าอัตโนมัติ การติดตามพาเลต ระบบติดตามสินค้า ระบบทางด่วนอัตโนมัติ การติดตามยานพาหนะ ระบบ smart warehouse ระบบ supply chain ระบบ management ระบบ IoT และ smart factory

กล่าวโดยสรุป electromagnetic backscatter coupling เป็นหลักการสำคัญของ RFID ระยะไกล โดยใช้การสะท้อนคลื่นแม่เหล็กไฟฟ้าแทนการเหนี่ยวนำแม่เหล็ก แท็กจะเปลี่ยนค่าอิมพีแดนซ์ของสายอากาศเพื่อมอดูเลตคลื่นสะท้อนกลับไปยังเครื่องอ่าน หลักการนี้คล้ายระบบเรดาร์ และเหมาะกับงานที่ต้องการระยะอ่านไกล ความเร็วสูง และการอ่านหลายแท็กพร้อมกัน เช่น โลจิสติกส์ คลังสินค้า และระบบติดตามอัตโนมัติในอุตสาหกรรมสมัยใหม่

3) การเชื่อมต่อระยะประชิด (Close Coupling)

Close coupling เป็นรูปแบบการเชื่อมต่อในระบบ RFID ที่แท็กและเครื่องอ่านต้องอยู่ใกล้กันมาก โดยทั่วไปมีระยะห่างประมาณไม่กี่มิลลิเมตรจนถึงประมาณ 1 cm ระบบนี้ถูกพัฒนาขึ้นเพื่อรองรับการส่งพลังงานในปริมาณสูงและการสื่อสารข้อมูลที่มีความน่าเชื่อถือสูง จึงเหมาะสำหรับงานที่ต้องการความปลอดภัยและความถูกต้องของข้อมูล เช่น สมาร์ตการ์ดทางการเงิน บัตรประจำตัวอิเล็กทรอนิกส์ และระบบควบคุมการเข้า–ออกที่มีความปลอดภัยสูง close coupling ถือเป็นรูปแบบแรก ๆ ของระบบ RFID และเป็นพื้นฐานสำคัญของเทคโนโลยีสมาร์ตการ์ดแบบไร้สัมผัสในยุคเริ่มต้น โดยมาตรฐานที่เกี่ยวข้องคือ ISO IEC 10536 ซึ่งเป็นมาตรฐานสำหรับ close coupling card

3.1) หลักการทำงานพื้นฐาน ระบบ close coupling

ระบบ close coupling อาศัยหลักการเหนี่ยวนำแม่เหล็กไฟฟ้าเช่นเดียวกับ inductive coupling แต่ทำงานในระยะที่ใกล้กว่ามาก ทำให้สามารถส่งพลังงานจากเครื่องอ่านไปยังแท็กได้อย่างมีประสิทธิภาพสูง เครื่องอ่านจะสร้างสนามแม่เหล็กสลับผ่านขดลวดของสายอากาศ เมื่อแท็กถูกนำเข้าใกล้ สนามแม่เหล็กจะตัดผ่านขดลวดของแท็กและเหนี่ยวนำให้เกิดแรงดันไฟฟ้าในวงจรของแท็กตามกฎของฟาราเดย์ ดังสมการ 4.1 แรงดันไฟฟ้าที่เหนี่ยวนำได้จะถูกนำไปเรียงกระแสและควบคุมแรงดัน ใช้เป็นพลังงานให้กับวงจรอิเล็กทรอนิกส์ภายในแท็ก เนื่องจากระยะห่างระหว่างเครื่องอ่านและแท็กมีค่าน้อยมาก ทำให้สนามแม่เหล็กมีความเข้มสูง ค่า coupling coefficient สูงและประสิทธิภาพการส่งพลังงานสูงกว่าระบบ RFID ทั่วไป

3.2) หลักการ near field ใน close coupling

Close coupling ทำงานอยู่ในบริเวณ near field อย่างสมบูรณ์ กล่าวคือพลังงานยังคงอยู่ในรูปสนามแม่เหล็ก ไม่ได้แพร่กระจายเป็นคลื่นแม่เหล็กไฟฟ้าแบบ far field เนื่องจากระยะใช้งานสั้นมาก การสูญเสียพลังงานจึงต่ำ และสามารถส่งกำลังไฟฟ้าให้แท็กได้มากพอสำหรับวงจรที่ใช้พลังงานสูง เช่น microprocessor, cryptographic processor, และ smart card controller จึงเหมาะกับระบบที่มีการประมวลผลข้อมูลภายในแท็กอย่างซับซ้อน

3.3) โครงสร้างของระบบ close coupling

3.3.1) เครื่องอ่าน (reader) ทำหน้าที่สร้างสนามแม่เหล็ก ส่งคำสั่ง รับข้อมูลตอบกลับ จ่ายพลังงานให้แท็ก loop coil antenna สร้างสนามแม่เหล็กเข้มสูงในระยะใกล้

3.3.2) แท็กหรือสมาร์ตการ์ด ภายในประกอบด้วย coil antenna, rectifier, voltage regulator, clock recovery circuit, EEPROM/memory, และ microprocessor ในระบบ close coupling ชิปภายในแท็กอาจมีความสามารถเทียบเท่าคอมพิวเตอร์ขนาดเล็กเหตุผลที่ close coupling ส่งพลังงานได้สูง ประสิทธิภาพการส่งพลังงานขึ้นกับค่า k (Finkenzeller, 2010)

$$k = \frac{M}{\sqrt{L_1 L_2}} \tag{4.6}$$

โดยที่ k คือ coupling coefficient, M คือ mutual inductance, L_1, L_2 คือ ค่าความเหนี่ยวนำของขดลวด

ในระบบ close coupling ระยะห่างต่ำมาก แนวแกนขดลวดสอดคล้องกัน สนามแม่เหล็กเข้มสูง จึงทำให้ค่า k สูงมาก และสามารถส่งพลังงานได้มีประสิทธิภาพ

3.4) ความแตกต่างระหว่าง close coupling และ inductive coupling

แม้ทั้งสองระบบใช้หลักการเหนี่ยวนำแม่เหล็กเหมือนกัน แต่ close coupling มีความแตกต่างสำคัญ ดังตารางที่ 4.5

ตารางที่ 4.5 ความแตกต่างระหว่าง Close Coupling และ Inductive Coupling

คุณสมบัติ	Close Coupling	Inductive Coupling
ระยะอ่าน	0–1 ซม.	หลาย ซม.–1 ม.
กำลังที่ส่งได้	สูง	ปานกลาง
ค่า Coupling	สูงมาก	ปานกลาง
การประมวลผลในแท็ก	ซับซ้อน	ไม่ซับซ้อนมาก
ความปลอดภัย	สูงมาก	สูง
การใช้งาน	smart card	RFID ทั่วไป

3.5) การสื่อสารข้อมูลในระบบ close coupling

การสื่อสารข้อมูลในระบบ close coupling เนื่องจากแท็กอยู่ใกล้เครื่องอ่านมาก สัญญาณตอบกลับจึงมีความแรงสูงและตรวจจับได้ง่าย จะใช้การมอดูเลต ASK และ PSK

3.5.1) จากเครื่องอ่านไปยังแท็กส่วนมากใช้ ASK และ PSK

3.5.2) จากแท็กไปยังเครื่องอ่านใช้ load modulation และ subcarrier modulation

3.6) ความปลอดภัยของระบบ

จุดเด่นสำคัญของ close coupling คือความปลอดภัยสูง เนื่องจาก

3.6.1) ระยะสื่อสารสั้นมาก ทำให้ยากต่อการดักฟังข้อมูล

3.6.2) สนามแม่เหล็กกระจุกตัว สัญญาณไม่กระจายไกล

3.6.3) รองรับระบบเข้ารหัสขั้นสูง เช่น DES, 3DES, AES, และ RSA

3.6.4) รองรับ mutual authentication ทั้งเครื่องอ่านและแท็กสามารถตรวจสอบตัวตนซึ่งกันและกันได้

3.7) ข้อดีและข้อจำกัดของระบบ close coupling

3.7.1) ข้อดีของ close coupling คือ (1) ส่งพลังงานได้สูง รองรับชิปที่ซับซ้อน (2) มีความปลอดภัยสูงมาก เหมาะกับงานทางการเงินและข้อมูลสำคัญ (3) มีความเสถียรสูง ถูกรบกวนจากสภาพแวดล้อมน้อย และ (4) ลดความผิดพลาดในการอ่าน เนื่องจากระยะสั้นและสนามเข้มสูง

3.7.1) ข้อจำกัดของ close coupling ได้แก่ (1) ระยะอ่านสั้นมาก ต้องนำบัตรเข้าใกล้เครื่องอ่านโดยตรง (2) ไม่เหมาะกับงานโลจิสติกส์ เพราะไม่รองรับการอ่านระยะไกล และ (3) ความเร็วในการใช้งานขึ้นกับตำแหน่งต้องจัดตำแหน่งแท็กให้เหมาะสม

3.8) การประยุกต์ใช้งาน

Close coupling นิยมใช้ในงานที่ต้องการความปลอดภัยสูง เช่น บัตรธนาคารสมาร์ตการ์ด บัตรประชาชนอิเล็กทรอนิกส์ SIM card ระบบ access control ระบบชำระเงิน

อิเล็กทรอนิกส์ และ secure authentication system ตัวอย่างมาตรฐานที่เกี่ยวข้อง close coupling card (มาตรฐาน ISO/IEC 10536), smart card (มาตรฐาน ISO/IEC 7816) และ banking smart card (มาตรฐาน Europay, MasterCard, and Visa: EMV)

กล่าวโดยสรุป close coupling เป็นระบบ RFID ระยะใกล้มากที่ใช้หลักการเหนี่ยวนำแม่เหล็กไฟฟ้าในการส่งพลังงานและข้อมูลระหว่างเครื่องอ่านกับแท็ก จุดเด่นสำคัญคือสามารถส่งพลังงานได้สูง เนื่องจากแท็กอยู่ใกล้เครื่องอ่านมาก ทำให้ค่า coupling coefficient สูงและมีการสูญเสียพลังงานต่ำ ระบบนี้จึงเหมาะสำหรับสมาร์ตการ์ดและงานที่ต้องการความปลอดภัยสูง รวมถึงรองรับการประมวลผลข้อมูลที่ซับซ้อนภายในแท็กได้ดีกว่าระบบ RFID ทั่วไป

4) การเชื่อมต่อแบบสนามไฟฟ้า (Electrical Coupling หรือ Capacitive Coupling)

Electrical coupling หรือ capacitive coupling เป็นวิธีการเชื่อมต่อในระบบ RFID ที่ใช้สนามไฟฟ้า (electric field) ในการส่งพลังงานและข้อมูลระหว่างเครื่องอ่าน (reader) และแท็ก (tag/transponder) แทนการใช้สนามแม่เหล็กเหมือนระบบ inductive coupling หลักการทำงานของระบบนี้อาศัยคุณสมบัติของตัวเก็บประจุ (capacitor) โดยเครื่องอ่านและแท็กจะทำหน้าที่เสมือน “แผ่นตัวนำสองแผ่น” ของตัวเก็บประจุ เมื่อทั้งสองอยู่ใกล้กัน จะเกิดสนามไฟฟ้าระหว่างกันและสามารถส่งผ่านพลังงานหรือข้อมูลได้ ระบบ capacitive coupling มักใช้กับระบบ RFID ระยะใกล้มาก (very short range RFID) และพบได้ในระบบ close coupling บางประเภท โดยเฉพาะระบบสมาร์ตการ์ดยุคแรกและระบบที่ต้องการการเชื่อมต่อระยะประชิด

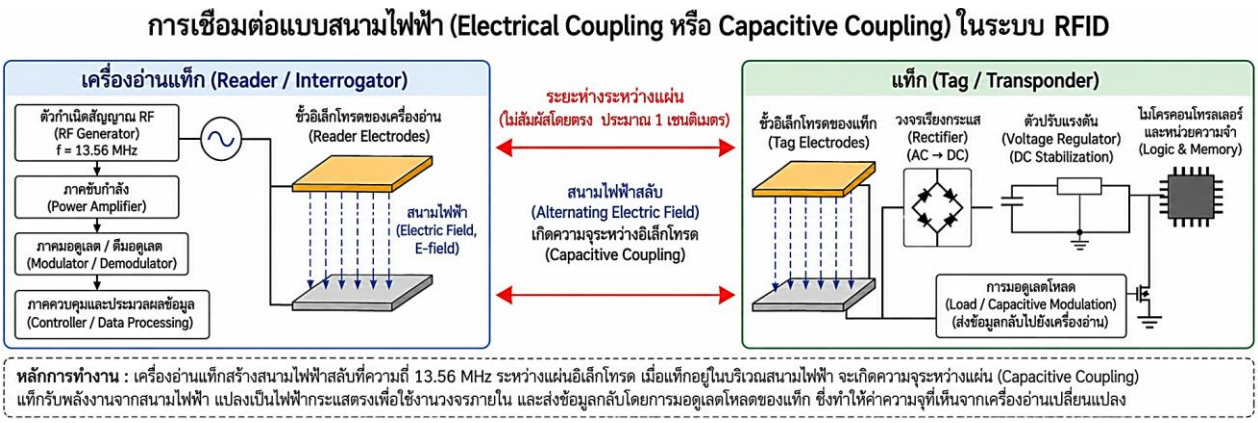
4.1) หลักการพื้นฐานของ capacitive coupling

ในระบบนี้เครื่องอ่านจะสร้างสนามไฟฟ้าสลับความถี่สูงระหว่างอิเล็กโทรด (electrode plates) หรือแผ่นตัวนำ เมื่อแท็กถูกนำเข้าใกล้ จะเกิดการเชื่อมต่อแบบ capacitive ระหว่างเครื่องอ่านและแท็ก ทำให้เกิดกระแสไฟฟ้ากระแสสลับขนาดเล็กไหลผ่านความจุไฟฟ้าที่เกิดขึ้นระหว่างกัน หลักการนี้สามารถอธิบายได้ด้วยสมการพื้นฐานของตัวเก็บประจุ

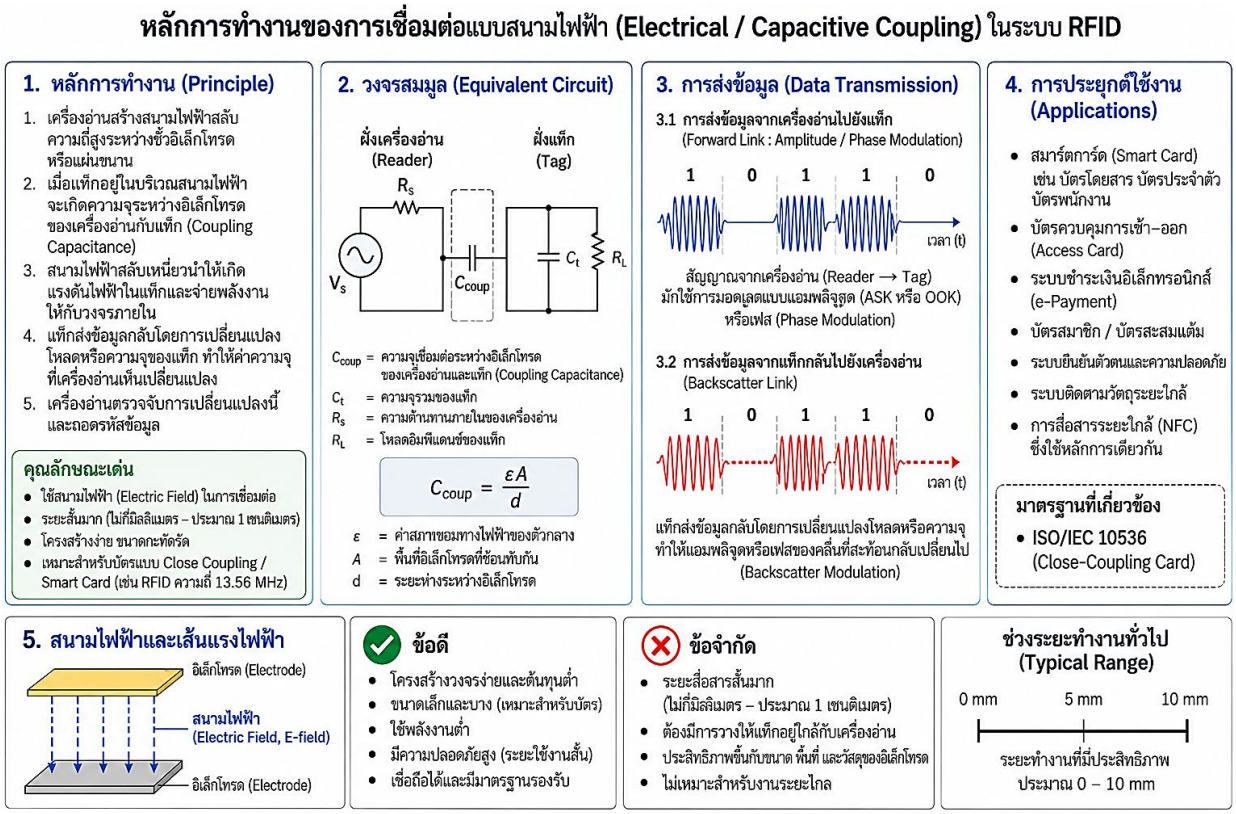
$$C = \frac{\varepsilon A}{d} \tag{4.7}$$

โดยที่ C คือ ค่าความจุไฟฟ้า (capacitance), ε คือ ค่าคงที่ไดอิเล็กทริกของตัวกลาง, A คือ พื้นที่ของแผ่นตัวนำ, และ d คือ ระยะห่างระหว่างแผ่นตัวนำ

จากสมการจะเห็นว่า หากระยะห่าง d ลดลง ทำให้ ค่า capacitance เพิ่มขึ้น หากพื้นที่อิเล็กโทรดมากขึ้น การเชื่อมต่อมีประสิทธิภาพสูงขึ้น ดังนั้น capacitive coupling จึงต้องทำงานในระยะใกล้มาก



(ก) หลักการเชื่อมต่อแบบสนามไฟฟ้า



(ข) หลักการทำงานของการเชื่อมต่อแบบสนามไฟฟ้า

รูปที่ 4.12 การเชื่อมต่อแบบสนามไฟฟ้า

4.2) หลักการสร้างสนามไฟฟ้า

ในระบบ capacitive coupling เครื่องอ่านจะสร้างแรงดันไฟฟ้าสลับความถี่สูงระหว่างอิเล็กโทรด ทำให้เกิดสนามไฟฟ้าสลับ เมื่อแท็กเข้าสู่บริเวณสนาม ทำให้ ประจุไฟฟ้าจะถูกเหนี่ยวนำบนอิเล็กโทรดของแท็ก จากนั้นเกิดกระแสไฟฟ้ากระแสสลับขนาดเล็ก ทำให้วงจร rectifier ภายในแท็กจะแปลงพลังงานดังกล่าวเป็นไฟ DC จากนั้นวงจรภายในแท็กจึงเริ่มทำงาน

4.3) โครงสร้างของระบบ capacitive coupling ระบบโดยทั่วไปประกอบด้วย

4.3.1) เครื่องอ่าน ประกอบด้วย RF oscillator, driver circuit, electrode plates, modulator/demodulator เครื่องอ่านจะสร้างสนามไฟฟ้าสลับระหว่างแผ่นอิเล็กโทรด

4.3.2) แท็ก จะประกอบด้วย electrode pads, rectifier circuit, voltage regulator, logic circuit, และ memory โดย เมื่อแท็กเข้าใกล้ reader เกิดการ coupling ทางไฟฟ้า

4.4) ลักษณะของสนามไฟฟ้า

ระบบ capacitive coupling ใช้ electric near field ซึ่งต่างจากระบบ inductive coupling ที่ใช้ magnetic near field ในบริเวณ near field พลังงานจะยังไม่แพร่กระจายเป็นคลื่นแม่เหล็กไฟฟ้าเต็มรูปแบบ แต่จะเก็บอยู่ในรูปสนามไฟฟ้าระหว่างอิเล็กโทรด การส่งพลังงานโดยกระแสไฟฟ้าที่เกิดขึ้นในแท็กสามารถคำนวณได้จากสมการของตัวเก็บประจุ

$$I = C\frac{dV}{dt} \tag{4.8}$$

โดยที่ I คือ กระแสไฟฟ้า, C คือ Capacitance, และ V คือ แรงดันไฟฟ้า

เมื่อแรงดันสลับเปลี่ยนแปลงอย่างรวดเร็ว จะเกิดกระแส AC ไหลผ่าน capacitive coupling พลังงานนี้จะถูกเรียงกระแสและใช้เลี้ยงวงจรภายในแท็ก

4.5) การส่งข้อมูลในระบบ capacitive coupling

การรับส่งข้อมูลสามารถทำได้หลายวิธี เช่น

4.5.1) Amplitude Modulation (AM) เปลี่ยนแอมปลิจูดของสนามไฟฟ้าเพื่อแทนข้อมูล

4.5.2) Load modulation แท็กเปลี่ยนโหลดภายใน ทำให้สนามไฟฟ้าของเครื่องอ่านเปลี่ยนแปลง

4.5.3) Capacitive load switching แท็กสลับค่าความจุไฟฟ้าภายใน เพื่อมอดูเลตข้อมูลกลับไปยังเครื่องอ่าน

4.6) คุณลักษณะสำคัญของ capacitive coupling

4.6.1) ใช้สนามไฟฟ้าแทนสนามแม่เหล็ก จึงต่างจาก RFID ทั่วไปที่ใช้ coil antenna

4.6.2) ระยะสื่อสารสั้นมาก โดยทั่วไปไม่เกิน 1 cm

4.6.3) ใช้โครงสร้างง่าย สามารถสร้างอิเล็กโทรดบน PCB หรือฟิล์มบางได้

4.6.4) ส่งพลังงานได้จำกัด เนื่องจากค่า capacitance มีขนาดเล็ก

4.6.5) ต้องการการจัดตำแหน่งที่แม่นยำ ระยะและแนวของอิเล็กโทรดส่งผลต่อประสิทธิภาพอย่างมาก

4.7) ข้อดีและข้อจำกัดของ capacitive coupling

4.7.1) ข้อดีของ capacitive coupling ได้แก่ (1) โครงสร้างแท็กบางและเรียบง่าย เหมาะกับ smart label และ smart card (2) ผลกระทบจากโลหะบางกรณีน้อยกว่า magnetic coupling เพราะใช้สนามไฟฟ้า (3) ความปลอดภัยสูง เนื่องจากระยะอ่านสั้นมาก และ (4) ใช้พลังงานต่ำ เหมาะกับวงจรขนาดเล็ก

4.7.2) ข้อจำกัดของ capacitive coupling ได้แก่ (1) ระยะอ่านสั้นมากเป็นข้อจำกัดหลักของระบบนี้ (2) ส่งพลังงานได้ต่ำ ไม่เหมาะกับชิปที่ใช้พลังงานสูง (3) ไวต่อความชื้นและสภาพแวดล้อม เพราะค่าคงที่ไดอิเล็กทริกของตัวกลางเปลี่ยนแปลงได้ และ (4) ประสิทธิภาพลดลงเมื่ออิเล็กโทรดไม่ตรงแนว ต้องควบคุมตำแหน่งอย่างแม่นยำ

4.8) การประยุกต์ใช้งาน

Capacitive coupling ถูกใช้งานในระบบที่ต้องการระยะใกล้มาก เช่น สมาร์ตการ์ดยุคแรก ระบบ close coupling card ระบบยืนยันตัวตนระยะประชิด smart label บางประเภท และระบบ secure identification ซึ่งระบบ capacitive coupling มีความเกี่ยวข้องกับมาตรฐาน ISO/IEC 10536 ซึ่งรองรับทั้ง capacitive coupling และ inductive coupling สำหรับ close coupling card

สรุปได้ว่า capacitive coupling เป็นเทคนิคการเชื่อมต่อในระบบ RFID ที่ใช้สนามไฟฟ้าในการส่งพลังงานและข้อมูลระหว่างเครื่องอ่านและแท็ก โดยทำงานในลักษณะคล้ายตัวเก็บประจุไฟฟ้า ระบบนี้เหมาะกับการสื่อสารระยะใกล้มากและงานที่ต้องการความปลอดภัยสูง แม้จะมีข้อจำกัดด้านระยะอ่านและกำลังส่งพลังงาน แต่มีจุดเด่นด้านโครงสร้างเรียบง่าย ขนาดเล็ก และเหมาะกับระบบสมาร์ตการ์ดหรืออุปกรณ์อิเล็กทรอนิกส์แบบบางในงานเฉพาะทาง

ตารางที่ 4.6 สรุปความแตกต่างระหว่าง Capacitive Coupling และ Inductive Coupling

คุณสมบัติ	Capacitive Coupling	Inductive Coupling
ลักษณะของสนามที่แพร่กระจาย	Electric field	Magnetic field
องค์ประกอบหลัก	Electrode	Coil
หลักการ	Capacitor	Transformer
ระยะอ่าน	สั้นมาก	สั้น–ปานกลาง
การส่งพลังงาน	ต่ำ	สูงกว่า
ความไวต่อแนววาง	สูง	ปานกลาง
การใช้งาน	Close coupling	HF/LF RFID

4.2.6 หลักการทำงานของ RFID มาตรฐาน ISO14443 Type A

มาตรฐานสำหรับสมาร์ตการ์ดแบบไร้สัมผัส (contactless smart card) ที่รองรับการอ่านและเขียนข้อมูล พร้อมทั้งมีระบบรักษาความปลอดภัยสูง นิยมใช้ในงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและการยืนยันตัวตน เช่น บัตรประชาชนอิเล็กทรอนิกส์ บัตรพนักงาน ระบบชำระเงินอิเล็กทรอนิกส์ และระบบ e-purchasing มาตรฐาน ISO/IEC 14443 สามารถแบ่งออกเป็น 2 ประเภทหลัก ได้แก่ type A และ B โดยมาตรฐาน type A ถูกนำมาใช้ในเทคโนโลยี MIFARE ของบริษัท NXP Semiconductors ซึ่งได้รับความนิยมอย่างแพร่หลายในระบบควบคุมการเข้า–ออก ขนส่งมวลชน และสมาร์ตการ์ดต่าง ๆ เนื่องจากสามารถในการรับส่งข้อมูลได้รวดเร็ว และรองรับระบบรักษาความปลอดภัยของข้อมูลได้อย่างมีประสิทธิภาพ ได้รับความนิยมในท้องตลาด ใช้ความถี่ 13.56 MHz ระยะรับส่งข้อมูลประมาณ 10 cm

1) ข้อดีและข้อจำจัดของ มาตรฐาน MIFARE

1.1) ข้อดีของมาตรฐาน MIFARE

1.1.1) สามารถนำไปใช้ในงานที่หลากหลาย

1.1.2) มีการเข้ารหัสในการเข้าถึงข้อมูลบนบัตร ทำให้ยากที่จะเข้าถึงและคัดลอกข้อมูล

1.1.3) ชิป MIFARE ยังสามารถนำไปใช้บนอุปกรณ์อื่น เช่น นาฬิกา

1.1.4) บัตร MIFARE ไม่ต้องสอดเข้าไปที่เครื่องอ่านบัตร เมื่อบัตรอยู่ในระยะของเครื่องอ่าน เครื่องก็สามารถส่งคำสั่งไปที่บัตรได้

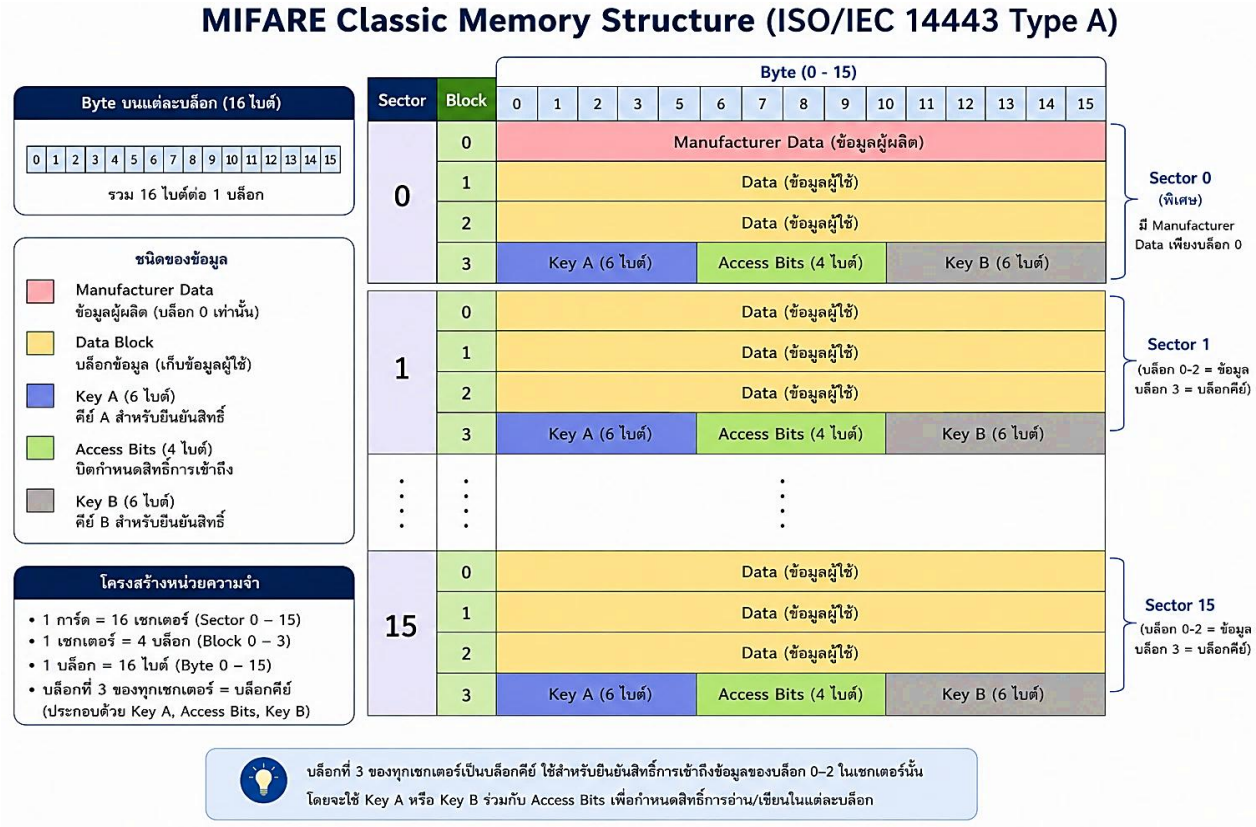
1.1.5) แต่ละบัตรมีเลข serial numbers ที่ไม่ซ้ำกัน

1.1.6) สามารถใช้ในสภาพแวดล้อมที่เปียกชื้นได้ โดยเครื่องอ่านต้องมีการป้องกันสภาพแวดล้อมต่าง ๆ นั้นไว้

1.2) ข้อเสียของมาตรฐาน MIFARE คือ บัตรมีราคาสูงเมื่อเทียบกับมาตรฐานอื่น

2) โครงสร้างข้อมูลของบัตร MIFARE

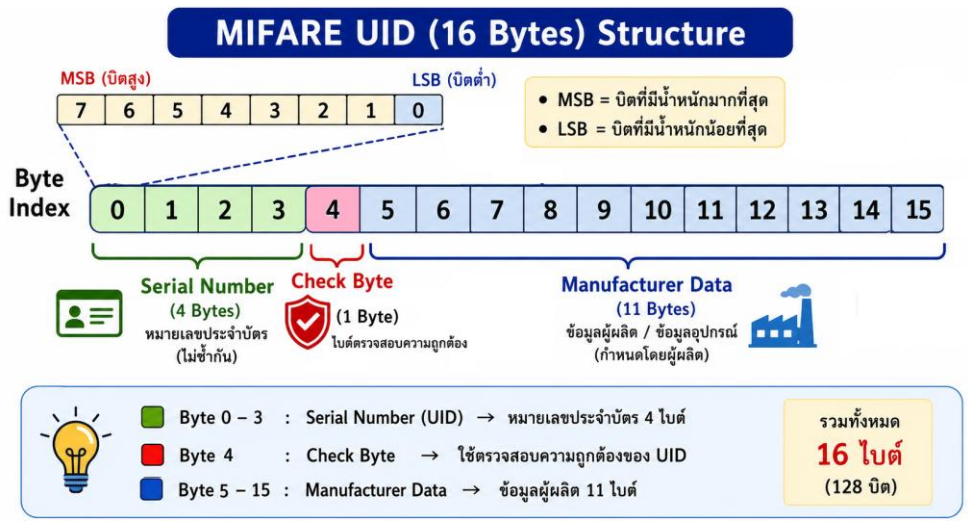
โครงสร้างข้อมูลของบัตร MIFARE ขนาด 1 kB บัตรแบ่งข้อมูลออกเป็นเซ็คเตอร์ (sector) ทั้งหมด 16 เซ็คเตอร์ (ตั้งแต่ 0 ถึง 15) ในแต่ละเซ็คเตอร์ประกอบด้วยชุดข้อมูล 4 บล็อค (block) แต่ละ block มีขนาด 16 bytes ดังนั้นความจุรวมคือ 16 X 4 X 16 = 1024 bytes จึงมีชื่อเรียกว่า MIFARE ขนาด 1 kB ส่วนของ MIFARE Classic 4kB ประกอบด้วย 40 sectors มีจำนวน block มากกว่าแบบ 1kB ซึ่งรองรับการเก็บข้อมูลปริมาณมากขึ้น



รูปที่ 4.13 โครงสร้างข้อมูลของบัตร MIFARE ขนาด 1 kB

จากรูปที่ 4.13 ประเภทของ block ในแต่ละ sector จะประกอบด้วย block 0 (data block), block 1(data block), block 2 (data block), และ block 3 (sector trailer) สำหรับ sector trailer เป็น block สำคัญที่ใช้กำหนดความปลอดภัยของ sector ประกอบด้วย key A, access bits, และ key B รายละเอียดการทำงานโดยบล็อคต่าง ๆ สำหรับการเก็บข้อมูลบนบัตร รายละเอียด ดังนี้

2.1) Sector 0 block 0 เก็บข้อมูลของบัตรหรือค่า Unique Identifier (UID) ขนาด 16 bit สามารถอ่านได้เพียงอย่างเดียวไม่สามารถเขียนได้



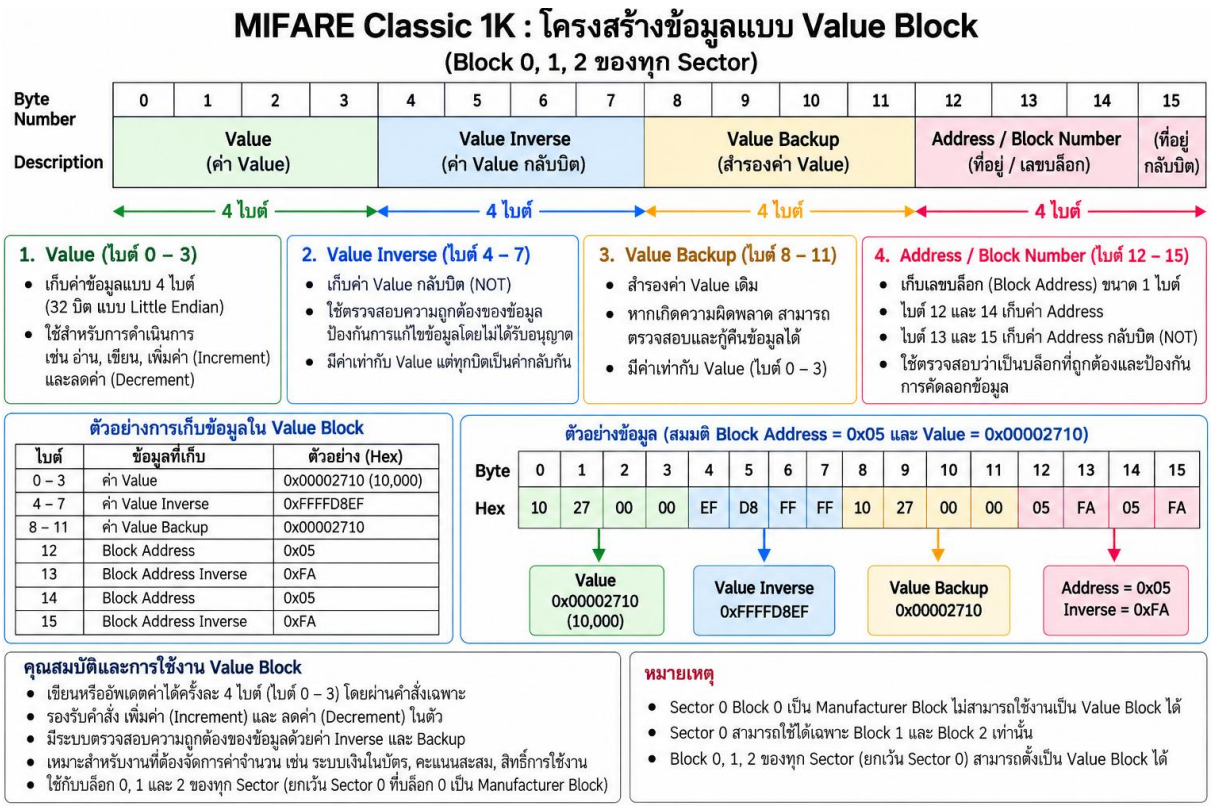
รูปที่ 4.14 โครงสร้างของ sector 0 block 0

2.2) Block 0, 1, 2 ของทุก sectors

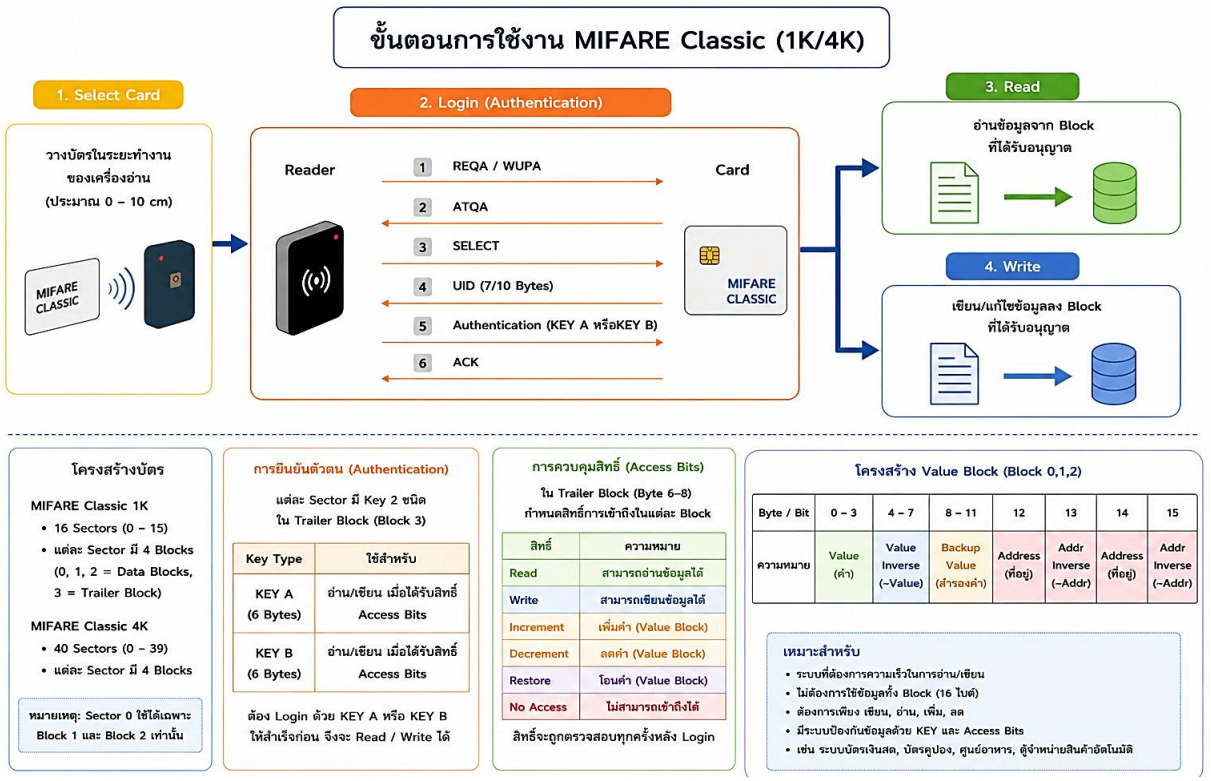
Block 0, 1, 2 ของทุก sectors (ยกเว้น sector 0 ที่ใช้ได้เฉพาะ block 1,2) ใช้เก็บข้อมูลที่ผู้ใช้ต้องการเขียน-อ่านบัตร แสดงดังรูปที่ 4.15

2.3) ขั้นตอนการอ่านและเขียนข้อมูลบนบัตร MIFARE

ขั้นตอนการอ่านและเขียนข้อมูลบนบัตร MIFARE เริ่มจาก เครื่องอ่านบัตรส่งคำสั่ง select card เพื่อตรวจสอบมีบัตรทาบอยู่หรือไม่ จากนั้นถ้าตรวจสอบว่ามีบัตร และเครื่องอ่านส่งคำสั่ง Login เพื่อเข้าถึงข้อมูลในบัตรโดยกำหนด sector ที่ต้องการ login และเลือกเป็น Key A และ Key B ตามด้วยรหัส Key ท้ายสุด ผู้ใช้สามารถเลือกได้ว่า ต้องการอ่านหรือเขียนข้อมูลไปที่บัตร เมื่อผู้ใช้ต้องการอ่านหรือเขียนข้อมูล ใน sector อื่นต้องส่งคำสั่ง login ไปใหม่



รูปที่ 4.15 โครงสร้างของ Block 0, 1, 2 ของทุก sector



รูปที่ 4.16 การอ่านและเขียนข้อมูลบนบัตร MIFARE

จากรูปที่ 4.16 ขั้นตอนการทำงานของระบบ MIFARE classic ภาพแสดงลำดับขั้นตอนการทำงานพื้นฐานของบัตร RFID ประเภท MIFARE classic ตั้งแต่การเลือกบัตร การยืนยันตัวตน ไปจนถึงการอ่านและเขียนข้อมูลภายในหน่วยความจำของบัตร โดยใช้มาตรฐาน ISO/IEC 14443 Type A ที่ความถี่ 13.56 MHz ซึ่งเป็นระบบ RFID แบบเหนี่ยวนำแม่เหล็ก

2.4.1) ขั้นตอน select card

เมื่อบัตร MIFARE classic ถูกนำเข้าสู่สนามแม่เหล็กของเครื่องอ่าน (reader) ภายในระยะประมาณ 0–10 cm ขดลวดของบัตรจะได้รับพลังงานจากสนามแม่เหล็กไฟฟ้าของเครื่องอ่านผ่านหลักการเหนี่ยวนำแม่เหล็กไฟฟ้า (electromagnetic induction) เครื่องอ่านจะส่งคำสั่งเริ่มต้นเพื่อค้นหาบัตรในบริเวณสนามแม่เหล็ก โดยใช้คำสั่ง REQA (Request command) หรือ WUPA (Wake-Up Command) เพื่อเรียกบัตรที่อยู่ในสนามให้ตอบสนองกลับมา เมื่อบัตรได้รับคำสั่งดังกล่าว วงจรภายในบัตรจะเริ่มทำงานและส่งข้อมูลตอบกลับเบื้องต้นเพื่อแจ้งว่า “มีบัตรอยู่ในสนาม”

2.4.2) ขั้นตอน login หรือ authentication

หลังจากเครื่องอ่านตรวจพบบัตรแล้ว จะเข้าสู่กระบวนการยืนยันตัวตน (authentication Process) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ขั้นตอนนี้ ดังนี้

2.4.2.1) REQA/WUPA เครื่องอ่านส่งคำสั่งค้นหาบัตร

2.4.2.2) ATQA (Answer to Request) บัตรตอบกลับข้อมูลเบื้องต้น เช่น ประเภทของบัตร ความสามารถของบัตร และ ขนาด UID

2.4.2.3) SELECT เครื่องอ่านเลือกบัตรที่ต้องการสื่อสาร ในกรณีที่มีหลายบัตรอยู่ในสนามพร้อมกัน ระบบจะใช้กระบวนการ Anti-collision เพื่อหลีกเลี่ยงการชนกันของข้อมูล

2.4.2.4) Unique Identifier (UID) บัตรส่งหมายเลขประจำตัวเฉพาะ ซึ่งอาจมีขนาด 4 Bytes, 7 Bytes, และ 10 Bytes โดย UID แต่ละใบไม่ให้ซ้ำกัน โปรแกรมสำหรับอ่านค่า UID ของ RFID ดังภาคผนวก ข (Arduino Code: 1)

2.4.2.5) Authentication ด้วย key A หรือ key B ก่อนเข้าถึงข้อมูลในแต่ละ sector เครื่องอ่านต้องทำการ authentication ด้วยกุญแจเข้ารหัส แต่ละ sector มี key อยู่ 2 ชุด คือ key A และ B ขนาด 6 bytes ข้อมูล key จะถูกเก็บไว้ใน sector trailer block ซึ่งเป็น block สุดท้ายของแต่ละ sector เครื่องอ่านจะส่ง key ไปยังบัตรเพื่อทำการตรวจสอบสิทธิ์ หาก key ถูกต้อง บัตรจะอนุญาตให้เข้าถึงข้อมูลภายใน sector นั้น

2.4.2.6) ACK (Acknowledge) เมื่อ authentication สำเร็จ บัตรจะตอบกลับ ACK เพื่อแจ้งว่าเครื่องอ่านได้รับสิทธิ์ในการเข้าถึงข้อมูล หลังจากนั้นจึงสามารถอ่านหรือเขียนข้อมูลได้

2.4.3) ขั้นตอน read data

หลังจาก Authentication สำเร็จ เครื่องอ่านสามารถอ่านข้อมูลจาก block ที่ได้รับอนุญาต ข้อมูลที่อ่านได้อาจประกอบด้วย ข้อมูลผู้ใช้ หมายเลขสมาชิก ยอดเงินคงเหลือ ข้อมูลสิทธิ์การเข้าใช้งาน และข้อมูลระบบ โดย เครื่องอ่านจะส่งคำสั่ง READ ไปยัง block ที่ต้องการ และบัตรจะตอบกลับข้อมูลขนาด 16 bytes ต่อ 1 block

2.4.4) ขั้นตอน write data

หากสิทธิ์ของ access bits อนุญาต เครื่องอ่านสามารถเขียนหรือแก้ไขข้อมูลใน block ได้ การเขียนข้อมูลจะใช้คำสั่ง WRITE และข้อมูลใหม่จะถูกบันทึกลง EEPROM ภายในบัตร กระบวนการนี้นิยมใช้กับระบบ เช่น e-purse ระบบสะสมแต้ม ระบบบัตรสมาชิก ระบบควบคุมการเข้า–ออก

2.5) การกำหนด access bits

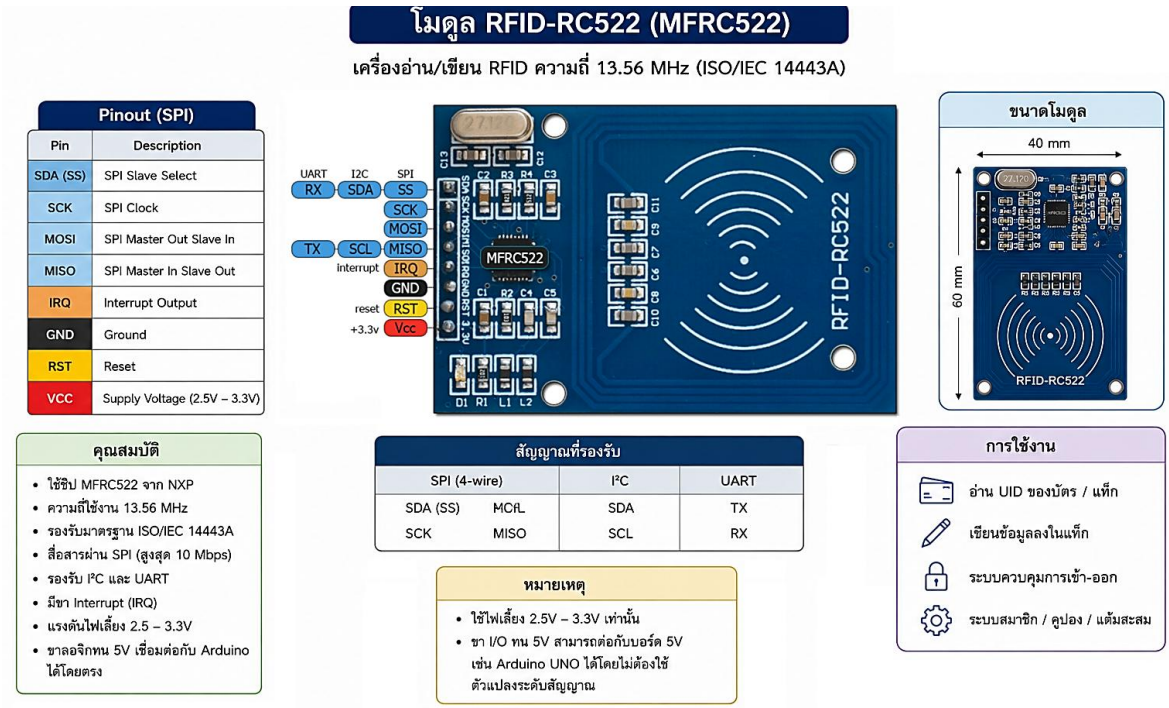
Access bits ใช้กำหนดสิทธิ์การเข้าถึงแต่ละ block ดังตารางที่ 4.7 โดยระบบจะตรวจสอบ access bits ทุกครั้งหลัง authentication

ตารางที่ 4.7 การกำหนด Access Bits

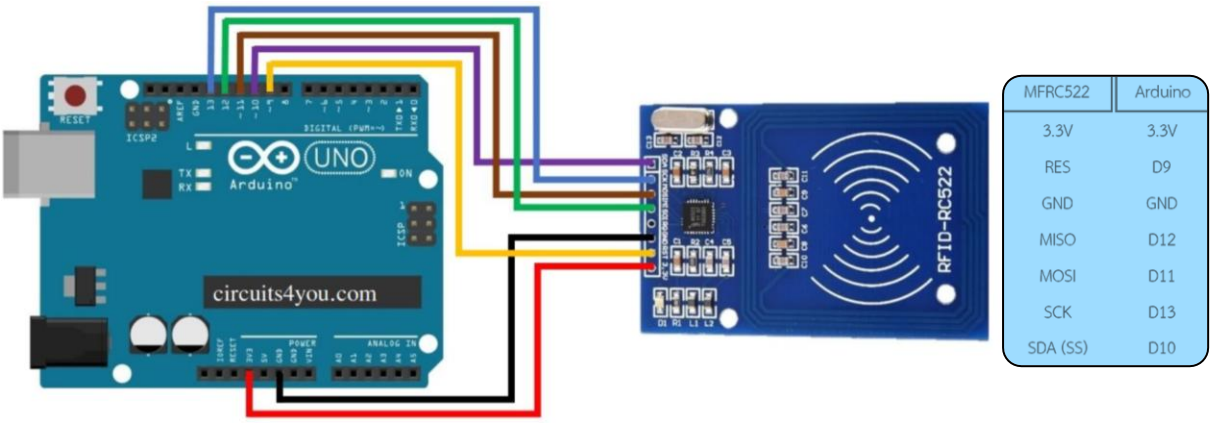
สิทธิ์	ความหมาย
Read	อ่านข้อมูล
Write	เขียนข้อมูล
Increment	เพิ่มค่า
Decrement	ลดค่า
Restore	กู้คืนค่า
No Access	ไม่อนุญาต

4.2.7 โครงสร้างของโมดูล RFID รุ่น RC522

โครงสร้างของโมดูล RFID รุ่น RC522 แสดงดังรูปที่ 4.17



(ก) โมดูล RFID รุ่น RC522



(ข) การต่อโมดูล RC522 กับ Arduino

รูปที่ 4.17 โมดูล RFID รุ่น RC522

1) ขาของโมดูล RC522 RFID (RC522 RFID module pinout)

โมดูล RC522 มีขาสัญญาณทั้งหมด 8 ขา สำหรับเชื่อมต่อกับอุปกรณ์ภายนอก โดยรายละเอียดของแต่ละขามีดังนี้

1.1) VCC

ใช้สำหรับจ่ายไฟเลี้ยงให้กับโมดูล รองรับแรงดันไฟฟ้าระหว่าง 2.5 ถึง 3.3 V สามารถเชื่อมต่อกับขา 3.3V ของบอร์ด Arduino ได้โดยตรง ไม่ควรเชื่อมต่อกับไฟ 5 V เพราะอาจทำให้โมดูลเสียหายได้

1.2) RST (Reset)

เป็นขาสำหรับรีเซตและปิดการทำงานของโมดูล (power-down) เมื่อขานี้มีสถานะลอจิกต่ำ (LOW) โดย (1) โมดูลจะเข้าสู่โหมดปิดการทำงาน (2) วงจรภายใน รวมถึงออสซิลเลเตอร์จะหยุดทำงาน และ (3) ขาสัญญาณอินพุตจะถูกตัดออกจากวงจรภายนอก และเมื่อสัญญาณเปลี่ยนจาก LOW เป็น HIGH โมดูลจะถูกรีเซตและเริ่มทำงานใหม่

1.3) GND

เป็นขากราวด์ของโมดูล ต้องเชื่อมต่อกับขา GND ของไมโครคอนโทรลเลอร์

1.4) IRQ (Interrupt Request)

เป็นขาสัญญาณอินเทอร์รัปต์ ใช้แจ้งเตือนไปยังไมโครคอนโทรลเลอร์เมื่อมีแท็ก RFID เข้ามาอยู่ในบริเวณตรวจจับของโมดูล ช่วยลดภาระในการตรวจสอบสถานะซ้ำ ๆ จากไมโครคอนโทรลเลอร์

1.5) MISO/SCL/TX

ขานี้สามารถทำงานได้หลายรูปแบบ ขึ้นอยู่กับโหมดการสื่อสารที่ใช้งาน

1.5.1) ในโหมด SPI จะทำหน้าที่เป็น MISO (Master in Slave Out) สำหรับส่งข้อมูลจากโมดูลไปยังไมโครคอนโทรลเลอร์

1.5.2) ในโหมด I²C จะทำหน้าที่เป็น SCL (serial clock) สำหรับส่งสัญญาณนาฬิกา

1.5.3) ในโหมด UART จะทำหน้าที่เป็น TX (transmit data) สำหรับส่งข้อมูลอนุกรมออกจากโมดูล

1.6) MOSI (Master Out Slave In)

ใช้ในโหมด SPI สำหรับรับข้อมูลจากไมโครคอนโทรลเลอร์เข้าสู่โมดูล RC522

1.7) SCK (Serial Clock)

ใช้ในโหมด SPI สำหรับรับสัญญาณนาฬิกา (clock pulse) จากอุปกรณ์ Master เช่น Arduino เพื่อกำหนดจังหวะการรับส่งข้อมูล

1.8) SS/SDA/RX

ขานี้สามารถทำงานได้หลายรูปแบบเช่นกัน ขึ้นอยู่กับโหมดการสื่อสาร โดยทั่วไป ขานี้มักถูกทำเครื่องหมายด้วยกรอบสี่เหลี่ยมบนแผงวงจร เพื่อใช้เป็นจุดอ้างอิงในการระบุตำแหน่งขาอื่น ๆ ของโมดูล

1.8.2) ในโหมด SPI จะทำหน้าที่เป็น SS (slave select) หรือขาเลือกอุปกรณ์ Slave

1.8.2) ในโหมด I²C จะทำหน้าที่เป็น SDA (serial data) สำหรับรับส่งข้อมูลอนุกรม

1.8.2) ในโหมด UART จะทำหน้าที่เป็น RX (receive data) สำหรับรับข้อมูลอนุกรมเข้าสู่โมดูล

4.3 เทคโนโลยีการสื่อสารระยะใกล้ (Near Field Communication: NFC)

4.3.1 ความหมายของระบบ NFC

เทคโนโลยีการสื่อสารระยะใกล้ หรือ Near Field Communication (NFC) เป็นเทคโนโลยีการสื่อสารข้อมูลแบบไร้สายระยะใกล้ (short-range wireless communication) ที่ได้รับการพัฒนาต่อยอดจากเทคโนโลยี RFID โดยออกแบบให้สามารถแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์สองเครื่องได้อย่างรวดเร็ว ปลอดภัย และไม่ต้องอาศัยการเชื่อมต่อผ่านสายสัญญาณ ทำงานที่ความถี่มาตรฐาน 13.56 MHz ตามมาตรฐาน ISO/IEC 14443 และ ISO/IEC 18092 ซึ่งเป็นมาตรฐานสากลสำหรับระบบสื่อสารแบบไร้สัมผัส (Rahul et al., 2015; Alrawais, 2020)คุณลักษณะของ NFC เมื่อเปรียบเทียบกับเทคโนโลยีไร้สายอื่น NFC มีคุณสมบัติที่โดดเด่น ดังนี้

1) ใช้ความถี่มาตรฐาน 13.56 MHz
2) ระยะการสื่อสารประมาณ 0–10 cm (ไม่เกิน 10 cm)
3) อัตราการรับส่งข้อมูลสูงสุด 424 kbps
4) ใช้พลังงานต่ำ
5) เชื่อมต่อได้รวดเร็วภายในเวลาไม่ถึง 0.1s
6) ไม่จำเป็นต้อง Pairing ก่อนใช้งาน

7) รองรับการสื่อสารแบบ active และ passive
8) มีความปลอดภัยสูงกว่าระบบไร้สายที่มีระยะไกล เนื่องจากระยะสื่อสารสั้น

รูปที่ 4.18 อุปกรณ์ในการสื่อสารด้วยเทคโนโลยี NFC

4.3.2 ความรู้พื้นฐานของเทคโนโลยี NFC

NFC ได้รับการออกแบบให้มีความสะดวกในการใช้งาน โดยผู้ใช้เพียงนำอุปกรณ์สองเครื่องมาแตะหรืออยู่ในระยะใกล้กัน ระบบจะเริ่มกระบวนการตรวจจับ (discovery) การพิสูจน์ตัวตน (authentication) และการแลกเปลี่ยนข้อมูลโดยอัตโนมัติ ทำให้ลดขั้นตอนการเชื่อมต่อเมื่อเปรียบเทียบกับเทคโนโลยี Bluetooth หรือ Wi-Fi ที่ต้องจับคู่ (pairing) ก่อนใช้งาน ส่งผลให้ NFC เหมาะสำหรับงานที่ต้องการความรวดเร็ว เช่น การชำระเงิน การยืนยันตัวตน และระบบควบคุมการเข้าออกอาคาร (Chang & Wang, 2025; Rahul et al., 2015) นอกจากนี้ NFC ยังสนับสนุนการสื่อสารแบบสองทิศทาง (bidirectional communication) ทำให้อุปกรณ์สามารถทำหน้าที่เป็นทั้งผู้ส่งและผู้รับข้อมูลได้ภายในกระบวนการเดียว อีกทั้งยังสามารถจำลองการทำงานของบัตรอัจฉริยะ (smart card emulation) อ่านหรือเขียนข้อมูลบนแท็กอิเล็กทรอนิกส์ (NFC tag) รวมถึงแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์เคลื่อนที่ได้อย่างมีประสิทธิภาพ ส่งผลให้ NFC ถูกนำไปประยุกต์ใช้ในระบบชำระเงินแบบไร้สัมผัส ระบบขนส่งสาธารณะ ระบบควบคุมการเข้าออก ระบบระบุตัวตน และอุปกรณ์ IoT อย่างแพร่หลาย (Chang & Wang, 2025; Guo & Shi, 2024)

เมื่อเปรียบเทียบกับ RFID แม้ว่า NFC จะพัฒนามาจากหลักการเดียวกันคือการเหนี่ยวนำสนามแม่เหล็กไฟฟ้า (electromagnetic induction) แต่ NFC มีข้อได้เปรียบด้านความปลอดภัยมากกว่า เนื่องจากกำหนดระยะการสื่อสารให้สั้นมาก จึงลดโอกาสในการดักจับข้อมูลจากระยะไกล และยังรองรับกลไกการพิสูจน์ตัวตน การเข้ารหัสข้อมูล และการใช้ secure element เพื่อจัดเก็บข้อมูลสำคัญ เช่น ข้อมูลบัตรเครดิต หรือข้อมูลการยืนยันตัวตนของผู้ใช้งาน (Alrawais, 2020; Chang & Wang, 2025) อย่างไรก็ตาม แม้ว่าระยะการสื่อสารที่สั้นจะช่วยเพิ่มระดับความปลอดภัย แต่ไม่ได้หมายความว่าระบบ NFC จะปลอดภัยโดยสมบูรณ์ เนื่องจากยังคงมีความเสี่ยงจากการโจมตีหลายรูปแบบ เช่น การดักฟังข้อมูล (eavesdropping) การโจมตีแบบรีเลย์ (relay Attack) การแทรกข้อมูล (data insertion) การปลอมแปลงแท็ก (tag replacement) การโจมตีแบบฟิชชิง (phishing) และการรบกวนสัญญาณ (jamming) ดังนั้น การพัฒนาระบบ NFC ในงานที่เกี่ยวข้องกับ

การเงินและการควบคุมการเข้าออกจึงจำเป็นต้องใช้เทคนิคด้านความมั่นคงปลอดภัยเพิ่มเติม เช่น การเข้ารหัสข้อมูล (AES, 3DES) การแลกเปลี่ยนกุญแจเข้ารหัส (RSA หรือ elliptic curve cryptography) การพิสูจน์ตัวตนแบบสองปัจจัย และการใช้ Secure Element (SE) เพื่อป้องกันข้อมูลสำคัญ (Alrawais, 2020; Rahul et al., 2015)

ในปัจจุบัน NFC ได้กลายเป็นหนึ่งในเทคโนโลยีสำคัญของการพัฒนาเมืองอัจฉริยะ (smart city) และระบบ IoT โดยมีบทบาทในการเชื่อมโยงอุปกรณ์อัจฉริยะ การชำระเงินผ่านโทรศัพท์มือถือ การตรวจสอบสิทธิ์การเข้าใช้งานอาคาร การติดตามสินค้า ระบบขนส่งสาธารณะ ตลอดจนการเชื่อมต่ออุปกรณ์สวมใส่อัจฉริยะ (wearable devices) ความสามารถดังกล่าวทำให้ NFC มีแนวโน้มเติบโตอย่างต่อเนื่อง และกลายเป็นโครงสร้างพื้นฐานสำคัญของระบบดิจิทัลในอนาคต (Chang & Wang, 2025; Bhatt & Vidani, 2024)

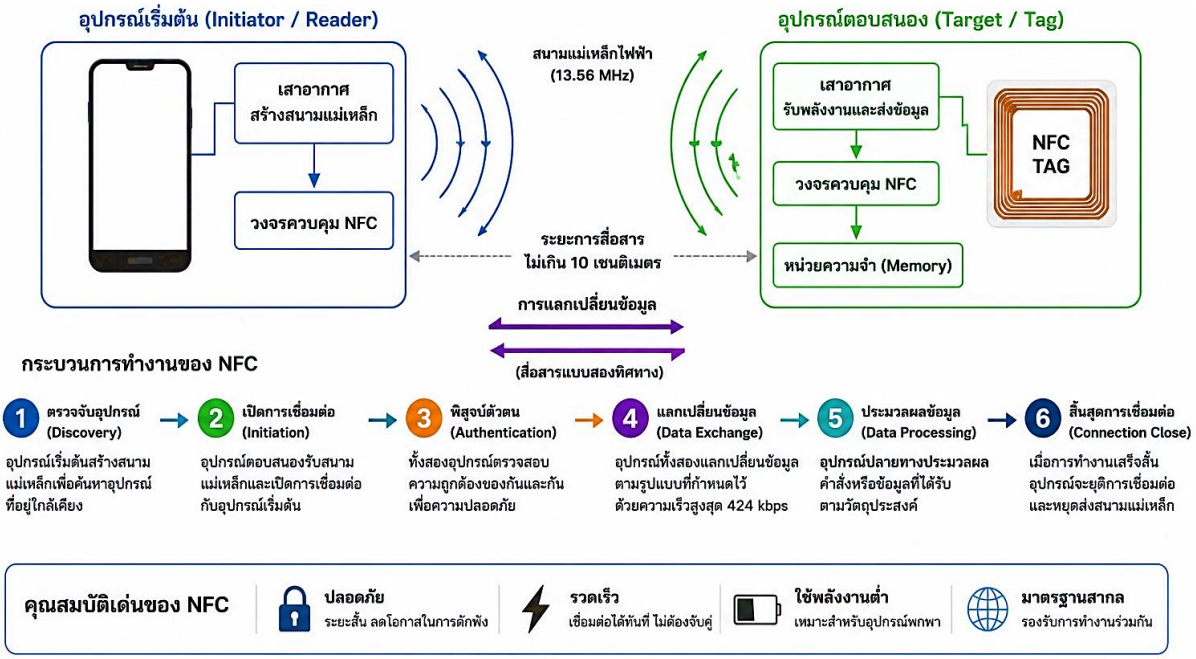
4.3.3 หลักการทำงานของ NFC

ระบบ NFC อาศัยหลักการ electromagnetic induction หรือการเหนี่ยวนำสนามแม่เหล็กไฟฟ้า โดยอุปกรณ์ต้นทาง (initiator) จะสร้างสนามแม่เหล็กความถี่ 13.56 MHz ผ่านขดลวดเสาอากาศ (antenna coil) เมื่ออุปกรณ์อีกตัวหนึ่งหรือ NFC tag เข้าอยู่ภายในสนามแม่เหล็ก จะเกิดการเหนี่ยวนำกระแสไฟฟ้า ทำให้สามารถแลกเปลี่ยนข้อมูลระหว่างกันได้ การสื่อสารของ NFC ประกอบด้วยอุปกรณ์ 2 ประเภท ได้แก่

1) Initiator เป็นอุปกรณ์ที่เริ่มต้นการสื่อสารและสร้างสนามแม่เหล็กไฟฟ้า

2) Target เป็นอุปกรณ์หรือแท็กที่ตอบสนองต่อสัญญาณจาก Initiator

ในกรณีที่ target เป็น NFC tag แบบ passive จะไม่ต้องใช้แหล่งจ่ายไฟของตนเอง แต่จะได้รับพลังงานจากสนามแม่เหล็กของ Initiator ทำให้ NFC Tag มีอายุการใช้งานยาวนานและไม่ต้องเปลี่ยนแบตเตอรี่



รูปที่ 4.19 หลักการทำงานของ NFC

4.3.4 โครงสร้างระบบของ NFC (NFC System Architecture)

ระบบ NFC ประกอบด้วยองค์ประกอบหลัก 4 ส่วน ได้แก่

1) NFC reader (initiator)

อุปกรณ์ที่ทำหน้าที่สร้างสนามแม่เหล็กไฟฟ้า ส่งคำร้องขอ และควบคุมการสื่อสาร ตัวอย่างเช่น เครื่องอ่านบัตร (access control reader) เครื่องรับชำระเงิน (POS terminal) สมาร์ตโฟน หรือเครื่องอ่านประตูอัตโนมัติ โดย reader จะเป็นผู้เริ่มต้นการสื่อสารทุกครั้ง และเป็นแหล่งพลังงานสำหรับ NFC tag แบบ passive (Rahul et al., 2015)

2) NFC tag หรือ smart card (target)

อุปกรณ์ที่ใช้เก็บข้อมูล เช่น UID หมายเลขบัตร URL ข้อมูลผู้ใช้ หรือ digital certificate NFC tag ส่วนใหญ่ไม่มีแบตเตอรี่ และได้รับพลังงานจากสนามแม่เหล็กของ reader ทำให้มีอายุการใช้งานยาวนานและไม่ต้องบำรุงรักษา (Guo & Shi, 2024)

3) NFC controller

วงจรควบคุมภายในอุปกรณ์ ทำหน้าที่ควบคุมการรับส่งข้อมูล ตรวจสอบโปรโตคอล เข้ารหัสข้อมูล และจัดการโหมดการสื่อสาร controller จะทำงานร่วมกับ secure element ที่เกี่ยวกับธุรกรรมทางการเงินและระบบรักษาความปลอดภัย (Rahul et al., 2015)

4) Secure Element (SE)

เป็นพื้นที่จัดเก็บข้อมูลที่มีความปลอดภัยสูง ใช้เก็บ encryption key, digital certificate, ข้อมูลบัตรเครดิต หรือ ข้อมูลสิทธิ์การเข้าออก secure element เป็นองค์ประกอบคัญของระบบ access control และ mobile payment เนื่องจากช่วยป้องกันการโจรกรรมข้อมูล (Rahul et al., 2015)

4.3.5 โหมดการทำงานของ NFC (Operating Modes)

NFC Forum กำหนดโหมดการทำงานหลักไว้ 3 รูปแบบ ได้แก่

1) Reader/Writer mode

Reader จะอ่านหรือเขียนข้อมูลลงบน NFC tag ตัวอย่าง เช่น อ่าน URL อ่านข้อมูลสินค้า โปรแกรม tag ระบบลงทะเบียน โหมดนี้นิยมใช้ในระบบ smart poster และระบบประชาสัมพันธ์ (Rahul et al., 2015)

2) Card Emulation Mode

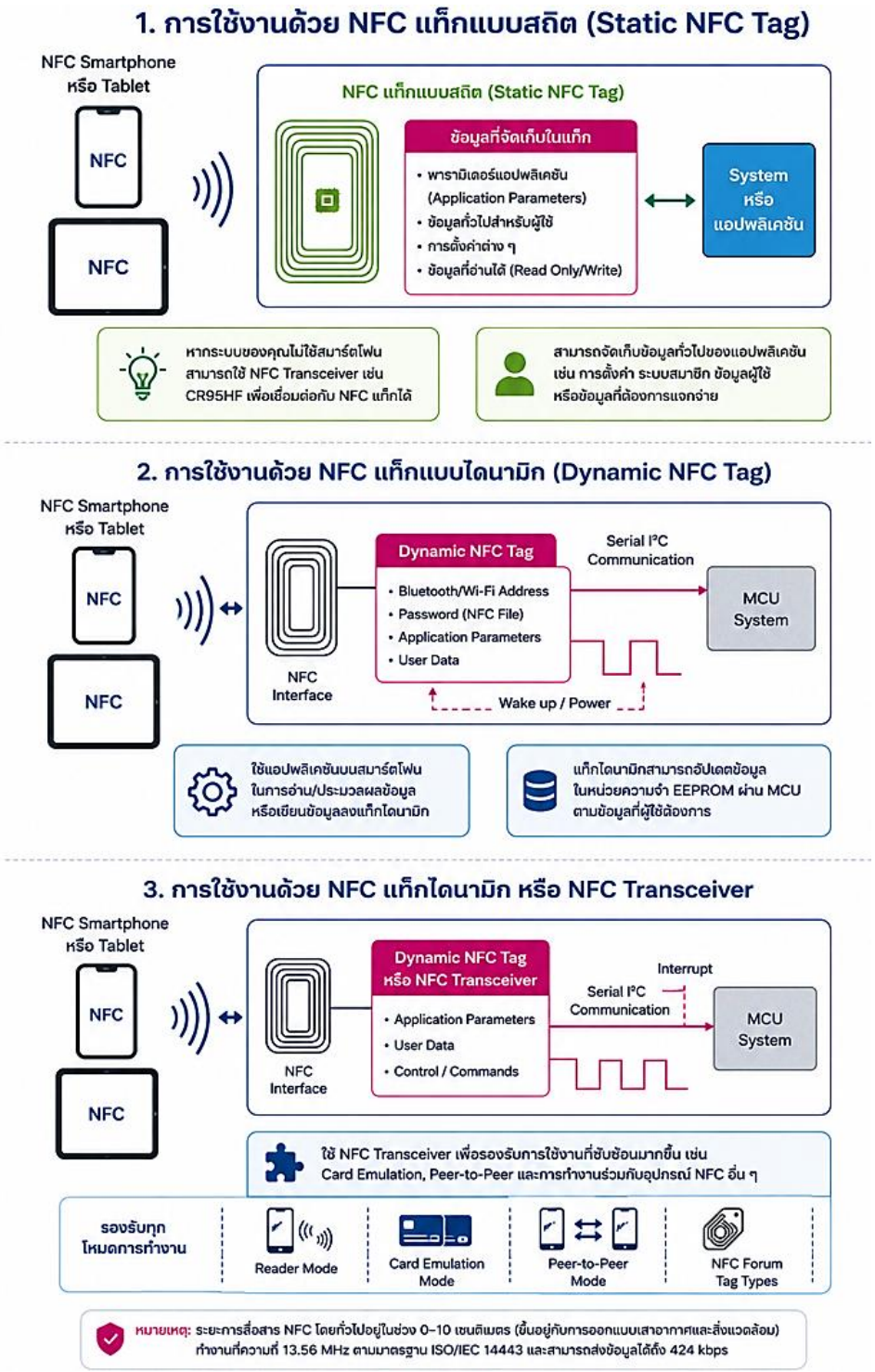
อุปกรณ์ NFC จะทำหน้าที่เสมือนบัตรอัจฉริยะ ตัวอย่าง เช่น access card, employee card, hotel key card, student card, และ mobile payment โหมดนี้เป็นโหมดที่ใช้มากที่สุดในระบบควบคุมการเข้าออก (Rahul et al., 2015; Guo & Shi, 2024)

3) Peer-to-Peer Mode

การแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ NFC สองเครื่อง ตัวอย่าง เช่น ส่งข้อมูลติดต่อ แชร์รูปภาพ ส่งไฟล์ จับคู่ Bluetooth หรือ Wi-Fi อย่างรวดเร็ว โหมดนี้ช่วยลดระยะเวลาการเชื่อมต่อเมื่อเทียบกับการจับคู่ Bluetooth แบบปกติ (Rahul et al., 2015)

4.3.6 ประเภทของอุปกรณ์ NFC และลักษณะการใช้งาน

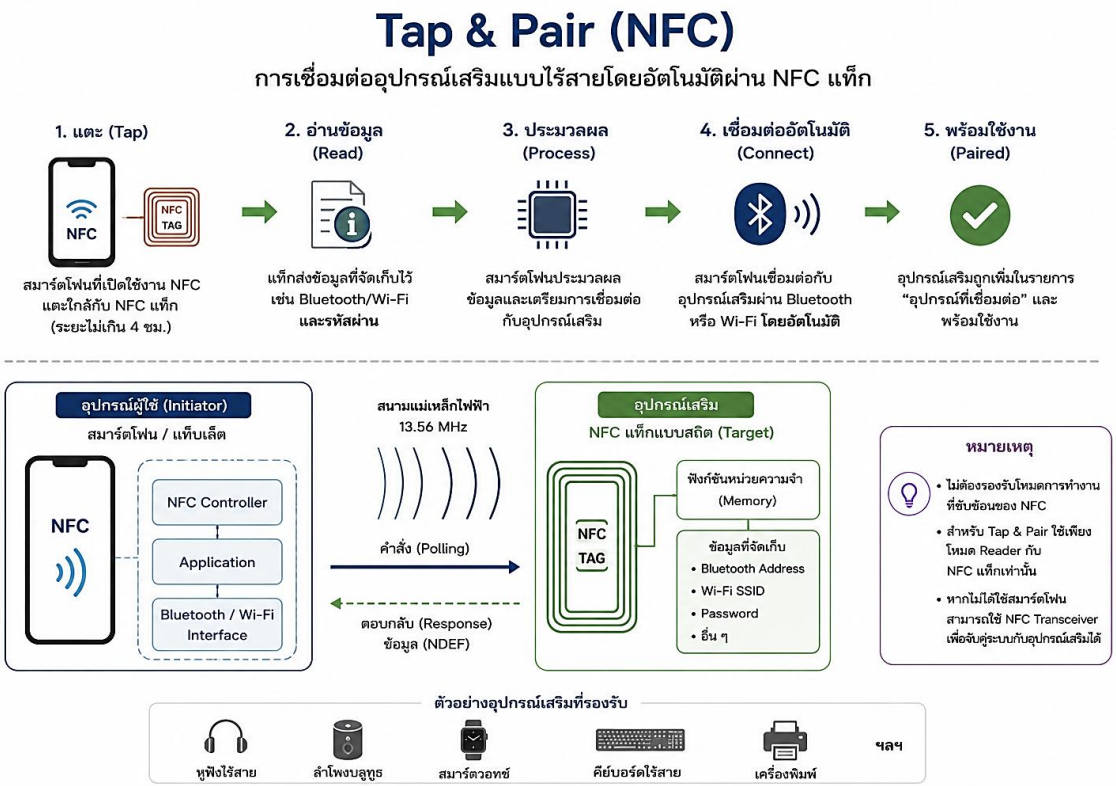
การทำงานของอุปกรณ์ NFC ทั้งสามประเภท ได้แก่ static NFC tag, dynamic NFC tag และ NFC transceiver ซึ่งมีระดับความสามารถในการประมวลผลและการสื่อสารแตกต่างกัน (Proehl, 2013; Coskun et al., 2015) แสดงดังรูปที่ 4.20



รูปที่ 4.20 การเปรียบเทียบลักษณะการใช้งานของแท็ก NFC แบบสแตติก แบบไดนามิก และอุปกรณ์ NFC transceiver

1) แท็กแบบสแตติก (Static NFC Tag)

เป็นแท็กแบบพาสซีฟที่มีหน่วยความจำสำหรับจัดเก็บข้อมูลคงที่ เช่น URL ข้อมูลแอปพลิเคชัน ข้อมูลผู้ใช้ หรือค่าการตั้งค่าระบบ โดยสมาร์ตโฟนหรือแท็บเล็ตที่รองรับ NFC จะทำหน้าที่เป็นอุปกรณ์เริ่มต้น (initiator) สำหรับอ่านข้อมูลจากแท็กผ่านการเหนี่ยวนำสนามแม่เหล็กไฟฟ้าที่ความถี่ 13.56 MHz ทั้งนี้ ข้อมูลภายในแท็กสามารถกำหนดให้เป็นแบบอ่านอย่างเดียว (read only) หรืออ่านและเขียนข้อมูลได้ (read/write)



รูปที่ 4.21 หลักการทำงานของการแตะเพื่อใช้งาน (tap & pair)

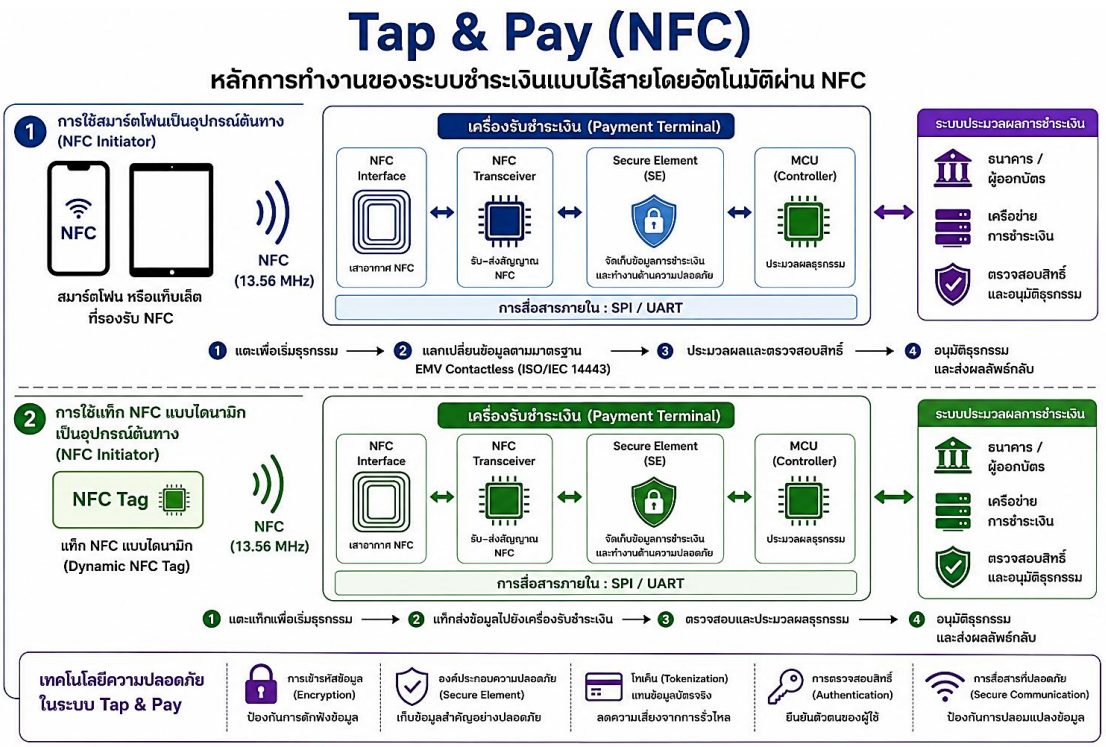
หลักการทำงานของ tap and pair โดยใช้ NFC แท็กแบบสแตติก ซึ่งสมาร์ตโฟนหรือแท็บเล็ตที่รองรับ NFC ทำหน้าที่เป็นอุปกรณ์เริ่มต้น (initiator) อ่านข้อมูลที่บันทึกอยู่ภายในแท็กผ่านการสื่อสารแบบ reader/writer mode ข้อมูลที่จัดเก็บอาจประกอบด้วยชื่อเครือข่าย Wi-Fi (SSID) รหัสผ่าน ที่อยู่ Bluetooth (Bluetooth address) หรือข้อมูลการกำหนดค่าอื่น ๆ ในรูปแบบ NFC Data Exchange Format (NDEF) หลังจากอ่านข้อมูลแล้ว สมาร์ตโฟนจะประมวลผลและดำเนินการเชื่อมต่อกับอุปกรณ์ปลายทางผ่าน Bluetooth หรือ Wi-Fi โดยอัตโนมัติ ทั้งนี้ NFC Tag ทำหน้าที่เพียงจัดเก็บข้อมูลแบบคงที่ (static data) และไม่มีการประมวลผลหรือปรับปรุงข้อมูลร่วมกับไมโครคอนโทรลเลอร์ จึงเหมาะสำหรับการตั้งค่าอุปกรณ์และการเชื่อมต่อแบบแตะเพื่อใช้งาน ที่ต้องการความรวดเร็วและประหยัดพลังงาน

2) แท็กแบบไดนามิก (Dynamic NFC Tag)

เป็นแท็กที่สามารถสื่อสารกับไมโครคอนโทรลเลอร์ (MCU) ผ่านอินเทอร์เฟซ serial I²C communication ทำให้สามารถปรับปรุงข้อมูลภายในหน่วยความจำของแท็กได้แบบเรียลไทม์ เช่น การอัปเดตข้อมูลเซนเซอร์ ข้อมูลการตั้งค่าเครือข่าย Wi-Fi หรือข้อมูลจากอุปกรณ์ IoT นอกจากนี้ยังรองรับฟังก์ชัน wake-up เพื่อปลุกไมโครคอนโทรลเลอร์เมื่อมีการตรวจพบสนามแม่เหล็กจากอุปกรณ์ NFC

3) NFC Transceiver

เป็นอุปกรณ์ที่มีความสามารถสูงกว่าการเป็นแท็กทั่วไป โดยสามารถทำงานร่วมกับไมโครคอนโทรลเลอร์เพื่อรับ ส่ง และประมวลผลข้อมูลแบบสองทิศทาง รองรับการทำงานหลายโหมด ได้แก่ reader/writer mode, card emulation mode และ peer-to-peer mode จึงเหมาะสำหรับระบบควบคุมการเข้าออก ระบบชำระเงินอิเล็กทรอนิกส์ (tap & pay) ระบบระบุตัวตน และการสื่อสารระหว่างอุปกรณ์อัจฉริยะ



รูปที่ 4.22 การทำงานของระบบชำระเงินอิเล็กทรอนิกส์

รูปที่ 4.22 แสดงหลักการทำงานของระบบชำระเงินแบบไร้สัมผัส (Tap & Pay) ที่ใช้เทคโนโลยี NFC ซึ่งรองรับการสื่อสารระยะใกล้ที่ความถี่ 13.56 MHz โดยแบ่งการทำงานออกเป็นสองรูปแบบ ได้แก่ การใช้สมาร์ตโฟนหรือแท็บเล็ตเป็นอุปกรณ์ต้นทาง (NFC initiator) โดยอุปกรณ์เคลื่อนที่จะสร้างสนามแม่เหล็กไฟฟ้าและแลกเปลี่ยนข้อมูลกับเครื่องรับชำระเงิน (payment terminal) ผ่านอินเทอร์เฟซ NFC ภายในเครื่องรับชำระเงินประกอบด้วยสายอากาศ (NFC antenna)

วงจรรับส่งสัญญาณ NFC transceiver วงจร Secure Element (SE) สำหรับจัดเก็บข้อมูลสำคัญและดำเนินการด้านความปลอดภัย และไมโครคอนโทรลเลอร์ (MCU) สำหรับประมวลผลข้อมูล ก่อนส่งข้อมูลธุรกรรมไปยังระบบประมวลผลการชำระเงินของธนาคารหรือผู้ให้บริการผ่านเครือข่ายสื่อสาร

การใช้ NFC tag แบบไดนามิก (dynamic NFC tag) เป็นอุปกรณ์ต้นทาง โดยแท็ก NFC จะส่งข้อมูลที่จัดเก็บหรือข้อมูลที่สร้างขึ้นแบบเรียลไทม์ไปยังเครื่องรับชำระเงินผ่านการสื่อสาร NFC จากนั้นข้อมูลจะถูกประมวลผลโดย NFC transceiver และไมโครคอนโทรลเลอร์ ก่อนส่งต่อไปยังระบบชำระเงินภายนอกเพื่อดำเนินการตรวจสอบสิทธิ์และอนุมัติธุรกรรม การสื่อสารระหว่าง NFC transceiver, secure element และ MCU ภายในเครื่องรับชำระเงินมักใช้บัสสื่อสาร เช่น SPI หรือ UART เพื่อให้สามารถรับส่งข้อมูลได้อย่างรวดเร็วและมีความน่าเชื่อถือ ขณะที่ระบบชำระเงินภายนอกจะดำเนินการตรวจสอบตัวตนของผู้ใช้งาน การยืนยันสิทธิ์ และการอนุมัติธุรกรรมตามมาตรฐานความปลอดภัยของระบบการเงิน จากนั้น ระบบ Tap & Pay มีการใช้เทคโนโลยีด้านความมั่นคงปลอดภัยหลายประการ ได้แก่ การเข้ารหัสข้อมูล (encryption) SE tokenization การพิสูจน์ตัวตน (authentication) และ การสื่อสารแบบเข้ารหัส (secure communication) เพื่อป้องกันการดักฟังข้อมูล การปลอมแปลงข้อมูล และการเข้าถึงข้อมูลการชำระเงินโดยไม่ได้รับอนุญาต ทำให้การชำระเงินผ่าน NFC มีความปลอดภัยและเป็นที่ยอมรับในการใช้งานเชิงพาณิชย์ในปัจจุบัน

4.4 ระบบล็อกประตูด้วยคิวอาร์โค้ด (QR Code Door Lock System)

ระบบล็อกประตูด้วยคิวอาร์โค้ด เป็นระบบควบคุมการเข้าออกที่ใช้ Quick Response Code (QR code) เป็นข้อมูลรับรองสิทธิ์ดิจิทัลของผู้ใช้งาน โดยเครื่องอ่านหรือกล้องจะถอดรหัสข้อมูลจาก QR code แล้วส่งไปยังหน่วยควบคุมเพื่อตรวจสอบกับข้อมูลที่ลงทะเบียนไว้ หากข้อมูลถูกต้อง ระบบจะสั่งกลไกล็อกประตูให้เปิด แต่หากข้อมูลไม่ถูกต้อง หมดอายุ หรือไม่ได้รับอนุญาต ระบบจะคงประตูไว้ในสถานะล็อก ระบบประเภทนี้มีจุดเด่นด้านความสะดวก ต้นทุนอุปกรณ์ไม่สูง และสามารถจัดการสิทธิ์ผ่านฐานข้อมูลส่วนกลางได้ โดยไม่จำเป็นต้องแจกกุญแจหรือบัตร RFID ให้ผู้ใช้งานทุกคน QR code ยังสามารถแสดงผ่านสมาร์ตโฟนหรือพิมพ์ลงบนเอกสารได้ จึงเหมาะสำหรับอาคารสำนักงาน สถานศึกษา ห้องปฏิบัติการ โรงแรม คลังสินค้า และพื้นที่ที่ต้องการกำหนดสิทธิ์เข้าใช้งานเป็นรายบุคคลหรือรายช่วงเวลา (Adedoyin & Olukoya, 2024; Jain et al., 2021; Jain et al., 2023; Guo et al., 2024)

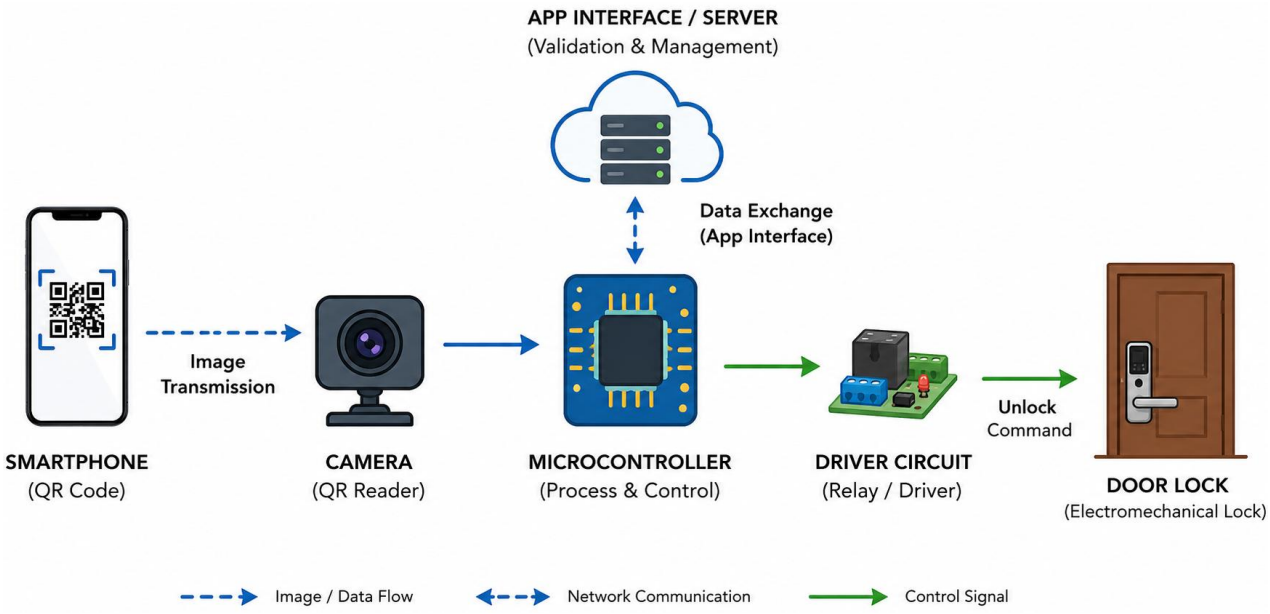
4.4.1 หลักการพื้นฐานของ QR Code

QR code เป็นบาร์โค้ดสองมิติที่จัดเก็บข้อมูลในรูปแบบของโมดูลสีดำและสีขาวบนพื้นที่สี่เหลี่ยม ข้อมูลถูกจัดวางทั้งในแนวนอนและแนวตั้ง ทำให้สามารถบรรจุข้อมูลได้มากกว่าบาร์โค้ดหนึ่งมิติทั่วไป เครื่องอ่านสามารถตรวจจับตำแหน่ง ทิศทาง และถอดรหัสข้อมูลจากภาพ QR code ได้อย่างรวดเร็ว แม้ภาพจะถูกอ่านจากหลายมุมก็ตาม ในระบบควบคุมการเข้าออก ข้อมูลที่บันทึกใน QR code อาจประกอบด้วย หมายเลขประจำตัวผู้ใช้งาน หมายเลขประจำระบบ รหัสโทเคน ข้อมูลสิทธิ์การเข้าใช้ หมายเลขประตู วันและเวลาที่อนุญาต ข้อมูลที่ผ่านการเข้ารหัส และ ลายมือชื่อดิจิทัล โดย Jain et al. (2023) และ Guo et al. (2024) อธิบายว่า QR code สามารถสร้างด้วย

ซอฟต์แวร์ เช่น Python และนำข้อมูลประจำตัวหรือหมายเลขระบบของผู้ใช้ไปเข้ารหัสเป็นภาพสำหรับใช้ตรวจสอบสิทธิ์ได้ อย่างไรก็ตาม สำหรับระบบจริงไม่ควรบันทึกชื่อ รหัสผ่าน หรือข้อมูลสำคัญเป็นข้อความธรรมดาโดยตรง ควรใช้โทเคนหรือข้อมูลที่ผ่านการเข้ารหัสแทน

4.4.2 สถาปัตยกรรมของระบบ QR Code Door Lock

ระบบล็อกประตูด้วย QR code โดยทั่วไปประกอบด้วย 6 ส่วนสำคัญ ดังรูปที่ 4.23



รูปที่ 4.23 องค์ประกอบของระบบ QR Code Door Lock

1) อุปกรณ์แสดง QR code

ผู้ใช้งานสามารถแสดง QR code ผ่านสมาร์ตโฟน แท็บเล็ต บัตรพิมพ์ หรือเอกสารอิเล็กทรอนิกส์ QR code อาจเป็นแบบคงที่หรือแบบเปลี่ยนค่าได้ตามเวลา

1.1) Static QR code มีข้อมูลเดิมทุกครั้ง เหมาะกับระบบพื้นฐาน แต่เสี่ยงต่อการคัดลอก

1.2) Dynamic QR code เปลี่ยนค่าตามเวลา ผู้ใช้ หรือธุรกรรม เหมาะกับระบบที่ต้องการความปลอดภัยสูงกว่า

2) เครื่องอ่าน QR code

เครื่องอ่านทำหน้าที่จับภาพ ตรวจหาตำแหน่ง และถอดรหัสข้อมูล เครื่องอ่านอาจเป็นกล้องเว็บแคม กล้องของสมาร์ตโฟน เครื่องสแกนบาร์โค้ดแบบสองมิติ หรือโมดูลกล้องที่เชื่อมต่อกับไมโครคอนโทรลเลอร์หรือคอมพิวเตอร์ ในระบบของ Adedoyin and Olukoya (2024) เครื่องอ่าน QR code รับข้อมูลจากหน้าจอสมาร์ตโฟน แล้วส่งข้อมูลที่ถอดรหัสแล้วไปยัง ESP8266 เพื่อประมวลผลและตรวจสอบกับเซิร์ฟเวอร์

3) หน่วยประมวลผลหรือไมโครคอนโทรลเลอร์

หน่วยประมวลผลทำหน้าที่ควบคุมการทำงานทั้งหมดของระบบ เช่น รับข้อมูลจากเครื่องอ่าน ตรวจสอบรูปแบบข้อมูล ส่งข้อมูลไปยังฐานข้อมูล ประมวลผลผลการอนุญาต สั่งรีเลย์ มอสเฟต หรือเซอร์โวมอเตอร์ แสดงสถานะผ่านจอ LCD หรือ LED และ บันทึกเหตุการณ์เข้าออก โดยESP8266 และ Arduino Uno เป็นหน่วยควบคุม โดย ESP8266 เหมาะกับระบบที่ต้องเชื่อมต่อ Wi-Fi และเซิร์ฟเวอร์ ส่วน Arduino Uno เหมาะกับระบบต้นแบบที่ตรวจสอบ UID ภายในระบบและควบคุมเซอร์โวมอเตอร์โดยตรง (Adedoyin & Olukoya, 2024; Jain et al., 2021; Jain et al., 2023; Guo et al., 2024)

4) ฐานข้อมูลและเซิร์ฟเวอร์

ฐานข้อมูลใช้จัดเก็บข้อมูลของผู้ใช้งานและสิทธิ์เข้าใช้ เช่น รหัสผู้ใช้งาน สถานะบัญชี ประตูที่ได้รับอนุญาต ช่วงเวลาที่อนุญาต ประวัติการเข้าออก สถานะการใช้ QR code หรือวันหมดอายุของสิทธิ์ โดยระบบแบบออนไลน์จะส่งข้อมูลจาก QR code ไปยังเซิร์ฟเวอร์เพื่อตรวจสอบแบบเวลาจริง ส่วนระบบแบบออฟไลน์อาจเก็บข้อมูลไว้ในหน่วยความจำของอุปกรณ์ แต่การปรับปรุงสิทธิ์และการเพิกถอนสิทธิ์จะทำได้ยากกว่า

5) วงจรขับกลไกล็อก

ไมโครคอนโทรลเลอร์ไม่สามารถขับกลอนไฟฟ้าที่ใช้กระแสสูงได้โดยตรง จึงต้องใช้วงจรตัวกลาง เช่น รีเลย์ ทรานซิสเตอร์ มอสเฟต มอเตอร์ไดรเวอร์ หรือชุดควบคุมกลอนไฟฟ้า ซึ่งวงจรนี้ทำหน้าที่รับสัญญาณควบคุมแรงดันต่ำ แล้วสวิตช์แหล่งจ่ายไฟให้กลไกล็อก

6) กลไกล็อกประตู

กลไกล็อกที่สามารถใช้ร่วมกับ QR code door lock ได้แก่ กลไกล็อกประตูที่ใช้ในระบบควบคุมการเข้าออก ได้แก่ กลอนไฟฟ้าแบบโซลินอยด์ (solenoid lock), ชุดรับกลอนไฟฟ้า (electric strike), กลอนไฟฟ้าแบบแม่เหล็กไฟฟ้า (electromagnetic lock), กลอนไฟฟ้าแบบกลไกไฟฟ้า (electromechanical lock), เซอร์โวมอเตอร์ (servo motor) และ กลอนเดดโบลต์แบบใช้มอเตอร์ (motorized deadbolt)

4.4.3 หลักการทำงานของระบบ QR Code Door Lock

กระบวนการทำงานของ QR code door lock แบ่งออกเป็นขั้นตอนได้ 9 ขั้นตอนดังนี้

1) การลงทะเบียนผู้ใช้งาน โดยผู้ดูแลระบบบันทึกข้อมูลของผู้ใช้งานลงในฐานข้อมูล เช่น ชื่อ รหัสประจำตัว ประเภทผู้ใช้งาน ประตูที่ได้รับสิทธิ์ และช่วงเวลาที่สามารถเข้าใช้งานได้

2) การสร้าง QR code ระบบจะนำข้อมูลที่จำเป็นมาสร้าง QR code อาจใช้เพียง UID หรือใช้โทเคนที่มีข้อมูลเวลาและลายมือชื่อดิจิทัลเพื่อเพิ่มความปลอดภัย

3) การนำเสนอ QR code ผู้ใช้งานแสดง QR code ต่อหน้าเครื่องอ่านบริเวณประตู ระบบจะตรวจจับและถอดรหัสข้อมูล

4) การส่งข้อมูลไปยังหน่วยควบคุม โดยเครื่องอ่านส่งข้อมูลที่ถอดรหัสแล้วไปยัง Arduino, ESP8266 หรือคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวควบคุม

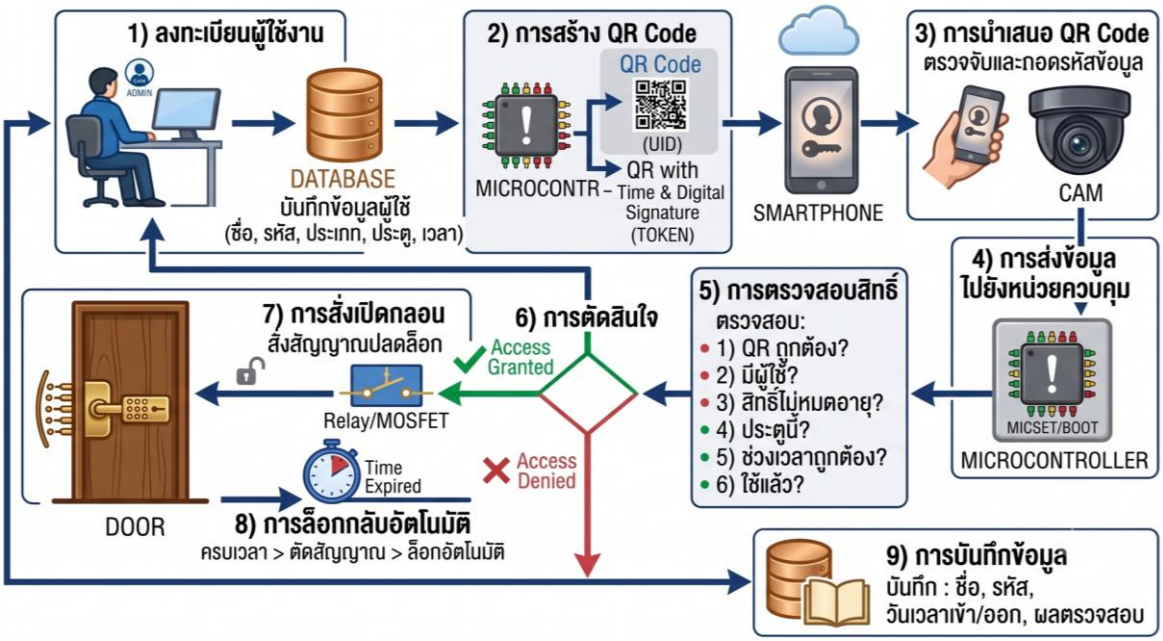
5) การตรวจสอบสิทธิ์ ดำเนินการโดยหน่วยควบคุมหรือเซิร์ฟเวอร์ตรวจสอบว่า QR code ถูกต้องหรือไม่ ผู้ใช้งานมีอยู่ในฐานข้อมูลหรือไม่ สิทธิ์ยังไม่หมดอายุหรือไม่ ผู้ใช้งานมีสิทธิ์เข้าประตูนี้หรือไม่ อยู่ในช่วงเวลาที่กำหนดหรือไม่ หรือ QR code ถูกใช้ไปแล้วหรือไม่

6) การตัดสินใจ หากข้อมูลถูกต้อง ระบบจะกำหนดสถานะเป็น access granted หากข้อมูลไม่ถูกต้อง ระบบจะกำหนดสถานะเป็น access denied

7) การสั่งเปิดกลอน เมื่อได้รับอนุญาต ไมโครคอนโทรลเลอร์จะส่งสัญญาณไปยังรีเลย์ มอสเฟต หรือเซอร์โวมอเตอร์ เพื่อปลดล็อกประตูชั่วระยะเวลาหนึ่ง

8) การล็อกกลับอัตโนมัติ เมื่อครบเวลาที่กำหนด ระบบจะตัดสัญญาณควบคุมและกลับเข้าสู่สถานะล็อกโดยอัตโนมัติ

9) การบันทึกข้อมูล ระบบบันทึกชื่อ รหัสผู้ใช้ วัน เวลาเข้า เวลาออก และผลการตรวจสอบลงในฐานข้อมูล เพื่อใช้ตรวจสอบย้อนหลังหรือวิเคราะห์การใช้งาน



รูปที่ 4.24 หลักการทำงานของระบบ QR Code Door Lock

ลำดับการทำงานดังกล่าวสอดคล้องกับแผนผังของ Jain et al. (2023) ซึ่งเริ่มจากการอ่าน QR code ตรวจสอบความถูกต้อง หมุนเซอร์โวมอเตอร์เพื่อเปิดประตู รอช่วงเวลาหนึ่ง แล้วหมุนกลับเพื่อปิดประตู นอกจากนี้ ระบบของ Adedoyin and Olukoya (2024) ยังเพิ่มการตรวจสอบ UID ผ่านเซิร์ฟเวอร์และแสดงผลสถานะผ่านจอ LCD ก่อนควบคุมรีเลย์และ solenoid lock

4.4.4 แบบจำลองการตรวจสอบสิทธิ์

แบบจำลองทางคณิตศาสตร์ที่ใช้อธิบายการทำงานหลักของระบบประกอบด้วย การสร้างรหัสคิวอาร์ (QR code generation) การเข้ารหัสข้อมูล (encryption) การตรวจสอบสิทธิ์การเข้าใช้งาน (access verification) และ การคำนวณเวลาตอบสนองของระบบ (response time calculation) (Adedoyin & Olukoya, 2024) ดังรายละเอียดต่อไปนี้

1) รหัสคิวอาร์ (QR code) เป็นรหัสแบบสองมิติที่ใช้แทนข้อมูลรับรองสิทธิ์ในการเข้าใช้งาน โดยข้อมูลจะถูกเข้ารหัสให้อยู่ในรูปของเมทริกซ์ที่ประกอบด้วยช่องสี่เหลี่ยมสีดำและสีขาว กระบวนการสร้างรหัสคิวอาร์สามารถเขียนในรูปสมการได้ดังนี้

$$Q(x,y) = f(d_1,d_2,\ldots,d_n) \tag{4.9}$$

โดยที่ $Q(x,y)$ คือ เมทริกซ์ของรหัสคิวอาร์ที่มีขนาด $x \times y$, $f(d_1,d_2,\ldots,d_n)$ คือ ฟังก์ชันการเข้ารหัสข้อมูลที่ใช้สร้างรหัสคิวอาร์จากข้อมูลผู้ใช้งาน, และ $d_1,d_2,\ldots,d_n$ คือ ชุดข้อมูลที่ใช้ในการสร้างรหัสคิวอาร์ เช่น หมายเลขประจำตัวผู้ใช้งาน ข้อมูลสิทธิ์การเข้าใช้งาน หรือข้อมูลที่ผ่านการเข้ารหัสแล้ว

ฟังก์ชันดังกล่าวทำหน้าที่แปลงข้อมูลดิจิทัลให้อยู่ในรูปของเมทริกซ์ที่ประกอบด้วยเซลล์สีดำและสีขาวตามมาตรฐานของ QR code

2) อัลกอริทึมการเข้ารหัสข้อมูล (Encryption Algorithm)

เพื่อเพิ่มความมั่นคงปลอดภัยของระบบ ข้อมูลรับรองสิทธิ์ที่บรรจุอยู่ภายใน QR code ควรผ่านกระบวนการเข้ารหัสก่อนนำไปใช้งาน โดยกระบวนการเข้ารหัสสามารถเขียนได้ดังนี้

$$E_k(M) = C \tag{4.10}$$

โดยที่ M คือ ข้อมูลต้นฉบับ (plaintext) หรือข้อมูลที่ต้องการบันทึกลงใน QR code, $E_k(\cdot)$ คือ ฟังก์ชันการเข้ารหัสโดยใช้กุญแจเข้ารหัส k, และ C คือ ข้อมูลรหัสลับ (ciphertext) ที่ได้จากกระบวนการเข้ารหัส

เมื่อระบบได้รับข้อมูลจาก QR code จะต้องทำการถอดรหัสก่อนตรวจสอบสิทธิ์ ซึ่งสามารถเขียนได้เป็น

$$D_k(C) = M \tag{4.11}$$

โดยที่ $D_k(C)$ คือ ฟังก์ชันการถอดรหัสที่ใช้กุญแจ k, C คือ ข้อมูลที่ถูกเข้ารหัส , และ M คือ ข้อมูลต้นฉบับที่ได้หลังจากการถอดรหัส

กระบวนการเข้ารหัสและถอดรหัสช่วยป้องกันการดักฟัง การปลอมแปลง และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3) การตรวจสอบสิทธิ์การเข้าใช้งาน (Access Verification)

เมื่อเครื่องอ่านสแกน QR code สำเร็จ ระบบจะนำข้อมูลที่ถอดรหัสแล้วไปเปรียบเทียบกับข้อมูลสิทธิ์ที่จัดเก็บไว้ในฐานข้อมูล การตรวจสอบสามารถอธิบายได้ด้วยฟังก์ชันดังนี้

$$V(A,B) = \begin{cases} 1, & \text{เมื่อ } A=B \\ 0, & \text{เมื่อ } A \neq B \end{cases} \tag{4.12}$$

โดยที่ A คือ ข้อมูลจาก QR code หลังผ่านกระบวนการถอดรหัส, B คือ ข้อมูลสิทธิ์การเข้าใช้งานที่จัดเก็บอยู่ในฐานข้อมูล, $V(A,B)$ คือ ฟังก์ชันตรวจสอบสิทธิ์ เมื่อ $V(A,B) = 1$ หมายถึง ข้อมูลตรงกัน และอนุญาตให้เข้าใช้งาน (grant access) และ $V(A,B) = 0$ หมายถึง ข้อมูลไม่ตรงกัน และปฏิเสธการเข้าใช้งาน (deny access)

ในระบบจริง นอกจากการเปรียบเทียบข้อมูลแล้ว ยังควรตรวจสอบเงื่อนไขอื่นร่วมด้วย เช่น อายุการใช้งานของ QR code สิทธิ์ของผู้ใช้งาน ช่วงเวลาที่อนุญาต และสถานะการเพิกถอนสิทธิ์ เพื่อเพิ่มระดับความมั่นคงปลอดภัยของระบบ

4) การคำนวณเวลาตอบสนองของระบบ (Response Time Calculation)

เวลาตอบสนองของระบบ (T_{total}) หมายถึง ระยะเวลาตั้งแต่เริ่มสแกน QR code จนกระทั่งระบบอนุญาตหรือปฏิเสธการเข้าใช้งาน โดยประกอบด้วยเวลาของแต่ละกระบวนการ ได้แก่ เวลาที่ใช้ในการสแกน QR code (T_{scan}), เวลาที่ใช้ในการถอดรหัสข้อมูล (T_{dec}), เวลาที่ใช้ในการตรวจสอบสิทธิ์ (T_{ver}), และ เวลาที่ใช้ในการสั่งงานกลอนไฟฟ้า (T_{lock}) ดังนั้น เวลาตอบสนองรวมของระบบสามารถคำนวณได้จาก

$$T_{total} = T_{scan} + T_{dec} + T_{ver} + T_{lock} \tag{4.13}$$

โดยที่ T_{total} คือ เวลาตอบสนองรวมของระบบ, T_{scan} คือ เวลาที่ใช้ในการอ่าน QR Code, T_{dec}คือ เวลาที่ใช้ในการถอดรหัสข้อมูล, T_{ver}คือ เวลาที่ใช้ในการตรวจสอบสิทธิ์กับฐานข้อมูล, T_{lock}คือ เวลาที่ใช้ในการสั่งเปิดหรือปิดกลอนไฟฟ้า

ค่าของ T_{total} เป็นตัวชี้วัดประสิทธิภาพของระบบ โดยยิ่งมีค่าน้อย แสดงว่าระบบสามารถตอบสนองต่อผู้ใช้งานได้รวดเร็ว ส่งผลให้ผู้ใช้ได้รับประสบการณ์การใช้งานที่ดี และลดเวลารอคอยในการผ่านเข้า–ออกพื้นที่ควบคุม

4.4.5 กลไกการทำงานของระบบล็อกประตูไฟฟ้า

1) การใช้เซอร์โวมอเตอร์

เซอร์โวมอเตอร์เหมาะสำหรับระบบต้นแบบหรือประตูขนาดเล็ก โดยควบคุมมุมหมุนเพื่อเลื่อนกลอนประตู เมื่อ QR code ถูกต้อง เซอร์โวมอเตอร์หมุนไปยังตำแหน่งเปิด และหมุนกลับไปยังตำแหน่งปิดเมื่อครบเวลาที่กำหนด

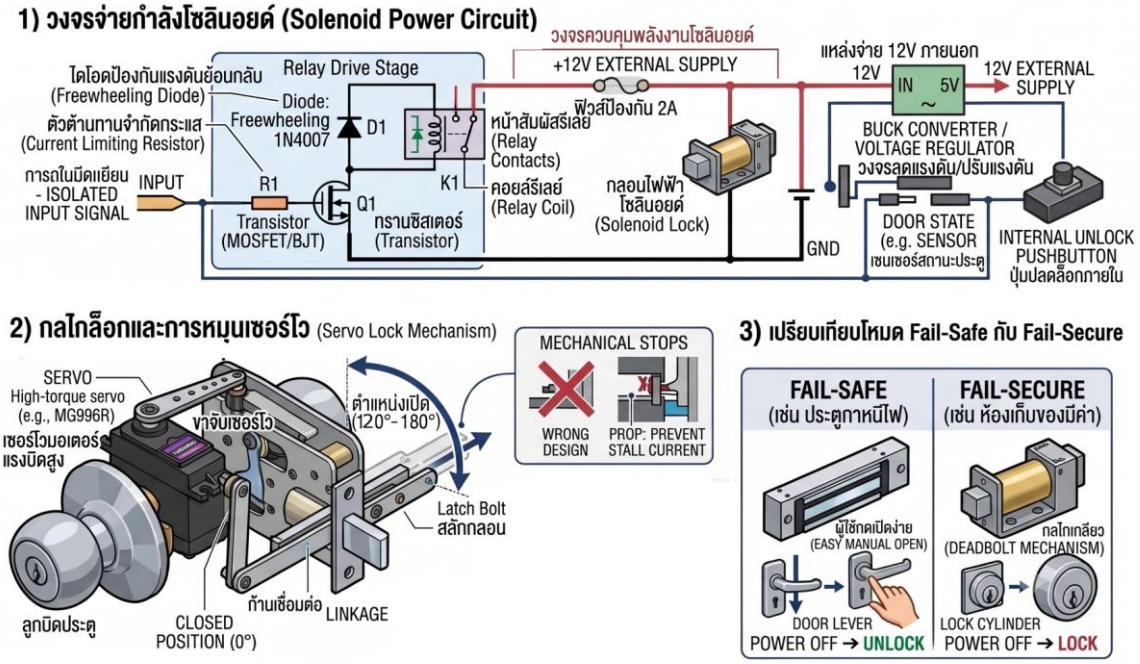
ข้อควรพิจารณา ได้แก่ ใช้แหล่งจ่ายไฟแยกจาก Arduino ต่อกราวด์ร่วมกัน ไม่ควรจ่ายไฟเซอร์โวมอเตอร์จากขา 5 V ของบอร์ดโดยตรงในกรณีที่กระแสสูง ต้องออกแบบกลไกไม่ให้มอเตอร์ค้างรับแรงตลอดเวลา

2) การใช้ solenoid lock

Solenoid lock ใช้ขดลวดแม่เหล็กไฟฟ้าดึงแกนกลอนเมื่อได้รับแรงดัน เหมาะกับประตูจริงมากกว่าเซอร์โวมอเตอร์ แต่ต้องใช้กระแสสูงกว่า จึงต้องใช้รีเลย์หรือมอสเฟตเป็นวงจรขับ วงจรควรประกอบด้วย แหล่งจ่าย 12 V รีเลย์หรือมอสเฟต ไดโอดป้องกันแรงดันย้อนกลับ ฟิวส์ วงจรลดแรงดันสำหรับไมโครคอนโทรลเลอร์ ปุ่มเปิดจากภายใน เซนเซอร์ตรวจสอบสถานะประตู

3) การเลือกแบบ Fail-Safe และ Fail-Secure

Fail-safe ประตูจะปลดล็อกเมื่อไฟดับ เหมาะกับประตูหนีไฟ ส่วน fail-secure ประตูจะยังคงล็อกเมื่อไฟดับ เหมาะกับพื้นที่ที่ต้องรักษาความปลอดภัยของทรัพย์สิน Lvov and Sotnik (2024) ชี้ว่ากลอนไฟฟ้าเป็นอุปกรณ์กระทำการหลักของระบบควบคุมการเข้าออก และการเลือกชนิดของกลอนต้องพิจารณาความปลอดภัย การติดตั้ง แหล่งจ่ายไฟ และพฤติกรรมเมื่อไฟดับร่วมกัน วงจรขับและกลไกการทำงานของระบบล็อกประตูไฟฟ้า (electric door lock driving circuit and lock mechanisms) ดังนี้



รูปที่ 4.25 วงจรขับและกลไกการทำงานของระบบล็อกประตูไฟฟ้า

รูปที่ 4.25 แสดงตัวอย่างการออกแบบระบบขับกลอนไฟฟ้าสำหรับระบบควบคุมการเข้าออก ประกอบด้วย (1) วงจรขับกลอนไฟฟ้าแบบโซลินอยด์ โดยใช้ไมโครคอนโทรลเลอร์ร่วมกับวงจรขับรีเลย์ มอสเฟต ไดโอดป้องกันแรงดันย้อนกลับ (flyback diode) ฟิวส์ และตัวแปลงแรงดันไฟฟ้า (DC/DC buck converter) (2) กลไกการขับกลอนด้วยเซอร์โวมอเตอร์ผ่านชุดข้อต่อ (linkage mechanism) เพื่อควบคุมตำแหน่งล็อกและปลดล็อก และ (3) การเปรียบเทียบหลักการทำงานของกลอนไฟฟ้าแบบ fail-safe ซึ่งจะปลดล็อกเมื่อไฟฟ้าดับ และแบบ Fail-secure ซึ่งจะคงสถานะล็อกเมื่อไฟฟ้าดับ โดยการเลือกใช้กลไกขึ้นอยู่กับข้อกำหนดด้านความปลอดภัยของสถานที่และลักษณะการใช้งาน

4.4.6 การบันทึกและติดตามการเข้าออก

จุดเด่นของระบบ QR code door lock คือสามารถเชื่อมโยงการเปิดประตูกับฐานข้อมูลได้ ระบบจึงสามารถบันทึก ชื่อผู้ใช้งาน หมายเลขประจำตัว วันและเวลาเข้า วันและเวลาออก ระยะเวลาที่อยู่ภายในพื้นที่ ประตูที่ใช้งาน ผลการตรวจสอบ แม้แต่ จำนวนครั้งที่เข้าใช้ โดย Jain et al. (2023) แสดงตัวอย่างการบันทึกชื่อ หมายเลขระบบ เวลาเข้า เวลาออก และระยะเวลาที่ผู้ใช้พักอยู่ในพื้นที่ ทำให้ระบบสามารถนำไปใช้ร่วมกับระบบลงเวลาเรียน ระบบลงเวลาทำงาน หรือระบบติดตามการใช้ห้องได้

4.4.7 ความมั่นคงปลอดภัยของระบบ QR Code Door Lock

QR code เป็นเพียงตัวกลางในการนำเสนอข้อมูล ไม่ได้มีความปลอดภัยโดยตัวเอง หากใช้ QR code แบบคงที่ ผู้ไม่หวังดีสามารถถ่ายภาพ ทำสำเนา หรือส่งต่อให้บุคคลอื่นได้ ดังนั้นระบบควรมีมาตรการดังต่อไปนี้

1) ใช้ dynamic QR code ควรกำหนดให้ QR code เปลี่ยนค่าตามเวลาและมีอายุสั้น เช่น 30–60 s เพื่อป้องกันการใช้ภาพถ่ายซ้ำ

2) ใช้โทเคนแบบใช้ครั้งเดียว ระบบควรออกหมายเลขโทเคนที่สามารถใช้ได้เพียงครั้งเดียว และบันทึกสถานะหลังใช้งาน

3) เข้ารหัสข้อมูล ข้อมูลใน QR code ควรผ่านการเข้ารหัสก่อนจัดเก็บ โดยเฉพาะข้อมูลประจำตัวและสิทธิ์เข้าใช้

4) ใช้ลายมือชื่อดิจิทัล การลงลายมือชื่อดิจิทัลช่วยให้เครื่องอ่านตรวจสอบได้ว่า QR code มาจากระบบที่เชื่อถือได้และไม่ถูกแก้ไข

5) ใช้การเชื่อมต่อแบบปลอดภัย การส่งข้อมูลระหว่าง ESP8266 กับเซิร์ฟเวอร์ควรใช้ HTTPS หรือ TLS ไม่ควรส่ง UID หรือรหัสผ่านเป็นข้อความธรรมดา

6) จำกัดสิทธิ์ตามบริบท ระบบควรตรวจสอบทั้งตัวตน เวลา ประตู สถานที่ และสถานะของผู้ใช้งาน

7) ใช้หลายปัจจัย พื้นที่สำคัญควรใช้ QR code ร่วมกับ PIN ใบหน้า ลายนิ้วมือ หรือบัตรพนักงาน โดย Adedoyin and Olukoya (2024) ระบุว่าระบบ QR code ยังเสี่ยงต่อการปลอมแปลง การทำสำเนา และการใช้ข้อมูลซ้ำ จึงต้องเสริมด้วยการเข้ารหัสและกลไกตรวจสอบที่ปลอดภัย

สรุปได้ว่าระบบล็อกประตูด้วย QR code เป็นระบบควบคุมการเข้าออกที่ใช้ QR code เป็นข้อมูลรับรองสิทธิ์ร่วมกับเครื่องอ่าน หน่วยประมวลผล ฐานข้อมูล และกลไกล็อกไฟฟ้า จุดเด่นคือใช้งานสะดวก ต้นทุนไม่สูง และสามารถจัดการสิทธิ์แบบดิจิทัลได้ อย่างไรก็ตาม ความปลอดภัยของระบบขึ้นอยู่กับการออกแบบวิธีสร้าง ตรวจสอบ และยกเลิก QR code การใช้ dynamic QR code การเข้ารหัส การลงลายมือชื่อดิจิทัล และการตรวจสอบผ่านเซิร์ฟเวอร์จะช่วยลดความเสี่ยงจากการคัดลอกหรือใช้รหัสซ้ำได้ ข้อดีของระบบ QR code door โดย Lock Jain et al. (2023) ระบุว่าระบบ QR code ช่วยลดการใช้เอกสาร ลดความผิดพลาดจากมนุษย์ และสามารถนำไปใช้ติดตามนักศึกษา บุคลากร หรือผู้เข้าใช้พื้นที่ได้อย่างเป็นระบบ มีข้อดีดังนี้ ไม่ต้องใช้กุญแจทางกายภาพ ไม่ต้องพกบัตรเพิ่มเติม สร้างและยกเลิกสิทธิ์ได้รวดเร็ว ต้นทุนเครื่องอ่านและสื่อข้อมูลไม่สูง รองรับการออกสิทธิ์ชั่วคราว บันทึกเวลาเข้าออกได้ เชื่อมโยงกับฐานข้อมูลส่วนกลางได้ เหมาะกับสมาร์ตโฟน รองรับการขยายหลายประตู ประยุกต์ใช้กับระบบ IoT ได้ ส่วน ข้อจำกัดที่สำคัญ ได้แก่ QR code แบบคงที่สามารถคัดลอกได้ การอ่านขึ้นอยู่กับคุณภาพกล้อง แสง และมุม หน้าจอสมาร์ตโฟนที่แตกหรือมีความสว่างต่ำอาจอ่านยาก ระบบออนไลน์ขึ้นอยู่กับเครือข่ายและเซิร์ฟเวอร์ กล้องหรือเครื่องอ่านราคาต่ำอาจประมวลผลช้า ต้องมีแหล่งจ่ายไฟสำรอง ต้องออกแบบทางออกฉุกเฉิน ต้องคุ้มครองข้อมูลส่วนบุคคล และต้องมีวิธีเปิดประตูเมื่อระบบล้มเหลว

บรรณานุกรมบทที่ 4

ปิยะ โควินท์ทวีวัฒน์, วีระศักดิ์ ชื่นตา, สัญญา ควรคิด, วิโรจน์ บัวงาม, และหฤทัย ดิ้นสกุล. (2551). *ระบบบ่งชี้ด้วยคลื่นความถี่วิทยุ*. มหาวิทยาลัยราชภัฏนครปฐม.

ทวีศักดิ์ สุขเจริญทรัพย์, ชลดา ปานสง, และคุณากร คิดดี. (2565). ชุดบัตรคำศัพท์อิเล็กทรอนิกส์ด้วยเทคโนโลยีอาร์เอฟไอดีเพื่อแก้ปัญหาการเขียนสลับตำแหน่งคำของเด็กสมาธิสั้น. *วารสารครุศาสตร์อุตสาหกรรม*, *21*(3), 89–98.

Adedoyin, M., & Olukoya, F. (2024). Development of a smart lock system using QR code technology. *ABUAD Journal of Engineering Research and Development (AJERD)*, *7*(2), 484–492. https://doi.org/10.53982/ajerd.2024.0702.46-j.

Alrawais, A. (2020). Security issues in Near Field Communications (NFC). *International Journal of Advanced Computer Science and Applications, 11*(11). https://doi.org/10.14569/IJACSA.2020.0111176.

Atlam, H. F., Azad, M. A., Alassafi, M. O., Alshdadi, A. A., & Alenezi, A. (2020). Risk-Based Access Control Model: A Systematic Literature Review. *Future Internet*, *12*(6), 103. https://doi.org/10.3390/fi12060103.

Bhatt, I., & Vidani, J. (2024). A study on the awareness of near field communication (NFC) technology. *International Journal of Integrative Research, 2*(12), 983–998. https://doi.org/10.59890/ijir.v2i12.152.

Chang, Y., & Wang, J. (2025). Near-field communication technology (NFC): Principle analysis and intelligent life application research. *Industry Science and Engineering, 2*(1). https://doi.org/10.62381/I255107.

Coskun, V., Ozdenizci, B., & Ok, K. (2015). The survey on near field communication. *Sensors*, *15*(6), 13348-13405. https://doi.org/10.3390/s150613348

Duroc, Y. (2022). From identification to sensing: RFID is one of the key technologies in the IoT field. *Sensors*, *22*(19), 7523. https://doi.org/10.3390/s22197523.

Farhadighalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati, S., & Barata, J. (2025). A systematic review of access control models: Background, existing research, and challenges. *IEEE Access, 13*, 17777–17806. https://doi.org/10.1109/ACCESS.2025.3533145.

Finkenzeller, K. (2010). *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication* (3rd ed.). Wiley.

Guo, Z., Wang, S., Zheng, Z., & Sun, K. (2024). Printer source identification of quick response codes using residual attention network and smartphones. *Engineering Applications of Artificial Intelligence, 131*, 107822. https://doi.org/10.1016/j.engappai.2023.107822

Guo, W., & Shi, Q. (2025). Research on the application of near field communication (NFC) digital technology in metal jewelry product design. In *ICADI '24: Proceedings of the 2024 International Conference on Artificial Intelligence, Digital Media Technology and Interaction Design* (pp. 372–377). Association for Computing Machinery. https://doi.org/10.1145/3726010.3726068

Hunt, V. D., Puglia, A., & Puglia, M. (2007). *RFID: A guide to radio frequency identification*. John Wiley & Sons.

International Organization for Standardization (ISO). (2018). *International standard ISO/IEC 14443-4:2018 cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol*. https://www.iso.org/standard/73599.html.

Jain, V., Jain, Y., Dhingra, H., Saini, D., Taplamacioglu, M. C., & Saka, M. (2021). A systematic literature review on QR code detection and pre-processing. *International Journal on "Technical and Physical Problems of Engineering" (IJTPE), 13*(1), 111–119.

Jain, A., Panwar, A., Azam, M., & Khanam, R. (2023). Smart door access control system based on QR code. *International Journal of Informatics and Communication Technology, 12*(2), 171–179. https://doi.org/10.11591/ijict.v12i2.pp171-179

Lvov, A., & Sotnik, S. (2024). Analysis of electronic locks existing systems. In *Manufacturing & mechatronic systems 2024: Proceedings of the VIII International Conference* (pp. 24–27). Kharkiv National University of Radio Electronics.

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. *International Journal of Web Information Systems*, *18*(2-3), 156–180. https://doi.org/10.1108/IJWIS-04-2022-0077.

Proehl, G. (2013). *An introduction to near field communications*. Mouser Electronics. https://th.mouser.com/applications/rfid-nfc-introduction/.

Rahul, A., Krishnan, G. G., Krishnan, U. H., & Rao, S. (2015). Near field communication (NFC) technology: A survey. *International Journal on Cybernetics & Informatics*, *4*(2), 133–144. https://doi.org/10.5121/ijci.2015.4213.

Sami, A., Tian, G. Y., Marindra, A. M. J., & Song, H. (2025). A comprehensive review of passive RFID sensors for structural health monitoring: Developments, challenges,

and opportunities. *Chinese Journal of Mechanical Engineering*, *29*(100117), 1-21. https://doi.org/10.1016/j.cjme.2025.100117.

U.S. Department of Transportation, Federal Highway Administration. (2022). *Roadside safety hardware identification methods*. https://highways.dot.gov/safety/rwd/reduce-crash-severity/roadside-safety-hardware-identification-methods/appendix-standards.

Violino, B. (2005). *A summary of RFID standards*. RFID Journal. https://www.rfidjournal.com/expert-views/a-summary-of-rfid-standards/76205/.

Zhang, J., Periaswamy, S. C. G., Mao, S., & Patton, J. (2019). *Standards for passive UHF RFID*. Auburn University.

สรุปสาระสำคัญของบทที่ 4
ระบบควบคุมการเข้าออก

ระบบควบคุมการเข้าออก (Access Control System)

ระบบควบคุมการเข้าออก (Access Control System: ACS) เป็นระบบที่ใช้กำหนด ตรวจสอบ และควบคุมสิทธิ์ในการเข้าถึงพื้นที่ อาคาร ห้อง หรือทรัพยากรสารสนเทศ โดยอนุญาตให้เฉพาะผู้ที่ได้รับสิทธิ์สามารถเข้าใช้งานได้ตามเงื่อนไขที่กำหนด และปฏิเสธการเข้าถึงของผู้ที่ไม่ได้รับอนุญาต ระบบดังกล่าวมีบทบาทสำคัญต่อการรักษาความมั่นคงปลอดภัยทั้งด้านกายภาพ (physical security) และด้านสารสนเทศ (information security) ช่วยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ลดความเสี่ยงจากการรั่วไหลของข้อมูล และสนับสนุนหลักการความมั่นคงปลอดภัยสารสนเทศ (CIA triad) ได้แก่ ความลับของข้อมูล (confidentiality) ความถูกต้องของข้อมูล (integrity) และความพร้อมใช้งานของระบบ (availability) รวมทั้งสามารถบันทึกข้อมูลการเข้าออกเพื่อใช้ในการตรวจสอบย้อนหลังและการตรวจประเมินด้านความปลอดภัยได้

หลักการทำงานของระบบเริ่มจากการที่ผู้ใช้งานแสดงข้อมูลยืนยันตัวตน เช่น บัตร RFID ลายนิ้วมือ ใบหน้า หรือรหัสผ่าน จากนั้นเครื่องอ่านข้อมูลจะส่งข้อมูลไปยังชุดควบคุมเพื่อตรวจสอบกับฐานข้อมูลและนโยบายการเข้าถึง เมื่อระบบตัดสินใจอนุญาตหรือปฏิเสธการเข้าใช้งานแล้ว จะสั่งงานอุปกรณ์ควบคุม เช่น กลอนไฟฟ้าหรือประตูอัตโนมัติ พร้อมบันทึกข้อมูลการเข้าออกไว้ในฐานข้อมูล

องค์ประกอบพื้นฐานของระบบควบคุมการเข้าออกประกอบด้วย 5 ส่วน ได้แก่ ผู้ใช้งาน (subject) ทรัพยากร (object) การดำเนินการ (action) สิทธิ์การเข้าถึง (permission) และนโยบายการเข้าถึง (access policy) ซึ่งทำงานร่วมกันเพื่อให้ระบบสามารถตัดสินใจได้อย่างถูกต้องและปลอดภัย นอกจากนี้ยังต้องเข้าใจความแตกต่างระหว่าง authentication ซึ่งเป็นการพิสูจน์ตัวตน authorization ซึ่งเป็นการตรวจสอบสิทธิ์ของผู้ใช้งาน และ access Control ซึ่งเป็นการบังคับใช้นโยบายเพื่ออนุญาตหรือปฏิเสธการเข้าถึงทรัพยากร

ระบบควบคุมการเข้าออกสมัยใหม่มีความสามารถรองรับการพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) การกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control: RBAC) การกำหนดสิทธิ์ตามคุณลักษณะ (Attribute-Based Access Control: ABAC) และการตัดสินใจตามบริบท (context-aware access control) อีกทั้งยังสามารถบูรณาการกับระบบกล้องวงจรปิด (CCTV) ระบบแจ้งเหตุบุกรุก ระบบแจ้งเหตุเพลิงไหม้ ระบบบริหารอาคารอัจฉริยะ (BMS) และระบบ Internet of Things (IoT) เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยแบบองค์รวม ปัจจุบันแนวโน้มของระบบมุ่งสู่การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) การวิเคราะห์พฤติกรรมผู้ใช้งาน และการควบคุมการเข้าออกตามระดับความเสี่ยง (risk-based access control) เพื่อให้การตัดสินใจด้านความปลอดภัยมีความแม่นยำ ยืดหยุ่น และเหมาะสมกับสถานการณ์มากยิ่งขึ้น

การศึกษาเทคโนโลยี RFID การเชื่อมต่อกับไมโครคอนโทรลเลอร์ การประยุกต์ใช้ควบคุมการเข้าออก และการทำงานร่วมกับระบบ IoT เพื่อพัฒนาระบบรักษาความปลอดภัยอัจฉริยะ

อาร์เอฟไอดีเบื้องต้น (RFID Basics)

RFID (Radio Frequency Identification) คือ เทคโนโลยีระบุและติดตามวัตถุหรือบุคคลด้วยคลื่นวิทยุ โดยไม่ต้องสัมผัสโดยตรง มาตรฐาน RFID ที่นิยมใช้งาน **มาตรฐาน** ISO 14443 type A, ISO 15693, EPC global, Electronic Article Surveillance (EAS) RFID ซึ่งมาตรฐาน ISO14443 type A เป็นมาตรฐานที่นิยมใช้ในบัตรนักศึกษา บัตรพนักงาน และระบบควบคุมการเข้าออกประตู โดยองค์ประกอบของ RFID ประกอบด้วย 4 ส่วน ดังนี้

1) RFID tag (แท็ก) ใช้เก็บข้อมูลประจำตัว

2) RFID reader (เครื่องอ่าน) ใช้อ่านข้อมูลจากแท็ก

3) Antenna (เสาอากาศ) ใช้รับส่งสัญญาณคลื่นวิทยุ

4) Database/controller ใช้จัดเก็บและประมวลผลข้อมูล

ประเภทของ RFID ได้แก่ passive tag (ไม่มีแบตเตอรี่) active tag (มีแบตเตอรี่) และ semi-passive tag โดยมีหลักการทำงาน ดังนี้

1) Reader ทำหน้าที่ ส่งคลื่นวิทยุ

2) Tag ทำหน้าที่ รับพลังงานและส่งข้อมูลกลับ

3) Reader ทำหน้าที่อ่านข้อมูล

4) ระบบประมวลผลและแสดงผล

การเชื่อมต่อระบบ RFID กับไมโครคอนโทรลเลอร์เบื้องต้น

โมดูล RFID RC522 เป็นโมดูลอ่านบัตร RFID ที่นิยมใช้ร่วมกับ Arduino และ NodeMCU ซึ่งการเชื่อมต่อ RC522 กับ Arduino เชื่อมต่อผ่านระบบสื่อสารแบบ SPI เช่น ขา SDA, SCK, MOSI, MISO, RST, VCC, และ GND

การติดตั้งไลบรารี MFRC522 ใช้สำหรับควบคุมและอ่านข้อมูลจากโมดูล RC522 ผ่าน Arduino IDE โดยมีการตรวจสอบการเชื่อมต่อ การอ่าน UID ของบัตร RFID และการตรวจสอบการสื่อสารระหว่าง Reader และไมโครคอนโทรลเลอร์

การประยุกต์ใช้งาน ใช้ RFID Tag ควบคุมการเปิด-ปิดไฟ การเปิด-ปิดอุปกรณ์ไฟฟ้า หรือควบคุมการเข้าถึงระบบต่าง ๆ

ระบบควบคุมการเข้าออกประตูด้วย RFID

ระบบควบคุมประตูด้วย Arduino หลักการทำงาน

1) แตะบัตร RFID

2) Reader อ่าน UID

3) Arduino เปรียบเทียบข้อมูล

4) หากตรงกับฐานข้อมูล จะปลดล็อกประตู โดยสั่งงานรีเลย์หรือเซอร์โวมอเตอร์

5) หากไม่ตรง ไม่อนุญาตให้เข้า

ระบบควบคุมประตูด้วย NodeMCU ESP8266 เพิ่มเติมความสามารถด้านเครือข่าย โดยการเชื่อมต่อ Wi-Fi มีการส่งข้อมูลขึ้น cloud บันทึกประวัติการเข้าออก แจ้งเตือนผ่านอินเทอร์เน็ต เพื่อประโยชน์ในด้านเพิ่มความปลอดภัย ลดการใช้กุญแจ ตรวจสอบผู้เข้าใช้งานได้

เทคโนโลยีการสื่อสารระยะใกล้ (Near Field Communication: NFC)

เทคโนโลยีการสื่อสารระยะใกล้ (Near Field Communication: NFC) เป็นเทคโนโลยีการสื่อสารข้อมูลแบบไร้สายระยะสั้นที่พัฒนาต่อยอดจากเทคโนโลยี RFID ความถี่สูง (high frequency RFID) โดยทำงานที่ความถี่ 13.56 MHz ตามมาตรฐาน ISO/IEC 14443, ISO/IEC 18092 (NFCIP-1) และ ISO/IEC 21481 (NFCIP-2) มีระยะการสื่อสารประมาณไม่เกิน 10 cm และมีอัตราการรับส่งข้อมูลสูงสุด 424 kbps จุดเด่นของ NFC คือการเชื่อมต่อที่รวดเร็ว ปลอดภัย และใช้งานง่าย เพียงนำอุปกรณ์เข้าใกล้กันก็สามารถแลกเปลี่ยนข้อมูลได้โดยไม่ต้องจับคู่ (pairing) เหมือนเทคโนโลยี Bluetooth

หลักการทำงานของ NFC อาศัยการเหนี่ยวนำสนามแม่เหล็กไฟฟ้า (electromagnetic induction) ระหว่างอุปกรณ์สองตัวที่อยู่ในระยะใกล้ โดยมีอุปกรณ์หนึ่งทำหน้าที่เป็น initiator สร้างสนามแม่เหล็กไฟฟ้า และอีกอุปกรณ์หนึ่งทำหน้าที่เป็น target รับและตอบสนองต่อสัญญาณ การสื่อสารสามารถทำงานได้ทั้งในรูปแบบ active mode ซึ่งทั้งสองอุปกรณ์สร้างสนามแม่เหล็กของตนเอง และ passive mode ซึ่งมีเพียงอุปกรณ์ Initiator ที่สร้างสนามแม่เหล็ก ส่วน target ใช้พลังงานจากสนามแม่เหล็กดังกล่าวในการสื่อสาร

NFC รองรับการทำงานหลัก 3 รูปแบบ ได้แก่ reader/writer mode สำหรับอ่านหรือเขียนข้อมูลบนแท็ก NFC, card emulation mode สำหรับจำลองสมาร์ตการ์ด เช่น บัตรโดยสาร บัตรพนักงาน หรือระบบชำระเงินผ่านโทรศัพท์มือถือ และ peer-to-peer mode สำหรับแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์สองเครื่อง เช่น การส่งข้อมูลติดต่อ รูปภาพ หรือการตั้งค่าการเชื่อมต่ออัตโนมัติ

เนื่องจาก NFC มีระยะการสื่อสารสั้น จึงมีความปลอดภัยสูงกว่าการสื่อสารไร้สายหลายประเภท ลดโอกาสการดักฟังข้อมูล และสามารถเสริมความปลอดภัยด้วยเทคนิคการเข้ารหัสข้อมูล (encryption) การพิสูจน์ตัวตน (authentication) และการจัดการกุญแจเข้ารหัส (cryptographic key management) ทำให้เหมาะสำหรับงานที่ต้องการความมั่นคงปลอดภัยสูง เช่น ระบบควบคุมการเข้าออก การชำระเงินอิเล็กทรอนิกส์ และการพิสูจน์ตัวตน

ปัจจุบัน NFC ถูกนำมาใช้งานอย่างแพร่หลายในหลายด้าน ได้แก่ ระบบควบคุมการเข้าออกอาคาร (access control system) การชำระเงินแบบไร้สัมผัส (contactless payment) บัตรโดยสารสาธารณะ ระบบลงเวลาทำงาน การยืนยันตัวตนในสมาร์ตโฟน การจับคู่กับอุปกรณ์ Internet of Things (IoT) และระบบสมาร์ตโฮม (smart home) ซึ่งช่วยเพิ่มความสะดวก รวดเร็ว และความปลอดภัยในการใช้งาน

คิวอาร์โค้ด (Quick Response Code: QR Code)

คิวอาร์โค้ด (Quick Response Code: QR Code) เป็นบาร์โค้ดสองมิติ (two-dimensional barcode) ที่พัฒนาโดยบริษัท Denso Wave ประเทศญี่ปุ่น ในปี พ.ศ. 2537 เพื่อใช้ติดตามชิ้นส่วนในสายการผลิตอุตสาหกรรมยานยนต์ ต่อมาได้ถูกนำมาประยุกต์ใช้อย่างแพร่หลายในด้านการจัดเก็บข้อมูล การระบุตัวตน การชำระเงิน การเข้าถึงเว็บไซต์ และระบบควบคุมการเข้าออก เนื่องจากสามารถจัดเก็บข้อมูลได้มากกว่าบาร์โค้ดแบบหนึ่งมิติ (one-dimensional barcode) และอ่านข้อมูลได้อย่างรวดเร็วจากทุกทิศทาง

โครงสร้างของ QR code ประกอบด้วยส่วนสำคัญ ได้แก่ ตำแหน่งกำหนดทิศทาง (finder pattern) รูปแบบกำหนดแนว (alignment pattern) เส้นกำหนดเวลา (timing pattern) ข้อมูลเวอร์ชัน (version information) ข้อมูลรูปแบบ (format information) พื้นที่จัดเก็บข้อมูล (data area) และข้อมูลสำหรับการตรวจสอบและแก้ไขข้อผิดพลาด (error correction code) ซึ่งช่วยให้สามารถอ่านข้อมูลได้แม้ว่าสัญลักษณ์จะมีรอยเปื้อน เสียหาย หรือถูกปิดบังบางส่วน

QR code รองรับข้อมูลได้หลายประเภท เช่น ข้อความ ตัวเลข ตัวอักษรและตัวเลข (Alphanumeric) ที่อยู่เว็บไซต์ (URL) ข้อมูลติดต่อ (vCard) พิกัดภูมิศาสตร์ (GPS coordinates) อีเมล และข้อมูลสำหรับการเชื่อมต่อเครือข่ายหรือระบบต่าง ๆ โดยใช้มาตรฐาน ISO/IEC 18004 และอัลกอริทึม reed–Solomon error correction ในการตรวจจับและแก้ไขข้อผิดพลาด ทำให้สามารถกู้คืนข้อมูลได้แม้ QR code จะเสียหายบางส่วน

หลักการทำงานของ QR code เริ่มจากการสร้างข้อมูลให้อยู่ในรูปของสัญลักษณ์สองมิติ จากนั้นผู้ใช้งานใช้กล้องหรือเครื่องอ่าน QR code สแกนภาพ สัญลักษณ์จะถูกถอดรหัส (decode) เพื่อแปลงกลับเป็นข้อมูลดิจิทัล และส่งต่อไปยังระบบหรือแอปพลิเคชันที่เกี่ยวข้อง เช่น เปิดเว็บไซต์ ยืนยันตัวตน หรือปลดล็อกประตูอัตโนมัติ

ในระบบควบคุมการเข้าออก (access control system) QR code นิยมใช้เป็นข้อมูลยืนยันตัวตนแบบดิจิทัล โดยระบบจะสร้าง QR code ที่มีข้อมูลผู้ใช้งาน สิทธิ์การเข้าใช้งาน หรือโทเค็น (token) ที่เข้ารหัสไว้ เมื่อผู้ใช้งานสแกน QR code ผ่านเครื่องอ่าน ระบบจะตรวจสอบข้อมูลกับฐานข้อมูลหรือเซิร์ฟเวอร์ หากข้อมูลถูกต้องและอยู่ภายใต้เงื่อนไขที่กำหนด ระบบจะอนุญาตให้เข้าใช้งานหรือปลดล็อกประตู พร้อมบันทึกข้อมูลการเข้าออกเพื่อใช้ในการตรวจสอบย้อนหลัง

ข้อดีของ QR code ได้แก่ สามารถจัดเก็บข้อมูลได้มาก อ่านข้อมูลได้รวดเร็วจากทุกมุมมอง มีต้นทุนการสร้างต่ำ รองรับการใช้งานผ่านสมาร์ตโฟนทั่วไป และสามารถกำหนดวันหมดอายุหรือใช้งานเพียงครั้งเดียว (one-time QR code) เพื่อเพิ่มความปลอดภัย อย่างไรก็ตาม หากไม่มีการเข้ารหัสข้อมูลหรือไม่มีระบบตรวจสอบความถูกต้อง อาจเสี่ยงต่อการคัดลอกหรือปลอมแปลง QR code ได้ ดังนั้นระบบสมัยใหม่จึงมักใช้การเข้ารหัส (encryption) ลายเซ็นดิจิทัล (digital signature) และโทเค็นแบบใช้ครั้งเดียว (one-time token) เพื่อเพิ่มความมั่นคงปลอดภัย

แบบฝึกหัดท้ายบทที่ 4
ระบบควบคุมการเข้าออก

<u>คำชี้แจง</u> จงเลือกคำตอบที่ถูกต้องที่สุดเพียงคำตอบเดียวแล้วทำเครื่องหมาย X ลงในข้อสอบ

1. RFID ย่อมาจากข้อใด
   ก. Radio Frequency Identification ข. Radio Function Information
   ค. Rapid Frequency Identification ง. Remote Frequency Information
2. RFID เป็นเทคโนโลยีที่ใช้สิ่งใดในการสื่อสาร
   ก. แสงอินฟราเรด ข. คลื่นวิทยุ
   ค. สายไฟฟ้า ง. คลื่นเสียง
3. ข้อใดไม่ใช่องค์ประกอบของระบบ RFID
   ก. RFID Tag ข. RFID Reader
   ค. Antenna ง. Projector
4. RFID Tag มีหน้าที่ใด
   ก. แสดงผลข้อมูล ข. เก็บข้อมูลประจำตัว
   ค. ส่งสัญญาณอินเทอร์เน็ต ง. ประมวลผลข้อมูล
5. RFID Reader ทำหน้าที่ใด
   ก. อ่านข้อมูลจาก Tag ข. เก็บข้อมูลในฐานข้อมูล
   ค. แสดงภาพจากกล้อง ง. ควบคุมเครือข่าย
6. เสาอากาศ (Antenna) ในระบบ RFID มีหน้าที่ใด
   ก. รับส่งสัญญาณคลื่นวิทยุ ข. จ่ายไฟฟ้า
   ค. บันทึกข้อมูล ง. ควบคุมระบบ
7. มาตรฐาน RFID ที่นิยมใช้กับบัตรพนักงานคือข้อใด
   ก. ISO 14443 Type A ข. ISO 9001
   ค. IEEE 802.11 ง. RS-232
8. RFID แบบใดไม่มีแบตเตอรี่
   ก. Active Tag ข. Passive Tag
   ค. Semi-passive Tag ง. Smart Tag
9. RFID แบบใดมีแบตเตอรี่ในตัว
   ก. Passive Tag ข. Active Tag
   ค. Mini Tag ง. Nano Tag
10. ข้อใดคือขั้นตอนแรกของการทำงาน RFID
   ก. Reader อ่านข้อมูล ข. Tag ส่งข้อมูล
   ค. Reader ส่งคลื่นวิทยุ ง. ฐานข้อมูลบันทึกข้อมูล

11. เมื่อ Tag ได้รับพลังงานจะทำสิ่งใด

ก. ส่งข้อมูลกลับไปยัง Reader ข. ปิดการทำงาน

ค. ลบข้อมูล ง. รีเซ็ตระบบ

12. ข้อใดเป็นข้อดีของ RFID

ก. ไม่ต้องสัมผัสโดยตรง ข. ใช้งานได้เฉพาะกลางวัน

ค. ใช้สายเชื่อมต่อเท่านั้น ง. ต้องเสียบอุปกรณ์ทุกครั้ง

13. ข้อใดเป็นตัวอย่างการใช้งาน RFID

ก. ระบบเปิดประตู ข. ระบบลำโพง

ค. ระบบเครื่องปรับอากาศ ง. เครื่องพิมพ์

14. RFID ใช้สำหรับงานใดมากที่สุด

ก. ระบุตัวตนและติดตามวัตถุ ข. ตกแต่งภาพ

ค. พิมพ์เอกสาร ง. สร้างเว็บไซต์

15. Active Tag เหมาะกับงานลักษณะใด

ก. ระยะอ่านไกล ข. ระยะอ่านสั้นมาก

ค. ไม่มีพลังงาน ง. ใช้ครั้งเดียว

16. RFID Reader ติดต่อกับ Tag ผ่านอะไร

ก. Bluetooth เท่านั้น ข. คลื่นวิทยุ

ค. สายสัญญาณเครือข่าย ง. สาย USB

17. RFID ประเภทใดได้รับพลังงานจาก Reader

ก. Passive Tag ข. Active Tag

ค. Semi-active ง. Battery Tag

18. ระบบ RFID ช่วยลดปัญหาใด

ก. การใช้กุญแจแบบเดิม ข. การใช้จอภาพ

ค. การใช้เครื่องพิมพ์ ง. การใช้ไฟฟ้า

19. ข้อมูลที่ใช้ระบุตัวตนของ Tag เรียกว่าอะไร

ก. UID ข. IP Address

ค. MAC Address ง. URL

20. RFID มาตรฐาน ISO14443 Type A นิยมใช้กับ

ก. บัตรนักศึกษา ข. โทรทัศน์

ค. เครื่องพิมพ์ ง. โปรเจคเตอร์

21. โมดูล RFID ที่นิยมใช้กับ Arduino คือข้อใด

ก. RC522 ข. HC-05

ค. ESP32-CAM ง. DHT11

22. RC522 ติดต่อกับ Arduino ผ่านระบบใด

ก. SPI ข. VGA

ค. HDMI ง. SATA

23. ข้อใดไม่ใชาขาของ RC522

ก. SDA ข. MOSI

ค. MISO ง. TXD

24. ขา VCC มีหน้าที่ใด

ก. จ่ายไฟให้โมดูล ข. รับข้อมูล

ค. ส่งข้อมูล ง. รีเซ็ตระบบ

25. ขา GND ใช้สำหรับอะไร

ก. กราวด์ของวงจร ข. ส่งข้อมูล

ค. รีเลย์ ง. เสาอากาศ

26. ไลบรารีที่ใช้ควบคุม RC522 คือข้อใด

ก. MFRC522 ข. Servo

ค. Wire ง. LiquidCrystal

27. การติดตั้งไลบรารีทำผ่านโปรแกรมใด

ก. Arduino IDE ข. Photoshop

ค. Excel ง. AutoCAD

28. หลังติดตั้งไลบรารีควรทำสิ่งใด

ก. ทดสอบอ่านบัตร ข. ลบโปรแกรม

ค. ปิดระบบ ง. ถอดโมดูล

29. การตรวจสอบการเชื่อมต่อทำโดย

ก. อ่าน UID ของบัตร ข. วัดอุณหภูมิ

ค. วัดแรงดันไฟฟ้า ง. ตรวจสอบอินเทอร์เน็ต

30. UID ย่อมาจากอะไร

ก. Unique Identifier ข. Universal Input Device

ค. User Information Data ง. Unique Internet Device

31. หาก Reader อ่าน UID ได้ แสดงว่า

ก. การเชื่อมต่อถูกต้อง ข. สายไฟขาด

ค. โปรแกรมผิด ง. ไม่มีไฟเลี้ยง

32. RC522 ใช้สำหรับ

ก. อ่านข้อมูล RFID ข. วัดอุณหภูมิ

ค. ตรวจจับควัน ง. ควบคุมมอเตอร์

33. RFID สามารถประยุกต์ควบคุมอะไรได้

ก. เปิด–ปิดอุปกรณ์ไฟฟ้า ข. พิมพ์เอกสาร

ค. เล่นเพลง ง. สแกนภาพ

34. อุปกรณ์ใดใช้สั่งเปิด–ปิดโหลดไฟฟ้า

ก. รีเลย์ ข. ตัวต้านทาน

ค. LED ง. ตัวเก็บประจุ

35. การใช้ RFID ควบคุมอุปกรณ์ช่วยเพิ่มอะไร

ก. ความสะดวกและความปลอดภัย ข. น้ำหนักระบบ

ค. การใช้พลังงาน ง. ขนาดอุปกรณ์

36. ระบบ Access Control หมายถึงอะไร

ก. ระบบควบคุมการเข้าออก ข. ระบบปรับอากาศ

ค. ระบบไฟฟ้า ง. ระบบเครือข่าย

37. อุปกรณ์ใดใช้ตรวจสอบสิทธิ์ผู้เข้าใช้งาน

ก. RFID Reader ข. Speaker

ค. Monitor ง. Printer

38. เมื่อบัตรได้รับอนุญาต ระบบจะทำอะไร

ก. ปลดล็อกประตู ข. ปิดระบบ

ค. รีสตาร์ตเครื่อง ง. ลบข้อมูล

39. หาก UID ไม่ตรงกับฐานข้อมูลจะเกิดอะไรขึ้น

ก. ไม่อนุญาตให้เข้า ข. เปิดประตูทันที

ค. ปิดไฟ ง. รีเซ็ตระบบ

40. Arduino ในระบบประตูทำหน้าที่ใด

ก. ประมวลผลข้อมูล ข. จ่ายไฟ

ค. แสดงภาพ ง. รับสัญญาณ Wi-Fi

41. อุปกรณ์ใดใช้ปลดล็อกประตู

ก. รีเลย์หรือเซอร์โวมอเตอร์ ข. จอ LCD

ค. Speaker ง. Keyboard

42. NodeMCU ESP8266 มีจุดเด่นด้านใด

ก. เชื่อมต่อ Wi-Fi ได้ ข. พิมพ์เอกสารได้

ค. ถ่ายภาพได้ ง. เล่นเสียงได้

43. NodeMCU ช่วยให้ระบบสามารถทำอะไรได้

ก. ส่งข้อมูลผ่านอินเทอร์เน็ต ข. เพิ่มแรงดันไฟฟ้า

ค. ลดอุณหภูมิ ง. พิมพ์รายงาน

44. ข้อใดเป็นประโยชน์ของระบบควบคุมประตูด้วย RFID

ก. ตรวจสอบผู้เข้าออกได้ ข. เพิ่มจำนวนสายไฟ

ค. เพิ่มขนาดอุปกรณ์ ง. ลดประสิทธิภาพ

45. ระบบนี้ช่วยลดการใช้สิ่งใด

ก. กุญแจแบบเดิม ข. อินเทอร์เน็ต

ค. ไฟฟ้า ง. เซนเซอร์

46. ไมโครคอนโทรลเลอร์ ESP8266 มีลักษณะการใช้งานที่<u>โดดเด่น</u>คือข้อใด

ก. มีแหล่งจ่ายไฟแรงดัน 3.3 V

ข. มีพอร์ตอินพุตและเอาต์พุตจำนวนมาก

ค. เชื่อมต่อ Wi-Fi ได้

ง. เชื่อมต่อ Bluetooth ได้

47. ไมโครคอนโทรลเลอร์ ESP8266 สามารถเขียนโปรแกรมได้ด้วยภาษาใดบ้าง

ก. C ข. C++

ค. LAU ง. ถูกทุกข้อ

48. ถ้าต้องการใช้สัญญาณนาฬิกา ควรเลือกใช้ตำแหน่งขาใด

ก. CMD ข. MISO

ค. RST ง. CLK

49. ตำแหน่งขาใด สามารถรับสัญญาณอินพุตแบบอนาล็อกและแบบดิจิตอลได้

ก. D0 ข. D1

ค. A0 ง. A1

50. ถ้าต้องการดาวโหลดโปรแกรม Arduino IDE สามารถดาวโหลดได้ที่เว็บไซต์ใด

ก. www.arduino.cc ข. www.android.cc

ค. www.arduino.in.th ง. www.android.in.th

51. สำหรับผู้ใช้งาน iMac จะต้องดาวโหลดตัวติดตั้ง Arduino IDE ระบบปฏิบัติการใด

ก. Windows ข. Mac OS X

ค. Linux 32 bits ง. Linux 64 bits

52. ปุ่ม มีหน้าที่อย่างไร

ก. ตรวจสอบโค้ด ข. อัพโหลดโค้ด

ค. เซฟไฟล์ ง. แสดงหน้าต่าง Serial Monitor

53. ถ้าต้องการดูหน้าจอ Serial Monitor ต้องกดปุ่มคำสั่งใด

ก. ข.

ค. ง.

54. โครงสร้างของโปรแกรม Arduino IDE ประกอบด้วยฟังก์ชันสำคัญอะไรบ้าง

ก. void setup ข. void main

ค. void setup และ void loop ง. void main และ void loop

55. โค้ดส่วนที่ใช้กำหนดค่าเริ่มต้น และทำครั้งเดียวเมื่อเริ่มทำงาน ต้องอยู่ในฟังก์ชันใด

ก. void main ข. void setup

ค. void loop ง. void node

56. ระบบ RFID สามารถระบุลักษณะของวัตถุด้วยวิธีการใด

ก. แสงเลเซอร์ ข. QR Code

ค. คลื่นความถี่วิทยุ ง. Barcode

57. ป้ายอิเล็กทรอนิกส์หรือแท็ก ที่<u>ไม่มี</u>แบตเตอรี่อยู่ภายใน คือแท็กชนิดใด

ก. Active RFID Tags ข. Passive RFID Tags

ค. Radio RFID Tags ง. Original RFID Tags

58. Active RFID Tags มีจุดเด่นคือข้อใด

ก. ไม่มีแบตเตอรี่ภายใน

ข. รับ-ส่งสัญญาณข้อมูลได้ระยะไกล

ค. ทำงานบริเวณที่มีสัญญาณรบกวนได้ดี

ง. ถูกทั้งข้อ ข. และ ค.

59. เครื่องอ่านบัตร (Reader) ทำหน้าที่อะไร

ก. ยิงเลเซอร์ลงป้ายอิเล็กทรอนิกส์

ข. อ่านหรือเขียนข้อมูลลงป้ายอิเล็กทรอนิกส์

ค. ถอดรหัสบาร์โค้ดบนป้ายอิเล็กทรอนิกส์

ง. ถูกทุกข้อ

60. การรับส่งข้อมูลระหว่างเครื่องอ่านกับแท็กอาศัยหลักการมอดูเลตแบบใด

ก. ASK ข. PSK

ค. PSK ง. ถูกทุกข้อ

61. เครื่องอ่านแท็กตรวจจับการอ่านแท็กด้วยวิธีการใด

ก. ปล่อยคลื่นแม่เหล็กไฟฟ้าบางเวลา

ข. ให้แท็กปล่อยคลื่นแม่เหล็กไฟฟ้า

ค. ปล่อยคลื่นแม่เหล็กไฟฟ้าตลอดเวลา

ง. ความทึบของตัวแท็ก

61. มาตรฐานบัตร RFID ที่มีสถานะการใช้งาน คือ 1 หรือ 0 คือมาตรฐานในข้อใด

ก. ISO11785 ข. ISO11784

ค. Bit Transponder (EAS) ง. ISO10536

62. บัตร Mifare อยู่ในมาตรฐานบัตร RFID ข้อใด

ก. ISO14443 ข. ISO11784

ค. ISO11785 ง. Bit Transponder (EAS)

63. Proximity card (f = 13.56 MHz) มีระยะรับส่งข้อมูลสูงสุดกี่เซนติเมตร

ก. 8 ซม. ข. 10 ซม.

ค. 12 ซม. ง. 14 ซม.

64. เทคโนโลยี Near Field Communication (NFC) ทำงานที่ความถี่ใด

ก. 125 kHz ข. 433 MHz

ค. 13.56 MHz ง. 2.45 GHz

65. NFC มีระยะการสื่อสารโดยทั่วไปไม่เกินเท่าใด

ก. 50 เซนติเมตร
ข. 1 เมตร
ค. 20 เมตร
ง. 10 เซนติเมตร

66. มาตรฐานหลักที่ใช้สำหรับเทคโนโลยี NFC คือข้อใด

ก. IEEE 802.11
ข. IEEE 802.15.4
ค. ISO/IEC 15693
ง. ISO/IEC 18092

67. โหมดการทำงานของ NFC ที่ใช้สำหรับการชำระเงินผ่านโทรศัพท์มือถือคือข้อใด

ก. Reader/Writer Mode
ข. Peer-to-Peer Mode
ค. Card Emulation Mode
ง. Broadcast Mode

68. ข้อใดไม่ใช่โหมดการทำงานของ NFC

ก. Reader/Writer Mode
ข. Card Emulation Mode
ค. Peer-to-Peer Mode
ง. Mesh Mode

69. ข้อดีสำคัญของ NFC เมื่อเทียบกับ Bluetooth คือข้อใด

ก. ส่งข้อมูลได้ไกลกว่า
ข. ใช้พลังงานมากกว่า
ค. เชื่อมต่อได้รวดเร็วโดยไม่ต้องจับคู่
ง. รองรับผู้ใช้งานจำนวนมากพร้อมกัน

70. NFC อาศัยหลักการใดในการรับส่งข้อมูล

ก. คลื่นอินฟราเรด
ข. คลื่นไมโครเวฟ
ค. คลื่นวิทยุ UHF
ง. การเหนี่ยวนำสนามแม่เหล็กไฟฟ้า

71. ในระบบควบคุมการเข้าออก NFC มักใช้ทำหน้าที่ใด

ก. ตรวจจับควันไฟ
ข. พิสูจน์ตัวตนของผู้ใช้งาน
ค. วัดอุณหภูมิ
ง. ตรวจจับการเคลื่อนไหว

72. QR Code จัดเป็นบาร์โค้ดประเภทใด

ก. บาร์โค้ดหนึ่งมิติ
ข. บาร์โค้ดสามมิติ
ค. บาร์โค้ดสองมิติ
ง. บาร์โค้ดเชิงเส้น

73. บริษัทใดเป็นผู้พัฒนา QR Code

ก. Sony
ข. Toshiba
ค. Panasonic
ง. Denso Wave

74. จุดเด่นของ QR Code เมื่อเปรียบเทียบกับบาร์โค้ดแบบหนึ่งมิติคือข้อใด

ก. อ่านได้เฉพาะแนวนอน
ข. จัดเก็บข้อมูลได้มากกว่า
ค. ใช้เฉพาะตัวเลข
ง. อ่านได้เฉพาะเครื่องสแกนเฉพาะทาง

75. ส่วนประกอบของ QR Code ที่ใช้กำหนดตำแหน่งสำหรับการอ่านคือข้อใด

ก. Timing Pattern
ข. Data Area
ค. Finder Pattern
ง. Version Information

76. อัลกอริทึมที่ใช้ตรวจสอบและแก้ไขข้อผิดพลาดของ QR Code คือข้อใด

ก. SHA-256
ข. AES
ค. RSA
ง. Reed-Solomon Error Correction

77. QR Code นิยมใช้ในระบบควบคุมการเข้าออกเพื่อวัตถุประสงค์ใด

ก. วัดอุณหภูมิ
ข. ยืนยันตัวตนของผู้ใช้งาน
ค. ควบคุมแรงดันไฟฟ้า
ง. ตรวจจับเปลวไฟ

78. ข้อใดเป็นข้อจำกัดของ QR Code เมื่อเปรียบเทียบกับ NFC

ก. ไม่สามารถใช้กับสมาร์ตโฟนได้
ข. สามารถถูกคัดลอกภาพได้ หากไม่มีการป้องกันเพิ่มเติม
ค. อ่านข้อมูลได้ช้าเสมอ
ง. ใช้ได้เฉพาะในอาคาร

79. วิธีใดช่วยเพิ่มความปลอดภัยของระบบเข้าออกที่ใช้ QR Code ได้ดีที่สุด

ก. เพิ่มขนาด QR Code
ข. ใช้กระดาษคุณภาพสูง
ค. ใช้ QR Code แบบใช้ครั้งเดียว
ง. ใช้สีของ QR Code หลายสี

80. หากต้องการให้ผู้ใช้แตะโทรศัพท์เพื่อเปิดประตูโดยไม่ต้องเปิดกล้อง ควรเลือกใช้เทคโนโลยีใด

ก. Bluetooth
ข. QR Code
ค. ZigBee
ง. NFC

81. หากต้องการส่งบัตรผ่านให้ผู้มาติดต่อทางอีเมลโดยไม่ต้องติดตั้งแอปพลิเคชัน ควรเลือกใช้เทคโนโลยีใด

ก. NFC
ข. RFID
ค. Bluetooth
ง. QR Code

82. ข้อใดเปรียบเทียบ NFC และ QR Code ได้ถูกต้องที่สุด

ก. ทั้งสองต้องใช้แบตเตอรี่ที่แท็กเสมอ
ข. NFC ใช้กล้อง ส่วน QR Code ใช้คลื่นวิทยุ
ค. NFC ใช้การสื่อสารด้วยคลื่นวิทยุระยะใกล้ ส่วน QR Code ใช้การสแกนภาพ
ง. ทั้งสองทำงานที่ความถี่ 13.56 MHz

83. หากต้องการระบบควบคุมการเข้าออกที่มีความปลอดภัยสูงที่สุด ควรเลือกแนวทางใด

ก. ใช้ QR Code เพียงอย่างเดียว
ข. ใช้ NFC เพียงอย่างเดียว
ค. ใช้รหัสผ่านเพียงอย่างเดียว

ง. ใช้ NFC หรือ QR Code ร่วมกับการพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)

84. ข้อใดเรียงลำดับขั้นตอนการทำงานของระบบควบคุมการเข้าออก ได้ถูกต้อง

ก. ผู้ใช้งานเปิดประตู > ระบบตรวจสอบสิทธิ์ > เครื่องอ่านข้อมูล > บันทึกข้อมูล > ปลดล็อกประตู

ข. ผู้ใช้งานยืนยันตัวตน > เครื่องอ่านข้อมูลส่งข้อมูลไปยังชุดควบคุม > ชุดควบคุมตรวจสอบฐานข้อมูลและนโยบายการเข้าถึง > ระบบตัดสินใจอนุญาตหรือปฏิเสธ > ปลดล็อกประตูและบันทึกข้อมูลการเข้าออก

ค. เครื่องอ่านข้อมูลตรวจสอบฐานข้อมูล > ผู้ใช้งานยืนยันตัวตน > ระบบปลดล็อกประตู > บันทึกข้อมูล

ง. ผู้ใช้งานยืนยันตัวตน > ระบบปลดล็อกประตู > ตรวจสอบสิทธิ์ > บันทึกข้อมูล

85. ข้อใดอธิบายความแตกต่างระหว่าง Authentication, Authorization และ Access Control ได้ถูกต้องที่สุด

ก. Authentication คือการกำหนดสิทธิ์ ส่วน Authorization คือการพิสูจน์ตัวตน และ Access Control คือการบันทึกข้อมูล

ข. Authentication คือการปลดล็อกประตู ส่วน Authorization คือการสแกนบัตร และ Access Control คือการบันทึกเวลาเข้าออก

ค. Authentication คือการพิสูจน์ตัวตนของผู้ใช้งาน, Authorization คือการตรวจสอบสิทธิ์หลังพิสูจน์ตัวตน และ Access Control คือการบังคับใช้นโยบายเพื่ออนุญาตหรือปฏิเสธการเข้าถึง

ง. Authentication, Authorization และ Access Control มีความหมายเหมือนกันทุกประการ

<u>คำชี้แจง</u> จงพิจารณาข้อความที่กำหนดให้ ถ้าถูกต้องให้ทำเครื่องหมาย ✓ ถ้าผิดให้ทำเครื่องหมาย **X** หน้าข้อนั้น ๆ

_____1. RFID ย่อมาจาก Radio Frequency Information

_____2. ระบบ RFID มีวัตถุประสงค์เพื่อนำไปใช้งานแทนระบบ Barcode

_____3. Passive RFID Tags มีระยะรับส่งข้อมูลที่ไกล

_____4. ภายในป้ายอิเล็กทรอนิกส์หรือแท็ก (Tag) ประกอบด้วยไมโครชิพ (Microchip) เป็นสำคัญ

_____5. องค์ประกอบของระบบ RFID ได้แก่ เครื่องอ่านบัตร และหน่วยประมวลข้อมูล

_____6. การรับส่งข้อมูลระหว่างเครื่องอ่านและแท็ก ใช้หลักการมอดูเลต เช่น AM FM เป็นต้น

_____7. นอกจากการรับส่งข้อมูลแล้วสายอากาศ ยังทำหน้าที่เป็นแหล่งจ่ายพลังงานให้กับแท็ก

_____8. บัตร MIFARE จัดอยู่ในมาตรฐาน ISO18000

_____9. ISO18000-6B/6C จัดอยู่ในย่าน UHF

_____10. มาตรฐานสำหรับการระบุรหัสประจำตัวสัตว์ทำงานที่ความถี่ 125-134 kHz

5 ระบบตรวจสอบอัตลักษณ์เพื่อความปลอดภัย

51

ระบบรักษาความปลอดภัยด้วยการยืนยันตัวตนด้วยลายนิ้วมือ

5.1.1 พื้นฐานของระบบตรวจสอบลายนิ้วมือ
5.1.2 หลักการทำงานของเครื่องสแกนลายนิ้วมือ
5.1.3 ประเภทของเซนเซอร์ลายนิ้วมือ
5.1.4 หลักการตรวจสอบลายนิ้วมือด้วยจุดลักษณะเฉพาะ
5.1.5 กระบวนการสแกนและตรวจสอบลายนิ้วมือ
5.1.6 การแปลงลายนิ้วมือเป็นข้อมูลดิจิทัลสำหรับการตรวจสอบอัตลักษณ์
5.1.7 การใช้งานเซนเซอร์สแกนลายนิ้วมือ
5.1.8 การประยุกต์ใช้งานเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์

52

ระบบรักษาความปลอดภัยด้วยการยืนยันตัวตนด้วยใบหน้า

5.2.1 หลักการตรวจสอบและจดจำใบหน้า
5.2.2 กระบวนการระบบจดจำใบหน้า
5.2.3 วิธีการตรวจจับใบหน้าด้วย OpenCV และ Haar Cascade
5.2.4 ความปลอดภัยของระบบตรวจสอบใบหน้า
5.2.5 ข้อดีและข้อจำกัดของระบบสแกนใบหน้า

53

ระบบจดจำเสียง

5.3.1 ความหมายของระบบจดจำเสียง
5.3.2 ประเภทของระบบจดจำเสียง
5.3.3 รูปแบบการรู้จำเสียง
5.3.4 หลักการทำงานของระบบจดจำเสียง
5.3.5 สถาปัตยกรรมของระบบรู้จำเสียงสมัยใหม่

บทที่ 5 ระบบตรวจสอบอัตลักษณ์เพื่อความปลอดภัย

Biometric Security Systems

ในการระบุตัวตนของบุคคลท่ามกลางประชากรจำนวนมาก จำเป็นต้องอาศัยคุณลักษณะเฉพาะทางกายภาพหรือพฤติกรรมของแต่ละบุคคล ซึ่งเรียกว่า ข้อมูลชีวมาตร (biometrics) โดยคุณลักษณะที่นิยมใช้ในการพิสูจน์และยืนยันตัวตน ได้แก่ ลายนิ้วมือ (fingerprint) ลายฝ่ามือ (palm print) ใบหน้า (face recognition) ม่านตา (iris recognition) ดีเอ็นเอ (DNA) ลายเซ็น และเสียงพูด (voice recognition) ระบบชีวมาตรจะทำการตรวจจับและแปลงคุณลักษณะดังกล่าวให้อยู่ในรูปแบบข้อมูลดิจิทัล จากนั้นนำไปเปรียบเทียบกับข้อมูลต้นแบบที่ถูกบันทึกไว้ในฐานข้อมูล เพื่อใช้ในการยืนยันหรือระบุตัวบุคคลได้อย่างถูกต้องและมีประสิทธิภาพ ช่วยเพิ่มความปลอดภัย ลดความผิดพลาดจากการใช้รหัสผ่านหรือบัตรประจำตัว และถูกนำมาใช้อย่างแพร่หลายในระบบรักษาความปลอดภัย ระบบควบคุมการเข้า ออก และระบบพิสูจน์ตัวตนในปัจจุบัน ในหน่วยนี้จะกล่าวถึงการประยุกต์ใช้ในระบบความปลอดภัย เช่น ระบบตรวจสอบลายนิ้วมือ ระบบตรวจสอบใบหน้า โดยมีรายละเอียดดังต่อไปนี้

5.1 ระบบรักษาความปลอดภัยด้วยการยืนยันตัวตนด้วยลายนิ้วมือ (Fingerprint Authentication System)

5.1.1 พื้นฐานของระบบตรวจสอบลายนิ้วมือ

การตรวจสอบลายนิ้วมือเป็นวิธีการพิสูจน์ตัวตนทางชีวมาตรที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบัน เนื่องจากลายนิ้วมือของแต่ละบุคคลมีลักษณะเฉพาะ ไม่ซ้ำกัน และมีความคงที่ตลอดชีวิต ลายนิ้วมือเริ่มพัฒนาตั้งแต่อยู่ในครรภ์มารดา และเมื่อเจริญเติบโตเป็นผู้ใหญ่รูปแบบของลายนิ้วมือยังคงเดิม แม้ขนาดของนิ้วจะเปลี่ยนแปลงตามร่างกายก็ตาม นอกจากนี้ หากผิวหนังบริเวณลายนิ้วมือเกิดการสึกหรอหรือบาดเจ็บเพียงเล็กน้อย ร่างกายสามารถซ่อมแซมผิวหนังให้กลับมามีรูปแบบลายนิ้วมือใกล้เคียงเดิมได้ ด้วยคุณสมบัติด้านความเฉพาะตัว ความคงทน และความสะดวกในการตรวจสอบ ลายนิ้วมือจึงได้รับการยอมรับอย่างกว้างขวางในการใช้ระบุตัวบุคคล (identification) และยืนยันตัวตน (authentication)

รูปแบบลายนิ้วมือพื้นฐานสามารถจำแนกได้ 3 ประเภท ได้แก่ ลายก้นหอย (whorl) ลายมัดหวายหรือแบบห่วง (loop) และลายโค้ง (arch) ซึ่งแต่ละรูปแบบมีลักษณะเฉพาะที่แตกต่างกันและถูกนำมาใช้ในการพิสูจน์อัตลักษณ์ของบุคคลในระบบชีวมาตร (biometric system) อย่างแพร่หลาย การนำลายนิ้วมือมาใช้ในการระบุตัวตนของบุคคลเป็นเทคโนโลยีชีวมาตรที่ได้รับการศึกษาและพัฒนาอย่างต่อเนื่องมาเป็นเวลานาน จนได้รับการยอมรับอย่างแพร่หลายว่ามีความถูกต้องและความน่าเชื่อถือสูง เนื่องจากลายนิ้วมือของมนุษย์แต่ละบุคคลมีลักษณะเฉพาะที่แตกต่างกัน และมีโอกาสซ้ำกันน้อยมาก (Kaushal & Kaushal, 2011; Tandee, 2014) ดังแสดงในรูปที่ 5.1

(ก) ลายโค้ง (arch) (ข) ลายมัดหวายหรือแบบห่วง (loop) (ค) ลายก้นหอย (whorl)

รูปที่ 5.1 ประเภทของลายนิ้วมือ (ดัดแปลงจาก Tandee, 2014)

5.1.2 ประเภทของเซนเซอร์ลายนิ้วมือ

เครื่องสแกนลายนิ้วมือ (fingerprint scanner หรือ finger scan) เป็นอุปกรณ์ที่ออกแบบมาเพื่ออ่านและวิเคราะห์ลักษณะเฉพาะของลายนิ้วมือของแต่ละบุคคล โดยอาศัยหลักการทางชีวมาตรในการตรวจสอบอัตลักษณ์ ซึ่งลายนิ้วมือของมนุษย์แต่ละคนจะมีรูปแบบแตกต่างกันและไม่ซ้ำกัน ทำให้สามารถนำมาใช้ในการพิสูจน์ตัวตนได้อย่างมีประสิทธิภาพ

หลักการทำงานของเครื่องสแกนลายนิ้วมือเริ่มจากการนำปลายนิ้วสัมผัสกับเซนเซอร์ของเครื่อง จากนั้นเซนเซอร์จะทำการอ่านลักษณะของเส้นลายนิ้วมือ เช่น จุดปลายเส้น จุดแยกของเส้น และรูปแบบของลายนิ้วมือ แล้วแปลงข้อมูลให้อยู่ในรูปแบบดิจิทัล ก่อนนำไปเปรียบเทียบกับข้อมูลลายนิ้วมือที่ถูกบันทึกไว้ในฐานข้อมูล หากข้อมูลตรงกัน ระบบจะอนุญาตให้เข้าใช้งานหรือบันทึกข้อมูลตามที่กำหนดไว้

รูปที่ 5.2 ตัวอย่างเครื่องสแกนลายนิ้วมือ

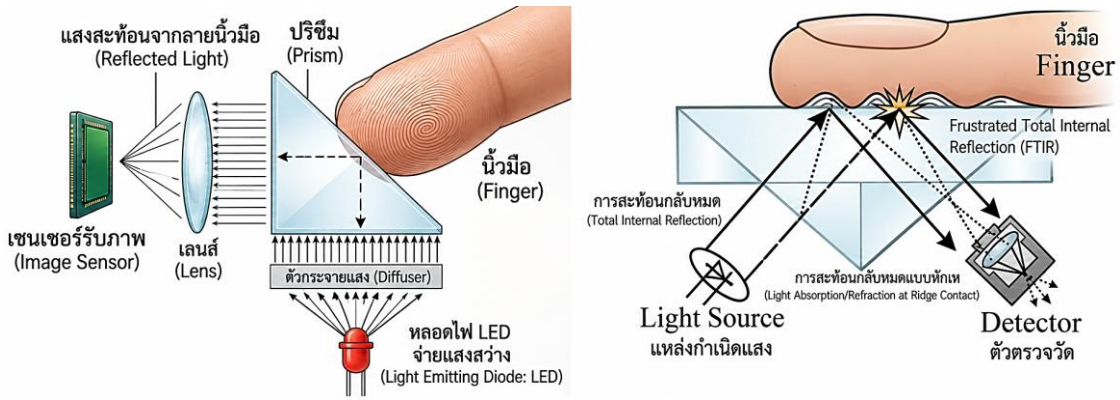
ปัจจุบัน เครื่องสแกนลายนิ้วมือถูกนำมาใช้งานอย่างแพร่หลาย ทั้งในระบบบันทึกเวลาปฏิบัติงาน ระบบควบคุมการเข้า ออกประตู (access control) และระบบรักษาความปลอดภัยต่าง ๆ เนื่องจากสามารถลดปัญหาการใช้บัตรแทนกัน หรือการลงเวลาแทนกัน (buddy punching) ได้อย่างมีประสิทธิภาพ เพราะลายนิ้วมือของแต่ละบุคคลมีความเฉพาะตัวและไม่สามารถใช้งานแทนกันได้ นอกจากนี้ เครื่องสแกนลายนิ้วมือรุ่นใหม่ยังสามารถใช้งานร่วมกับวิธีการยืนยันตัวตนรูปแบบอื่นได้ เช่น การกดรหัสผ่าน (password/PIN code) การใช้บัตร RFID หรือการสแกนใบหน้าเพื่อเพิ่มความยืดหยุ่นและความปลอดภัยในการใช้งาน โดยเฉพาะในกรณีที่ผู้ใช้งานมีลายนิ้วมือไม่ชัดเจนหรือเกิดความเสียหายบริเวณปลายนิ้ว โดยทั่วไป เครื่องสแกนลายนิ้วมือสามารถตรวจสอบข้อมูลได้อย่างรวดเร็ว ใช้เวลาในการสแกนประมาณ 1 วินาทีต่อคน ทำให้เหมาะสำหรับใช้งานในองค์กรหรือสถานที่ที่มีผู้ใช้งานจำนวนมาก

5.1.3 ประเภทของเซนเซอร์ลายนิ้วมือ (Fingerprint Sensor Types)

เซนเซอร์ลายนิ้วมือแต่ละประเภทมีหลักการทำงาน คุณสมบัติ และประสิทธิภาพแตกต่างกันขึ้นอยู่กับเทคโนโลยีที่ใช้ในการออกแบบและวัสดุที่ใช้ในการผลิต ดังนั้น การเลือกใช้งานหัวอ่านลายนิ้วมือจึงควรพิจารณาให้เหมาะสมกับลักษณะงาน สภาพแวดล้อม และงบประมาณ เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพและมีความแม่นยำสูงสุด เครื่องสแกนลายนิ้วมือสามารถแบ่งประเภทตามลักษณะของเซนเซอร์ที่ใช้ในการตรวจสอบได้ 4 ประเภทหลัก ดังนี้

1) เซนเซอร์ลายนิ้วมือแบบใช้แสง (Optical Fingerprint Sensor)

เซนเซอร์ลายนิ้วมือแบบใช้แสงเป็นเซนเซอร์ที่อาศัยหลักการสะท้อนของแสงเพื่อสร้างภาพลายนิ้วมือ โดยภายในระบบประกอบด้วยแหล่งกำเนิดแสง เช่น หลอด LED ตัวกระจายแสง ปริซึม เลนส์ และเซนเซอร์รับภาพ



ก) การทำงานของหัวอ่าน ข) การตรวจสอบลายนิ้วมือ

รูปที่ 5.3 หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบใช้แสง (ดัดแปลงจาก Hsu, 2016)

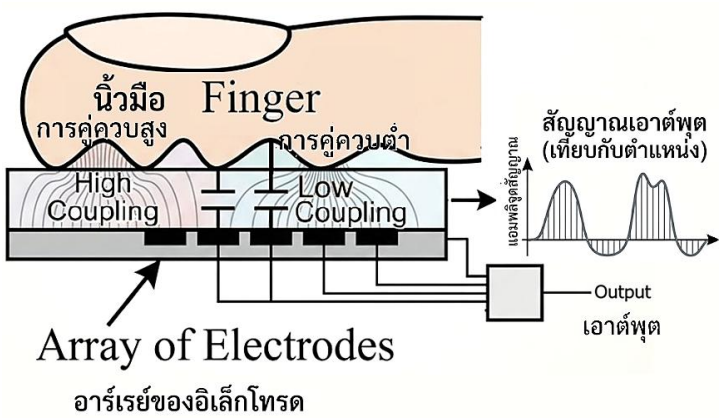
จากรูปที่ 5.3 เมื่อผู้ใช้นำปลายนิ้ววางลงบนผิวกระจกหรือปริซึมของเครื่องสแกน แสงจากหลอด LED จะถูกส่งผ่านตัวกระจายแสงเพื่อให้แสงกระจายอย่างสม่ำเสมอ จากนั้นแสงจะเดินทางเข้าสู่ปริซึมและตกกระทบบริเวณผิวสัมผัสของนิ้วมือ ลายนิ้วมือของมนุษย์ประกอบด้วยส่วนที่

เป็น สันลายนิ้วมือ และ ร่องลายนิ้วมือ โดยสันลายนิ้วมือจะสัมผัสกับผิวกระจกหรือปริซึมโดยตรง ส่วนร่องลายนิ้วมือจะมีช่องว่างอากาศระหว่างผิวหนังกับผิวกระจก ทำให้แต่ละบริเวณสะท้อนแสงกลับมาไม่เท่ากัน ความแตกต่างของแสงสะท้อนนี้ทำให้เกิดภาพลายนิ้วมือที่มีบริเวณมืดและสว่างแตกต่างกัน แสงสะท้อนจากลายนิ้วมือจะถูกส่งผ่านเลนส์ไปยังเซนเซอร์รับภาพ เช่น CCD หรือ CMOS เพื่อแปลงสัญญาณแสงให้เป็นข้อมูลภาพดิจิทัล จากนั้นระบบจะนำภาพที่ได้ไปประมวลผลโดยตรวจหาจุดสำคัญของลายนิ้วมือ เช่น จุดสิ้นสุดของเส้นลายและจุดแยกของเส้นลาย แล้วเปรียบเทียบกับข้อมูลลายนิ้วมือที่บันทึกไว้ในฐานข้อมูล หากลักษณะของลายนิ้วมือที่ตรวจพบตรงกับข้อมูลที่จัดเก็บไว้ ระบบจะยืนยันตัวตนและอนุญาตให้ใช้งาน เช่น บันทึกเวลา เปิดประตู หรือเข้าสู่ระบบ แต่หากข้อมูลไม่ตรงกัน ระบบจะปฏิเสธการเข้าใช้งาน

โดยสรุปเซนเซอร์ลายนิ้วมือแบบ optical ใช้หลักการ “แสงสะท้อนจากลายนิ้วมือ” เพื่อสร้างภาพลายนิ้วมือ แล้วนำภาพนั้นไปวิเคราะห์และเปรียบเทียบกับข้อมูลเดิม จึงเป็นเทคโนโลยีที่นิยมใช้ในเครื่องสแกนลายนิ้วมือทั่วไป เนื่องจากมีต้นทุนไม่สูง ใช้งานง่าย และให้ภาพลายนิ้วมือที่ชัดเจน

2) เซนเซอร์ลายนิ้วมือแบบวัดค่าความจุไฟฟ้า (Capacitive Fingerprint Sensor)

หัวอ่านลายนิ้วมือแบบอาศัยหลักการวัดค่าความจุไฟฟ้า (capacitive fingerprint sensor) เป็นเทคโนโลยีตรวจสอบลายนิ้วมือที่อาศัยหลักการวัดค่าความจุไฟฟ้า (capacitance) ระหว่างผิวหนังของนิ้วมือกับแผงเซนเซอร์อิเล็กทรอนิกส์ โดยไม่ใช้แสงในการสร้างภาพลายนิ้วมือเหมือนหัวอ่านแบบ optical จึงมีความแม่นยำสูงและสามารถป้องกันการปลอมแปลงได้ดีกว่า



รูปที่ 5.4 หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบ capacitive fingerprint sensor (ดัดแปลงจาก Hsu, 2016)

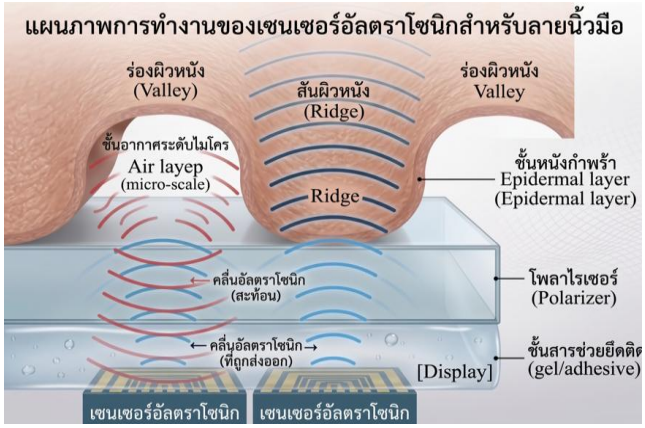
จากรูปที่ 5.4 ภายในเซนเซอร์จะประกอบด้วยชุดอิเล็กโทรดขนาดเล็กจำนวนมาก (array of electrodes) ซึ่งทำหน้าที่ตรวจจับค่าความจุไฟฟ้าในแต่ละตำแหน่งของลายนิ้วมือ เมื่อผู้ใช้นำปลายนิ้วสัมผัสบนพื้นผิวของเซนเซอร์ บริเวณที่เป็น “สันลายนิ้วมือ” (ridge) จะสัมผัสกับเซนเซอร์โดยตรง ทำให้เกิดค่าความจุไฟฟ้าสูง ส่วนบริเวณที่เป็น “ร่องลายนิ้วมือ” (valley) จะมีช่องว่างอากาศคั่นอยู่ จึงเกิดค่าความจุไฟฟ้าต่ำกว่า เซนเซอร์จะทำการวัดความแตกต่างของค่าความจุไฟฟ้าในแต่ละตำแหน่ง แล้วนำข้อมูลที่ได้มาสร้างเป็นภาพลายนิ้วมือในรูปแบบดิจิทัล

จากนั้นระบบประมวลผลจะวิเคราะห์ลักษณะเฉพาะของลายนิ้วมือ เช่น จุดสิ้นสุดของเส้นลาย จุดแตกแขนง และรูปแบบของลายนิ้วมือ เพื่อนำไปเปรียบเทียบกับข้อมูลต้นแบบที่ถูกจัดเก็บไว้ในฐานข้อมูล หากข้อมูลลายนิ้วมือที่ตรวจจับได้ตรงกับข้อมูลที่บันทึกไว้ ระบบจะยืนยันตัวตนและอนุญาตให้ใช้งาน แต่หากข้อมูลไม่ตรงกัน ระบบจะปฏิเสธการเข้าใช้งานทันที

ข้อดีของเซนเซอร์แบบ capacitive คือ สามารถอ่านลายนิ้วมือได้ละเอียดและแม่นยำสูง มีขนาดเล็ก ใช้พลังงานต่ำ และสามารถป้องกันการปลอมแปลงจากภาพถ่ายหรือแบบจำลองลายนิ้วมือได้ดีกว่าหัวอ่านแบบใช้แสง เนื่องจากระบบต้องตรวจจับคุณสมบัติทางไฟฟ้าของผิวหนังจริง จึงนิยมใช้งานในสมาร์ตโฟน อุปกรณ์อิเล็กทรอนิกส์พกพา และระบบรักษาความปลอดภัยสมัยใหม่

3) เซนเซอร์ลายนิ้วมือแบบอัลตราโซนิก (Ultrasonic Fingerprint Sensor)

เป็นหัวอ่านที่ใช้คลื่นเสียงความถี่สูง (ultrasonic wave) ในการสแกนลายนิ้วมือ โดยสามารถอ่านข้อมูลลายนิ้วมือได้ทั้งบนพื้นผิวและใต้ชั้นผิวหนัง ทำให้มีความแม่นยำสูง และสามารถทำงานได้ดีแม้ปลายนิ้วมีความชื้นหรือสิ่งสกปรก



รูปที่ 5.5 หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบอัลตราโซนิก (ดัดแปลงจาก Samsung Display, n.d.)

จากรูปที่ 5.5 แสดงหลักการทำงานของเซนเซอร์สแกนลายนิ้วมือแบบอัลตราโซนิก ซึ่งเป็นเทคโนโลยีตรวจสอบลายนิ้วมือที่ใช้ “คลื่นเสียงความถี่สูง” ในการสร้างภาพลายนิ้วมือแบบสามมิติ (3D fingerprint imaging) โดยนิยมใช้งานในสมาร์ตโฟนและระบบรักษาความปลอดภัยสมัยใหม่ เนื่องจากมีความแม่นยำสูงและสามารถป้องกันการปลอมแปลงได้ดี

จากรูปเมื่อผู้ใช้นำปลายนิ้วสัมผัสบนพื้นผิวหน้าจอหรือแผ่นเซนเซอร์ ระบบจะส่งคลื่นอัลตราโซนิก จากตัวส่งสัญญาณภายในเซนเซอร์ขึ้นไปยังผิวหนังของนิ้วมือ คลื่นเสียงดังกล่าวจะสะท้อนกลับแตกต่างกันตามลักษณะของลายนิ้วมือ ซึ่งประกอบด้วยส่วนที่เป็น “สันลายนิ้วมือ” และ “ร่องลายนิ้วมือ” โดยบริเวณที่เป็นสันลายนิ้วมือจะสัมผัสกับพื้นผิวเซนเซอร์โดยตรง ทำให้คลื่นเสียงสะท้อนกลับในลักษณะหนึ่ง ขณะที่บริเวณร่องลายนิ้วมือจะมีชั้นอากาศขนาดเล็ก (air layer) คั่นอยู่ระหว่างผิวหนังกับพื้นผิวเซนเซอร์ จึงทำให้คลื่นเสียงสะท้อนกลับแตกต่างออกไป เซนเซอร์จะ

ตรวจจับเวลาการสะท้อนกลับและความเข้มของคลื่นเสียง เพื่อนำข้อมูลมาสร้างเป็นภาพลายนิ้วมือแบบดิจิทัล องค์ประกอบสำคัญได้แก่

3.1) Ridge (สันลายนิ้วมือ) เป็นส่วนที่สัมผัสกับพื้นผิวเซนเซอร์โดยตรง

3.2) Valley (ร่องลายนิ้วมือ) เป็นส่วนที่มีช่องว่างอากาศคั่นอยู่

3.3) Ultrasonic sensor เป็นตัวส่งและรับคลื่นอัลตราโซนิก

3.4) Air layer (micro-scale) เป็นชั้นอากาศขนาดเล็กบริเวณร่องลายนิ้วมือ

3.5) Coupling layer (gel/adhesive) เป็นชั้นตัวกลางช่วยส่งผ่านคลื่นเสียง

3.6) Display เป็นชั้นหน้าจอที่ติดตั้งเซนเซอร์ไว้ด้านล่าง

3.7) Epidermal layer เป็นชั้นผิวหนังบริเวณปลายนิ้วมือ

ข้อดีของเทคโนโลยี ultrasonic fingerprint sensor คือ สามารถอ่านลายนิ้วมือได้ละเอียดทั้งบริเวณพื้นผิวและใต้ชั้นผิวหนัง ทำงานได้ดีแม้นิ้วเปียก มีความชื้น หรือมีสิ่งสกปรก อีกทั้งยังสามารถสร้างภาพลายนิ้วมือแบบสามมิติ จึงช่วยเพิ่มความแม่นยำและความปลอดภัยในการยืนยันตัวตนได้สูงกว่าหัวอ่านลายนิ้วมือแบบ optical และ capacitive

4) เซนเซอร์ลายนิ้วมือแบบตรวจจับความร้อน (Thermal Fingerprint Sensor)

เซนเซอร์ลายนิ้วมือแบบ thermal fingerprint sensor เป็นเทคโนโลยีที่ใช้หลักการตรวจจับ “ความแตกต่างของอุณหภูมิ” ระหว่างบริเวณสันลายนิ้วมือ และร่องลายนิ้วมือ เพื่อสร้างภาพลายนิ้วมือสำหรับการยืนยันตัวตน เมื่อผู้ใช้นำปลายนิ้วสัมผัสบนพื้นผิวเซนเซอร์ ความร้อนจากผิวหนังจะถูกถ่ายเทลงมายังชุดตรวจจับความร้อน (heat sensor หรือ thermal sensor array) ที่อยู่ภายในอุปกรณ์ บริเวณที่เป็น “สันลายนิ้วมือ” จะสัมผัสกับพื้นผิวเซนเซอร์โดยตรง ทำให้เกิดการถ่ายเทความร้อนได้มากกว่าส่วนบริเวณที่เป็น “ร่องลายนิ้วมือ” จะมีช่องอากาศขนาดเล็ก (air gap หรือ micro-voids) คั่นอยู่ จึงทำให้การถ่ายเทความร้อนน้อยกว่า เซนเซอร์จะตรวจวัดความแตกต่างของอุณหภูมิในแต่ละตำแหน่ง แล้วแปลงข้อมูลดังกล่าวเป็นสัญญาณไฟฟ้า ก่อนนำไปสร้างเป็นภาพลายนิ้วมือในรูปแบบดิจิทัล จากนั้นระบบประมวลผลจะวิเคราะห์ลักษณะเฉพาะของลายนิ้วมือ เช่น รูปแบบเส้นลาย จุดสิ้นสุดของเส้นลาย และจุดแตกแขนง เพื่อนำไปเปรียบเทียบกับข้อมูลที่จัดเก็บไว้ในฐานข้อมูล องค์ประกอบสำคัญในรูปที่ 5.6

4.1) สันลายนิ้วมือ (ridge) ส่วนของผิวหนังที่สัมผัสกับเซนเซอร์โดยตรง ทำให้ถ่ายเทความร้อนได้มาก

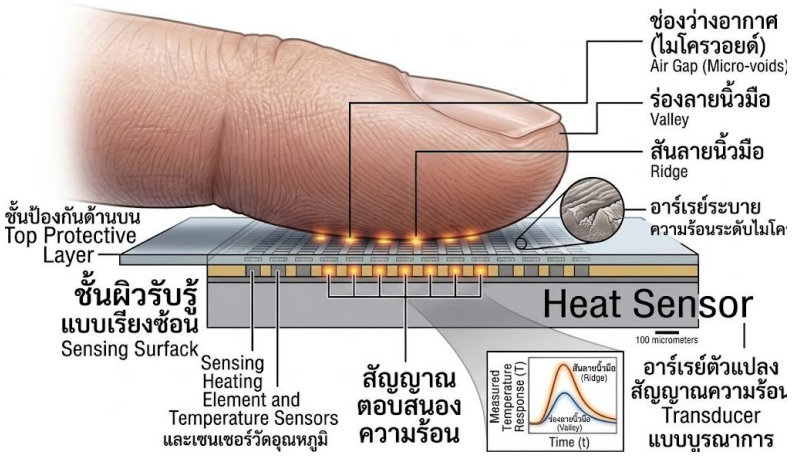
4.2) ร่องลายนิ้วมือ (valley) ส่วนที่ไม่สัมผัสกับเซนเซอร์โดยตรง มีช่องอากาศคั่นอยู่ ทำให้ถ่ายเทความร้อนได้น้อยกว่า

4.3) Air gap (micro-voids) ช่องอากาศขนาดเล็กระหว่างร่องลายนิ้วมือกับพื้นผิวเซนเซอร์

4.4) Heat sensor/thermal array ชุดตรวจจับอุณหภูมิที่ใช้วัดความแตกต่างของความร้อนจากแต่ละตำแหน่งของลายนิ้วมือ

4.5) Heat response signal สัญญาณตอบสนองทางความร้อนที่ถูกแปลงเป็นข้อมูลดิจิทัล

4.6) Protective layer ชั้นป้องกันพื้นผิวเซนเซอร์จากการสัมผัสและความเสียหาย



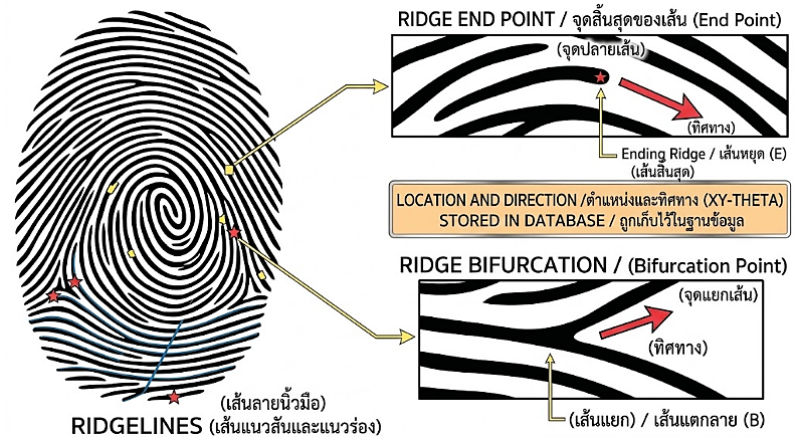
รูปที่ 5.6 หลักการทำงานของเซนเซอร์ลายนิ้วมือแบบตรวจจับความร้อน

ข้อดีของ thermal fingerprint sensor ได้แก่ (1) สามารถตรวจจับลายนิ้วมือจาก "คุณสมบัติทางความร้อน" ของผิวหนังจริง (2) ป้องกันการปลอมแปลงด้วยภาพถ่ายหรือวัสดุเทียมได้ดีกว่าระบบ optical บางประเภท (3) มีความแม่นยำในการตรวจจับลักษณะของลายนิ้วมือ ส่วนข้อจำกัด ได้แก่ (1) หากอุณหภูมิของนิ้วมือใกล้เคียงกับอุณหภูมิสภาพแวดล้อมมาก อาจส่งผลต่อความแม่นยำ (2) ใช้เวลาในการตรวจจับมากกว่าหัวอ่านบางประเภท และ (3) ปัจจุบันไม่นิยมใช้แพร่หลายเท่ากับ capacitive และ ultrasonic fingerprint sensor

5.1.4 หลักการตรวจสอบลายนิ้วมือด้วยจุดลักษณะเฉพาะ (Minutiae-Based Fingerprint Recognition)

การตรวจสอบลายนิ้วมือเป็นเทคโนโลยีที่ได้รับความนิยมมากที่สุด เนื่องจากมีความแม่นยำสูง ใช้งานสะดวก และมีต้นทุนไม่สูงเมื่อเทียบกับระบบชีวมาตรประเภทอื่น หลักการสำคัญของการตรวจสอบลายนิ้วมือ คือ การวิเคราะห์ลักษณะเฉพาะของเส้นลายนิ้วมือ ซึ่งเกิดจากโครงสร้างของสันและร่องลายนิ้วมือ ที่มีรูปแบบแตกต่างกันในแต่ละบุคคล เมื่อขยายภาพลายนิ้วมือจะพบว่า เส้นลายนิ้วมือมีลักษณะคล้ายแนวคลื่นหรือสันเขา โดยแต่ละเส้นจะมีจุดสำคัญที่เรียกว่า "จุดลักษณะเฉพาะ" (minutiae) เช่น จุดสิ้นสุดของเส้นลาย (ridge ending) และจุดแตกแขนงของเส้นลาย (bifurcation) ซึ่งจุดเหล่านี้ถือเป็นข้อมูลสำคัญที่ใช้ในการเปรียบเทียบและยืนยันตัวตน

โดยทั่วไปลายนิ้วมือของมนุษย์แต่ละคนจะมีจุดลักษณะเฉพาะประมาณ 50 จุด ระบบตรวจสอบลายนิ้วมือจะทำการบันทึกตำแหน่งและทิศทางของจุดเหล่านี้แทนการเก็บภาพลายนิ้วมือทั้งหมด เพื่อลดขนาดข้อมูลและเพิ่มประสิทธิภาพในการประมวลผล นอกจากนี้ ตามระบบการจำแนกลายนิ้วมือแบบ Henry classification system ซึ่งพัฒนาโดย Sir Edward Richard Henry ได้ระบุว่า หากลายนิ้วมือมีจุดลักษณะเฉพาะตรงกันอย่างน้อย 13 จุด ก็สามารถยืนยันได้ว่าเป็นลายนิ้วมือของบุคคลเดียวกัน (Tandee, 2014; Martins et al., 2024; Maiti et al., 2025)



รูปที่ 5.7 หลักการตรวจสอบลายนิ้วมือด้วยจุดลักษณะเฉพาะ (ดัดแปลงจาก Tandee, 2014)

จากรูปที่ 5.7 แสดงลักษณะของ “จุดลักษณะเฉพาะของลายนิ้วมือ” (fingerprint minutiae) ซึ่งเป็นข้อมูลสำคัญที่ระบบตรวจสอบลายนิ้วมือใช้ในการยืนยันตัวตน โดยระบบจะไม่เก็บภาพลายนิ้วมือทั้งหมด แต่จะจัดเก็บตำแหน่งและทิศทางของจุดลักษณะเฉพาะแทน เพื่อเพิ่มประสิทธิภาพในการประมวลผลและลดขนาดข้อมูล จากภาพสามารถแบ่งองค์ประกอบได้ดังนี้

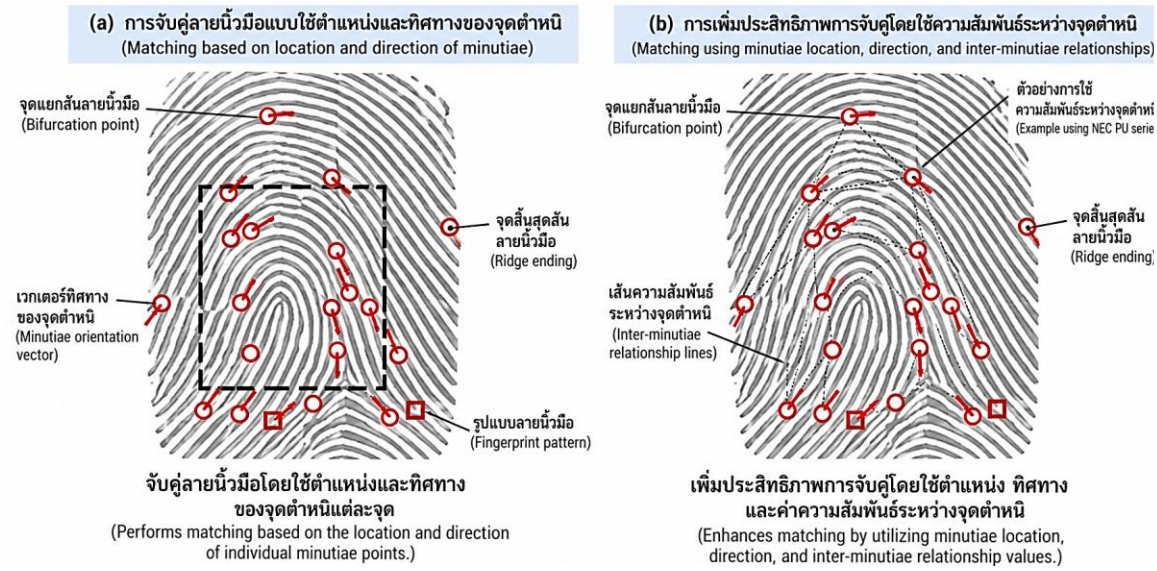
1) Ridgelines คือ เส้นสันลายนิ้วมือ (fingerprint ridges) ซึ่งเป็นลวดลายหลักบนปลายนิ้วของมนุษย์ โดยแต่ละบุคคลจะมีรูปแบบเส้นลายแตกต่างกัน

2) Ridge end point (ending ridge) คือ จุดสิ้นสุดของเส้นลายนิ้วมือ ซึ่งเป็นตำแหน่งที่เส้นลายหยุดลงกะทันหัน จุดนี้ถือเป็นจุดลักษณะเฉพาะสำคัญที่ใช้ในการเปรียบเทียบลายนิ้วมือ ในภาพแสดงด้วยคำว่า ending ridge (E)

3) Ridge bifurcation คือ จุดแตกแขนงของเส้นลายนิ้วมือ ซึ่งเกิดจากเส้นลายหนึ่งเส้นแยกออกเป็นสองเส้น จุดนี้เป็นอีกหนึ่งคุณลักษณะสำคัญที่ระบบชีวมาตรใช้ในการระบุตัวบุคคล ในภาพแสดงด้วยคำว่า bifurcating ridge (B)

4) Location and direction (XY-theta) ระบบตรวจสอบลายนิ้วมือจะจัดเก็บ (1) ตำแหน่งของจุดลักษณะเฉพาะ (X, Y) และ (2) ทิศทางหรือมุมของเส้นลาย (theta)

ข้อมูลดังกล่าวจะถูกจัดเก็บในฐานข้อมูลเพื่อใช้เปรียบเทียบกับลายนิ้วมือที่อ่านได้ในภายหลัง โดยระบบจะนำข้อมูลจุดลักษณะเฉพาะที่อ่านได้มาเปรียบเทียบกับข้อมูลที่จัดเก็บไว้ในฐานข้อมูล กระบวนการตรวจสอบลายนิ้วมือสามารถแบ่งได้เป็น 2 รูปแบบ ได้แก่ (1) การตรวจสอบแบบหนึ่งต่อหนึ่ง (one-to-one matching) ซึ่งเป็นการเปรียบเทียบลายนิ้วมือกับข้อมูลของบุคคลที่ระบุไว้แล้ว เช่น การยืนยันตัวตนร่วมกับรหัสผ่าน หมายเลขประจำตัว หรือบัตรประจำตัว และ (2) การตรวจสอบแบบหนึ่งต่อกลุ่ม (one-to-many identification) โดยเป็นการนำลายนิ้วมือที่อ่านได้ไปเปรียบเทียบกับข้อมูลทั้งหมดภายในฐานข้อมูล เพื่อค้นหาว่าลายนิ้วมือนั้นตรงกับบุคคลใด



(ก) การตรวจสอบลายนิ้วมือแบบใช้เฉพาะจุดลักษณะเฉพาะ (วิธีการแบบดั้งเดิม)

(ข) การตรวจสอบลายนิ้วมือแบบวิเคราะห์จุดลักษณะเฉพาะและความสัมพันธ์ระหว่างจุด (เทคโนโลยีของ NEC)

รูปที่ 5.8 หลักการตรวจสอบลายนิ้วมือด้วยการวิเคราะห์จุดลักษณะเฉพาะและความสัมพันธ์ของจุด (ดัดแปลงจาก Tandee, 2014; Martins et al., 2024)

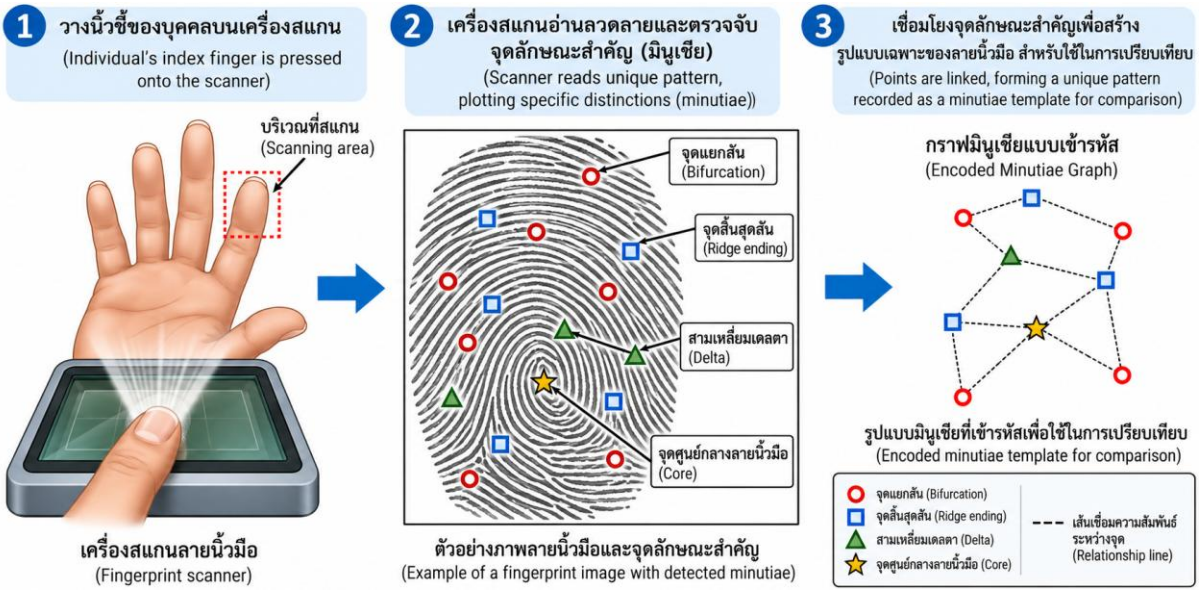
จากรูปที่ 5.8 แสดงการเปรียบเทียบหลักการตรวจสอบลายนิ้วมือ 2 รูปแบบ ได้แก่ การตรวจสอบลายนิ้วมือแบบใช้เฉพาะจุดลักษณะเฉพาะ (minutiae-only recognition method) และการตรวจสอบลายนิ้วมือแบบวิเคราะห์ความสัมพันธ์ระหว่างจุดลักษณะเฉพาะ (minutiae & relationship-based recognition method) ซึ่งเป็นเทคนิคที่ใช้ในระบบตรวจสอบลายนิ้วมือสมัยใหม่ ภาพด้านซ้ายเป็นการตรวจสอบลายนิ้วมือแบบ minutiae-only recognition method ซึ่งเป็นวิธีการดั้งเดิม โดยระบบจะพิจารณาเฉพาะ “จุดลักษณะเฉพาะ” (minutiae points) ของลายนิ้วมือ เช่น จุดสิ้นสุดของเส้นลายนิ้วมือ (ridge ending) และจุดแตกแขนงของเส้นลายนิ้วมือ (bifurcation point) รวมทั้งตำแหน่งและทิศทางของจุดเหล่านี้ จากนั้นนำข้อมูลไปเปรียบเทียบกับฐานข้อมูลลายนิ้วมือ วิธีการนี้มีข้อดีคือประมวลผลได้รวดเร็วและใช้ข้อมูลไม่มาก แต่เนื่องจากใช้จุดอ้างอิงในการเปรียบเทียบน้อย จึงอาจทำให้เกิดความคลาดเคลื่อนหรืออัตราการยอมรับผิดพลาด (False Acceptance Rate: FAR) สูงกว่าในบางกรณี

ส่วนรูป (ข) เป็นการตรวจสอบลายนิ้วมือแบบ minutiae and relationship-based recognition method ซึ่งเป็นเทคนิคที่พัฒนาต่อยอดจากวิธีดั้งเดิม โดยนอกจากจะพิจารณาตำแหน่งและทิศทางของจุดลักษณะเฉพาะแล้ว ระบบยังวิเคราะห์ “ความสัมพันธ์ระหว่างจุดลักษณะเฉพาะ” (inter-minutiae relationship) เช่น ระยะห่าง การเชื่อมโยง รูปแบบการกระจายตัวของจุดต่าง ๆ บนลายนิ้วมือร่วมด้วย (Tandee, 2014; Martins et al., 2024; Maiti et al., 2025) จึงช่วยเพิ่มความแม่นยำในการตรวจสอบและลดโอกาสเกิดความผิดพลาดในการยืนยันตัวตน จากภาพจะเห็นเส้นเชื่อมโยงระหว่างจุดลักษณะเฉพาะจำนวนมาก ซึ่งแสดงถึงโครงสร้างความสัมพันธ์ของจุดต่าง ๆ

ภายในลายนิ้วมือ ทำให้ระบบสามารถวิเคราะห์ลายนิ้วมือได้ละเอียดและมีประสิทธิภาพสูงกว่าวิธีแบบเดิม โดยแนวคิดนี้ถูกนำมาใช้ในระบบตรวจสอบลายนิ้วมือขั้นสูงและระบบพิสูจน์อัตลักษณ์บุคคลสมัยใหม่ ดังนั้น ภาพนี้จึงแสดงให้เห็นว่า ระบบตรวจสอบลายนิ้วมือสมัยใหม่ไม่ได้พิจารณาเฉพาะจุดลักษณะเฉพาะของลายนิ้วมือเท่านั้น แต่ยังวิเคราะห์ความสัมพันธ์ระหว่างจุดต่าง ๆ เพื่อเพิ่มความถูกต้อง ความแม่นยำ และความปลอดภัยในการยืนยันตัวตนอีกด้วย

5.1.5 กระบวนการสแกนและตรวจสอบลายนิ้วมือ (Fingerprint Scanning and Identification Process)

กระบวนการสแกนและตรวจสอบลายนิ้วมือ เป็นหลักการทำงานพื้นฐานของระบบตรวจสอบอัตลักษณ์ด้วยลายนิ้วมือ (fingerprint recognition system) โดยอาศัยการวิเคราะห์จุดลักษณะเฉพาะของลายนิ้วมือ หรือที่เรียกว่า minutiae เพื่อใช้ในการยืนยันตัวตนของบุคคล (Tandee, 2014; Martins et al., 2024) การทำงานสามารถอธิบายได้เป็นลำดับขั้นดังรูปที่ 5.9



รูปที่ 5.9 กระบวนการสแกนและตรวจสอบลายนิ้วมือ (ดัดแปลงจาก Tandee, 2014; Martins et al., 2024)

1) ขั้นตอนที่ 1 การวางนิ้วบนเครื่องสแกน (Fingerprint Acquisition)

ผู้ใช้งานนำปลายนิ้ว โดยทั่วไปมักใช้นิ้วชี้ วางลงบนพื้นที่สแกนของเครื่องอ่านลายนิ้วมือ (scanning area) เซนเซอร์ภายในเครื่องจะทำหน้าที่ตรวจจับลักษณะของเส้นลายนิ้วมือ ซึ่งประกอบด้วยสันลายและร่องลาย แล้วแปลงเป็นข้อมูลภาพดิจิทัล

2) ขั้นตอนที่ 2 การวิเคราะห์ลักษณะเฉพาะของลายนิ้วมือ (Feature Extraction)

หลังจากได้ภาพลายนิ้วมือ ระบบจะทำการวิเคราะห์และค้นหาจุดลักษณะเฉพาะ (minutiae points) ที่สำคัญบนลายนิ้วมือ เช่น (1) จุดสิ้นสุดของเส้นลายนิ้วมือ (ridge ending) (2) จุดแตกแขนงของเส้นลายนิ้วมือ (bifurcation) (3) จุดศูนย์กลางของลายนิ้วมือ (core) และ

(4) จุดที่แนวเส้นลายนิ้วมือแยกตัวเป็นลักษณะคล้ายสามเหลี่ยม (delta) ระบบจะบันทึกตำแหน่ง ทิศทาง และรูปแบบของจุดเหล่านี้ เพื่อนำไปใช้ในการเปรียบเทียบและยืนยันตัวตน

3) ขั้นตอนที่ 3 การสร้างข้อมูลแม่แบบลายนิ้วมือ (Template Creation)

เมื่อระบบตรวจพบจุดลักษณะเฉพาะแล้ว จะทำการเชื่อมโยงความสัมพันธ์ระหว่างจุดต่าง ๆ และแปลงเป็นข้อมูลดิจิทัลที่เรียกว่า “encoded minutiae graph” หรือ “fingerprint template” ข้อมูลดังกล่าวจะถูกจัดเก็บไว้ในฐานข้อมูลเพื่อใช้ในการตรวจสอบตัวตนในภายหลัง โดยระบบจะไม่เก็บภาพลายนิ้วมือทั้งหมดโดยตรง แต่จะเก็บเฉพาะข้อมูลคุณลักษณะสำคัญ เพื่อเพิ่มความรวดเร็วในการประมวลผลและลดขนาดของข้อมูล

หลักการสำคัญของระบบตรวจสอบลายนิ้วมือ ระบบตรวจสอบลายนิ้วมืออาศัยแนวคิดว่าลายนิ้วมือของแต่ละบุคคลมีรูปแบบและจุดลักษณะเฉพาะที่แตกต่างกัน และแทบไม่มีโอกาสซ้ำกัน จึงสามารถนำมาใช้ในการยืนยันตัวตนได้อย่างมีประสิทธิภาพ โดยระบบจะเปรียบเทียบข้อมูลจุดลักษณะเฉพาะของลายนิ้วมือที่สแกนใหม่กับข้อมูลที่จัดเก็บไว้ในฐานข้อมูล หากข้อมูลมีความสอดคล้องกันตามเกณฑ์ที่กำหนด ระบบจะยืนยันว่าเป็นบุคคลเดียวกัน (Tandee, 2014; Martins et al., 2024)

5.1.6 การแปลงลายนิ้วมือเป็นข้อมูลดิจิทัลสำหรับการตรวจสอบอัตลักษณ์ (Fingerprint Template Generation Process)

กระบวนการประมวลผลลายนิ้วมือในระบบชีวมาตร (biometric system) ตั้งแต่การรับภาพลายนิ้วมือ การสกัดจุดลักษณะเฉพาะ ไปจนถึงการแปลงเป็นข้อมูลดิจิทัลสำหรับใช้ในการยืนยันตัวตน โดยอาศัยหลักการวิเคราะห์จุดลักษณะเฉพาะของลายนิ้วมือ (minutiae-based recognition) ซึ่งเป็นเทคนิคที่ใช้กันอย่างแพร่หลายในระบบสแกนลายนิ้วมือสมัยใหม่ แสดงดังรูปที่ 5.10 ซึ่งมี 4 ขั้นตอนหลัก รายละเอียด ดังนี้

1) Biometric

ขั้นตอนแรกคือการรับภาพลายนิ้วมือจากเซนเซอร์สแกนลายนิ้วมือ โดยระบบจะบันทึกรูปแบบของเส้นลายนิ้วมือ (fingerprint ridge pattern) ซึ่งประกอบด้วยสันลายและร่องลายที่มีลักษณะเฉพาะแตกต่างกันในแต่ละบุคคล

2) Minutiae Points

หลังจากได้ภาพลายนิ้วมือ ระบบจะทำการวิเคราะห์และค้นหาจุดลักษณะเฉพาะ (minutiae points) ซึ่งเป็นจุดสำคัญที่ใช้ในการระบุตัวตน ได้แก่ (1) จุดสิ้นสุดของสันลาย (ridge ending) และ (2) จุดแตกแขนงของสันลาย (bifurcation) โดยตำแหน่งและทิศทางของจุดเหล่านี้จะแตกต่างกันในแต่ละบุคคล จึงสามารถใช้เป็นข้อมูลอ้างอิงในการตรวจสอบอัตลักษณ์ได้อย่างมีประสิทธิภาพ

3) Minutiae Map

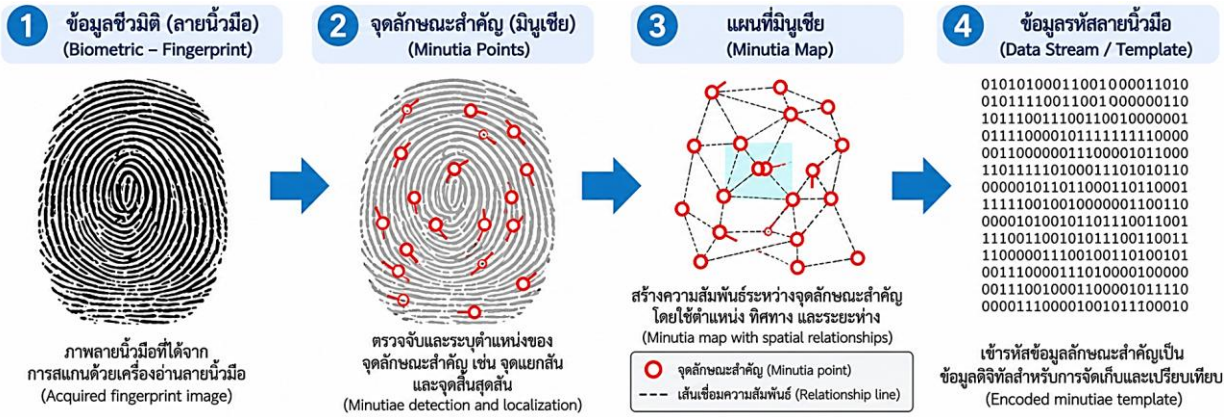
เมื่อได้จุดลักษณะเฉพาะแล้ว ระบบจะสร้างแผนผังความสัมพันธ์ระหว่างจุดต่าง ๆ (minutiae map) โดยคำนวณข้อมูล เช่น (1) ตำแหน่งพิกัด (X,Y) (2) ระยะห่างระหว่างจุด (3) มุมหรือทิศทางของจุด และ (4) ความสัมพันธ์ระหว่างจุดลักษณะเฉพาะ ซึ่งข้อมูลดังกล่าวจะถูก

จัดเก็บในรูปแบบโครงสร้างเชิงเรขาคณิตหรือกราฟ (graph structure) เพื่อใช้ในการเปรียบเทียบลายนิ้วมือในภายหลัง

4) Data Stream

ในขั้นตอนสุดท้าย ข้อมูลจาก minutiae map จะถูกเข้ารหัสและแปลงเป็นข้อมูลดิจิทัล (digital template) หรือกระแสข้อมูล (data stream) ในรูปแบบเลขฐานสอง (binary)

ระบบจะจัดเก็บข้อมูลดังกล่าวเป็น แม่แบบลายนิ้วมือ (fingerprint template) แทนการจัดเก็บภาพลายนิ้วมือจริง ซึ่งช่วยลดพื้นที่จัดเก็บ เพิ่มความเร็วในการประมวลผล และเพิ่มความปลอดภัยของข้อมูลชีวมาตร



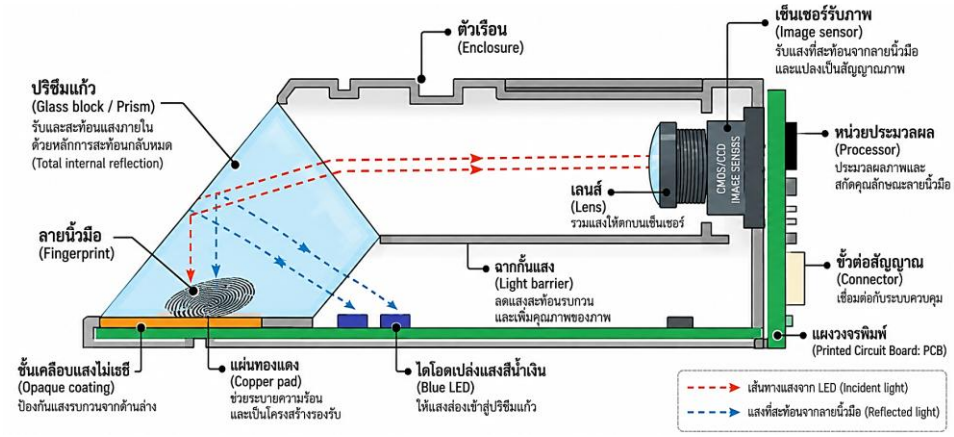
รูปที่ 5.10 กระบวนการแปลงลายนิ้วมือเป็นข้อมูลดิจิทัล (ดัดแปลงจาก (Tandee, 2014; Martins et al., 2024)

กล่าวโดยสรุป กระบวนการสร้างแม่แบบลายนิ้วมือ (fingerprint template generation) โดยเริ่มจากการรับภาพลายนิ้วมือ การตรวจหาจุดลักษณะเฉพาะ (minutiae points) การสร้างแผนผังความสัมพันธ์ระหว่างจุด (minutiae map) และการแปลงข้อมูลเป็นรูปแบบดิจิทัล (data stream) เพื่อใช้ในการจัดเก็บและเปรียบเทียบอัตลักษณ์ของบุคคลในระบบตรวจสอบลายนิ้วมืออัตโนมัติ (Automated Fingerprint Identification System: AFIS) และระบบยืนยันตัวตนทางชีวมาตร (biometric authentication system)

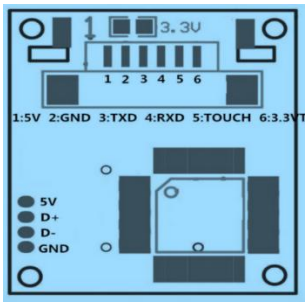
5.1.7 การใช้งานเซนเซอร์สแกนลายนิ้วมือ

1) โครงสร้างของเซนเซอร์สแกนลายนิ้วมือ

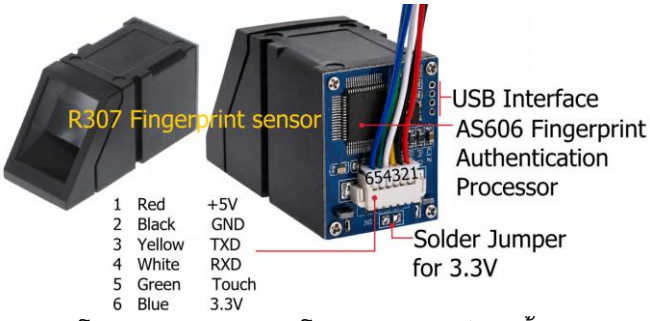
โครงสร้างและขาต่อสัญญาณของ เซนเซอร์สแกนลายนิ้วมือรุ่น R307 (Hangzhou Grow Technology Co., Ltd., 2011; Mohanan, 2021) ซึ่งเป็นอุปกรณ์ตรวจสอบอัตลักษณ์ทางชีวมาตร (biometric identification device) ที่นิยมใช้ร่วมกับไมโครคอนโทรลเลอร์ เช่น Arduino, ESP8266 และ ESP32 สำหรับงานควบคุมการเข้าออก ระบบรักษาความปลอดภัย และระบบยืนยันตัวตนด้วยลายนิ้วมือ



(ก) หลักการสร้างภาพลายนิ้วมือด้วยเทคโนโลยี optical fingerprint sensing



(ข) แผนผังขาและอินเทอร์เฟซ
การสื่อสารของโมดูล



(ค) โครงสร้างภายนอกโมดูลเซนเซอร์ลายนิ้วมือ R307
และหน่วยประมวลผล AS606

รูปที่ 5.11 โครงสร้าง หลักการทำงาน และส่วนประกอบของเซนเซอร์สแกนลายนิ้วมือ R307

จากรูปที่ 5.11 สามารถอธิบายหลักการทำงานได้ ดังนี้

1.1) ส่วนหัวอ่านลายนิ้วมือ (Fingerprint Sensor Module)

บริเวณด้านหน้าของอุปกรณ์เป็นส่วนหัวอ่านลายนิ้วมือ (optical fingerprint sensor) ทำหน้าที่รับภาพลายนิ้วมือของผู้ใช้งาน เมื่อผู้ใช้นำปลายนิ้วสัมผัสบนพื้นผิวสแกน (1) เซนเซอร์จะใช้แหล่งกำเนิดแสงภายในส่องไปยังผิวหนัง (2) ตรวจจับความแตกต่างระหว่างสันลาย และร่องลาย (3) สร้างเป็นภาพลายนิ้วมือในรูปแบบดิจิทัล และ (4) ส่งข้อมูลเข้าสู่หน่วยประมวลผลภายในโมดูล โดยเซนเซอร์ชนิดนี้เป็น optical fingerprint sensor ที่ใช้หลักการสะท้อนแสงในการสร้างภาพลายนิ้วมือ

1.2) หน่วยประมวลผลลายนิ้วมือ AS606

บริเวณแผงวงจรด้านหลังติดตั้งชิป AS606 fingerprint authentication processor ซึ่งเป็นไมโครโปรเซสเซอร์สำหรับประมวลผลลายนิ้วมือโดยเฉพาะ หน้าที่สำคัญ ได้แก่

1.2.1) การประมวลผลภาพลายนิ้วมือ (ชิป AS606) ทำหน้าที่ (1) รับภาพจากหัวอ่าน (2) ปรับปรุงคุณภาพของภาพ (3) กรองสัญญาณรบกวน และ (4) เพิ่มความคมชัดของเส้นลายนิ้วมือ

1.2.2) การสกัดคุณลักษณะเฉพาะ (feature extraction) โดยระบบจะวิเคราะห์จุดสำคัญบนลายนิ้วมือ เช่น ridge ending (จุดสิ้นสุดของสันลาย) และ bifurcation (จุดแตกแขนงของสันลาย) ซึ่งจุดเหล่านี้เรียกว่า minutiae points ซึ่งเป็นข้อมูลสำคัญสำหรับการยืนยันตัวตน

1.2.3) การสร้างแม่แบบลายนิ้วมือ (fingerprint template) โดยหลังจากวิเคราะห์จุด Minutiae แล้ว ชิป AS606 จะสร้าง fingerprint template ซึ่งเป็นข้อมูลทางคณิตศาสตร์แทนลายนิ้วมือ โดยไม่ได้เก็บภาพลายนิ้วมือทั้งหมด จะช่วยเพิ่ม ความเร็วในการประมวลผล ความปลอดภัยของข้อมูล และลดพื้นที่จัดเก็บข้อมูล

1.2.4) การเปรียบเทียบลายนิ้วมือ ชิป AS606 สามารถดำเนินการได้ทั้ง verification (1:1) เปรียบเทียบลายนิ้วมือกับ ID ที่กำหนด หรือ identification (1:N) ค้นหาลายนิ้วมือจากฐานข้อมูลทั้งหมด จากนั้นส่งผลลัพธ์กลับไปยังไมโครคอนโทรลเลอร์

1.3) USB Interface

บริเวณด้านขวาของแผงวงจรเป็น USB interface ใช้สำหรับเชื่อมต่อกับคอมพิวเตอร์เพื่อ (1) ลงทะเบียนลายนิ้วมือ (2) ทดสอบการทำงาน (3) จัดการฐานข้อมูลลายนิ้วมือ และ (4) อัปเดตเฟิร์มแวร์ โดยสามารถใช้งานร่วมกับโปรแกรมของผู้ผลิตได้โดยตรง

1.4) Solder Jumper for 3.3 V

บริเวณด้านล่างของแผงวงจรเป็น solder jumper ใช้สำหรับเลือกแรงดันไฟฟ้าของระบบ 3.3 V หรือ 5 V เพื่อให้สามารถใช้งานร่วมกับไมโครคอนโทรลเลอร์หลายประเภท เช่น Arduino UNO (5V), ESP8266 (3.3V), และ ESP32 (3.3V)

1.5) ขาสัญญาณของเซนเซอร์ R307

เซนเซอร์ R307 ใช้สายสัญญาณทั้งหมด 6 เส้น ดังแสดงในตารางที่ 5.1

ตารางที่ 5.1 สายสัญญาณสำหรับเชื่อมต่อของเซนเซอร์ R307

ลำดับ	สีสาย	ขาสัญญาณ	หน้าที่
1	แดง (Red)	+5 V	จ่ายไฟเลี้ยงให้เซนเซอร์
2	ดำ (Black)	GND	กราวด์ของระบบ
3	เหลือง (Yellow)	TXD	ส่งข้อมูลจากเซนเซอร์
4	ขาว (White)	RXD	รับข้อมูลจากไมโครคอนโทรลเลอร์
5	เขียว (Green)	Touch	ตรวจจับการสัมผัสนิ้ว
6	น้ำเงิน (Blue)	3.3V	ไฟเลี้ยงวงจรตรวจจับสัมผัส

1.6) หลักการสื่อสารข้อมูล

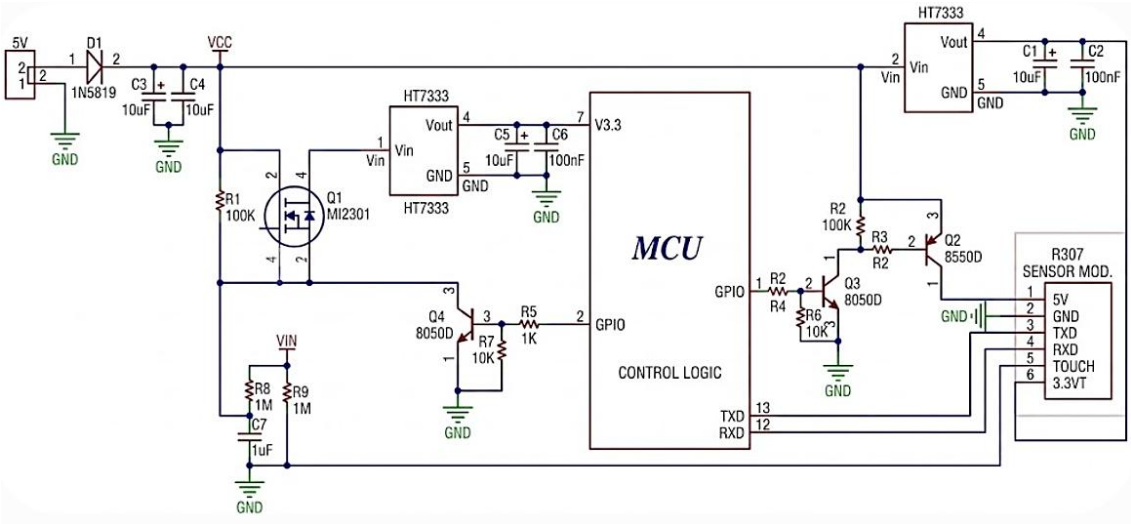
R307 ใช้การสื่อสารแบบ Universal Asynchronous Receiver/Transmitter (UART) ผ่านขา TXD (transmit data) และ RXD (receive data) โดยมีอัตรารับส่งข้อมูลเริ่มต้น (default baud rate) 57,600 bps และสามารถปรับได้ตั้งแต่ 9,600–115,200 bps ทำให้สามารถเชื่อมต่อกับ Arduino, ESP8266, ESP32 และคอมพิวเตอร์ได้อย่างสะดวก

กล่าวโดยสรุป เซนเซอร์สแกนลายนิ้วมือ R307 เป็นโมดูลตรวจสอบอัตลักษณ์ทางชีวมาตรที่ประกอบด้วยหัวอ่านลายนิ้วมือแบบออปติคัลและหน่วยประมวลผล AS606 ภายในตัว สามารถดำเนินการตั้งแต่การรับภาพลายนิ้วมือ การสกัดจุดลักษณะเฉพาะ (minutiae extraction) การสร้าง

แม่แบบลายนิ้วมือ (fingerprint template) ไปจนถึงการเปรียบเทียบลายนิ้วมือแบบ 1:1 และ 1:N ได้ภายในโมดูลเอง ทำให้ลดภาระการประมวลผลของไมโครคอนโทรลเลอร์และเพิ่มประสิทธิภาพในการพัฒนาระบบรักษาความปลอดภัยและระบบควบคุมการเข้า ออกด้วยลายนิ้วมือได้อย่างมีประสิทธิภาพสูง

2) การเชื่อมต่อและควบคุมเซนเซอร์สแกนลายนิ้วมือร่วมกับไมโครคอนโทรลเลอร์

การเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือ R307 เข้ากับไมโครคอนโทรลเลอร์ (MCU) โดยใช้การสื่อสารแบบอนุกรม (UART serial communication) สำหรับรับส่งข้อมูลลายนิ้วมือ และมีวงจรควบคุมการจ่ายไฟเพื่อประหยัดพลังงานและเพิ่มความเสถียรในการทำงานของระบบ โดยมีวงจรพื้นฐานสำหรับการเชื่อมต่อแสดงดังรูปที่ 5.12



รูปที่ 5.12 วงจรเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือ R307 ร่วมกับไมโครคอนโทรลเลอร์

จากรูปที่ 5.12 การทำงานของวงจรเริ่มจากแหล่งจ่ายไฟภายนอกที่ต่อเข้าทางด้านซ้ายของวงจร โดยกระแสไฟฟ้าจะไหลผ่านไดโอด 1N5819 ซึ่งทำหน้าที่ป้องกันการต่อขั้วไฟกลับ (reverse polarity protection) จากนั้นแรงดันไฟจะถูกกรองสัญญาณรบกวนด้วยตัวเก็บประจุ ก่อนเข้าสู่วงจรควบคุมแรงดันไฟฟ้า

ภายในวงจรใช้ตัวควบคุมแรงดันไฟฟ้า HT7333 เพื่อแปลงแรงดันไฟฟ้าให้คงที่ที่ 3.3 V สำหรับจ่ายให้กับไมโครคอนโทรลเลอร์และวงจรลอจิกต่าง ๆ โดยมีตัวเก็บประจุ C1–C6 ทำหน้าที่ลดสัญญาณรบกวนและรักษาเสถียรภาพของแรงดันไฟ

ไมโครคอนโทรลเลอร์ ทำหน้าที่ควบคุมการทำงานทั้งหมดของระบบ โดยติดต่อสื่อสารกับเซนเซอร์ลายนิ้วมือ R307 ผ่านขาสัญญาณ TXD สำหรับส่งข้อมูลจากเซนเซอร์ไปยัง MCU และ RXD สำหรับรับคำสั่งจาก MCU ไปยังเซนเซอร์ การสื่อสารดังกล่าวใช้มาตรฐาน UART ซึ่งเป็นการสื่อสารแบบอนุกรมที่นิยมใช้ในระบบสมองกลฝังตัว (embedded systems)

นอกจากนี้วงจรยังใช้ทรานซิสเตอร์ S8050 และ S8550 ร่วมกับตัวต้านทาน R2–R7 เพื่อควบคุมการจ่ายไฟและสัญญาณ Touch ของเซนเซอร์ R307 เมื่อผู้ใช้นำปลายนิ้วสัมผัสบริเวณหัวอ่านเซนเซอร์จะส่งสัญญาณ touch ไปยัง MCU เพื่อแจ้งให้ระบบเริ่มกระบวนการสแกนลายนิ้วมือ

ทำให้ไมโครคอนโทรลเลอร์สามารถเข้าสู่โหมดประหยัดพลังงานเมื่อไม่มีการใช้งาน และเริ่มทำงานเฉพาะเมื่อมีการตรวจพบนิ้วมือเท่านั้น วงจรนี้ประกอบด้วย 3 ส่วนหลัก ได้แก่

2.1) วงจรจ่ายไฟและควบคุมแรงดันไฟฟ้า ทำหน้าที่จ่ายไฟและป้องกันความเสียหายจากการต่อไฟผิดขั้ว

2.2) วงจรไมโครคอนโทรลเลอร์ (MCU) ทำหน้าที่ประมวลผลและควบคุมการทำงานของระบบ

2.3) วงจรเซนเซอร์ลายนิ้วมือ R307 ทำหน้าที่อ่าน วิเคราะห์ และส่งข้อมูลลายนิ้วมือเพื่อใช้ในการยืนยันตัวตนของผู้ใช้งาน

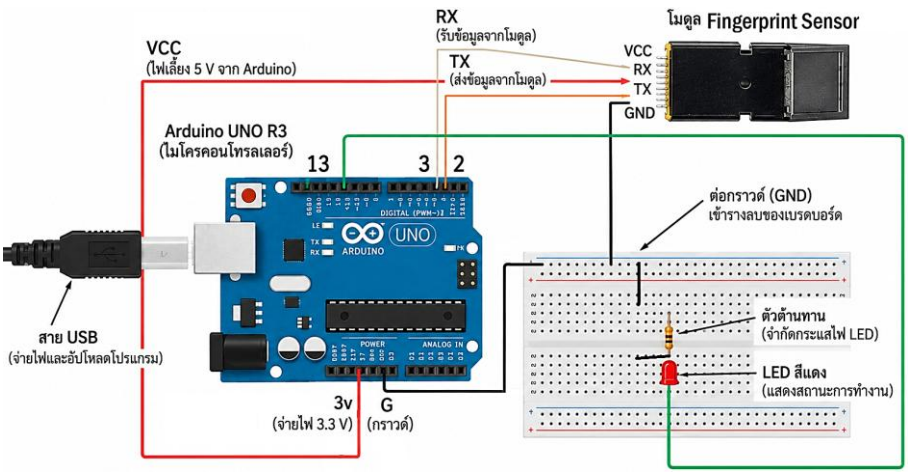
วงจรลักษณะนี้นิยมใช้ในระบบควบคุมการเข้า ออก ระบบบันทึกเวลา และระบบรักษาความปลอดภัยที่อาศัยการยืนยันตัวตนด้วยลายนิ้วมือ เป็นหลัก

4.1.8 การประยุกต์ใช้งานเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์

การเชื่อมต่อระหว่างไมโครคอนโทรลเลอร์ Arduino UNO กับ เซนเซอร์สแกนลายนิ้วมือ และหลอด LED เพื่อแสดงสถานะ เพื่อใช้ศึกษาการทำงานของระบบตรวจสอบลายนิ้วมือเบื้องต้น โดยอาศัยการสื่อสารข้อมูลแบบอนุกรมระหว่าง Arduino กับเซนเซอร์ลายนิ้วมือ

1) การเชื่อมต่อกับไมโครคอนโทรลเลอร์ Arduino UNO

การเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือ เชื่อมต่อเซนเซอร์ลายนิ้วมือ รุ่นJM101B ประกอบด้วยขาที่ใช้งานที่สำคัญ 4 ขา ได้แก่ VCC, GND, TX, และ RX โดยสามารถเชื่อมต่อกับไมโครคอนโทรลเลอร์ Arduino UNO ดังตารางที่ 5.2



รูปที่ 5.13 แผนผังการเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์เบื้องต้น

ตารางที่ 5.2 การเชื่อมต่อขาเซนเซอร์กับไมโครคอนโทรลเลอร์ Arduino UNO

ขาเซนเซอร์	เชื่อมต่อกับ Arduino UNO	หน้าที่
VCC	5V	จ่ายไฟเลี้ยงให้เซนเซอร์
GND	GND	กราวด์ร่วมของระบบ
TX	ขา Digital 2 (D2)	ส่งข้อมูลจากเซนเซอร์ไปยัง Arduino
RX	ขา Digital 3 (D3)	รับข้อมูลจาก Arduino

ในการใช้งานไมโครคอนโทรลเลอร์ Arduino จะใช้ไลบรารี SoftwareSerial เพื่อจำลองพอร์ตอนุกรม โดยกำหนด ขา D2 เป็น RX ของ Arduino และ ขา D3 เป็น TX ของ Arduino เพื่อให้สามารถรับส่งข้อมูลระหว่างอุปกรณ์ได้อย่างถูกต้อง ดังนั้น

- TX ของเซนเซอร์ เชื่อมต่อกับ ขา D2 ของ Arduino
- RX ของเซนเซอร์ เชื่อมต่อกับ ขา D3 ของ Arduino

ส่วนภาคแสดงผลใช้หลอด LED เชื่อมต่อกับขา D13 ของ Arduino ผ่านตัวต้านทานขนาด 220 Ω โดยมีการต่อวงจร ดังนี้

- ขั้วบวก LED (Anode) เชื่อมต่อกับ D13
- ขั้วลบ LED (Cathode) เชื่อมผ่านตัวต้านทาน 220 Ω ไปยัง GND
- ตัวต้านทาน 220 Ω มีหน้าที่จำกัดกระแสไฟฟ้าที่ไหลผ่าน LED เพื่อป้องกันความเสียหายของหลอด LED และขาเอาต์พุตของ Arduino

5.2 ระบบรักษาความปลอดภัยด้วยการยืนยันตัวตนด้วยใบหน้า (Facial Authentication System)

เทคโนโลยีการจดจำใบหน้า (face recognition) เป็นเทคโนโลยีชีวมาตร (biometric technology) ที่ใช้ลักษณะเฉพาะของใบหน้าในการระบุตัวตนหรือยืนยันตัวตนของบุคคล โดยอาศัยกล้องดิจิทัลร่วมกับอัลกอริทึมการประมวลผลภาพและปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อวิเคราะห์และเปรียบเทียบลักษณะทางกายภาพของใบหน้ากับข้อมูลที่จัดเก็บไว้ในฐานข้อมูล เทคโนโลยีนี้ได้รับความนิยมอย่างแพร่หลายในระบบควบคุมการเข้าออก ระบบรักษาความปลอดภัย สมาร์ตโฟน กล้องวงจรปิดอัจฉริยะ และระบบเฝ้าระวังสาธารณะ เนื่องจากสามารถระบุตัวบุคคลได้อย่างรวดเร็ว สะดวก และไม่จำเป็นต้องสัมผัสอุปกรณ์

รูปที่ 5.14 เครื่องสแกนใบหน้าและวิธีการจดจำใบหน้า

5.2.1 หลักการตรวจสอบและจดจำใบหน้า (Principles of Face Verification and Recognition)

การตรวจสอบใบหน้าเป็นกระบวนการทางชีวมิติ (biometric authentication) ที่ใช้ลักษณะเฉพาะของใบหน้าบุคคลเป็นข้อมูลสำหรับตรวจสอบอัตลักษณ์ โดยระบบจะวิเคราะห์รูปแบบหรือลักษณะของใบหน้าที่ได้จากภาพดิจิทัลหรือเฟรมวิดีโอ แล้วเปรียบเทียบกับข้อมูลใบหน้าที่ได้ลงทะเบียนไว้ก่อนหน้า เพื่อพิจารณาว่าเป็นบุคคลเดียวกันหรือไม่ เทคโนโลยีดังกล่าวสามารถนำไปใช้ในการยืนยันตัวบุคคล การอนุญาตให้เข้าถึงระบบหรือพื้นที่ และระบบเฝ้าระวังด้านความปลอดภัยได้ (EL Fadel, 2025) ในทางปฏิบัติ ควรแยกความหมายระหว่าง การตรวจจับใบหน้า (face detection) กับ การจดจำใบหน้า (face recognition) ให้ชัดเจน การตรวจจับใบหน้ามีหน้าที่ค้นหาว่า “บริเวณใดของภาพเป็นใบหน้า” ขณะที่การจดจำใบหน้าเป็นขั้นตอนวิเคราะห์คุณลักษณะของใบหน้าที่ตรวจพบ แล้วนำไปเปรียบเทียบกับข้อมูลอ้างอิงเพื่อระบุตัวตนหรือตรวจสอบอัตลักษณ์ ระบบสมัยใหม่จึงเป็นการทำงานร่วมกันระหว่างการประมวลผลภาพ (image processing) คอมพิวเตอร์วิทัศน์ (computer vision) การเรียนรู้ของเครื่อง (machine learning) และการเรียนรู้เชิงลึก (deep learning) โดยเฉพาะโครงข่ายประสาทเทียมแบบคอนโวลูชัน (Convolutional Neural Network: CNN) ซึ่งมีบทบาทสำคัญต่อการเพิ่มประสิทธิภาพของระบบจดจำใบหน้า (EL Fadel, 2025) มีกระบวนการดังนี้

1) การรับภาพใบหน้า (Face Image Acquisition)

ขั้นตอนแรกคือการรับข้อมูลภาพของบุคคลจากอุปกรณ์รับภาพ เช่น กล้องดิจิทัล กล้องเว็บแคม กล้อง IP หรือกล้องของอุปกรณ์เคลื่อนที่ โดยข้อมูลอาจอยู่ในรูปภาพนิ่งหรือเฟรมของวิดีโอ ในระบบรักษาความปลอดภัย กล้องมักติดตั้งบริเวณจุดควบคุมการเข้า–ออกเพื่อรับภาพบุคคลที่เข้ามาในพื้นที่ จากนั้นภาพจะถูกส่งเข้าสู่กระบวนการประมวลผลต่อไป การรับข้อมูลเป็นขั้นตอนพื้นฐานของระบบชีวมิติ โดย EL Fadel (2025) อธิบายกระบวนการทั่วไปว่าเริ่มจากการรับข้อมูลชีวมิติผ่านเซนเซอร์ ก่อนเข้าสู่การสกัดคุณลักษณะ การสร้างตัวแทนข้อมูล การเปรียบเทียบและการตัดสินใจ ในระบบประตูอัจฉริยะ ตัวอย่างจาก Trang และ Hao (2023) แสดงให้เห็นว่ากล้องสามารถจับภาพผู้ใช้แล้วส่งข้อมูลไปยังบริการประมวลผลใบหน้าเพื่อดำเนินการตรวจสอบก่อนส่งผลกลับมายังระบบควบคุมประตู

2) การตรวจจับใบหน้า (Face Detection)

เมื่อได้รับภาพแล้ว ระบบจะค้นหาตำแหน่งของใบหน้าในภาพและแยกบริเวณใบหน้าออกจากพื้นหลัง กระบวนการนี้มีความสำคัญเนื่องจากภาพจากกล้องอาจประกอบด้วยวัตถุหลายชนิดและอาจมีบุคคลมากกว่าหนึ่งคน ระบบจึงต้องกำหนดบริเวณใบหน้า (Region of Interest: ROI) ก่อนนำข้อมูลเข้าสู่ขั้นตอนการวิเคราะห์อัตลักษณ์

เทคนิคสำหรับตรวจจับใบหน้ามีทั้งวิธีดั้งเดิมและวิธีที่อาศัยการเรียนรู้เชิงลึก ตัวอย่างงานที่รวบรวมในไฟล์ของ Rivera et al. (2024) กล่าวถึงการใช้ OpenCV และตัวจำแนกสำหรับการตรวจจับและจดจำใบหน้า ขณะที่แนวทางสมัยใหม่สามารถใช้โครงข่ายประสาทเทียมเพื่อรองรับการประมวลผลภาพแบบเวลาจริง (real-time processing)

3) การปรับสภาพและจัดแนวใบหน้า (Face Preprocessing and Alignment)

หลังจากตรวจพบใบหน้าแล้ว ภาพใบหน้าควรได้รับการปรับสภาพก่อนการสกัดคุณลักษณะ เช่น การปรับขนาดภาพ (resizing) การปรับค่าความเข้มและการทำให้ข้อมูลอยู่ในช่วงมาตรฐาน (normalization) ตลอดจนการจัดแนวใบหน้า (face alignment) เพื่อลดผลกระทบจากตำแหน่งและมุมของใบหน้า จุดสำคัญบนใบหน้า (facial landmarks) เช่น ตา จมูก และปาก สามารถใช้เป็นข้อมูลประกอบในการกำหนดตำแหน่งและจัดแนวใบหน้า ตัวอย่างระบบ Face API ในงานของ Trang และ Hao (2023) แสดงให้เห็นว่าบริการตรวจจับใบหน้าสามารถส่งคืนทั้งรหัสใบหน้า (face ID) และตำแหน่งจุดสำคัญบนใบหน้า (face landmarks)

ขั้นตอนนี้มีความสำคัญต่อความสม่ำเสมอของข้อมูล เพราะความแตกต่างด้านมุมใบหน้า ความละเอียด ความเบลอ และสภาพการรับภาพสามารถส่งผลต่อประสิทธิภาพของการจดจำ จาก Labinjan et al. (2026) แสดงให้เห็นว่าคุณภาพและความแปรปรวนของชุดข้อมูล เช่น ความละเอียด ความเบลอ และความแตกต่างภายในบุคคลเดียวกัน ส่งผลโดยตรงต่อประสิทธิภาพของระบบจดจำใบหน้า

4) การสกัดคุณลักษณะใบหน้า (Facial Feature Extraction)

ขั้นตอนสำคัญของการจดจำใบหน้าคือการแปลงภาพใบหน้าให้เป็นข้อมูลเชิงตัวเลขที่แสดงคุณลักษณะสำคัญของใบหน้า ในระบบสมัยใหม่ แบบจำลอง deep learning สามารถสร้างเวกเตอร์คุณลักษณะ (feature vector) หรือ face embedding ซึ่งเป็นตัวแทนของลักษณะใบหน้าในปริภูมิหลายมิติ

หลักการสำคัญคือ ภาพใบหน้าของบุคคลเดียวกันควรให้เวกเตอร์ที่อยู่ใกล้กันในปริภูมิคุณลักษณะ ในขณะที่ใบหน้าของคนต่างกันควรมีเวกเตอร์ที่แยกห่างจากกัน ดังนั้น ระบบจึงไม่จำเป็นต้องเปรียบเทียบภาพดิบแบบพิกเซลต่อพิกเซล แต่สามารถเปรียบเทียบตัวแทนเชิงตัวเลขของใบหน้าแทน ตัวอย่างคือ Labinjan et al. (2026) โดยใช้ Contrastive Language–Image Pre-Training (CLIP) สกัดคุณลักษณะจากภาพใบหน้าเป็นเวกเตอร์ขนาด 512 มิติ และเชื่อมโยง embedding แต่ละรายการเข้ากับอัตลักษณ์ที่ทราบ เพื่อสร้างฐานข้อมูลสำหรับใช้ในขั้นตอนการจดจำ

5) การเปรียบเทียบใบหน้า (Face Matching)

เมื่อได้ face embedding ของบุคคลที่ต้องการตรวจสอบแล้ว ระบบจะนำเวกเตอร์ดังกล่าวไปเปรียบเทียบกับเวกเตอร์อ้างอิง (reference template) ที่เก็บไว้ในฐานข้อมูล โดยคำนวณค่าความคล้ายคลึง (similarity) หรือ ระยะห่าง (distance) ระหว่างเวกเตอร์ ตัวอย่างหนึ่งคือการใช้ Euclidean distance (L2 distance) โดยกำหนดเวกเตอร์ใบหน้าสองเวกเตอร์เป็น A และ B และคำนวณระยะห่าง (Labinjan et al., 2026) ดังนี้

$$d(A,B) = \sqrt{\sum_{i=1}^{n} (a_i - b_i)^2} \qquad (5.1)$$

โดยทั่วไป หากค่าระยะห่างมีค่าน้อย แสดงว่าเวกเตอร์ทั้งสองมีความใกล้เคียงกันมากกว่า ตัวอย่างระบบของ Labinjan et al. (2026) ใช้ FAISS จัดเก็บ face embeddings และค้นหาเวกเตอร์ที่ใกล้เคียงด้วย L2 distance เพื่อใช้ในการเปรียบเทียบและจำแนกใบหน้า

6) การตรวจสอบหรือระบุตัวบุคคล (Verification and Identification)

การประยุกต์ใช้การจดจำใบหน้าสามารถแบ่งตามลักษณะของการเปรียบเทียบได้เป็น 2 กรณีสำคัญ ได้แก่ การตรวจสอบตัวตน (face verification) และ การระบุตัวบุคคล (face identification) การจดจำใบหน้าสามารถทำงานได้ 2 รูปแบบ (EL Fadel, 2025) ได้แก่

6.1) การยืนยันตัวตน (verification: 1:1 matching) เป็นการเปรียบเทียบใบหน้าของผู้ใช้งานกับข้อมูลที่ระบุไว้ล่วงหน้าเพียงหนึ่งรายการ เช่น การปลดล็อกโทรศัพท์มือถือหรือการเข้าสู่ระบบด้วยใบหน้า

6.2) การระบุตัวตน (identification: 1: N matching) เป็นการนำใบหน้าที่สแกนมาเปรียบเทียบกับข้อมูลทั้งหมดในฐานข้อมูล เพื่อค้นหาว่าบุคคลนั้นเป็นใคร เช่น ระบบเฝ้าระวังในสนามบิน สถานีรถไฟ หรือพื้นที่สาธารณะ

ปัจจุบันระบบสแกนใบหน้าสมัยใหม่ได้พัฒนาไปสู่การตรวจจับใบหน้าแบบสามมิติ (3D face recognition) โดยใช้กล้องอินฟราเรด (infrared camera) หรือเซนเซอร์วัดความลึก (depth sensor) เพื่อสร้างแบบจำลองใบหน้าแบบสามมิติ ทำให้สามารถตรวจสอบรูปทรง ความลึกและมิติของใบหน้าได้อย่างแม่นยำมากขึ้น ลดปัญหาการปลอมแปลงด้วยภาพถ่าย

7) การกำหนดเกณฑ์และการตัดสินใจ (Threshold and Decision)

ผลจากการเปรียบเทียบไม่ได้หมายความว่าระบบจะยอมรับบุคคลทันที แต่ต้องนำ Matching Score, Similarity Score หรือ Distance ไปเปรียบเทียบกับค่าเกณฑ์ที่กำหนดไว้ (decision threshold) แล้วจึงตัดสินใจว่าใบหน้าตรงกับข้อมูลอ้างอิงหรือไม่ ดังนั้น หลักการตัดสินใจสามารถแสดงอย่างง่ายได้ว่า

$$\text{Decision} = \begin{cases} \text{Accept}, & \text{เมื่อคะแนนผ่านเกณฑ์ที่กำหนด} \\ \text{Reject}, & \text{เมื่อคะแนนไม่ผ่านเกณฑ์ที่กำหนด} \end{cases} \tag{5.2}$$

EL Fadel (2025) อธิบายกระบวนการทางชีวมิติว่าหลังจากเปรียบเทียบตัวอย่างแล้ว ระบบจะตัดสินใจยืนยันหรือปฏิเสธอัตลักษณ์ตามว่าคะแนนการจับคู่ผ่านเกณฑ์ที่กำหนดหรือไม่ ตัวอย่างเชิงประยุกต์จาก Rivera et al. (2024) ใช้ค่าความเข้ากันได้มากกว่า 0.98 เป็นเงื่อนไขของระบบทดลองเพื่ออนุญาตให้ผู้ใช้เข้าถึงระบบ อย่างไรก็ตาม ค่า 0.98 เป็นค่าที่ใช้ในระบบทดลองนั้น ไม่ควรถือเป็นค่าเกณฑ์สากลสำหรับระบบจดจำใบหน้าทุกระบบ

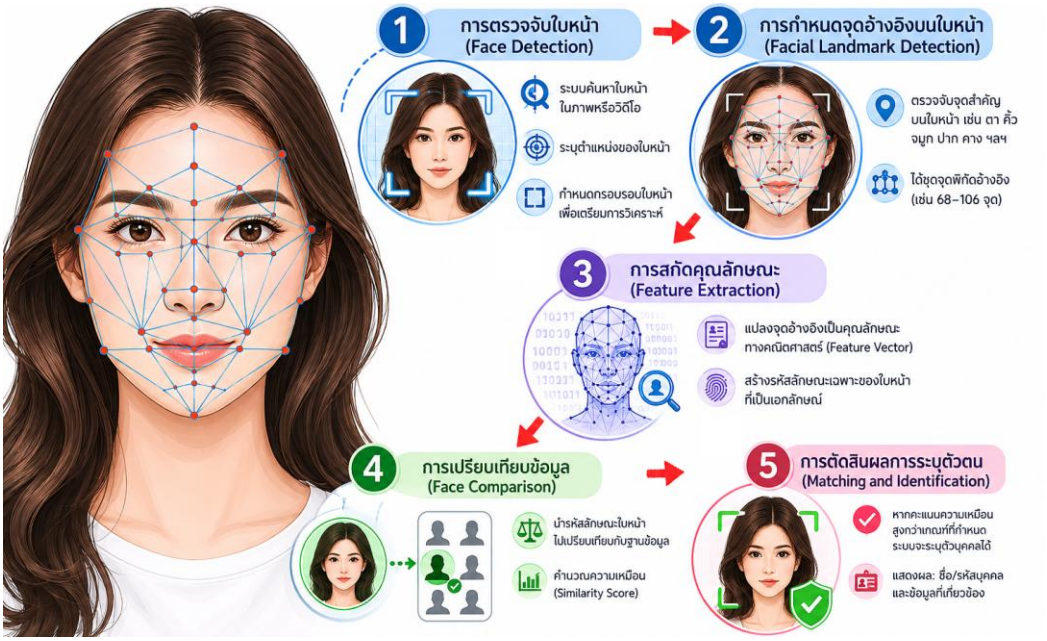
8) การนำผลไปควบคุมระบบรักษาความปลอดภัย

ในระบบรักษาความปลอดภัยอัจฉริยะ ผลลัพธ์จาก face verification หรือ Face Identification สามารถเชื่อมต่อกับระบบควบคุมการเข้า–ออก (access control system) ได้โดยตรง เช่น หากตรวจสอบผ่าน ระบบสามารถส่งคำสั่งไปยังรีเลย์หรือชุดควบคุมเพื่อปลดล็อกประตู บันทึกเวลาเข้า–ออก หรือส่งข้อมูลไปยังระบบส่วนกลาง แต่หากไม่ผ่านการตรวจสอบ ระบบ

สามารถคงสถานะล็อก บันทึกเหตุการณ์ หรือส่งสัญญาณแจ้งเตือนไปยังผู้ดูแล ตัวอย่างจาก Trang และ Hao (2023) แสดงการทำงานในลักษณะดังกล่าวอย่างชัดเจน โดยกล้องจับภาพผู้ใช้ ส่งภาพไปประมวลผลและเปรียบเทียบ จากนั้นระบบจะเปิดประตูเมื่อยืนยันใบหน้าสำเร็จ หรือคงประตูไว้ในสถานะล็อกเมื่อไม่สามารถยืนยันผู้ใช้ได้

5.2.2 กระบวนการระบบจดจำใบหน้า

การจดจำใบหน้าแตกต่างจากการมองเห็นภาพทั่วไป เนื่องจากระบบไม่ได้พิจารณาเพียงรูปภาพของบุคคล แต่จะวิเคราะห์ลักษณะทางเรขาคณิตของใบหน้า (facial geometry) และตำแหน่งของจุดสำคัญบนใบหน้า (facial landmarks) เช่น ตำแหน่งดวงตา คิ้ว จมูก ปาก คาง และโครงสร้างใบหน้า เพื่อนำมาสร้างเป็นข้อมูลดิจิทัลเฉพาะบุคคลที่เรียกว่า face template หรือ faceprint ซึ่งเปรียบเสมือนลายนิ้วมือของใบหน้า กระบวนการระบบจดจำใบหน้าประกอบด้วยขั้นตอนสำคัญ ดังนี้



รูปที่ 5.15 กระบวนการจดจำใบหน้าด้วยเทคโนโลยีไบโอเมตริกซ์

1) การตรวจจับใบหน้า (Face Detection)

ระบบจะใช้กล้องหรืออุปกรณ์รับภาพในการบันทึกภาพนิ่งหรือภาพเคลื่อนไหว จากนั้นอัลกอริทึมจะทำการค้นหาและแยกบริเวณใบหน้าออกจากพื้นหลัง รวมถึงตรวจสอบตำแหน่งและทิศทางของใบหน้า เพื่อให้สามารถนำข้อมูลไปวิเคราะห์ต่อได้อย่างถูกต้อง

2) การกำหนดจุดอ้างอิงบนใบหน้า (Facial Landmark Detection)

หลังจากตรวจพบใบหน้าแล้ว ระบบจะวิเคราะห์จุดสำคัญบนใบหน้าหลายจุด เช่น มุมตาซ้ายและขวา ปลายจมูก รูจมูก มุมปาก แนวคิ้ว โหนกแก้ม แนวกราม คาง เป็นต้น จุดอ้างอิง

เหล่านี้อาจมีจำนวนตั้งแต่ 68 จุด ไปจนถึงมากกว่า 100 จุด ขึ้นอยู่กับเทคโนโลยีที่ใช้ เพื่อสร้างโครงข่ายความสัมพันธ์ขององค์ประกอบบนใบหน้า

3) การสกัดคุณลักษณะ (Feature Extraction)

ระบบจะคำนวณคุณลักษณะทางเรขาคณิตของใบหน้า เช่น ระยะห่างระหว่างดวงตา ความกว้างของจมูก รูปร่างของปาก ความยาวของคาง ความลึกของเบ้าตา หรือลักษณะพื้นผิวของใบหน้า (facial texture) โดยข้อมูลเหล่านี้จะถูกแปลงเป็นข้อมูลเชิงตัวเลข (numerical features) และจัดเก็บเป็น face template สำหรับใช้ในการเปรียบเทียบ

4) การเปรียบเทียบข้อมูล (Face Comparison)

ระบบจะนำ face template ที่ได้จากการสแกนมาเปรียบเทียบกับข้อมูลใบหน้าที่จัดเก็บไว้ในฐานข้อมูล โดยใช้เทคนิคการประมวลผลภาพและอัลกอริทึมปัญญาประดิษฐ์ เพื่อคำนวณค่าความคล้ายคลึง (similarity score)

5) การตัดสินผลการระบุตัวตน (Matching and Identification)

เมื่อเปรียบเทียบเสร็จสิ้น ระบบจะประเมินผลตามค่าความคล้ายคลึงที่กำหนด หากข้อมูลตรงกับบุคคลในฐานข้อมูล ระบบจะยืนยันตัวตนและอนุญาตให้เข้าถึงระบบหรือพื้นที่ที่ได้รับสิทธิ์ แต่หากไม่ตรงกัน ระบบจะปฏิเสธการเข้าถึง

5.2.3 วิธีการตรวจจับใบหน้าด้วย OpenCV และ Haar Cascade

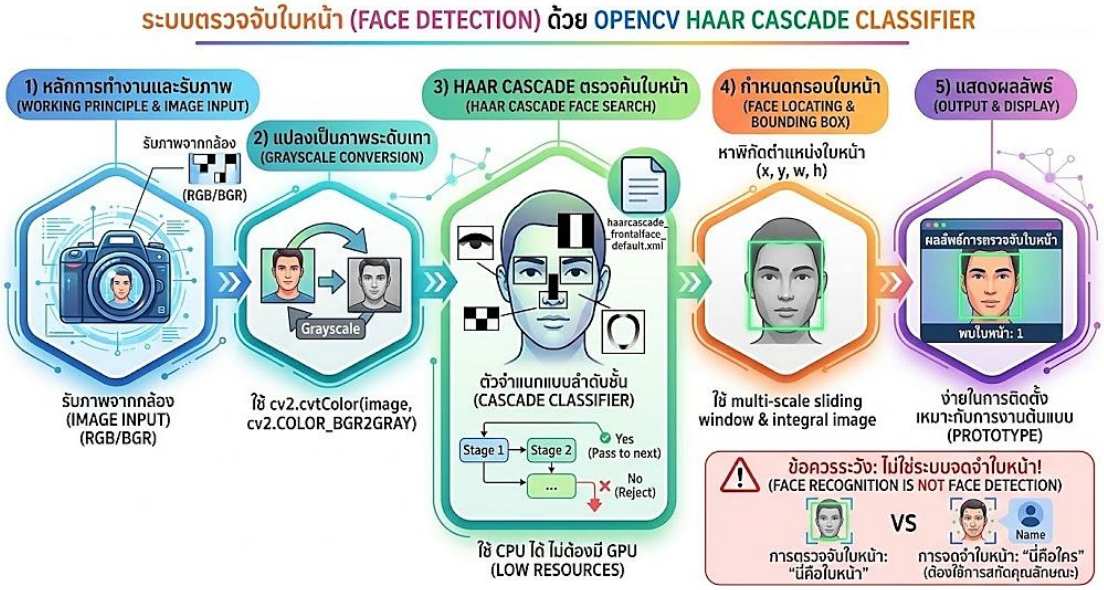
ระบบตรวจจับใบหน้า (face detection) โดยใช้ Haar Cascade Classifier ใน OpenCV สำหรับการตรวจจับใบหน้า ง่ายในการติดตั้ง ใช้ทรัพยากรไม่มาก เหมาะกับการงานต้นแบบ และมีงานในไฟล์แนบที่กล่าวถึงการใช้ OpenCV ร่วมกับตัวจำแนกแบบ cascade สำหรับระบบควบคุมการเข้า–ออกด้วยใบหน้า อย่างไรก็ตาม Haar Cascade ใช้สำหรับ “ตรวจจับใบหน้า” ว่ามีใบหน้าอยู่ตรงไหนในภาพ ไม่ใช่การ “จดจำว่าเป็นใคร” (face recognition) ซึ่งต้องมีขั้นตอนสกัดคุณลักษณะและเปรียบเทียบกับฐานข้อมูลเพิ่มเติม ระบบจดจำใบหน้าจริงจึงประกอบด้วยการรับภาพ ตรวจจับใบหน้า สกัดหรือวิเคราะห์ลักษณะใบหน้า และเปรียบเทียบกับข้อมูลอ้างอิง (Rivera et al., 2024; EL Fadel, 2025; Labinjan et al., 2026) วิธีการตรวจจับใบหน้าด้วย OpenCV และ Haar Cascade มีขั้นตอนดังต่อไปนี้

1) หลักการทำงานของ Haar cascade

Haar cascade เป็นวิธีตรวจจับวัตถุที่ใช้ตัวจำแนกแบบลำดับชั้น (cascade classifier) เพื่อตรวจสอบว่าบริเวณต่าง ๆ ของภาพมีรูปแบบที่สอดคล้องกับใบหน้าหรือไม่ ในการใช้งานไม่จำเป็นต้องฝึกโมเดลใหม่เอง เพราะ OpenCV มีไฟล์โมเดลที่ผ่านการฝึกมาแล้ว เช่น

```
haarcascade_frontalface_default.xml
```

ไฟล์ดังกล่าวใช้สำหรับตรวจจับ ใบหน้าที่หันค่อนข้างตรงเข้าหากล้อง (frontal face) เหมาะสำหรับการทดลองในห้องเรียน ระบบเช็กชื่อ หรือระบบประตูต้นแบบ เนื่องจากใช้ CPU ได้ และไม่จำเป็นต้องมี GPU กระบวนการทำงานสามารถสรุปได้ดังนี้



รูปที่ 5.16 กระบวนการตรวจจับใบหน้าด้วย OpenCV และ Haar Cascade

แนวทางนี้สอดคล้องกับไฟล์ Rivera et al. (2024) ซึ่งกล่าวถึงการใช้ OpenCV สำหรับการตรวจจับและประมวลผลใบหน้า และการนำไปใช้ร่วมกับระบบ Raspberry Pi สำหรับระบบควบคุมการเข้า–ออก

2) อุปกรณ์และซอฟต์แวร์ที่ใช้

สำหรับการทดลองขั้นพื้นฐาน ใช้เพียงคอมพิวเตอร์หรือโน้ตบุ๊กที่มีกล้อง Webcam ก็เพียงพอ ไม่จำเป็นต้องใช้ Raspberry Pi ในขั้นแรก เนื่องจากจะช่วยลดความซับซ้อนของการติดตั้ง ให้ทำการติดตั้ง Python 3, OpenCV, และกล้อง Webcam การติดตั้ง OpenCV ด้วยคำสั่ง

```
pip install opencv-python
```

หลังจากติดตั้งแล้ว OpenCV จะมี Haar Cascade หลายแบบอยู่ภายในแพ็กเกจ ทำให้ไม่จำเป็นต้องดาวน์โหลดไฟล์ XML แยกเอง

3) ขั้นตอนที่ 1 นำเข้า OpenCV และโหลดโมเดล เริ่มต้นด้วย

```
import cv2

face_cascade = cv2.CascadeClassifier(
  cv2.data.haarcascades +"haarcascade_frontalface_default.xml"
)
```

คำสั่ง CascadeClassifier() ทำหน้าที่โหลดตัวจำแนกใบหน้าที่ผ่านการฝึกไว้แล้ว ควรตรวจสอบว่าโหลดโมเดลสำเร็จหรือไม่

```
if face_cascade.empty():
    print("Cannot load Haar Cascade model")
    exit()
```

ส่วนนี้มีความสำคัญ เพราะหากไฟล์โมเดลไม่ถูกต้อง โปรแกรมจะไม่สามารถตรวจจับใบหน้าได้

4) ขั้นตอนที่ 2 เปิดกล้อง ใช้คำสั่ง

```
cap = cv2.VideoCapture(0)
```

ค่า 0 หมายถึงกล้องหลักของคอมพิวเตอร์ หากมีหลายกล้องอาจเปลี่ยนเป็น 1 หรือ 2 ในการตรวจสอบว่ากล้องเปิดได้หรือไม่

```
if not cap.isOpened():
    print("Cannot open camera")
    exit()
```

5) ขั้นตอนที่ 3 อ่านภาพจากกล้อง ใช้ลูปเพื่ออ่านภาพต่อเนื่อง

```
while True:
    ret, frame = cap.read()

    if not ret:
        break
```

ตัวแปร frame คือภาพที่รับจากกล้องในแต่ละเฟรม

ระบบจดจำใบหน้าแบบเวลาจริงจำเป็นต้องประมวลผลเฟรมต่อเนื่องจากกล้อง ซึ่งแนวคิดการใช้ live video มีข้อดีตรงที่สามารถรวบรวมข้อมูลใบหน้าได้หลายเฟรมและลดผลกระทบจากความผิดปกติของเฟรมใดเฟรมหนึ่ง เช่น ภาพเบลอ มุมใบหน้า หรือแสงไม่เหมาะสม

6) ขั้นตอนที่ 4 แปลงภาพเป็นระดับเทา

Haar Cascade โดยทั่วไปทำงานกับภาพระดับเทา (grayscale image) จึงควรแปลงจากภาพสี BGR เป็น grayscale ก่อน การใช้ภาพระดับเทาช่วยลดข้อมูลที่ต้องประมวลผลจาก 3 ช่องสีเหลือเพียง 1 ช่อง ทำให้กระบวนการตรวจจับทำงานได้รวดเร็วขึ้น

```
gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
```

สามารถเพิ่มการปรับความแตกต่างของความสว่างได้ด้วย

```
gray = cv2.equalizeHist(gray)
```

ซึ่งอาจช่วยในกรณีที่แสงไม่สม่ำเสมอ อย่างไรก็ตาม ปัจจัยด้านแสง มุมใบหน้า ความละเอียด และคุณภาพภาพยังคงมีผลต่อประสิทธิภาพของระบบตรวจจับและจดจำใบหน้าในงานจริง

7) ขั้นตอนที่ 5 ตรวจจับใบหน้า ใช้คำสั่ง

```
faces = face_cascade.detectMultiScale(
    gray,
    scaleFactor=1.1,
    minNeighbors=5,
    minSize=(80, 80)
)
```

ค่าที่สำคัญมีดังนี้

➲ scaleFactor = 1.1 หมายถึงการลดขนาดภาพลงทีละประมาณ 10% เพื่อค้นหาใบหน้าในหลายขนาด หากตั้งใกล้ 1 มากขึ้นจะตรวจละเอียดขึ้น แต่ใช้เวลาประมวลผลมากขึ้น

➲ minNeighbors = 5 หมายถึงจำนวนบริเวณใกล้เคียงขั้นต่ำที่ต้องสนับสนุนว่าตำแหน่งนั้นเป็นใบหน้า ค่าสูงช่วยลด False Positive แต่หากสูงมากเกินไปอาจตรวจไม่พบใบหน้าบางภาพ

➲ minSize = (80,80) กำหนดขนาดใบหน้าขั้นต่ำที่ต้องการตรวจจับ ช่วยลดการตรวจจับวัตถุขนาดเล็กที่ไม่จำเป็น สำหรับการทดลองในห้องเรียน ค่า

➲ scaleFactor = 1.1

➲ minNeighbors = 5

➲ minSize = (80, 80)

ถือเป็นจุดเริ่มต้นที่เหมาะสม แล้วจึงปรับตามระยะกล้องและสภาพแสง

8) ขั้นตอนที่ 6 วาดกรอบรอบใบหน้า

ค่าที่ได้จาก detectMultiScale() คือ x, y, w, h โดย

➲ x = ตำแหน่งด้านซ้าย

➲ y = ตำแหน่งด้านบน

➲ w = ความกว้าง

➲ h = ความสูง

นำมาใช้วาดกรอบ

```
for (x, y, w, h) in faces:
    cv2.rectangle(
        frame,
        (x, y),
        (x + w, y + h),
        (0, 255, 0),
        2
    )
```

จากนั้นแสดงจำนวนใบหน้าที่ตรวจพบได้ด้วย

```
cv2.putText(
    frame,
    f"Faces: {len(faces)}",
    (20, 40),
    cv2.FONT_HERSHEY_SIMPLEX,
    1,
    (0, 255, 0),
    2
)
```

9) ขั้นตอนที่ 7 แสดงภาพ ใช้คำสั่ง

```
cv2.imshow("Face Detection", frame)
```

และกำหนดให้กด q เพื่อออกจากโปรแกรม

```
if cv2.waitKey(1) & 0xFF == ord('q'):
    break
```

หลังจบการทำงานต้องคืนทรัพยากรให้ระบบ

```
cap.release()
cv2.destroyAllWindows()
```

5.2.4 ความปลอดภัยของระบบตรวจสอบใบหน้า

สำหรับระบบรักษาความปลอดภัย การมีความแม่นยำในการจดจำเพียงอย่างเดียวยังไม่เพียงพอ เพราะระบบอาจถูกโจมตีด้วยการปลอมแปลงข้อมูลชีวมิติ เช่น ภาพถ่าย วิดีโอ หรือสื่อสังเคราะห์ประเภท deepfake งานของ Šalko et al. (2024) แสดงให้เห็นว่า deepfake สามารถใช้โจมตีระบบยืนยันตัวตนด้วยใบหน้าเชิงพาณิชย์บางระบบได้ และเสนอให้พิจารณามาตรการป้องกันการโจมตีดังกล่าว ดังนั้น ระบบ smart security ที่ใช้ใบหน้าควรพิจารณากลไก Presentation Attack Detection (PAD) หรือ liveness detection ร่วมด้วย เพื่อประเมินว่าข้อมูลที่นำเสนอต่อกล้องมาจากบุคคลจริง ไม่ใช่ภาพ วิดีโอ หรือข้อมูลสังเคราะห์ที่ใช้เพื่อหลอกระบบ โดยเฉพาะระบบที่ทำงานโดยไม่มีเจ้าหน้าที่ตรวจสอบแบบเวลาจริง เนื่องจากงานดังกล่าวพบว่าสภาพแวดล้อมที่ขาดการกำกับดูแลโดยมนุษย์และใช้ข้อมูลวิดีโอในการยืนยันตัวตนอาจเอื้อต่อการโจมตีด้วย Deepfake มากขึ้น

นอกจากนี้ ประสิทธิภาพของระบบจดจำใบหน้าไม่ได้ขึ้นอยู่กับอัลกอริทึมเพียงอย่างเดียว แต่ยังได้รับผลกระทบจากคุณภาพภาพ แสง มุมใบหน้า การบดบัง ความละเอียดของภาพ ความเบลอ และความหลากหลายของข้อมูลที่ใช้เป็นข้อมูลอ้างอิง งานทบทวนของ EL Fadel (2025) ชี้ว่าการเปลี่ยนแปลงของแสงและสภาวะการรับภาพยังคงเป็นความท้าทายต่อระบบจดจำใบหน้า ขณะที่ Labinjan et al. (2026) พบว่าคุณภาพและความแปรปรวนของชุดข้อมูลมีผลโดยตรงต่อประสิทธิภาพการจดจำ ดังนั้น การออกแบบระบบสำหรับงานรักษาความปลอดภัยจริงควรให้ความสำคัญกับทั้งคุณภาพของข้อมูล การกำหนด threshold ที่เหมาะสม การป้องกันการปลอมแปลง และการคุ้มครองข้อมูลชีวมิติของผู้ใช้

5.2.5 ข้อดีและข้อจำกัดของระบบสแกนใบหน้า

1) ข้อดีของระบบสแกนใบหน้า ได้แก่ ไม่ต้องสัมผัสอุปกรณ์ ใช้งานสะดวกและรวดเร็ว ลดปัญหาการลืมรหัสผ่านหรือสูญหายของบัตร สามารถตรวจสอบตัวตนจากระยะไกลได้ และรองรับการทำงานร่วมกับระบบ AI และกล้องวงจรปิด

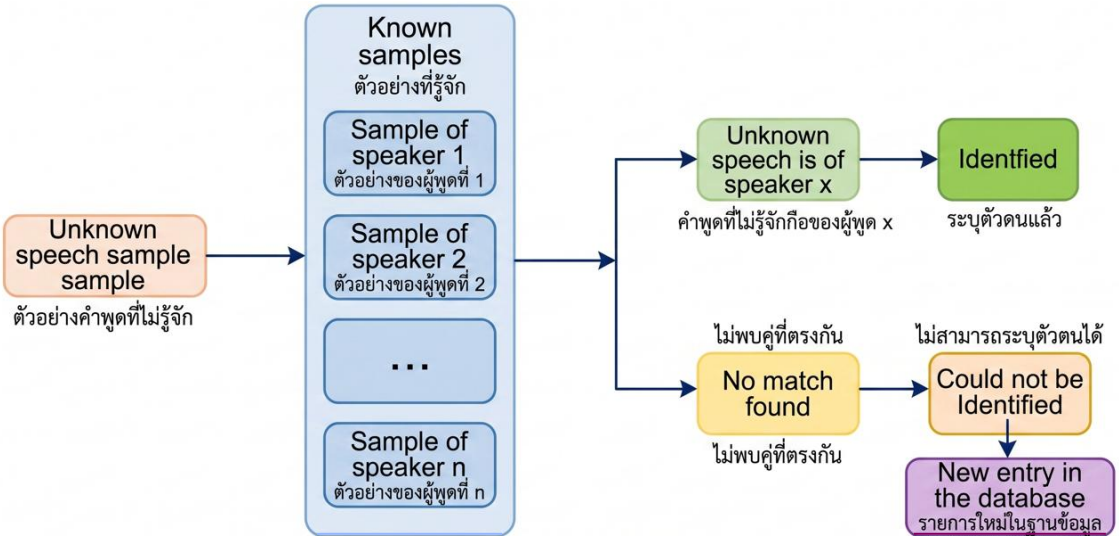
2) ข้อจำกัดของระบบสแกนใบหน้า ได้แก่ ประสิทธิภาพอาจลดลงในสภาพแสงที่ไม่เหมาะสม อาจได้รับผลกระทบจากการสวมหน้ากาก แว่นตา หรือการเปลี่ยนแปลงของใบหน้า ต้องใช้ฐานข้อมูลที่มีคุณภาพและเป็นปัจจุบัน และมีประเด็นด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลที่ต้องพิจารณา

เทคโนโลยีการจดจำใบหน้าเป็นหนึ่งในเทคโนโลยีชีวมาตรที่มีบทบาทสำคัญในระบบรักษาความปลอดภัยสมัยใหม่ โดยอาศัยการวิเคราะห์ลักษณะเฉพาะของใบหน้าและการประมวลผลด้วยปัญญาประดิษฐ์เพื่อระบุตัวตนของบุคคลอย่างแม่นยำ เทคโนโลยีจดจำใบหน้าถูกนำไปใช้งานในหลากหลายด้าน ได้แก่ ระบบควบคุมการเข้าออกอาคาร (access control) ระบบบันทึกเวลาปฏิบัติงาน (time attendance) การปลดล็อกสมาร์ตโฟนและคอมพิวเตอร์ ระบบรักษาความปลอดภัยในสนามบินและด่านตรวจคนเข้าเมือง ระบบกล้องวงจรปิดอัจฉริยะ (smart CCTV) ระบบค้นหาบุคคลสูญหายหรือผู้ต้องสงสัย หรือระบบยืนยันตัวตนทางการเงินและธุรกรรมอิเล็กทรอนิกส์ (e-KYC) ช่วยเพิ่มความสะดวก รวดเร็ว และความปลอดภัย

5.3 ระบบจดจำเสียง (Voice Recognition Systems)

5.3.1 ความหมายของระบบจดจำเสียง

ระบบจดจำเสียง (voice recognition system) เป็นเทคโนโลยีปัญญาประดิษฐ์ที่ใช้วิเคราะห์และประมวลผลสัญญาณเสียงของมนุษย์เพื่อระบุผู้พูด (speaker recognition) หรือแปลงคำพูดให้เป็นข้อความ (Automatic Speech Recognition: ASR)



รูปที่ 5.17 แนวคิดระบบระบุตัวผู้พูด

โดยอาศัยคุณลักษณะทางเสียง (acoustic features) ซึ่งมีลักษณะเฉพาะของแต่ละบุคคล เช่น ความถี่เสียง (frequency) ระดับความดัง (amplitude) จังหวะการพูด (prosody) ความเร็วในการพูด (speaking rate) และลักษณะการออกเสียง (articulation) คุณลักษณะเหล่านี้ทำให้สามารถใช้เสียงเป็นข้อมูลชีวมิติ (biometric data)

สำหรับการพิสูจน์ตัวตนและการควบคุมการเข้าถึงระบบได้ (Li et al., 2023; Nisha, 2017) ในปัจจุบัน ระบบจดจำเสียงถูกนำไปใช้ในอุปกรณ์อัจฉริยะและระบบรักษาความปลอดภัยอย่างแพร่หลาย เช่น ผู้ช่วยอัจฉริยะ (Google assistant, Siri และ Alexa) ระบบควบคุมบ้านอัจฉริยะ ระบบควบคุมหุ่นยนต์ ระบบธนาคารทางโทรศัพท์ ระบบควบคุมการเข้าออกด้วยเสียง และระบบ

สั่งงานด้วยเสียงในรถยนต์ โดยการพัฒนาของปัญญาประดิษฐ์และการเรียนรู้เชิงลึก (deep learning) ทำให้ความแม่นยำของระบบจดจำเสียงสูงขึ้นอย่างต่อเนื่อง แม้ในสภาพแวดล้อมที่มีเสียงรบกวน (Li et al., 2023)

5.3.2 ประเภทของระบบจดจำเสียง

ระบบจดจำเสียงสามารถแบ่งออกได้หลายลักษณะ ดังนี้

1) ระบบระบุผู้พูด (Speaker Identification)

เป็นกระบวนการระบุว่าเสียงที่ได้รับเป็นของบุคคลใดจากฐานข้อมูลผู้ใช้หลายคน โดยระบบจะเปรียบเทียบคุณลักษณะของเสียงกับข้อมูลที่บันทึกไว้ และเลือกผู้ที่มีความคล้ายคลึงสูงที่สุด หากไม่พบข้อมูลที่ตรงกัน ระบบอาจกำหนดให้เป็นผู้ใช้รายใหม่ (Nisha, 2017) ระบบประเภทนี้มักใช้ในงานนิติวิทยาศาสตร์ การสืบสวน การค้นหาบุคคลจากฐานข้อมูลเสียง และการวิเคราะห์เสียงในงานด้านความมั่นคง

2) ระบบตรวจสอบผู้พูด (Speaker Verification)

เป็นกระบวนการยืนยันตัวตนของผู้ใช้งาน โดยผู้ใช้จะอ้างสิทธิ์ว่าตนเองเป็นบุคคลใด จากนั้นระบบจะเปรียบเทียบเสียงที่พูดกับแบบจำลองเสียงของบุคคลนั้น หากระดับความคล้ายคลึงสูงกว่าค่าที่กำหนด (threshold) ระบบจะอนุญาตให้เข้าถึง แต่หากต่ำกว่าค่าที่กำหนดจะปฏิเสธการเข้าถึง (Nisha, 2017) ระบบนี้นิยมใช้ในระบบควบคุมการเข้าออก การยืนยันตัวตนสำหรับธุรกรรมทางการเงิน และการเข้าสู่ระบบอุปกรณ์อัจฉริยะ

3) ระบบรู้จำคำพูดอัตโนมัติ (Automatic Speech Recognition: ASR)

Automatic Speech Recognition (ASR) เป็นเทคโนโลยีที่แปลงสัญญาณเสียงของมนุษย์ให้เป็นข้อความ (speech-to-text) โดยระบบจะวิเคราะห์ลักษณะทางเสียงและตีความเป็นคำหรือประโยคที่มีความหมาย แตกต่างจาก speaker recognition ซึ่งมุ่งเน้นการระบุตัวผู้พูด ASR มุ่งเน้นการทำความเข้าใจเนื้อหาของคำพูด (Li et al., 2023)

5.3.3 รูปแบบการรู้จำเสียง

การรู้จำเสียงสามารถแบ่งได้เป็น 2 รูปแบบ ได้แก่

1) Text-Dependent Voice Recognition

ผู้ใช้งานต้องพูดข้อความที่กำหนดไว้ล่วงหน้า เช่น "open the door" ระบบจะเปรียบเทียบทั้งข้อความและลักษณะเสียง จึงมีความแม่นยำสูง เหมาะสำหรับงานด้านความปลอดภัย

2) Text-Independent Voice Recognition

ผู้ใช้สามารถพูดข้อความใดก็ได้ ระบบจะวิเคราะห์เฉพาะลักษณะของเสียงผู้พูด จึงมีความยืดหยุ่นมากกว่า แต่ต้องใช้แบบจำลองที่ซับซ้อนกว่า (Nisha, 2017)

5.3.4 หลักการทำงานของระบบจดจำเสียง

โดยทั่วไป ระบบจดจำเสียงประกอบด้วยขั้นตอนสำคัญ ดังนี้

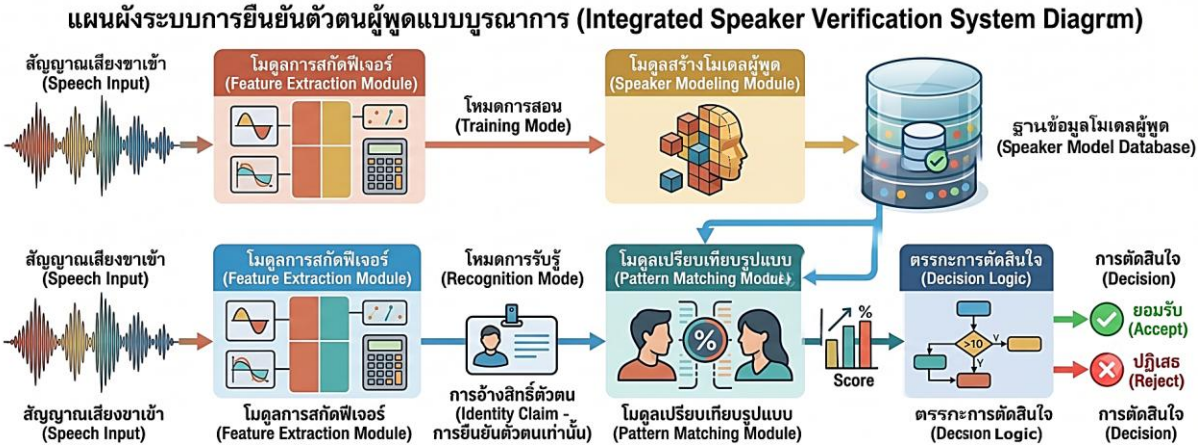
1) การรับสัญญาณเสียง (voice acquisition) โดยใช้ไมโครโฟนรับคลื่นเสียงจากผู้ใช้งาน

2) การประมวลผลเบื้องต้น (pre-processing) เช่น การลดสัญญาณรบกวน (Noise Reduction) การตรวจจับช่วงที่มีเสียงพูด (Voice Activity Detection: VAD) และการแบ่งเฟรมของสัญญาณเสียง

3) การสกัดคุณลักษณะ (feature extraction) เพื่อแปลงสัญญาณเสียงเป็นเวกเตอร์คุณลักษณะ เช่น MFCC, LPC หรือ PLP

4) การสร้างแบบจำลอง (modeling) โดยใช้แบบจำลองทางสถิติหรือแบบจำลองการเรียนรู้เชิงลึก

5) การเปรียบเทียบและตัดสินใจ (pattern matching and decision making) เพื่อระบุผู้พูดหรือแปลงคำพูดเป็นข้อความ (Li et al., 2023; Nisha, 2017)



รูปที่ 5.18 แผนภาพการทำงานของระบบยืนยันตัวตนผู้พูดแบบบูรณาการ

จากรูปที่ 5.18 ระบบยืนยันตัวตนผู้พูด (speaker verification system) ประกอบด้วยกระบวนการทำงานหลัก 2 ส่วน ได้แก่ โหมดการฝึกสอน (training mode) และ โหมดการยืนยันตัวตน (verification mode)

โหมดการฝึกสอน (training mode) ระบบจะรับสัญญาณเสียงจากผู้ใช้งานผ่านไมโครโฟน จากนั้นนำสัญญาณเสียงเข้าสู่ โมดูลการสกัดคุณลักษณะ (feature extraction module) เพื่อแปลงสัญญาณเสียงให้อยู่ในรูปของเวกเตอร์คุณลักษณะ (feature vector) ซึ่งเป็นตัวแทนของลักษณะเฉพาะของผู้พูด เช่น Mel Frequency Cepstral Coefficients (MFCC), Linear Predictive Coding (LPC) หรือคุณลักษณะเชิงลึกที่ได้จากโครงข่ายประสาทเทียม หลังจากนั้นข้อมูลจะถูกส่งเข้าสู่ โมดูลสร้างแบบจำลองผู้พูด (speaker modeling module) เพื่อสร้างแบบจำลองชีวมิติของผู้ใช้งาน (speaker model) และจัดเก็บไว้ใน ฐานข้อมูลแบบจำลองผู้พูด (speaker model database) สำหรับใช้เป็นข้อมูลอ้างอิงในอนาคต เมื่อเข้าสู่ โหมดการยืนยันตัวตน (verification mode) ผู้ใช้งานจะกล่าวข้อความเพื่ออ้างสิทธิ์ตัวตน (identity claim) ระบบจะดำเนินการสกัดคุณลักษณะของเสียงด้วย

กระบวนการเดียวกับช่วงการฝึกสอน จากนั้นเวกเตอร์คุณลักษณะที่ได้จะถูกส่งไปยัง โมดูลเปรียบเทียบรูปแบบ (pattern matching module) เพื่อเปรียบเทียบกับแบบจำลองผู้พูดที่จัดเก็บไว้ในฐานข้อมูล พร้อมคำนวณค่าความคล้ายคลึง (similarity score) ค่าความคล้ายคลึงดังกล่าวจะถูกส่งเข้าสู่ โมดูลตรรกะการตัดสินใจ (decision logic) ซึ่งจะเปรียบเทียบคะแนนกับค่าเกณฑ์ (decision threshold) ที่กำหนดไว้ หากคะแนนสูงกว่าค่าเกณฑ์ ระบบจะยอมรับการยืนยันตัวตน (accept) และอนุญาตให้เข้าถึงระบบหรือพื้นที่ที่ได้รับสิทธิ์ แต่หากคะแนนต่ำกว่าค่าเกณฑ์ ระบบจะปฏิเสธการยืนยันตัวตน (reject) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

สถาปัตยกรรมดังกล่าวเป็นพื้นฐานของระบบพิสูจน์ตัวตนด้วยเสียงในงานด้านความมั่นคงปลอดภัยชีวมิติ (biometric security) และถูกนำไปประยุกต์ใช้ในระบบควบคุมการเข้าออก (access control systems) ระบบธนาคารทางโทรศัพท์ (telephone banking) ผู้ช่วยอัจฉริยะ (voice assistants) และ IoT ที่รองรับการสั่งงานด้วยเสียง (Li et al., 2023; Nisha, 2017)

5.3.5 สถาปัตยกรรมของระบบรู้จำเสียงสมัยใหม่

ระบบที่ใช้ speaker separation เพื่อแยกเสียงของผู้พูดออกจากเสียงรบกวน ก่อนเข้าสู่โมเดล conformer-based ASR ซึ่งผสานข้อดีของโครงข่าย Convolutional Neural Network (CNN) และ transformer เพื่อเรียนรู้ทั้งคุณลักษณะเชิงพื้นที่และความสัมพันธ์ระยะยาวของข้อมูลเสียง ส่งผลให้สามารถรู้จำเสียงได้อย่างมีประสิทธิภาพในสภาพแวดล้อมจริงที่มีเสียงรบกวน และนำผลลัพธ์ไปใช้ควบคุมหุ่นยนต์เคลื่อนที่แบบอัตโนมัติได้ (Li et al., 2023)งานวิจัยในปัจจุบันได้พัฒนาระบบรู้จำเสียงโดยใช้โครงข่ายประสาทเทียมเชิงลึก (deep neural networks) แทนแบบจำลองดั้งเดิม เนื่องจากสามารถเรียนรู้รูปแบบของข้อมูลเสียงที่ซับซ้อนได้ดีกว่า ระบบทั่วไปประกอบด้วยองค์ประกอบหลัก ได้แก่

1) การตรวจจับกิจกรรมของเสียงพูด (VAD) เป็นการตรวจสอบช่วงเวลาที่มีเสียงพูดและแยกออกจากช่วงที่เป็นความเงียบหรือสัญญาณรบกวน

2) การแยกเสียงผู้พูด (speaker separation) เป็นการแยกเสียงของผู้พูดเป้าหมายออกจากเสียงของบุคคลอื่นหรือเสียงรบกวนในสภาพแวดล้อมเดียวกัน

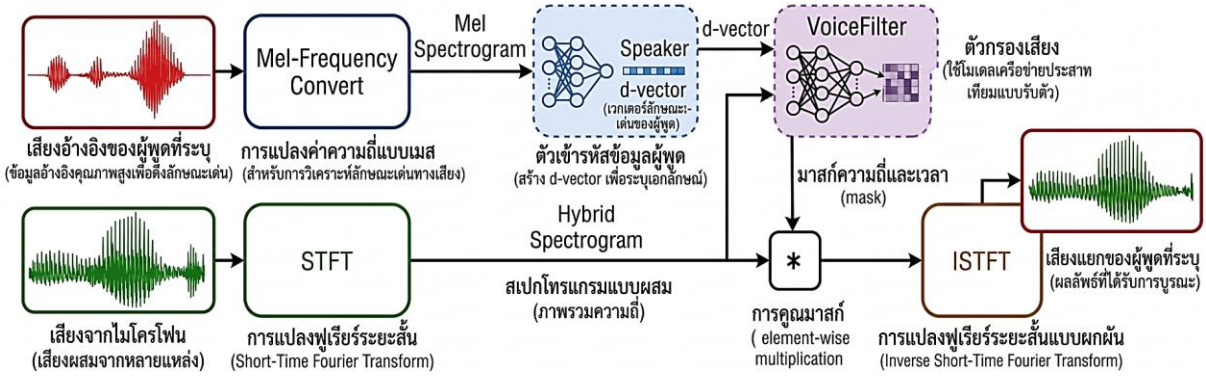
3) ตัวเข้ารหัสลักษณะเฉพาะของผู้พูด (speaker encoder) สร้างเวกเตอร์คุณลักษณะ (speaker embedding หรือ d-vector/x-vector) ที่ใช้แทนเอกลักษณ์ของผู้พูด

4) การสกัดคุณลักษณะ (feature extraction) เป็นการแปลงสัญญาณเสียงให้อยู่ในรูปของคุณลักษณะที่เหมาะสมต่อการประมวลผล เช่น MFCC, Log-Mel Spectrogram หรือ LPC

5) การรู้จำคำพูดอัตโนมัติ (ASR) เป็นการแปลงสัญญาณเสียงที่ได้รับให้เป็นข้อความ

6) การประมวลผลภาษาธรรมชาติ (NLP) เป็นการวิเคราะห์ความหมายของข้อความที่ได้จาก ASR เพื่อทำความเข้าใจเจตนาหรือคำสั่งของผู้ใช้

7) โมดูลการตัดสินใจ (decision module) เป็นการประมวลผลผลลัพธ์จาก NLP แล้วเลือกการทำงานที่เหมาะสม เช่น เปิดประตู เปิดไฟ หรือสั่งงานอุปกรณ์ภายในระบบอัจฉริยะ



รูปที่ 5.19 สถาปัตยกรรมของระบบแยกเสียงผู้พูดเป้าหมาย

จากรูปที่ 5.19 แสดงสถาปัตยกรรมของระบบแยกเสียงผู้พูดเป้าหมาย (target speaker separation) ซึ่งมีวัตถุประสงค์เพื่อแยกเสียงของผู้พูดที่ต้องการออกจากสัญญาณเสียงผสมที่ประกอบด้วยเสียงของผู้พูดหลายคนหรือเสียงรบกวน ก่อนนำข้อมูลไปใช้ในระบบรู้จำเสียงอัตโนมัติ (Automatic Speech Recognition: ASR) หรือระบบพิสูจน์ตัวตนด้วยเสียง (speaker verification) กระบวนการทำงานเริ่มจากการใช้ เสียงอ้างอิงของผู้พูด (reference speech) ซึ่งเป็นตัวอย่างเสียงของผู้พูดเป้าหมายเข้าสู่กระบวนการ Mel-frequency conversion เพื่อสร้าง Mel spectrogram ซึ่งเป็นการแสดงพลังงานของสัญญาณเสียงในสเกลความถี่แบบเมล (Mel scale) ที่สอดคล้องกับการรับรู้เสียงของมนุษย์ จากนั้นข้อมูลจะถูกส่งเข้าสู่ ตัวเข้ารหัสผู้พูด (speaker encoder) เพื่อสร้างเวกเตอร์ลักษณะเฉพาะของผู้พูด (speaker embedding หรือ d-vector) ซึ่งใช้แทนอัตลักษณ์ของผู้พูดแต่ละบุคคล ในขณะเดียวกัน สัญญาณเสียงจากไมโครโฟน ซึ่งอาจประกอบด้วยเสียงพูดหลายคนและเสียงรบกวน จะถูกแปลงเป็นสเปกโตรแกรมด้วย การแปลงฟูเรียร์ระยะสั้น (Short-Time Fourier Transform: STFT) เพื่อแสดงข้อมูลในโดเมนเวลาและความถี่ จากนั้นสเปกโตรแกรมจะถูกรวมกับข้อมูล d-vector เพื่อสร้าง hybrid spectrogram ซึ่งประกอบด้วยทั้งข้อมูลลักษณะของเสียงและอัตลักษณ์ของผู้พูด ข้อมูลดังกล่าวจะถูกส่งเข้าสู่ โมเดลแยกเสียงผู้พูด (voice filter model) ซึ่งเป็นโครงข่ายประสาทเทียมเชิงลึก (deep neural network) ทำหน้าที่สร้าง หน้ากากสเปกตรัม (spectral mask) สำหรับระบุส่วนของสัญญาณที่เป็นเสียงของผู้พูดเป้าหมาย พร้อมลดทอนเสียงของผู้พูดคนอื่นและสัญญาณรบกวน จากนั้นหน้ากากสเปกตรัมที่ได้จะถูกนำไปคูณแบบสมาชิกต่อสมาชิก (element-wise multiplication) กับสเปกโตรแกรมของสัญญาณเสียงผสม เพื่อให้เหลือเฉพาะองค์ประกอบของเสียงผู้พูดเป้าหมาย หลังจากนั้นระบบจะใช้ การแปลงฟูเรียร์ระยะสั้นแบบผกผัน (Inverse Short-Time Fourier Transform: ISTFT) เพื่อแปลงข้อมูลจากโดเมนความถี่กลับเป็นสัญญาณเสียงในโดเมนเวลา ทำให้ได้ สัญญาณเสียงของผู้พูดเป้าหมายที่ผ่านการแยกแล้ว ซึ่งสามารถนำไปใช้ในระบบรู้จำคำพูด ระบบยืนยันตัวตนด้วยเสียง ได้อย่างมีประสิทธิภาพ

สถาปัตยกรรมดังกล่าวช่วยเพิ่มความแม่นยำของระบบรู้จำเสียงในสภาพแวดล้อมจริงที่มีผู้พูดหลายคนหรือมีเสียงรบกวนสูง และเป็นเทคนิคสำคัญที่ใช้ในระบบผู้ช่วยอัจฉริยะ (voice assistants) หุ่นยนต์เคลื่อนที่อัตโนมัติ (mobile robots) ระบบสมาร์ตโฮม (smart home) และระบบควบคุมการเข้าออกด้วยเสียง (voice-based access control) (Li et al., 2023)

บรรณานุกรมบทที่ 5

Bagchi, T., Mahapatra, A., Yadav, D., Mishra, D., Pandey, A., Chandrasekhar, P., & Kumar, A. (2022). Intelligent security system based on face recognition and IoT. *Materials Today: Proceedings, 62*(4), 2133–2137. https://doi.org/10.1016/j.matpr.2022.03.353.

EL Fadel, N. (2025). Facial recognition algorithms: A systematic literature review. *Journal of Imaging, 11*(2), 58. https://doi.org/10.3390/jimaging11020058.

Hangzhou Grow Technology Co., Ltd. (2011). *R307 fingerprint module user manual* (Version 1.20). Alldatasheet. https://www.alldatasheet.com/datasheet-pdf/view/1756584/GROW/R307.html.

Hsu, D. S. (2016). *Fingerprint sensor technology and security requirements*. SemiEngineering. https://semiengineering.com/fingerprint-senor-technology-and-security-requirements/.

Kaushal, N., & Kaushal, P. (2011). Human identification and fingerprints: A review. *Journal of Biometrics & Biostatistics, 2*(4), 123. https://doi.org/10.4172/2155-6180.1000123.

Labinjan, A., Baressi Šegota, S., Lorencin, I., & TankoviĆ, N. (2026). Face recognition system using CLIP and FAISS for scalable and real-time identification. *Mathematical and Computational Applications, 31*(2), 36. https://doi.org/10.3390/mca31020036.

Li, S.-A., Liu, Y.-Y., Chen, Y.-C., Feng, H.-M., Shen, P.-K., & Wu, Y.-C. (2023). Voice interaction recognition design in real-life scenario mobile robot applications. *Applied Sciences, 13*(5), 3359. https://doi.org/10.3390/app13053359.

Maiti, D., Basak, M., & Das, D. (2025). A review on fingerprint based authentication—Its challenges and applications. *Computer Science Review, 57*, 100735. https://doi.org/10.1016/j.cosrev.2025.100735.

Martins, N., Silva, J. S., & Bernardino, A. (2024). Fingerprint recognition in forensic scenarios. *Sensors*, *24*(2), 664. https://doi.org/10.3390/s24020664.

Nisha. (2017). Voice recognition technique: A review. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *5*(5), 262–268.

Samsung Display. (n.d.). *[Learn Display] 60. Fingerprint on Display (FoD).* Samsung Display Newsroom. https://global.samsungdisplay.com/30345/feed/.

Tandee. (2014). *淺談指紋辨識原理：指紋辨識安全性？電容式、光學式技術差異* . Cool3C. https://www.cool3c.com/article/84035.

Rivera, G. S. C., Polo, M. J. A., & Andrade-Arenas, L. (2024). Implementation of an authentication system based on facial recognition, artificial intelligence and blockchain. *International Journal of Engineering Trends and Technology, 72*(1), 130–140. https://doi.org/10.14445/22315381/IJETT-V72I1P113.

Šalko, M., Firc, A., & Malinka, K. (2024). Security implications of deepfakes in face authentication. In *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing (SAC '24)*. Association for Computing Machinery. https://doi.org/10.1145/3605098.3635953.

Trang, L. T., & Hao, N. T. V. (2023). Building a face authentication system using Face API in the data center system. *International Journal of Progressive Sciences and Technologies, 36*(2), 428–435.

สรุปสาระสำคัญของบทที่ 5
ระบบตรวจสอบอัตลักษณ์เพื่อความปลอดภัย

ระบบตรวจสอบลายนิ้วมือเพื่อความปลอดภัย

ลายนิ้วมือเป็นข้อมูลชีวมิติ (biometric) ที่มีเอกลักษณ์เฉพาะบุคคล ไม่มีบุคคลใดมีลายนิ้วมือเหมือนกันทั้งหมด จึงถูกนำมาใช้ในการยืนยันตัวตน ควบคุมการเข้า–ออก และป้องกันการปลอมแปลงตัวตน โดยการใช้ลายนิ้วมือเป็นข้อมูลเฉพาะบุคคลเพื่อยืนยันตัวตน

หลักการทำงานของเครื่องสแกนลายนิ้วมือ เริ่มจากเครื่องสแกนจะอ่านลายนิ้วมือผ่านเซนเซอร์ จากนั้นแปลงเป็นข้อมูลดิจิทัลและเปรียบเทียบกับข้อมูลที่เก็บในฐานข้อมูล หากข้อมูลตรงกัน ระบบจะอนุญาตให้เข้าใช้งาน (สแกน >ประมวลผล > เปรียบเทียบ > ยืนยันตัวตน) เซนเซอร์ลายนิ้วมือมีหลายประเภท ได้แก่

1) Optical sensor ใช้แสงถ่ายภาพลายนิ้วมือ

2) Capacitive sensor ตรวจจับประจุไฟฟ้าบนผิวหนัง

3) Ultrasonic sensor ใช้คลื่นเสียงสร้างภาพ 3 มิติ

4) Thermal sensor ตรวจจับความแตกต่างของอุณหภูมิ

หลักการตรวจสอบลายนิ้วมือด้วยจุดลักษณะเฉพาะ โดยระบบจะวิเคราะห์จุดสำคัญของลายนิ้วมือ เช่น จุดปลายเส้นและจุดแตกแขนงของสันลายนิ้วมือ แล้วนำตำแหน่งของจุดเหล่านี้มาเปรียบเทียบกับข้อมูลที่บันทึกไว้ ซึ่งกระบวนการสแกนและตรวจสอบลายนิ้วมือ ดังนี้

1) รับภาพลายนิ้วมือ

2) ปรับปรุงคุณภาพภาพ

3) แยกจุดสำคัญ

4) สร้างข้อมูลอ้างอิง

5) เปรียบเทียบกับฐานข้อมูล

6) แสดงผลการยืนยันตัวตน

กระบวนการแปลงลายนิ้วมือเป็นข้อมูลดิจิทัล จะเริ่มกระบวนการหลังจากสแกน ระบบจะสร้าง template หรือชุดข้อมูลที่แทนลักษณะของลายนิ้วมือ เพื่อจัดเก็บในฐานข้อมูล ทำให้ค้นหาและเปรียบเทียบได้รวดเร็ว การใช้งานเซนเซอร์สแกนลายนิ้วมือนิยมใช้ในในงาน (1)ระบบเปิดปิดประตู (2) ระบบลงเวลาพนักงาน (3) ระบบควบคุมการเข้าถึงพื้นที่สำคัญ และ (4)ระบบรักษาความปลอดภัยของอุปกรณ์อิเล็กทรอนิกส์

การประยุกต์ใช้งานเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์ โดยสามารถเชื่อมต่อกับ Arduino, ESP32 หรือ Raspberry Pi เพื่อสร้างระบบอัตโนมัติ เช่น ประตูอัจฉริยะ ตู้ล็อกเกอร์อัจฉริยะ หรือระบบบันทึกข้อมูลออนไลน์ และสามารถประยุกต์งานร่วมกับ RFID เป็นด่านแรกในการระบุตัวตน และใช้ลายนิ้วมือเป็นด่านที่สองในการยืนยัน ทำให้ระบบมีความปลอดภัยมากขึ้น ซึ่งเป็นการยืนยันตัวตนแบบสองชั้น (two-factor authentication)

เทคโนโลยีการจดจำใบหน้าเพื่อความปลอดภัย

หลักการทำงานของระบบสแกนใบหน้า โดยกล้องจะจับภาพใบหน้า จากนั้นซอฟต์แวร์จะวิเคราะห์จุดสำคัญบนใบหน้า เช่น ดวงตา จมูก และปาก แล้วเปรียบเทียบกับฐานข้อมูลเพื่อยืนยันตัวตน โดยรูปแบบการตรวจสอบตัวตนด้วยใบหน้า

1) Face verification (1:1) เปรียบเทียบใบหน้ากับข้อมูลของบุคคลที่ระบุไว้

2) Face identification (1:N) เปรียบเทียบใบหน้ากับข้อมูลหลายคนในฐานข้อมูล

ข้อดีและข้อจำกัดของระบบสแกนใบหน้า

ข้อดี ได้แก่ ไม่ต้องสัมผัสอุปกรณ์ ตรวจสอบได้รวดเร็ว และสะดวกต่อการใช้งาน

ข้อจำกัด คือ ได้รับผลกระทบจากแสงและมุมกล้อง ความแม่นยำลดลงเมื่อมีสิ่งปกปิดใบหน้า และมีประเด็นด้านความเป็นส่วนตัว

การประยุกต์ใช้งานระบบจดจำใบหน้าในระบบรักษาความปลอดภัย สามารถนำไปใช้ในระบบควบคุมการเข้าออกอาคาร ระบบลงเวลาพนักงาน ระบบเฝ้าระวัง และระบบ smart security เพื่อตรวจจับบุคคลต้องสงสัย และระบบสามารถส่งข้อมูลการตรวจสอบตัวตนไปเก็บบน cloud และบันทึกลง Google Sheets เพื่อดูข้อมูลย้อนหลัง วิเคราะห์ข้อมูล และจัดทำรายงานได้สะดวก

หน่วยนี้ศึกษาระบบตรวจสอบอัตลักษณ์ (biometric security) 2 รูปแบบหลัก คือ ลายนิ้วมือ และ การจดจำใบหน้า ซึ่งช่วยเพิ่มความปลอดภัยในการยืนยันตัวตน ลดการปลอมแปลง และสามารถประยุกต์ใช้ร่วมกับเทคโนโลยี IoT, RFID และ cloud computing เพื่อพัฒนาระบบรักษาความปลอดภัยอัจฉริยะได้อย่างมีประสิทธิภาพ

ระบบจดจำเสียงพูด (Speech Recognition System)

ระบบจดจำเสียงพูด (speech recognition system) หรือ การรู้จำคำพูดอัตโนมัติ (Automatic Speech Recognition: ASR) เป็นเทคโนโลยีที่ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) และการประมวลผลสัญญาณดิจิทัล (Digital Signal Processing: DSP) ในการแปลงสัญญาณเสียงของมนุษย์ให้เป็นข้อความหรือคำสั่งที่คอมพิวเตอร์สามารถประมวลผลได้ โดยระบบจะวิเคราะห์คุณลักษณะทางเสียง (acoustic features) เช่น ความถี่ ความเข้มของเสียง จังหวะการพูด และรูปแบบการออกเสียง เพื่อนำไปเปรียบเทียบกับแบบจำลองทางภาษา (language model) และแบบจำลองทางเสียง (acoustic model) ก่อนแสดงผลเป็นข้อความหรือดำเนินการตามคำสั่งของผู้ใช้งาน

ระบบจดจำเสียงพูดประกอบด้วยกระบวนการทำงานหลายขั้นตอน เริ่มจากการรับสัญญาณเสียงผ่านไมโครโฟน จากนั้นดำเนินการประมวลผลเบื้องต้น (pre-processing) เพื่อลดสัญญาณรบกวนและแยกช่วงที่มีเสียงพูด ต่อมาระบบจะสกัดคุณลักษณะของเสียง (feature extraction) ด้วยเทคนิคต่าง ๆ เช่น Mel Frequency Cepstral Coefficients (MFCC), Linear Predictive Coding (LPC) หรือ Perceptual Linear Prediction (PLP) ก่อนนำข้อมูลเข้าสู่แบบจำลองการรู้จำเสียง เช่น Hidden Markov Model (HMM) หรือโครงข่ายประสาทเทียมเชิงลึก (Deep Neural Network: DNN) เพื่อแปลงเสียงเป็นข้อความและวิเคราะห์ความหมายของคำสั่ง ปัจจุบัน

ระบบจดจำเสียงพูดได้รับการพัฒนาอย่างมากด้วยเทคโนโลยีการเรียนรู้เชิงลึก (deep learning) และแบบจำลองสมัยใหม่ เช่น conformer และ transformer ซึ่งช่วยเพิ่มความแม่นยำในการรู้จำเสียง โดยเฉพาะในสภาพแวดล้อมที่มีเสียงรบกวนหรือมีผู้พูดหลายคน นอกจากนี้ยังมีการประยุกต์ใช้เทคนิคการแยกเสียงผู้พูด (speaker separation) และการสร้างเวกเตอร์ลักษณะเฉพาะของผู้พูด (speaker embedding หรือ d-vector) เพื่อเพิ่มประสิทธิภาพในการรู้จำเสียงและการพิสูจน์ตัวตน

แบบฝึกหัดท้ายบทที่ 5
ระบบตรวจสอบอัตลักษณ์เพื่อความปลอดภัย

<u>คำชี้แจง</u> จงเลือกคำตอบที่ถูกต้องที่สุดเพียงคำตอบเดียวแล้วทำเครื่องหมาย x ลงในข้อสอบ

1. ข้อใดกล่าวถึงลักษณะของข้อมูลชีวมิติ (Biometric) ได้ถูกต้อง
   ก. เปลี่ยนแปลงได้ง่าย ข. มีลักษณะเฉพาะของแต่ละบุคคล
   ค. สามารถยืมใช้แทนกันได้ ง. เป็นข้อมูลสาธารณะ
2. ข้อใดเป็นข้อมูลชีวมิติ
   ก. รหัสผ่าน ข. บัตรประชาชน
   ค. ลายนิ้วมือ ง. หมายเลขโทรศัพท์
3. ระบบสแกนลายนิ้วมือมีวัตถุประสงค์หลักเพื่ออะไร
   ก. บันทึกภาพ ข. ตรวจสอบตัวตน
   ค. บันทึกเสียง ง. วัดอุณหภูมิ
4. ลายนิ้วมือส่วนใดที่ใช้ในการเปรียบเทียบตัวตน
   ก. สีผิว ข. ความยาวนิ้ว
   ค. จุดลักษณะเฉพาะ ง. รูปร่างมือ
5. เซนเซอร์ Optical ใช้หลักการใด
   ก. คลื่นเสียง ข. สนามแม่เหล็ก
   ค. แสง ง. ความร้อน
6. เซนเซอร์ Capacitive ตรวจจับด้วยอะไร
   ก. ประจุไฟฟ้า ข. แสง
   ค. อุณหภูมิ ง. เสียง
7. เซนเซอร์ Ultrasonic ใช้หลักการใด
   ก. คลื่นเสียงความถี่สูง ข. เลเซอร์
   ค. อินฟราเรด ง. แม่เหล็ก
8. ขั้นตอนแรกของการตรวจสอบลายนิ้วมือคือข้อใด
   ก. เปรียบเทียบข้อมูล ข. รับภาพลายนิ้วมือ
   ค. บันทึกข้อมูล ง. เปิดประตู
9. Template Fingerprint คืออะไร
   ก. ภาพถ่าย ข. ฐานข้อมูลรูปภาพ
   ค. ข้อมูลดิจิทัลของลายนิ้วมือ ง. โปรแกรมควบคุม
10. ข้อใดไม่ใช่การใช้งานระบบลายนิ้วมือ
   ก. ลงเวลางาน ข. เปิดประตู
   ค. ตรวจสอบตัวตน ง. วัดแรงดันไฟฟ้า

11. ข้อใดเป็นจุดเด่นของระบบลายนิ้วมือ

ก. จำรหัสผ่านหลายชุด ข. ปลอมแปลงได้ง่าย

ค. มีเอกลักษณ์เฉพาะบุคคล ง. ใช้งานเฉพาะคอมพิวเตอร์

12. ระบบลายนิ้วมือช่วยเพิ่มความปลอดภัยอย่างไร

ก. ลดการใช้กระดาษ ข. ลดการปลอมแปลงตัวตน

ค. เพิ่มความเร็วอินเทอร์เน็ต ง. ลดการใช้ไฟฟ้า

13. หากสแกนลายนิ้วมือไม่ผ่าน ควรทำสิ่งใดเป็นอันดับแรก

ก. เปลี่ยนเครื่อง ข. ทำความสะอาดนิ้วและเซนเซอร์

ค. ปิดระบบ ง. เปลี่ยนรหัสผ่าน

14. ข้อใดเป็นอุปกรณ์ที่ใช้ร่วมกับระบบสแกนลายนิ้วมือ

ก. กลอนแม่เหล็กไฟฟ้า ข. เครื่องพิมพ์

ค. เครื่องแฟกซ์ ง. เครื่องสแกนเอกสาร

15. ข้อใดเป็นข้อจำกัดของระบบลายนิ้วมือ

ก. ใช้ได้เฉพาะกลางวัน ข. นิ้วเปียกหรือสกปรกอาจสแกนไม่ผ่าน

ค. ไม่มีความปลอดภัย ง. ไม่สามารถบันทึกข้อมูลได้

16. ระบบลายนิ้วมือสามารถเชื่อมต่อกับอุปกรณ์ใดได้

ก. Arduino ข. ESP32

ค. Raspberry Pi ง. ถูกทุกข้อ

17. RFID มีหน้าที่หลักคืออะไร

ก. ตรวจจับเสียง ข. ระบุตัวตนด้วยคลื่นวิทยุ

ค. บันทึกภาพ ง. วัดอุณหภูมิ

18. การใช้ RFID ร่วมกับลายนิ้วมือเรียกว่าอะไร

ก. Face Recognition ข. Two-Factor Authentication

ค. Cloud Computing ง. IoT Gateway

19. ประโยชน์ของการยืนยันตัวตน 2 ชั้นคืออะไร

ก. ลดต้นทุน ข. เพิ่มความปลอดภัย

ค. ลดเวลาเปิดประตู ง. ลดพื้นที่จัดเก็บ

20. ข้อใดเป็นตัวอย่างการประยุกต์ใช้งานระบบลายนิ้วมือ

ก. ตู้ล็อกเกอร์อัจฉริยะ ข. ประตูอัตโนมัติ

ค. ระบบลงเวลา ง. ถูกทุกข้อ

21. หากต้องการสร้างระบบเปิดประตูอัตโนมัติ ควรใช้อุปกรณ์ใดควบคุม

ก. รีเลย์ ข. พัดลม

ค. ลำโพง ง. ไมโครโฟน

22. ระบบ IoT มีข้อดีอย่างไรต่อระบบรักษาความปลอดภัย

ก. ควบคุมและตรวจสอบผ่านอินเทอร์เน็ตได้ ข. ลดการใช้ไฟ

ค. ลดพื้นที่ติดตั้ง ง. ไม่ต้องใช้เซนเซอร์

23. หากต้องการบันทึกข้อมูลการเข้าออกผ่าน Cloud ควรใช้บริการใด

ก. Google Sheets ข. Google Cloud

ค. Firebase ง. ถูกทุกข้อ

24. ข้อใดเป็นข้อมูลที่ควรบันทึกเมื่อมีการสแกนผ่าน

ก. ชื่อผู้ใช้ ข. วันเวลา

ค. สถานะการเข้าออก ง. ถูกทุกข้อ

25. การทดสอบระบบหลังติดตั้งมีวัตถุประสงค์ใด

ก. ตรวจสอบความถูกต้องของระบบ ข. เพิ่มความสวยงาม

ค. ลดต้นทุน ง. เพิ่มความเร็วอินเทอร์เน็ต

1) ข้อใดสรุปแนวคิดของระบบตรวจสอบอัตลักษณ์ได้ดีที่สุด

ก. ใช้ข้อมูลส่วนบุคคลทั่วไป

ข. ใช้ข้อมูลชีวมิติยืนยันตัวตนเพื่อเพิ่มความปลอดภัย

ค. ใช้เฉพาะรหัสผ่าน

ง. ใช้เฉพาะบัตร RFID

27. ข้อใดอธิบายความหมายของระบบจดจำเสียงพูด (Speech Recognition System) ได้ถูกต้องที่สุด

ก. ระบบที่ใช้ระบุอายุของผู้พูดจากเสียง

ข. ระบบที่ใช้แปลงสัญญาณเสียงเป็นข้อความหรือคำสั่งที่คอมพิวเตอร์เข้าใจได้

ค. ระบบที่ใช้วิเคราะห์ความดังของเสียงเท่านั้น

ง. ระบบที่ใช้สร้างคลื่นเสียงสังเคราะห์

28. ข้อใดเป็นลำดับการทำงานของระบบจดจำเสียงพูดที่ถูกต้อง

ก. การสกัดคุณลักษณะ > รับเสียง > ตัดสินใจ > แปลงข้อความ

ข. รับเสียง > การประมวลผลเบื้องต้น >การสกัดคุณลักษณะ > การรู้จำเสียง > แสดงผล

ค. รับเสียง > แสดงผล > การสกัดคุณลักษณะ > การตัดสินใจ

ง. การรู้จำเสียง > การสกัดคุณลักษณะ > รับเสียง

29. ข้อใดเป็นหน้าที่หลักของการประมวลผลเบื้องต้น (pre-processing)

ก. เพิ่มความดังของเสียงเท่านั้น

ข. แปลงเสียงเป็นข้อความ

ค. ลดสัญญาณรบกวนและเตรียมสัญญาณก่อนการวิเคราะห์

ง. สร้างฐานข้อมูลผู้พูด

30. ข้อใดเป็นเทคนิคที่นิยมใช้ในการสกัดคุณลักษณะของเสียงพูด

ก. QR Code ข. NFC

ค. MFCC ง. SHA-256

31. เทคนิค Mel Frequency Cepstral Coefficients (MFCC) ถูกออกแบบมาเพื่อ

ก. เข้ารหัสข้อมูลด้วยวิธี AES

ข. วิเคราะห์สัญญาณภาพ

ค. สกัดคุณลักษณะของเสียงให้สอดคล้องกับการรับรู้เสียงของมนุษย์

ง. เพิ่มกำลังขยายของไมโครโฟน

32. ข้อใดกล่าวถึง Automatic Speech Recognition (ASR) ได้ถูกต้อง

ก. ใช้ระบุว่าใครเป็นผู้พูดเท่านั้น ข. ใช้ตรวจจับใบหน้าของผู้ใช้งาน

ค. ใช้แปลงคำพูดของมนุษย์ให้เป็นข้อความ ง. ใช้เข้ารหัสข้อมูลเสียง

33. ข้อใดเป็นการประยุกต์ใช้ระบบจดจำเสียงพูด

ก. ระบบ RFID ข. ระบบควบคุมประตูด้วยรหัสผ่าน

ค. ผู้ช่วยอัจฉริยะ เช่น Siri และ Google Assistant ง. ระบบกล้องวงจรปิดแบบแอนะล็อก

34. หากต้องการให้ระบบทำงานได้ดีในสภาพแวดล้อมที่มีเสียงรบกวน ควรใช้เทคนิคใดเพิ่มเติม

ก. Voice Activity Detection (VAD) ข. QR Code

ค. Reed-Solomon ง. NFC

36. ข้อใดเป็นข้อดีของเทคโนโลยี Deep Learning ในระบบจดจำเสียงพูด

ก. ลดขนาดไมโครโฟน

ข. เพิ่มความเร็วของอินเทอร์เน็ต

ค. เพิ่มความแม่นยำในการรู้จำเสียง โดยเฉพาะในสภาพแวดล้อมที่มีเสียงรบกวน

ง. ลดการใช้หน่วยความจำของระบบปฏิบัติการ

37. หากต้องการนำระบบจดจำเสียงพูดมาใช้ในระบบควบคุมการเข้าออก ควรใช้ร่วมกับเทคโนโลยีใดเพื่อเพิ่มความปลอดภัยมากที่สุด

ก. การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)

ข. Barcode

ค. Bluetooth

ง. ZigBee

<u>คำชี้แจง</u> จงเขียนคำตอบสั้น ๆ ที่ถูกต้องที่เหมาะสมที่สุดลงในข้อสอบ

1) ระบบตรวจสอบอัตลักษณ์ คือ

ตอบ_____

2) โรงงานมีพนักงาน 500 คน ควรใช้ระบบใดบันทึกเวลา

ตอบ_____

3) ผู้ใช้งานสวมถุงมืออยู่ตลอดเวลา ควรเลือกใช้วิธีใดแทน

ตอบ_____

4) อาคารสำนักงานต้องการบันทึกประวัติการเข้าออกออนไลน์

ตอบ_____

5) ต้องการลดการใช้บัตรผ่านเพื่อลดการสูญหาย

ตอบ_____

6) ระบบที่มีการป้องกันด้วย RFID และระบบสแกนใบหน้า เรียกระบบนี้ว่าอะไร

ตอบ_____

7) ระบบจดจำใบหน้าใช้ข้อมูลใดในการตรวจสอบตัวตน

ตอบ_____

8) อุปกรณ์หลักที่ใช้ในระบบจดจำใบหน้าคืออะไร

ตอบ_____

9) Face Verification คืออะไร

ตอบ_____

10) Face Identification คืออะไร

ตอบ_____

11) ข้อใดเป็นจุดเด่นของระบบสแกนใบหน้า

ตอบ_____

12) ปัจจัยใดบ้างมีผลต่อความแม่นยำของระบบจดจำใบหน้า

ตอบ_____

13) การสวมหน้ากากอาจส่งผลอย่างไร

ตอบ_____

14) AI มีบทบาทอย่างไรในระบบสแกนใบหน้า

ตอบ_____

15) ข้อใดเป็นตัวอย่างการใช้งาน Face Recognition

ตอบ_____

16) ระบบจดจำใบหน้าเหมาะกับพื้นที่ใด

ตอบ_____

17) Face Recognition สามารถใช้ร่วมกับระบบใดได้

ตอบ_____

18) ข้อใดเป็นข้อจำกัดของระบบสแกนใบหน้า

ตอบ_____

19) ข้อใดเป็นข้อมูลที่ระบบวิเคราะห์

ตอบ_____

20) ระบบสแกนใบหน้าสามารถบันทึกข้อมูลลงระบบใด

ตอบ_____

21) ประโยชน์สำคัญของ Face Recognition คืออะไร

ตอบ_____

22) โรงเรียนต้องการควบคุมการเข้าออกนักเรียน ควรเลือกใช้ระบบใด

ตอบ_____

23) ห้องเก็บเอกสารลับควรใช้ระบบใด

ตอบ_____

24) หากต้องการลดการสัมผัสอุปกรณ์ในโรงพยาบาล ควรเลือกใช้ระบบใด

ตอบ_____

25) บริษัทต้องการดูข้อมูลเข้าออกย้อนหลังผ่านอินเทอร์เน็ต ควรใช้ระบบใดร่วมด้วย

ตอบ_____

26) ข้อใดเหมาะสมที่สุดสำหรับระบบ Smart Security

ตอบ_____

27) หากระบบสแกนลายนิ้วมือไม่ทำงาน ควรตรวจสอบสิ่งใดก่อน

ตอบ_____

28) เหตุใดจึงควรทดสอบระบบก่อนใช้งานจริง

ตอบ_____

29) การเชื่อมต่อ Google Sheets มีประโยชน์อย่างไร

ตอบ_____

30) หากต้องการให้แจ้งเตือนเมื่อมีผู้เข้าออก ควรใช้เทคโนโลยีใดร่วมด้วย

ตอบ_____

31) การบันทึกข้อมูลบน Cloud ช่วยเรื่องใดมากที่สุด

ตอบ_____

32) หากต้องการยืนยันตัวตนที่มีความแม่นยำสูง ควรใช้วิธีใด

ตอบ_____

33) Face Identification เหมาะกับงานประเภทใด

ตอบ_____

34) Face Verification เหมาะกับงานประเภทใด

ตอบ_____

35) หากต้องการพัฒนาระบบประตูอัจฉริยะด้วยตนเอง ควรใช้บอร์ดใด

ตอบ_____

6 ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัย

61

ความรู้เบื้องต้นเกี่ยวกับเครือข่ายในระบบรักษาความปลอดภัย

6.1.1 ความหมายของเครือข่ายในระบบรักษาความปลอดภัย
6.1.2 ความสำคัญของระบบเครือข่ายในระบบรักษาความปลอดภัย
6.1.3 องค์ประกอบของเครือข่ายในระบบรักษาความปลอดภัย

62

โครงสร้างการเชื่อมต่อเครือข่าย

6.2.1 โทโพโลยีแบบบัส
6.2.2 โทโพโลยีแบบดาว
6.2.3 โทโพโลยีแบบวงแหวน
6.2.4 โทโพโลยีแบบตาข่าย
6.2.5 โทโพโลยีแบบผสม

63

ชุดโปรโตคอล TCP/IP

6.3.1 ความหมายของโปรโตคอล
6.3.2 แนวคิดของการแบ่งชั้นโปรโตคอล
6.3.3 หลักการสำคัญของ Protocol Layering
6.3.4 การเชื่อมต่อเชิงตรรกะระหว่างชั้น
6.3.5 สถาปัตยกรรมของชุดโปรโตคอล TCP/IP
6.3.6 บทบาทของ Host, Switch และ Router ใน TCP/IP
6.3.7 การสื่อสารแบบ End-to-End และ Hop-to-Hop
6.3.8 หน่วยข้อมูลในแต่ละชั้นการสื่อสาร
6.3.9 การห่อหุ้มข้อมูลและการถอดห่อหุ้มข้อมูล

64

IP ADDRESS และ SUBNET

6.4.1 Internet Protocol Address
6.4.2 การกำหนด IP Address
6.4.3 ส่วนประกอบของ IPv4 Address

65 **เครือข่ายท้องถิ่น**

6.5.1 องค์ประกอบของเครือข่าย LAN
6.5.2 คุณลักษณะของ LAN ในระบบรักษาความปลอดภัย

66 **เครือข่ายบริเวณกว้าง**

6.6.1 องค์ประกอบของเครือข่าย WAN
6.6.2 โครงข่ายแกนกลางของ WAN
6.6.3 สื่อส่งสัญญาณที่ใช้ในโครงข่าย WAN
6.6.4 โปรโตคอลกำหนดเส้นทาง

67 **เทคโนโลยีเครือข่ายแบบใช้สาย**

6.7.1 ความหมายและวิวัฒนาการของ Ethernet
6.7.2 สถาปัตยกรรมของ Ethernet
6.7.3 Ethernet Frame Format
6.7.4 หลักการทำงานของ CSMA/CD
6.7.5 Ethernet Switching

68 **WI-FI**

6.8.1 Wi-Fi และ Wireless
6.8.2 สถาปัตยกรรม Wi-Fi
6.8.3 วิธีเข้าถึงสื่อของ Wi-Fi
6.8.4 การรักษาความมั่นคงปลอดภัยของ Wi-Fi

69 **ZIGBEE**

6.9.1 ย่านความถี่และอัตราการรับส่งข้อมูล
6.9.2 การออกแบบวงจรความถี่วิทยุสำหรับอุปกรณ์ Zigbee
6.9.3 หลักการทำงานของ Zigbee
6.9.4 คุณลักษณะของเครือข่าย Zigbee
6.9.5 รูปแบบโครงสร้างเครือข่ายของ Zigbee
6.9.6 ประเภทของเครือข่าย Zigbee

6.10 Z-WAVE

6.10.1 คุณลักษณะของ Z-Wave
6.10.2 สถาปัตยกรรมเครือข่าย Z-Wave
6.10.3 โหนดในเครือข่าย Z-Wave
6.10.4 รูปแบบการทำงานของอุปกรณ์เครือข่าย Z-Wave

6.11 LORAWAN

6.11.1 ความหมายของ LoRaWAN
6.11.2 หลักการทำงานของ LoRaWAN
6.11.3 คุณลักษณะของ LoRaWAN
6.11.4 คลาสของอุปกรณ์ LoRaWAN
6.11.5 สถาปัตยกรรมเครือข่าย LoRaWAN
6.11.6 โครงสร้างพื้นฐานของเครือข่าย LoRaWAN
6.11.7 ความปลอดภัยของ LoRaWAN
6.11.8 การประยุกต์ใช้ LoRaWAN ในระบบรักษาความปลอดภัยอัจฉริยะ

6.12 เครือข่ายท้องถิ่นเสมือน

6.12.1 หลักการทำงานของ VLAN
6.12.2 VLAN กับ Subnet
6.12.3 การกำหนดสมาชิกของ VLAN
6.12.4 Access Port และ Trunk Port
6.12.5 มาตรฐาน IEEE 802.1Q
6.12.6 การประยุกต์ใช้ VLAN ในระบบรักษาความปลอดภัยอัจฉริยะ
6.12.7 ประโยชน์ของ VLAN ต่อระบบรักษาความปลอดภัยอัจฉริยะ
6.12.8 ข้อจำกัดของ VLAN
6.12.9 แนวทางการออกแบบ VLAN อย่างปลอดภัย

6.13 POWER OVER ETHERNET (POE)

6.13.1 ความหมายของ Power over Ethernet (PoE)
6.13.2 หลักการทำงานของ PoE
6.13.3 องค์ประกอบของระบบ PoE
6.13.4 มาตรฐานของ PoE
6.13.5 การประยุกต์ใช้ PoE ในระบบรักษาความปลอดภัยอัจฉริยะ

บทที่ 6 ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัย

Networking for Smart security systems

ระบบรักษาความปลอดภัยอัจฉริยะ (smart security system) ในปัจจุบันได้พัฒนาจากระบบรักษาความปลอดภัยแบบแยกส่วน (standalone security system) ไปสู่ระบบที่สามารถเชื่อมโยงอุปกรณ์หลากหลายชนิดผ่านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต โดยอาศัยเทคโนโลยี IoT ทำให้อุปกรณ์ เช่น กล้องโทรทัศน์วงจรปิดชนิด Internet Protocol (IP camera) ระบบควบคุมการเข้าออก (access control system) เซนเซอร์ตรวจจับการบุกรุก (intrusion detection sensors) เซนเซอร์ตรวจจับควันและก๊าซ ระบบแจ้งเตือนอัคคีภัย และระบบบริหารจัดการอาคาร สามารถสื่อสาร แลกเปลี่ยนข้อมูล และทำงานร่วมกันแบบอัตโนมัติผ่านเครือข่ายเดียวกันได้

6.1 ความรู้เบื้องต้นเกี่ยวกับเครือข่ายในระบบรักษาความปลอดภัย

เครือข่ายจึงถือเป็นโครงสร้างพื้นฐาน (network infrastructure) ที่สำคัญที่สุดระบบรักษาความปลอดภัยอัจริยะ เนื่องจากเป็นตัวกลางในการรับส่งข้อมูลระหว่างอุปกรณ์ปลายทาง (end devices) อุปกรณ์ควบคุม (controllers) เซิร์ฟเวอร์ (servers) และบริการคลาวด์ (cloud services) หากระบบเครือข่ายมีประสิทธิภาพสูง จะช่วยให้การสื่อสารมีความรวดเร็ว มีความน่าเชื่อถือ และสามารถตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้แบบเวลาจริง (real-time response) ในทางตรงกันข้าม หากเครือข่ายมีข้อจำกัดด้านแบนด์วิดท์ ความหน่วงเวลา หรือมีช่องโหว่ด้านความปลอดภัย อาจส่งผลให้ข้อมูลสูญหาย การแจ้งเตือนล่าช้า หรือเปิดโอกาสให้ผู้ไม่หวังดีเข้าควบคุมระบบได้ (Yin, 2024) นอกจากนี้ การเพิ่มจำนวนของอุปกรณ์ IoT ภายในบ้าน อาคาร และโรงงานอัจฉริยะ ส่งผลให้เครือข่ายต้องรองรับอุปกรณ์จำนวนมากที่ใช้มาตรฐานการสื่อสารแตกต่างกัน เช่น Wi-Fi, Ethernet, Zigbee, Bluetooth Low Energy (BLE), LoRaWAN และเครือข่ายเซลลูลาร์ (4G/5G) ดังนั้นการออกแบบเครือข่ายของระบบรักษาความปลอดภัยอัจริยะ จึงต้องคำนึงถึงความสามารถในการรองรับอุปกรณ์จำนวนมาก (scalability) ความเข้ากันได้ระหว่างอุปกรณ์ (interoperability) ความมั่นคงปลอดภัย (security) และความต่อเนื่องในการให้บริการ (availability) เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพในระยะยาว (Gupta, 2013)

6.1.1 ความหมายของเครือข่ายในระบบรักษาความปลอดภัย

เครือข่ายในระบบรักษาความปลอดภัย (networking for smart security systems) หมายถึงการออกแบบ ติดตั้ง และบริหารจัดการระบบเครือข่ายที่เชื่อมโยงอุปกรณ์รักษาความปลอดภัยอัจฉริยะทั้งหมดเข้าด้วยกัน เพื่อให้สามารถแลกเปลี่ยนข้อมูล ควบคุมการทำงาน และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้อย่างถูกต้อง รวดเร็ว และปลอดภัย

ระบบเครือข่ายดังกล่าวครอบคลุมตั้งแต่ physical layer, data link layer, network layer, transport layer, application layer, รวมถึงอุปกรณ์เครือข่ายซึ่งทำหน้าที่รับส่งข้อมูลระหว่างอุปกรณ์ในระบบความปลอดภัยอัจฉริยะทั้งหมด

6.1.2 ความสำคัญของระบบเครือข่ายในระบบรักษาความปลอดภัย

ระบบเครือข่ายมีบทบาทสำคัญต่อการทำงานของระบบความปลอดภัยอัจฉริยะ ดังนี้

1) เชื่อมโยงอุปกรณ์ (Device Connectivity)

ทำให้อุปกรณ์รักษาความปลอดภัย เช่น กล้อง IP เซนเซอร์ ระบบควบคุมประตู และระบบแจ้งเตือน สามารถแลกเปลี่ยนข้อมูลระหว่างกันได้อย่างต่อเนื่อง

2) สนับสนุนการสื่อสารแบบเวลาจริง (Real-Time Communication)

การตรวจจับเหตุการณ์ผิดปกติจำเป็นต้องส่งข้อมูลถึงศูนย์ควบคุมภายในเวลาอันสั้น เพื่อให้สามารถแจ้งเตือนหรือสั่งการได้ทันที

3) รองรับการบริหารจัดการจากระยะไกล (Remote Monitoring and Control)

ผู้ใช้งานสามารถตรวจสอบภาพจากกล้องวงจรปิด เปิด-ปิดระบบรักษาความปลอดภัย หรือควบคุมอุปกรณ์ผ่านสมาร์ตโฟนหรือเว็บแอปพลิเคชันได้

4) สนับสนุนการบูรณาการระบบ (System Integration)

เครือข่ายช่วยให้ระบบย่อยต่าง ๆ เช่น CCTV, access control, fire alarm และ Building Management System (BMS) สามารถทำงานร่วมกันเป็นระบบเดียว

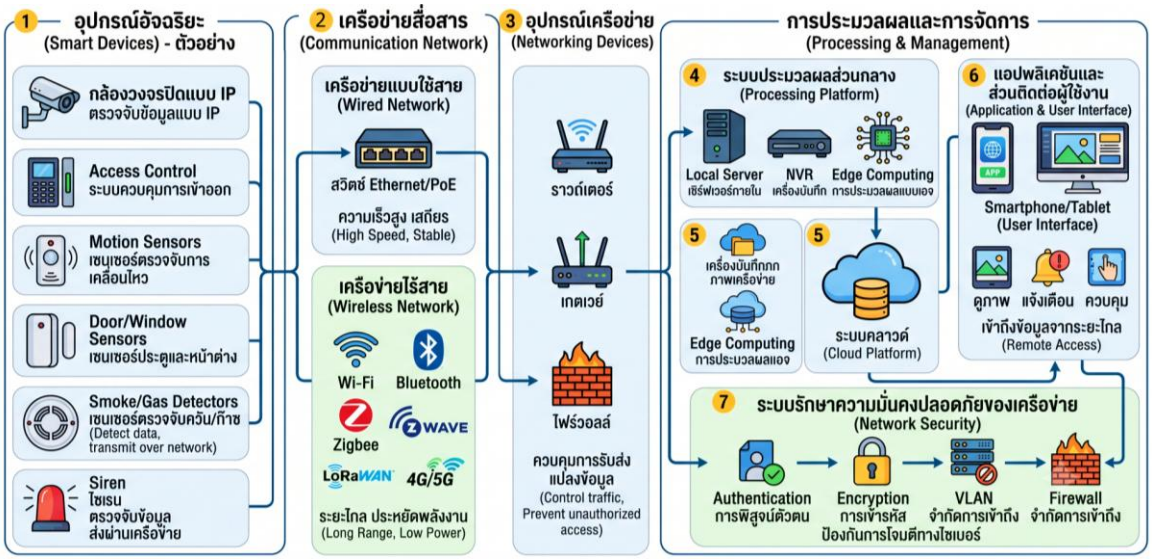
5) เพิ่มความมั่นคงปลอดภัยของระบบ (Cybersecurity)

ใช้เทคนิคการเข้ารหัสข้อมูล (encryption) การพิสูจน์ตัวตน (authentication) การควบคุมสิทธิ์ (access control) ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) และระบบป้องกันการบุกรุก (Intrusion Prevention System: IPS) ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ (Vardakis et al., 2024; Yin, 2024)

เครือข่ายที่ใช้ในระบบความปลอดภัยอัจฉริยะ ควรมีคุณลักษณะสำคัญ ดังนี้ มีความพร้อมใช้งานสูง (high availability) ความน่าเชื่อถือ (reliability) ความสามารถในการขยายระบบ (scalability) รองรับอุปกรณ์หลายมาตรฐาน (interoperability) มีความหน่วงต่ำ (low latency) รองรับการประมวลผลแบบเวลาจริง (real-time processing) มีความมั่นคงปลอดภัย (cybersecurity) สามารถจัดลำดับความสำคัญของข้อมูล (Quality of Service: QoS) รองรับการจัดการจากส่วนกลาง (centralized management) และรองรับการเชื่อมต่อกับ cloud และ Edge computing (Gupta, 2013; Boussard et al., 2018)

6.1.3 องค์ประกอบของเครือข่ายในระบบรักษาความปลอดภัย

ระบบเครือข่ายสำหรับระบบความปลอดภัยอัจฉริยะ ประกอบด้วยองค์ประกอบหลายส่วนที่ทำงานร่วมกันเพื่อให้สามารถรับส่งข้อมูล ตรวจสอบสถานะของอุปกรณ์ และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้แบบเวลาจริง โครงสร้างเครือข่ายครอบคลุมตั้งแต่ระดับอุปกรณ์ตรวจจับ (perception layer) ระดับการสื่อสารข้อมูล (network layer) ไปจนถึงระดับการประมวลผลและการให้บริการ (application layer) ซึ่งช่วยให้ระบบสามารถเชื่อมโยงอุปกรณ์หลากหลายชนิดเข้าด้วยกันภายใต้เครือข่ายเดียว (Vardakis et al., 2024) องค์ประกอบสำคัญของเครือข่ายระบบรักษาความปลอดภัย ประกอบด้วยดังต่อไปนี้



รูปที่ 6.1 องค์ประกอบสำคัญของเครือข่ายระบบรักษาความปลอดภัย

1) อุปกรณ์อัจฉริยะ (Smart Devices)

อุปกรณ์อัจฉริยะเป็นองค์ประกอบพื้นฐานของระบบ ทำหน้าที่ตรวจจับ อุปกรณ์เหล่านี้มักติดตั้งเซนเซอร์ ตัวประมวลผล และโมดูลสื่อสารไว้ภายใน ทำให้สามารถรับส่งข้อมูลผ่านเครือข่ายได้โดยตรง เช่น กล้องวงจรปิดแบบ IP ระบบควบคุมการเข้าออก เครื่องอ่านบัตร RFID เครื่องสแกนลายนิ้วมือ เครื่องสแกนใบหน้า เซนเซอร์ตรวจจับการเคลื่อนไหว เซนเซอร์ประตูและหน้าต่าง เซนเซอร์ตรวจจับควัน เซนเซอร์ตรวจจับก๊าซ เซนเซอร์ตรวจจับเปลวไฟ โดยจะทำหน้าที่รวบรวมข้อมูลจากสภาพแวดล้อมและส่งข้อมูลเข้าสู่ระบบเครือข่ายเพื่อให้ระบบส่วนกลางนำไปวิเคราะห์และประมวลผล (Gupta, 2013)

2) เครือข่ายสื่อสาร (Communication Network)

เครือข่ายสื่อสารทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลระหว่างอุปกรณ์ทั้งหมดภายในระบบรักษาความปลอดภัยอัจริยะ สามารถแบ่งออกเป็นเครือข่ายแบบใช้สาย (wired network) และเครือข่ายไร้สาย (wireless network) โดยเครือข่ายแบบใช้สาย เช่น Ethernet, fast Ethernet, gigabit Ethernet หรือ Power over Ethernet (PoE) โดยเครือข่ายแบบใช้สายเหมาะสำหรับอุปกรณ์ที่ต้องการความเร็วสูงและความเสถียร เช่น กล้องวงจรปิดความละเอียดสูง เครื่องบันทึกภาพ และเซิร์ฟเวอร์ ส่วนเครือข่ายไร้สายที่ใช้งาน เช่น Wi-Fi, BLE, Zigbee, Z-Wave, Thread, LoRaWAN, NB-IoT, หรือ 4G/5G การเลือกใช้เทคโนโลยีขึ้นอยู่กับระยะทาง อัตราการรับส่งข้อมูล การใช้พลังงาน และลักษณะของอุปกรณ์แต่ละประเภท (Gupta, 2013; Vardakis et al., 2024)

3) อุปกรณ์เครือข่าย (Networking Devices)

อุปกรณ์เครือข่ายทำหน้าที่ควบคุมการรับส่งข้อมูลและเชื่อมโยงอุปกรณ์ทั้งหมดภายในระบบเข้าด้วยกัน ประกอบด้วย router, network switch, PoE switch, wireless access point, gateway, และ firewall ซึ่ง gateway มีบทบาทสำคัญในการแปลงข้อมูลระหว่างอุปกรณ์ที่ใช้

มาตรฐานการสื่อสารแตกต่างกัน เช่น Zigbee หรือ Bluetooth ให้สามารถสื่อสารกับเครือข่าย IP ได้ ขณะที่ router และ firewall ช่วยกำหนดเส้นทางข้อมูลและป้องกันการเข้าถึงจากภายนอกโดยไม่ได้รับอนุญาต (Boussard et al., 2018)

4) ระบบประมวลผลส่วนกลาง (Processing Platform)

ข้อมูลที่ได้รับจากอุปกรณ์ทั้งหมดจะถูกส่งมายังระบบประมวลผลส่วนกลางเพื่อดำเนินการวิเคราะห์ ตัดสินใจ และควบคุมการทำงานของอุปกรณ์ต่าง ๆ ระบบประมวลผลอาจอยู่ในรูปแบบ เช่น Edge computing, local server, Network Video Recorder (NVR), Video Management System (VMS), Security Management System (SMS), และ BMS การประมวลผลที่ Edge ช่วยลดความหน่วงของระบบและลดปริมาณข้อมูลที่ต้องส่งไปยังคลาวด์ ขณะที่การประมวลผลบนคลาวด์ช่วยเพิ่มความสามารถในการวิเคราะห์ข้อมูลขนาดใหญ่และการบริหารจัดการจากระยะไกล (Boussard et al., 2018)

5) ระบบคลาวด์ (Cloud Platform)

ระบบคลาวด์ทำหน้าที่จัดเก็บข้อมูล ประมวลผลข้อมูล และให้บริการแก่ผู้ใช้งานผ่านอินเทอร์เน็ต โดยช่วยให้สามารถดูภาพจากกล้องวงจรปิดผ่านสมาร์ตโฟน จัดเก็บข้อมูลบน cloud storage วิเคราะห์ข้อมูลด้วย AI แจ้งเตือนผ่าน mobile application สำรองข้อมูลอัตโนมัติโดย cloud platform ยังช่วยให้สามารถบริหารจัดการระบบรักษาความปลอดภัยหลายสาขาจากศูนย์กลางเดียวได้อย่างมีประสิทธิภาพ (Vardakis et al., 2024)

6) แอปพลิเคชันและส่วนติดต่อผู้ใช้งาน (Application and User Interface)

ผู้ใช้งานสามารถติดต่อกับระบบผ่านซอฟต์แวร์หรือแอปพลิเคชันที่ทำหน้าที่ แสดงสถานะของอุปกรณ์ แสดงภาพจากกล้องวงจรปิดและแจ้งเตือน สามารถควบคุมอุปกรณ์จากระยะไกล กำหนดสิทธิ์ผู้ใช้งาน หรือจัดทำรายงานและบันทึกเหตุการณ์ โดยแอปพลิเคชันสามารถทำงานได้ทั้งบนคอมพิวเตอร์ เว็บเบราว์เซอร์ และอุปกรณ์เคลื่อนที่ ทำให้ผู้ดูแลระบบสามารถบริหารจัดการระบบได้จากทุกที่ที่มีการเชื่อมต่ออินเทอร์เน็ต (Vardakis et al., 2024)

7) ระบบรักษาความมั่นคงปลอดภัยของเครือข่าย (Network Security)

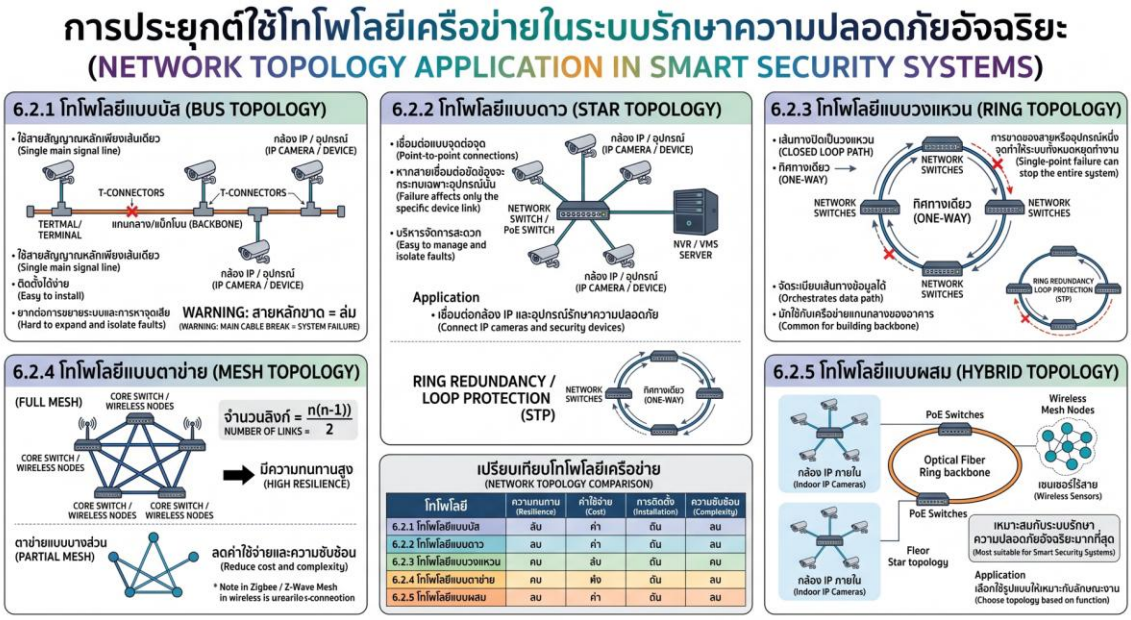
เนื่องจากระบบความปลอดภัยอัจฉริยะ เชื่อมต่อกับเครือข่ายและอินเทอร์เน็ต จึงจำเป็นต้องมีมาตรการรักษาความมั่นคงปลอดภัยของเครือข่าย เพื่อป้องกันการโจมตีและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต มาตรการที่สำคัญ ได้แก่ การพิสูจน์ตัวตน (authentication), การกำหนดสิทธิ์การเข้าถึง (authorization), การเข้ารหัสข้อมูล (encryption), firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), IDS, IPS, หรือการตรวจสอบและบันทึกเหตุการณ์ (logging and monitoring) การรักษาความมั่นคงปลอดภัยในระดับเครือข่ายควรจำกัดการสื่อสารของอุปกรณ์แต่ละชนิดให้เฉพาะบริการที่จำเป็น (least privilege networking) พร้อมทั้งใช้การตรวจจับความผิดปกติของทราฟฟิก (anomaly detection) เพื่อระบุพฤติกรรมที่อาจเกิดจากการโจมตีหรือมัลแวร์ ซึ่งช่วยลดความเสี่ยงภัยคุกคามภายในเครือข่ายอย่างมีประสิทธิภาพ (Serror et al., 2018)

กล่าวโดยสรุป เครือข่ายรักษาความปลอดภัยอัจฉริยะ มีองค์ประกอบหลัก 7 ส่วน ได้แก่ (1) อุปกรณ์อัจฉริยะ (2) เครือข่ายสื่อสาร (3) อุปกรณ์เครือข่าย (4) ระบบประมวลผลส่วนกลาง (5)

ระบบคลาวด์ (6) แอปพลิเคชันและส่วนติดต่อผู้ใช้งาน และ (7) ระบบรักษาความมั่นคงปลอดภัยของเครือข่าย องค์ประกอบเหล่านี้ทำงานร่วมกันเป็นโครงสร้างพื้นฐานที่สนับสนุนการตรวจจับ การสื่อสาร การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้อย่างรวดเร็ว มีประสิทธิภาพ และปลอดภัย

6.2 โครงสร้างการเชื่อมต่อเครือข่าย (Network Topology)

โทโพโลยีเครือข่าย หมายถึง รูปแบบการเชื่อมต่อและความสัมพันธ์ระหว่างอุปกรณ์ภายในเครือข่าย โดยแบ่งเป็นโทโพโลยีทางกายภาพ (physical topology) ซึ่งแสดงการติดตั้งและการเชื่อมต่ออุปกรณ์จริง และโทโพโลยีทางตรรกะ (logical topology) ซึ่งแสดงเส้นทางและลักษณะการไหลของข้อมูลในเครือข่าย (Forouzan, 2013) การเลือกโทโพโลยีสำหรับระบบรักษาความปลอดภัยอัจฉริยะควรพิจารณา ความน่าเชื่อถือ การขยายระบบ ความสะดวกในการตรวจสอบและแก้ไขความขัดข้อง ค่าใช้จ่าย และผลกระทบจากความล้มเหลวของอุปกรณ์หรือสายสัญญาณ เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและต่อเนื่อง โทโพโลยีเครือข่ายดังรูปที่ 6.2 รายละเอียดดังนี้



รูปที่ 6.2 โทโพโลยีเครือข่ายในระบบรักษาความปลอดภัยอัจฉริยะ

6.2.1 โทโพโลยีแบบบัส (Bus Topology)

ใช้สายสัญญาณหลักเพียงเส้นเดียวเป็นแกนกลางหรือแบ็กโบน อุปกรณ์ทุกตัวเชื่อมต่อเข้ากับสายหลัก ข้อมูลที่ส่งออกจากอุปกรณ์หนึ่งจะเดินทางไปตามสายหลัก และสามารถผ่านอุปกรณ์ทุกตัวที่เชื่อมต่ออยู่ โครงสร้างนี้ใช้สายสัญญาณค่อนข้างน้อยและติดตั้งได้ง่าย ระบบมีขนาดเล็ก แต่การเพิ่มอุปกรณ์ การหาจุดเสีย และการแก้ไขปัญหาทำได้ยาก หากสายหลักเกิดการขาดหรือชำรุด การสื่อสารของเครือข่ายส่วนใหญ่หรือทั้งหมดอาจหยุดทำงานได้ (Forouzan, 2013) Ethernet รุ่น

แรกที่ใช้สายโคแอกเชียล เช่น 10Base5 และ 10Base2 เคยใช้โครงสร้างแบบบัส แต่ปัจจุบันระบบรักษาความปลอดภัยไม่เป็นที่นิยมเนื่องจากมีข้อจำกัดด้านความน่าเชื่อถือ การขยายระบบ และการแยกความผิดปกติ จึงไม่เหมาะกับระบบที่ต้องทำงานตลอด 24 ชั่วโมง

6.2.2 โทโพโลยีแบบดาว (Star Topology)

โทโพโลยีแบบดาวเป็นรูปแบบเครือข่ายที่อุปกรณ์แต่ละตัวเชื่อมต่อแบบจุดต่อจุด (point-to-point) ไปยังอุปกรณ์ศูนย์กลาง โดยเครือข่าย Ethernet มักใช้ network switch หรือ PoE switch เป็นศูนย์กลาง ข้อดีคือ หากสายเชื่อมต่อของอุปกรณ์ใดขัดข้องจะกระทบเฉพาะอุปกรณ์นั้น ขณะที่ส่วนอื่นของเครือข่ายยังทำงานได้ จึงติดตั้ง บริหารจัดการ และแยกจุดขัดข้องได้สะดวก (Forouzan, 2013) ในระบบรักษาความปลอดภัยอัจฉริยะสามารถประยุกต์โทโพโลยีแบบดาวโดยเชื่อมต่อกล้อง IP และอุปกรณ์รักษาความปลอดภัยเข้าสู่ access, PoE switch แล้วเชื่อมต่อไปยัง NVR, VMS server หรือ core switch ตามสถาปัตยกรรมของระบบ

6.2.3 โทโพโลยีแบบวงแหวน (Ring Topology)

ใช้เชื่อมต่ออุปกรณ์แต่ละตัวเข้ากับอุปกรณ์ข้างเคียงสองด้าน ทำให้เกิดเส้นทางปิดเป็นวงแหวน ข้อมูลเดินทางผ่านอุปกรณ์แต่ละจุดไปจนถึงปลายทาง ข้อดีคือสามารถจัดระเบียบเส้นทางข้อมูลและตรวจหาตำแหน่งที่ขัดข้องได้ แต่ในวงแหวนแบบทิศทางเดียว การขาดของสายหรือความผิดปกติของอุปกรณ์เพียงจุดเดียวอาจทำให้ระบบทั้งหมดหยุดทำงานได้ ปัญหานี้สามารถลดลงด้วยวงแหวนคู่หรือกลไกเปลี่ยนเส้นทางอัตโนมัติ (Forouzan, 2013) ในระบบรักษาความปลอดภัยโครงสร้างแบบวงแหวนมักใช้กับเครือข่ายแกนกลางของอาคาร โรงงาน หรือพื้นที่ขนาดใหญ่ เพื่อสร้างเส้นทางสำรองระหว่างสวิตช์ หากสายสัญญาณด้านหนึ่งขาดข้อมูลสามารถเปลี่ยนไปใช้เส้นทางได้ จะใช้ในโปรโตคอลป้องกันลูป (loop protection protocol) เช่น Spanning Tree Protocol (STP) หรือเทคโนโลยีวงแหวนเฉพาะของผู้ผลิต

6.2.4 โทโพโลยีแบบตาข่าย (Mesh Topology)

เป็นการเชื่อมต่ออุปกรณ์หนึ่งเข้ากับอุปกรณ์อื่นหลายตัว หากเป็นแบบตาข่ายสมบูรณ์ อุปกรณ์ทุกตัวจะมีเส้นทางตรงถึงกัน จำนวนลิงก์สำหรับระบบที่มีอุปกรณ์ n ตัว เท่ากับ

$$\text{จำนวนลิงก์สำหรับระบบที่มีอุปกรณ์ } n \text{ ตัว} = \frac{n(n-1)}{2} \qquad (6.1)$$

โครงสร้างนี้มีความทนทานสูง เนื่องจากเมื่อเส้นทางหนึ่งขัดข้อง ข้อมูลสามารถเลือกใช้เส้นทางอื่นได้ แต่ต้องใช้พอร์ตและสายสัญญาณจำนวนมาก ส่งผลให้มีค่าใช้จ่ายและความซับซ้อนสูง (Forouzan, 2013) ในระบบรักษาความปลอดภัยอัจฉริยะ มักใช้โครงข่ายแบบบางส่วนมากกว่าโครงข่ายสมบูรณ์ เชื่อมต่อเฉพาะ core switch, distribution switch หรือ wireless nodes ที่สำคัญเข้าด้วยกันหลายเส้นทางโดยไม่เพิ่มค่าใช้จ่ายมากเกินไป สำหรับ Zigbee และ Z-Wave โทโพโลยีแบบ Mesh ยังช่วยให้อุปกรณ์ที่อยู่ไกลจากตัวควบคุมสามารถส่งต่อข้อมูลผ่านอุปกรณ์ใกล้เคียงได้

6.2.5 โทโพโลยีแบบผสม (Hybrid Topology)

เป็นการรวมโทโพโลยีหลายแบบไว้ในระบบเดียว เช่น อุปกรณ์กล้อง IP ภายในแต่ละชั้นเชื่อมต่อแบบดาวเข้ากับ PoE switch ขณะที่สวิตช์ของแต่ละชั้นเชื่อมต่อกันเป็นวงแหวนด้วยสายใยแก้วนำแสง ส่วนเซนเซอร์ไร้สายอาจเชื่อมต่อเป็นแบบตาข่ายผ่าน Zigbee โครงสร้างแบบผสมเหมาะสมกับระบบระบบความปลอดภัยอัจฉริยะมากที่สุด เพราะสามารถเลือกใช้รูปแบบการเชื่อมต่อให้เหมาะกับลักษณะงานแต่ละส่วน กล่าวคือ ใช้โครงสร้างแบบดาวสำหรับการติดตั้งอุปกรณ์ปลายทาง ใช้วงแหวนหรือตาข่ายสำหรับโครงข่ายแกนกลาง และใช้ Mesh สำหรับเซนเซอร์ไร้สายที่กระจายอยู่ในพื้นที่

6.3 ชุดโปรโตคอล Transmission Control Protocol/Internet Protocol (TCP/IP)

การสื่อสารผ่านเครือข่ายประกอบด้วยหลายหน้าที่ เช่น การสร้างและแบ่งข้อมูล การกำหนดต้นทางปลายทาง การตรวจสอบความผิดพลาด การเลือกเส้นทาง และการแปลงข้อมูลเป็นสัญญาณเพื่อส่งผ่านสื่อกลาง หากรวมหน้าที่ทั้งหมดไว้ในระบบเดียวจะทำให้การออกแบบและพัฒนามีความซับซ้อน จึงใช้แนวคิด การแบ่งชั้นโปรโตคอล (protocol layering) เพื่อแบ่งกระบวนการสื่อสารออกเป็นชั้นที่มีหน้าที่เฉพาะและทำงานประสานกันตามลำดับ ในระบบรักษาความปลอดภัยอัจฉริยะ ข้อมูลจากเซนเซอร์ต่าง ๆ จะผ่านกระบวนการของชุดโปรโตคอล TCP/IP ก่อนส่งถึงระบบบริหารจัดการ ตัวอย่างเช่น ข้อมูลภาพจากกล้องจะถูกสร้างในชั้นแอปพลิเคชัน แบ่งเป็นหน่วยข้อมูลในชั้นขนส่ง กำหนดที่อยู่ IP ในชั้นเครือข่าย ห่อหุ้มเป็นเฟรมสำหรับส่งผ่านเครือข่ายท้องถิ่นและส่งเป็นสัญญาณผ่านสื่อกลาง กระบวนการแบบแบ่งชั้นช่วยให้การสื่อสารมีโครงสร้างชัดเจนและสามารถทำงานร่วมกันระหว่างอุปกรณ์และระบบที่แตกต่างกันได้ (Forouzan, 2013)

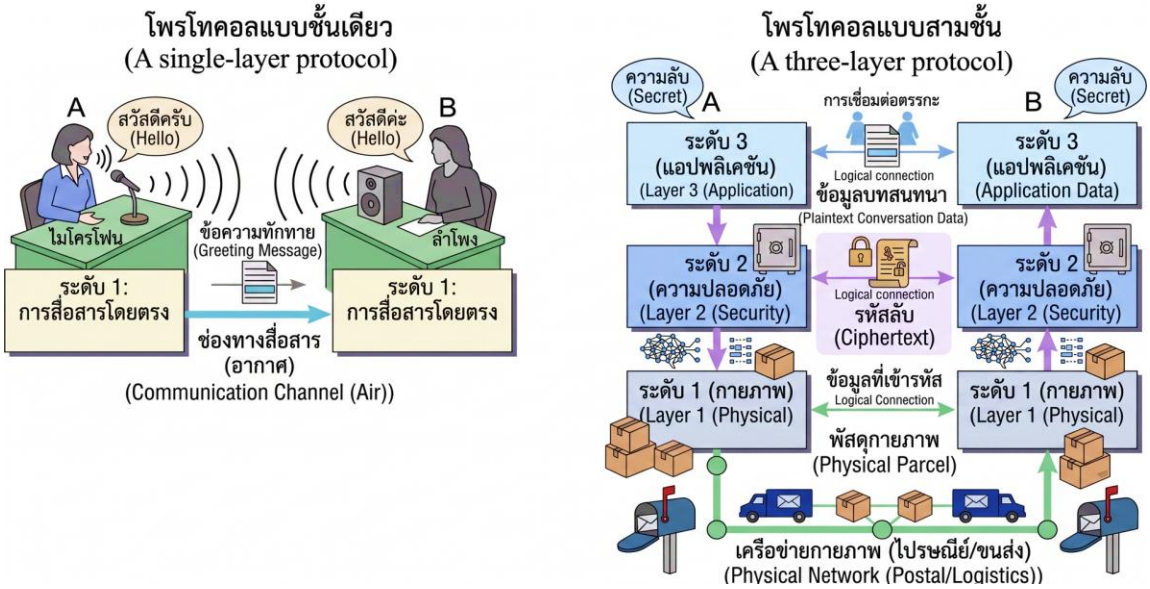
6.3.1 ความหมายของโปรโตคอล (Protocol)

โปรโตคอล คือ ชุดกฎหรือข้อตกลงที่กำหนดวิธีการสื่อสารระหว่างผู้ส่ง ผู้รับ และอุปกรณ์ตัวกลาง เพื่อให้อุปกรณ์ที่อาจผลิตโดยผู้ผลิตต่างกันสามารถแลกเปลี่ยนข้อมูลกันได้อย่างถูกต้อง โปรโตคอลกำหนดรายละเอียดสำคัญ เช่น รูปแบบของข้อมูล ลำดับการส่งและรับข้อมูล วิธีระบุผู้ส่งและผู้รับ วิธีตรวจสอบความผิดพลาด วิธีตอบรับข้อมูล วิธีควบคุมความเร็วในการส่ง และวิธีจัดการเมื่อข้อมูลสูญหายหรือเกิดความแออัด ในสถานการณ์การสื่อสารอย่างง่าย อาจใช้กฎเพียงชุดเดียว แต่เมื่อการสื่อสารมีความซับซ้อน จำเป็นต้องแบ่งงานออกเป็นหลายชั้น โดยแต่ละชั้นมีโปรโตคอลที่เหมาะกับหน้าที่ของตนเอง แนวคิดนี้เรียกว่า protocol layering (Forouzan, 2013)

6.3.2 แนวคิดของการแบ่งชั้นโปรโตคอล

การแบ่งชั้นโปรโตคอลสามารถอธิบายได้จากตัวอย่างการสื่อสารของบุคคลสองคน หากบุคคลทั้งสองอยู่ใกล้กันและใช้ภาษาเดียวกัน การสื่อสารอาจเกิดขึ้นในชั้นเดียว คือการพูดและการฟัง แต่หากอยู่ห่างกันและต้องส่งจดหมายที่เป็นความลับ มีหน้าที่เพิ่มขึ้น ได้แก่ (1) การสร้างและทำความ

เข้าใจข้อความ (2) การเข้ารหัสและถอดรหัสข้อความ และ (3) การส่งและรับจดหมายผ่านระบบไปรษณีย์ (Forouzan, 2013)



รูปที่ 6.3 เปรียบเทียบแนวคิดของการแบ่งชั้นโปรโตคอล (ดัดแปลงจาก Forouzan, 2013)

จากรูปที่ 6.3 แต่ละหน้าที่เปรียบได้กับชั้นหนึ่งของระบบสื่อสาร ชั้นบนสุดรับผิดชอบเนื้อหาที่ผู้ใช้ต้องการสื่อสาร ชั้นกลางดูแลการรักษาความลับ ส่วนชั้นล่างรับผิดชอบการนำส่งข้อมูลจริง แนวคิดนี้สะท้อนหลักการของเครือข่ายคอมพิวเตอร์ว่าแต่ละชั้นควรให้บริการแก่ชั้นที่อยู่เหนือขึ้นไปและใช้บริการจากชั้นที่อยู่ต่ำกว่า (Forouzan, 2013) ข้อดีของการแบ่งชั้น คือ เมื่อเทคโนโลยีหรือวิธีการในชั้นหนึ่งเปลี่ยนแปลง ไม่จำเป็นต้องปรับเปลี่ยนทั้งระบบ เช่น หากเปลี่ยนจากสายทองแดงเป็นสายใยแก้วนำแสง หน้าที่ในชั้นกายภาพเปลี่ยน แต่แอปพลิเคชันที่ใช้ดูภาพกล้องไม่จำเป็นต้องเปลี่ยนตาม

6.3.3 หลักการสำคัญของ Protocol Layering

1) แต่ละชั้นต้องรองรับการสื่อสารสองทิศทาง

หากระบบต้องรับส่งข้อมูลแบบสองทิศทาง แต่ละชั้นต้องสามารถดำเนินงานในทิศทางตรงกันข้ามได้ เช่น (1) ชั้นแอปพลิเคชันต้องส่งและรับข้อความ (2) ชั้นขนส่งต้องแบ่งข้อมูลและประกอบข้อมูลกลับ (3) ชั้นเครือข่ายต้องส่งและรับแพ็กเก็ต (4) ชั้นเชื่อมโยงข้อมูลต้องสร้างและตรวจสอบเฟรม และ (5) ชั้นกายภาพต้องส่งและรับสัญญาณ เช่น ในระบบกล้อง IP กล้องทำหน้าที่ส่งภาพไปยัง NVR ขณะเดียวกัน NVR อาจส่งคำสั่งควบคุมกลับไปยังกล้อง เช่น คำสั่งหมุนกล้อง ปรับมุม หรือเปลี่ยนค่าการบันทึก ดังนั้น ทุกชั้นต้องรองรับการสื่อสารทั้งสองทิศทาง

2) หน่วยข้อมูลในชั้นเดียวกันของผู้ส่งและผู้รับต้องสอดคล้องกัน

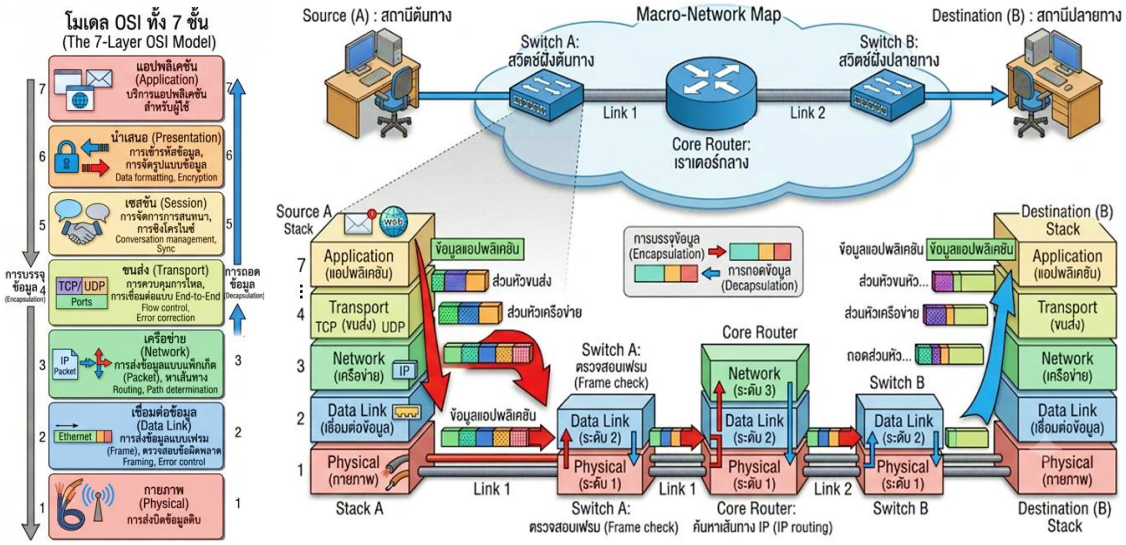
หน่วยข้อมูลที่เกิดขึ้นในชั้นเดียวกันของต้นทางและปลายทางต้องมีรูปแบบที่เข้าใจกันได้ เช่น ชั้นแอปพลิเคชันแลกเปลี่ยนข้อความหรือข้อมูลแอปพลิเคชัน ชั้นขนส่งแลกเปลี่ยน segment หรือ user datagram ชั้นเครือข่ายแลกเปลี่ยน IP datagram ชั้นเชื่อมโยงข้อมูลแลกเปลี่ยน frame หรือ ชั้นกายภาพแลกเปลี่ยน Bit แม้ข้อมูลจะผ่านอุปกรณ์ตัวกลาง แต่หลักการเชิงตรรกะถือว่าชั้นเดียวกันของต้นทางและปลายทางสื่อสารกันด้วยกฎเดียวกัน

6.3.4 การเชื่อมต่อเชิงตรรกะระหว่างชั้น

การเชื่อมต่อเชิงตรรกะ (logical connection) หมายถึง ความสัมพันธ์เสมือนระหว่างชั้นเดียวกันของอุปกรณ์ต้นทางและปลายทาง แม้ในทางกายภาพข้อมูลต้องเดินทางผ่านชั้นล่าง อุปกรณ์สวิตช์ และเราเตอร์ก็ตาม ตัวอย่างเช่น แอปพลิเคชันบนกล้อง IP ดูเสมือนสื่อสารกับแอปพลิเคชันของ NVR โดยตรง แต่ในความเป็นจริงข้อมูลจะถูกส่งลงมาตามลำดับชั้น ผ่านสายสัญญาณ สวิตช์ และเราเตอร์ ก่อนถูกส่งขึ้นไปยังแอปพลิเคชันปลายทาง การเชื่อมต่อเชิงตรรกะระหว่างชั้นช่วยให้อธิบายหน้าที่ของแต่ละชั้นได้ง่ายขึ้นไม่จำเป็นต้องพิจารณากระบวนการทุกชั้นพร้อมกัน การเชื่อมต่อของสามชั้นบน ได้แก่ application, transport และ network มีขอบเขตแบบ end-to-end ส่วน physical และ data link มีขอบเขตแบบ hop-to-hop ระหว่างอุปกรณ์ที่อยู่ติดกันในเส้นทาง (Forouzan, 2013)

6.3.5 สถาปัตยกรรมของชุดโปรโตคอล TCP/IP

TCP/IP เป็นชุดโปรโตคอลพื้นฐานของอินเทอร์เน็ตและเครือข่าย คำว่า protocol suite หมายถึง กลุ่มโปรโตคอลหลายชนิดที่จัดเป็นลำดับชั้น โดยแต่ละโปรโตคอลมีหน้าที่เฉพาะและทำงานร่วมกันเป็นระบบ เช่น แบบจำลอง OSI (Open Systems Interconnection Model) แบ่งการสื่อสารออกเป็น 7 ชั้น ได้แก่ physical, data link, network, transport, session, presentation, และ application layer ส่วนแบบจำลอง TCP/IP ซึ่งใช้งานจริงบนเครือข่ายอินเทอร์เน็ต แบ่งเป็น 4 หรือ 5 ชั้น โดยรวมหน้าที่ของ session layer และ presentation layer เข้าไว้ใน application layer ดังนั้นโปรโตคอล เช่น Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), Message Queuing Telemetry Transport (MQTT), Real-Time Streaming Protocol (RTSP), หรือ Open Network Video Interface Forum (ONVIF) จึงถูกจัดอยู่ใน application layer ของ TCP/IP แม้ว่าจะมีหน้าที่บางส่วนสอดคล้องกับ presentation layer หรือ session layer ของ OSI ก็ตาม (Forouzan, 2013; Stallings, 2017)



(ก) แบบจำลอง OSI (ข) TCP/IP

รูปที่ 6.4 การเปรียบเทียบการสื่อสารข้อมูลระหว่างแบบจำลอง OSI กับ TCP/IP ระหว่างสถานีต้นทางและสถานีปลายทาง

จากรูปที่ 6.4 เมื่อข้อมูลถูกส่งจากสถานีต้นทาง ข้อมูลจะถูกห่อหุ้ม (encapsulation) ตามลำดับชั้นจาก application layer ลงสู่ physical layer โดยแต่ละชั้นจะเพิ่มข้อมูลควบคุมที่จำเป็น เช่น หมายเลขพอร์ต ที่อยู่ IP และ Medium Access Control (MAC) address ก่อนส่งข้อมูลในรูปของสัญญาณผ่านสื่อกลางไปยังเครือข่าย โดยเมื่อข้อมูลผ่าน switch อุปกรณ์จะพิจารณา MAC address ของเฟรมเพื่อส่งต่อไปยังพอร์ตที่เหมาะสม ส่วน router จะนำข้อมูลจากเฟรมมาพิจารณาที่ network layer และใช้ IP address เพื่อเลือกเส้นทางไปยังเครือข่ายปลายทาง จากนั้นจะสร้างเฟรมใหม่สำหรับลิงก์ถัดไป เมื่อข้อมูลถึงสถานีปลายทาง จะเกิดกระบวนการ ถอดส่วนห่อหุ้ม (decapsulation) จาก physical layer ขึ้นไปตามลำดับจนถึง application layer เพื่อส่งมอบข้อมูลให้แก่ปลายทาง การทำงานแต่ละชั้นดังนี้

1) ชั้นกายภาพ (Physical Layer)

ชั้นกายภาพ เป็นชั้นล่างสุดของแบบจำลอง OSI ทำหน้าที่รับ-ส่ง ข้อมูลbitผ่านสื่อกลางทางกายภาพ โดยแปลงbitให้เป็นสัญญาณที่เหมาะสมกับสื่อ เช่น สัญญาณไฟฟ้า สัญญาณแสง หรือคลื่นแม่เหล็กไฟฟ้า และแปลงกลับเป็นbitเมื่อถึงปลายทาง ชั้นนี้เกี่ยวข้องกับคุณลักษณะทางกายภาพและทางไฟฟ้าของการสื่อสาร เช่น สื่อส่งสัญญาณ หัวต่อ อัตราbit การเข้ารหัสสัญญาณและรูปแบบการรับ-ส่งข้อมูล

ในระบบรักษาความปลอดภัยอัจฉริยะ ชั้นกายภาพครอบคลุมเทคโนโลยีและอุปกรณ์ที่ใช้ส่งสัญญาณ เช่น สายคู่บิดเกลียว (twisted-pair cable) ใยแก้วนำแสง (fiber-optic cable) พอร์ตและหัวต่อ โมดูล SFP และสื่อไร้สาย ตัวอย่างเช่น กล้อง IP ที่เชื่อมต่อกับ PoE switch ผ่านสายคู่บิดเกลียวจะรับ-ส่งข้อมูลด้วยสัญญาณทางกายภาพตามมาตรฐาน Ethernet ที่เกี่ยวข้อง

หากเกิดปัญหา เช่น สายขาด ช็อต หัวต่อหลวม สัญญาณลดทอน หรือสัญญาณรบกวน การสื่อสารของชั้นที่สูงกว่าจะไม่สามารถดำเนินการได้ตามปกติ

2) ชั้นเชื่อมโยงข้อมูล (Data Link Layer)

ชั้นเชื่อมโยงข้อมูล ทำหน้าที่รับ-ส่งข้อมูลระหว่างอุปกรณ์บนลิงก์หรือเครือข่ายท้องถิ่นเดียวกัน โดยรับแพ็กเก็ตจาก network layer มาห่อหุ้มเป็น frame ก่อนส่งต่อไปยัง physical layer หน้าที่สำคัญ ได้แก่ การสร้างเฟรม การใช้ MAC address การควบคุมการเข้าถึงสื่อ และการตรวจจับข้อผิดพลาดของเฟรม รวมถึงรองรับกลไก เช่น VLAN Tagging ใน Ethernet โดย Ethernet และ Wi-Fi มีการทำงานที่เกี่ยวข้องทั้ง data link และ physical layer

ในระบบรักษาความปลอดภัยอัจฉริยะ switch จะตรวจสอบ MAC address ปลายทางของ Ethernet frame เพื่อส่งเฟรมไปยังพอร์ตที่เหมาะสม ตัวอย่างเช่น หากกล้อง IP และ NVR อยู่ใน VLAN เดียวกัน สามารถสื่อสารผ่านการสวิตช์ใน layer 2 ได้ แต่หากอยู่คนละ VLAN จะต้องอาศัยอุปกรณ์ layer 3 เช่น router หรือ switch เพื่อทำ inter-VLAN routing การทำงานของชั้นนี้มีขอบเขตเป็นลิงก์ต่อหนึ่งช่วง (hop-to-hop) ดังนั้นเมื่อแพ็กเก็ตผ่าน router เฟรมของลิงก์เดิมจะสิ้นสุดลง และข้อมูลระดับ network layer จะถูกนำไปห่อหุ้มเป็นเฟรมใหม่ให้เหมาะสมกับลิงก์ถัดไป

3) ชั้นเครือข่าย (Network Layer)

ชั้นเครือข่ายทำหน้าที่ส่งข้อมูลจากต้นทางไปปลายทางที่อาจอยู่ต่างเครือข่ายกัน โดยใช้ Internet Protocol (IP) เป็นโปรโตคอลหลัก และใช้ IP address เพื่อระบุต้นทางและปลายทาง หน่วยข้อมูลในชั้นนี้เรียกว่า IP packet หรือ datagram หน้าที่สำคัญ ได้แก่ การกำหนดที่อยู่เชิงตรรกะ การส่งต่อแพ็กเก็ต (forwarding) และการเลือกเส้นทาง (routing) ระหว่างเครือข่าย โดย IP ทำงานแบบ connectionless และ best-effort คือไม่จำเป็นต้องสร้างการเชื่อมต่อก่อนส่ง และไม่รับประกันว่าแพ็กเก็ตจะถึงปลายทางครบถ้วน หรือเรียงตามลำดับ ดังนั้นกลไกด้านความน่าเชื่อถือจึงเป็นหน้าที่ของโปรโตคอลในชั้นที่สูงกว่า เช่น TCP ใน transport layer อุปกรณ์สำคัญของชั้นนี้คือ router และ layer 3 switch ซึ่งพิจารณา IP address ปลายทางและข้อมูลการกำหนดเส้นทางเพื่อส่งแพ็กเก็ตไปยังเครือข่ายถัดไป ตัวอย่างในระบบรักษาความปลอดภัยอัจฉริยะ เมื่อผู้ใช้เข้าถึงกล้อง IP จากต่างเครือข่าย network layer จะทำหน้าที่ส่ง IP packet ผ่านเครือข่ายและเราเตอร์ต่าง ๆ ไปยังปลายทางตามเส้นทางที่เหมาะสม

4) ชั้นขนส่ง (Transport Layer)

ชั้นขนส่งทำหน้าที่สื่อสารระหว่างแอปพลิเคชันหรือกระบวนการ (process-to-process communication) ของอุปกรณ์ต้นทางและปลายทาง โดยใช้ port number เพื่อระบุบริการหรือแอปพลิเคชันที่รับ-ส่งข้อมูล โปรโตคอลหลักที่ใช้ ได้แก่ Transmission Control Protocol (TCP) และ User Datagram Protocol (UDP)

4.1) TCP เป็นโปรโตคอลแบบ connection-oriented ที่สร้างการเชื่อมต่อเชิงตรรกะก่อนรับ-ส่งข้อมูล และให้บริการส่งข้อมูลที่เชื่อถือได้ โดยมีการตรวจสอบลำดับ ตรวจจับข้อมูลสูญหาย ส่งข้อมูลซ้ำเมื่อจำเป็น รวมถึงควบคุมการไหลและความแออัดของเครือข่าย โดย TCP เหมาะกับงานที่ต้องการความถูกต้องและครบถ้วนของข้อมูล เช่น การเข้าถึงระบบผ่าน HTTPS การ

กำหนดค่าอุปกรณ์ การรับ-ส่งข้อมูลฐานข้อมูล และการดาวน์โหลดไฟล์บันทึกหรือวิดีโอหลักฐาน อย่างไรก็ตาม กลไกควบคุมและการส่งซ้ำอาจเพิ่มความหน่วงเมื่อเทียบกับ UDP

4.2) UDP คือโปรโตคอล connectionless ที่ส่ง datagram โดยไม่สร้างการเชื่อมต่อก่อน และไม่รับประกันการส่งถึงปลายทาง การเรียงลำดับ หรือการส่งซ้ำเมื่อข้อมูลสูญหาย จึงมีโครงสร้างเรียบง่ายและมี overhead ต่ำ ซึ่ง UDP เหมาะกับงานที่ให้ความสำคัญกับ ความรวดเร็วและเวลาจริง และสามารถยอมรับการสูญหายของข้อมูลบางส่วนได้ เช่น การส่งวิดีโอหรือเสียงแบบเวลาจริง และการสื่อสารแบบ multicast ในระบบรักษาความปลอดภัย การสตรีมวิดีโอสดอาจใช้ UDP เพื่อลดความหน่วง ขณะที่การดาวน์โหลดไฟล์วิดีโอหลักฐานมักเลือกการขนส่งที่เชื่อถือได้ เช่น TCP เพื่อรักษาความครบถ้วนของข้อมูล

5) ชั้นเซสชัน (Session Layer)

ชั้นเซสชัน ทำหน้าที่ สร้าง จัดการ และยุติเซสชัน ระหว่างแอปพลิเคชันของอุปกรณ์ต้นทางและปลายทาง เพื่อให้การแลกเปลี่ยนข้อมูลดำเนินไปอย่างต่อเนื่องและเป็นระบบ หน้าที่สำคัญ ได้แก่ การสร้างและยุติเซสชัน การควบคุมการสนทนาระหว่างแอปพลิเคชัน และการซิงโครไนซ์ (synchronization) ซึ่งอาจใช้จุดตรวจสอบ (checkpoint) เพื่อช่วยให้สามารถดำเนินการต่อจากจุดที่กำหนดเมื่อเกิดการหยุดชะงัก (Stallings, 2017) ส่วนในแบบจำลอง TCP/IP ไม่มีการแยก session layer เป็นชั้นเฉพาะ หน้าที่ดังกล่าวโดยทั่วไปจึงรวมอยู่ใน application layer และดำเนินการโดยโปรโตคอลหรือซอฟต์แวร์ระดับแอปพลิเคชัน

ในระบบรักษาความปลอดภัยอัจฉริยะ แนวคิดของเซสชันพบได้ในการติดต่อระหว่างโปรแกรมบริหารจัดการวิดีโอ (VMS) กับเซิร์ฟเวอร์หรืออุปกรณ์เครือข่าย เช่น การเข้าสู่ระบบเพื่อดูภาพจากกล้อง IP และการยุติเซสชันเมื่อผู้ใช้ออกจากระบบ ทั้งนี้ การรักษาหรือกู้คืนเซสชันเมื่อการเชื่อมต่อขาดหายขึ้นอยู่กับการออกแบบของแอปพลิเคชันและโปรโตคอลที่ใช้งาน

6) ชั้นนำเสนอข้อมูล (Presentation Layer)

ชั้นนำเสนอข้อมูล ทำหน้าที่จัดรูปแบบและแปลงข้อมูล ให้อยู่ในรูปแบบที่แอปพลิเคชันต้นทางและปลายทางสามารถตีความร่วมกันได้ แม้ระบบจะใช้รูปแบบการแทนข้อมูลที่แตกต่างกัน หน้าที่สำคัญคือ การแปลงรูปแบบข้อมูล (data translation) การเข้ารหัสอักขระ (character encoding) การบีบอัดและคลายข้อมูล (compression and decompression) และการเข้ารหัสและถอดรหัสข้อมูล (encryption and decryption) (Stallings, 2017) ในการอธิบายตามแนวคิดของแบบจำลอง OSI การเข้ารหัสและถอดรหัสข้อมูลเพื่อรักษาความลับสามารถจัดเป็นหน้าที่ของ presentation layer ได้ อย่างไรก็ตามใน แบบจำลอง TCP/IP ไม่มีการแยก presentation layer เป็นชั้นเฉพาะ หน้าที่เหล่านี้โดยทั่วไปจึงดำเนินการโดย application layer แอปพลิเคชัน ไลบรารี หรือโปรโตคอลที่เกี่ยวข้อง

ในระบบรักษาความปลอดภัยอัจฉริยะ ตัวอย่างหน้าที่ที่สอดคล้องกับชั้นนี้ เช่น การเข้ารหัสวิดีโอด้วย H.264 หรือ H.265 เพื่อลดปริมาณข้อมูลจากกล้อง IP การบีบอัดภาพด้วย JPEG และการใช้ UTF-8 เพื่อให้ระบบสามารถตีความและแสดงข้อความได้อย่างถูกต้อง

7) ชั้นประยุกต์ (Application Layer)

ชั้นประยุกต์ เป็นชั้นบนสุดของแบบจำลอง OSI ทำหน้าที่ ให้บริการด้านการสื่อสาร

เครือข่ายแก่โปรแกรมประยุกต์ของผู้ใช้ และเป็นส่วนเชื่อมต่อระหว่างซอฟต์แวร์ประยุกต์กับบริการของระบบเครือข่าย โดย application layer ไม่ใช่ตัวโปรแกรมประยุกต์โดยตรง แต่เป็นชั้นที่กำหนดบริการและโปรโตคอลที่แอปพลิเคชันใช้ในการแลกเปลี่ยนข้อมูลผ่านเครือข่าย (Forouzan, 2013; Stallings, 2017) หน้าที่สำคัญของ application layer ได้แก่ การให้บริการแลกเปลี่ยนข้อมูลระหว่างแอปพลิเคชัน การร้องขอและตอบสนองข้อมูล การเข้าถึงทรัพยากรและบริการเครือข่าย และการสนับสนุนบริการจากระยะไกล โดยในบางโปรโตคอลระดับแอปพลิเคชันอาจมีกลไกสำหรับการพิสูจน์ตัวตนและการควบคุมการเข้าถึงร่วมด้วย การบริหารจัดการอุปกรณ์ผ่านเครือข่าย ตัวอย่างโปรโตคอลที่เกี่ยวข้อง ได้แก่ (1) Hypertext Transfer Protocol (HTTP) สำหรับการสื่อสารเว็บ (2) Hypertext Transfer Protocol Secure (HTTPS) สำหรับการสื่อสารเว็บแบบเข้ารหัส (3) Domain Name System (DNS) สำหรับแปลงชื่อโดเมนเป็น IP address (4) Dynamic Host Configuration Protocol (DHCP) สำหรับแจกจ่ายค่าการตั้งค่าเครือข่ายโดยอัตโนมัติ (5) File Transfer Protocol (FTP) สำหรับถ่ายโอนไฟล์ (6) SSH File Transfer Protocol (SFTP) สำหรับถ่ายโอนไฟล์ผ่านการเชื่อมต่อ secure shell (7) Simple Mail Transfer Protocol (SMTP) สำหรับส่งจดหมายอิเล็กทรอนิกส์ (8) Post Office Protocol Version 3 (POP3) และ Internet Message Access Protocol (IMAP) สำหรับรับจดหมายอิเล็กทรอนิกส์ (9) Simple Network Management Protocol (SNMP) สำหรับตรวจสอบและบริหารอุปกรณ์เครือข่าย (10) Secure Shell (SSH) สำหรับบริหารระบบจากระยะไกลอย่างปลอดภัย (11) Message Queuing Telemetry Transport (MQTT) สำหรับการสื่อสารของอุปกรณ์ IoT (12) Real-Time Streaming Protocol (RTSP) สำหรับการสตรีมวิดีโอ และ (13) Open Network Video Interface Forum (ONVIF) สำหรับกำหนดมาตรฐานการทำงานร่วมกันของอุปกรณ์วิดีโอเครือข่าย

ในระบบรักษาความปลอดภัยอัจฉริยะ Application Layer รองรับการทำงานของบริการต่าง ๆ เช่น การเข้าถึงระบบบริหารจัดการผ่านเว็บ การรับ-ส่งข้อมูลจากอุปกรณ์ IoT การสตรีมวิดีโอจากกล้อง IP

6.3.6 บทบาทของ Host, Switch และ Router ใน TCP/IP

อุปกรณ์แต่ละประเภทประมวลผลชั้นของ TCP/IP แตกต่างกันตามหน้าที่ ดังนี้

1) Host เช่น กล้อง IP, NVR, server ทำงานครบทั้ง 5 ชั้น เพราะต้องสร้างหรือรับข้อมูลใน application layer และส่งข้อมูลผ่านทุกชั้นจนถึง physical layer link-layer switch

2) สวิตช์ทำงานหลักใน physical layer และ data link layer โดยสวิตช์รับสัญญาณจากพอร์ตหนึ่ง อ่าน Ethernet frame และส่งเฟรมออกพอร์ตที่เหมาะตาม MAC address สวิตช์ layer 2 ทั่วไปไม่จำเป็นต้องประมวลผล IP, TCP หรือข้อมูลแอปพลิเคชัน

3) เราเตอร์ทำงานหลักใน physical layer, data link layer, network layer ซึ่งเราเตอร์อ่าน IP address เพื่อเลือกเส้นทาง เมื่อรับแพ็กเก็ตจากลิงก์หนึ่ง จะถอด frame ของลิงก์เดิม ตรวจสอบ IP datagram และสร้าง frame ใหม่สำหรับลิงก์ถัดไป เราเตอร์อาจจะมีอินเทอร์เฟซหลายตัว และแต่ละอินเทอร์เฟซอาจใช้โปรโตคอลใน physical และ data link layer ต่างกันได้

6.3.7 การสื่อสารแบบ End-to-End และ Hop-to-Hop

การสื่อสารใน TCP/IP แบ่งตามขอบเขตได้ 2 ลักษณะ ได้แก่

1) End-to-End Communication

เป็นการสื่อสารระหว่างอุปกรณ์ต้นทางกับปลายทาง โดยครอบคลุม application layer, transport layer, และ network layer ในเชิงตรรกะ ตัวอย่างคือ แอปพลิเคชันของกล้องส่งวิดีโอไปยัง VMS server โดย transport layer และ network layer ทำหน้าที่นำข้อมูลจาก host ต้นทางไปยัง host ปลายทาง

2) Hop-to-Hop Communication

เป็นการสื่อสารระหว่างอุปกรณ์ที่อยู่ติดกันในเส้นทาง เช่น กล้องกับสวิตช์ สวิตช์กับเราเตอร์ เราเตอร์กับสวิตช์ถัดไป โดย physical layer และ data link layer ทำงานแบบ hop-to-hop เพราะสัญญาณและเฟรมถูกส่งภายในลิงก์หนึ่งเท่านั้น เมื่อผ่านเราเตอร์จะสร้างเฟรมใหม่ตามเทคโนโลยีของลิงก์ถัดไป

6.3.8 หน่วยข้อมูลในแต่ละชั้นการสื่อสาร

เมื่อข้อมูลเคลื่อนลงตามชั้น ชื่อของหน่วยข้อมูลจะเปลี่ยนไปตามหน้าที่ของชั้นนั้น ๆ ตัวอย่างดังตารางที่ 6.1

ตารางที่ 6.1 หน่วยข้อมูลในแต่ละชั้นของการสื่อสาร

ชั้น	หน่วยข้อมูล
Application	Message หรือ Data
Transport	TCP Segment หรือ UDP User Datagram
Network	IP Datagram หรือ IP Packet
Data Link	Frame
Physical	Bits หรือ Signals

การใช้ชื่อที่ถูกต้องช่วยให้วิเคราะห์เครือข่ายได้แม่นยำ เช่น เมื่อกล่าวว่า “เฟรมเสียหาย” หมายถึงปัญหาในระดับ data link แต่เมื่อกล่าวว่า “TCP segment สูญหาย” หมายถึงปัญหาที่ transport layer ต้องจัดการ

6.3.9 การห่อหุ้มข้อมูลและการถอดห่อหุ้มข้อมูล (Encapsulation and Decapsulation)

1) การห่อหุ้มข้อมูล (Encapsulation)

กระบวนการเพิ่มข้อมูลควบคุมหรือ header ลงบนข้อมูลที่ได้รับจากชั้นบน ตัวอย่างการส่งภาพจากกล้อง IP ไปยัง NVR มีลำดับดังนี้

1.1) Application layer สร้างข้อมูลวิดีโอ

1.2) Transport layer เพิ่ม TCP หรือ UDP header

1.3) Network layer เพิ่ม IP header

1.4) Data link layer เพิ่ม Ethernet header และ trailer

1.5) Physical layer แปลงเฟรมเป็นbitและสัญญาณ

สามารถเขียนแนวคิด Application Data ได้ ดังนี้

- TCP/UDP header + data
- IP Header + TCP/UDP segment
- Ethernet header + IP packet + trailer
- Bits/signals

โดย header แต่ละชั้นบรรจุข้อมูลที่จำเป็น เช่น port number, IP address, MAC address, sequence number และข้อมูลตรวจสอบความผิดพลาด

2) การถอดห่อหุ้มข้อมูล (Decapsulation)

เมื่อข้อมูลถึงปลายทาง จะเกิดกระบวนการย้อนกลับ เรียกว่า decapsulation

2.1) Physical layer รับสัญญาณและแปลงเป็นbit

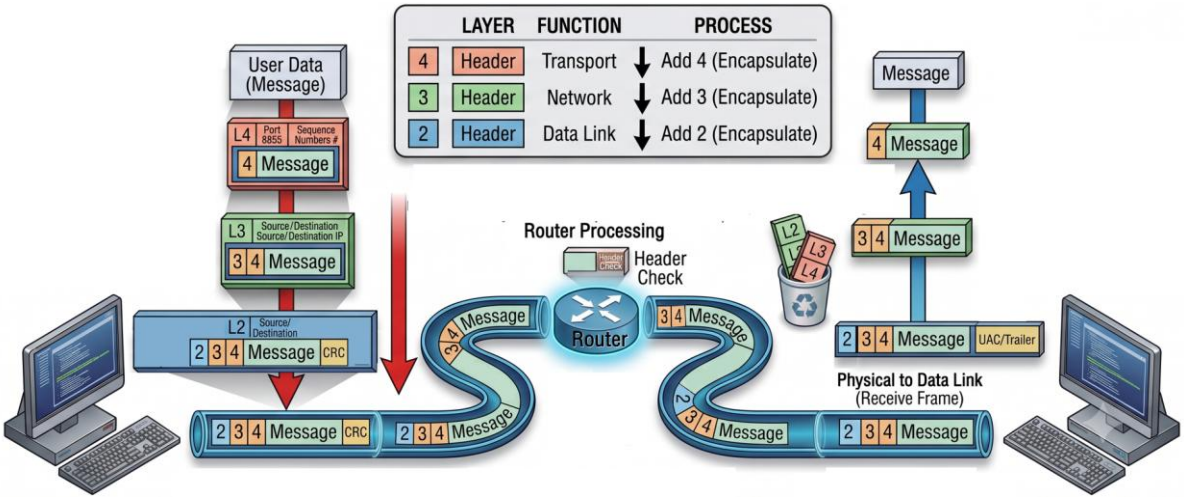
2.2) Data link layer ตรวจสอบและถอด Ethernet header/trailer

2.3) Network layer ตรวจสอบและถอด IP header

2.4) Transport layer ตรวจสอบ port number และถอด TCP/UDP header

2.5) Application layer รับข้อมูลต้นฉบับไปประมวลผล

เมื่อความผิดพลาดในชั้นใด กระบวนการจะหยุดลง เช่น frame check sequence ไม่ถูกต้อง data link layer อาจทิ้งเฟรม หรือหาก TCP segment ไม่ครบ TCP จะร้องขอให้ส่งใหม่



รูปที่ 6.5 การห่อหุ้มข้อมูลและการถอดห่อหุ้มข้อมูล

6.4 IP Address

6.4.1 Internet Protocol Address (IP Address)

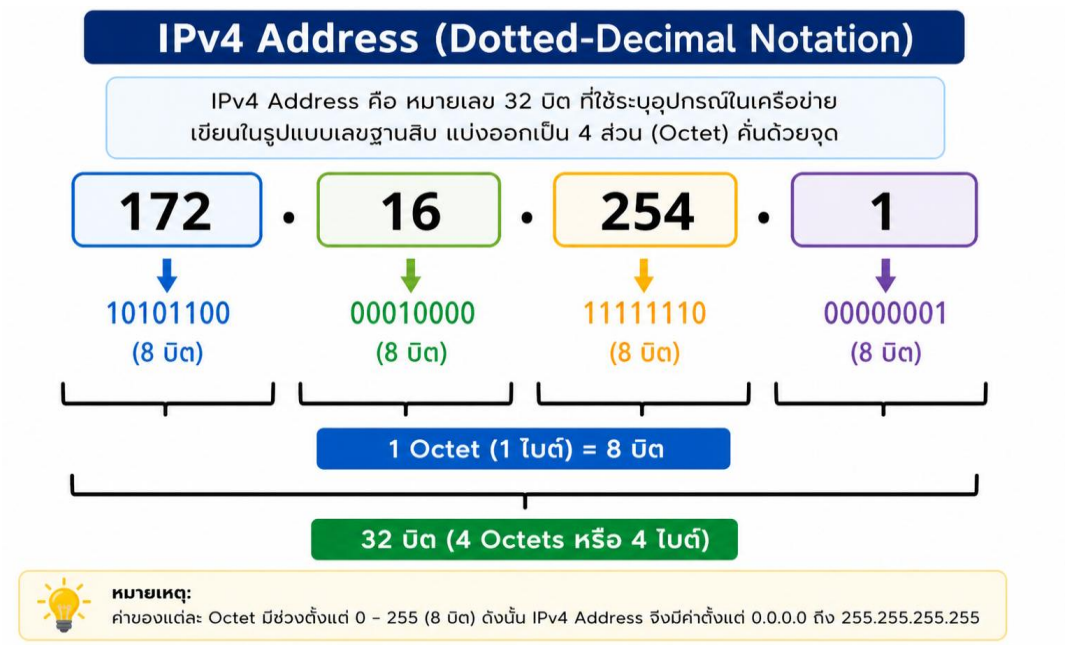
IP address คือ หมายเลขประจำตัวของอุปกรณ์ในเครือข่าย เช่น คอมพิวเตอร์ กล้องโทรทัศน์วงจรปิด หรืออุปกรณ์เครือข่ายอื่น ๆ ที่ใช้สำหรับระบุและแยกความแตกต่างของอุปกรณ์แต่ละตัวใน

การสื่อสารข้อมูล ทั้งในเครือข่ายภายใน (LAN) และเครือข่ายภายนอก (internet) โดยเปรียบเสมือน “เลขที่บ้าน” ที่ใช้ระบุตำแหน่งของอุปกรณ์ IP address เป็นที่อยู่เชิงตรรกะใน network layer ที่ใช้ระบุอินเทอร์เฟซของอุปกรณ์และเครือข่ายที่อุปกรณ์นั้นเชื่อมต่ออยู่

IP address แตกต่างจาก MAC address ซึ่งใช้ในระดับลิงก์ มีขอบเขตภายใน LAN โดยเราเตอร์จะพิจารณา IP address เพื่อส่งแพ็กเก็ตข้ามเครือข่าย และจะเปลี่ยน MAC address ของเฟรมเมื่อส่งต่อข้อมูลไปยังลิงก์ถัดไป (Forouzan, 2013) ซึ่ง IPv4 มีขนาด 32 bit แบ่งเป็น 4 ออกเทต (octet) ออคเตตละ 8 bit แสดงในรูปแบบตัวเลขฐานสิบคั่นด้วยจุด โดย IP address ประกอบด้วย 2 ส่วนสำคัญ ได้แก่ network ID ใช้ระบุเครือข่าย และ host ID ใช้ระบุอุปกรณ์ภายในเครือข่าย เช่น 192.168.10.25 ส่วน IPv6 มีขนาด 128 bit ใช้เลขฐานสิบหก เช่น 2001:db8:10::25

6.4.2 การกำหนด IP Address

กำหนด IP address จะต้องไม่ซ้ำกันภายในเครือข่ายเดียวกัน เนื่องจากจะทำให้เกิดปัญหาในการสื่อสารข้อมูล (IP conflict) โดยการทำงานภายใน IP address ยังมีการแบ่งออกเป็นระดับชั้น (class) ต่าง ๆ 5 class คือ A, B, C, D, และ E ซึ่งในแต่ละ class จะมีหมายเลข IP จะมีทั้งหมด 32 bit แบ่งออกเป็น 4 ฟิลด์ โดยแต่ละฟิลด์จะมี 8 bit ซึ่งการแบ่งเป็น 4 ฟิลด์นั้นความจริงเป็นการกำหนดหมายเลขของเครื่องเครือข่ายและหมายเลขของเครื่องคอมพิวเตอร์ การแบ่งประเภท IP address ดังรูปที่ 6.6 และตารางที่ 6.2



รูปที่ 6.6 โครงสร้าง IP address

ตารางที่ 6.2 รายละเอียดของแต่ละชั้นของหมายเลขของ IP

ระดับชั้น (Class)	หมายเลขของ IP Address	การทำงาน
Class A	เริ่มตั้งแต่ 1.0.0.0 ถึง 127.255.255.255	ใช้กับเครือข่ายขนาดใหญ่มาก ซึ่งเหมาะสมสำหรับเครือข่ายที่มีขนาดใหญ่ เนื่องจากสามารถรองรับจะมีเครือข่ายได้ 126 เน็ตเวิร์ค และในแต่ละเครือข่ายสามารถมีเครื่องคอมพิวเตอร์ได้ประมาณ 16 ล้านเครื่อง
Class B	เริ่มตั้งแต่ 128.0.0.0 ถึง 191.255.255.255	ใช้กับเครือข่ายขนาดกลาง จะมีเครือข่ายขนาด 16384 เน็ตเวิร์ค และจำนวนเครื่องลูกข่ายในเครือข่ายได้ 64,516 เครื่อง
Class C	เริ่มตั้งแต่ 192.0.0.0 ถึง 223.255.255.255	ใช้กับเครือข่ายขนาดเล็ก จะมีจำนวนเครือข่ายขนาด 2M+ เน็ตเวิร์ค และเครื่องลูกข่ายในแต่ละเครือข่ายได้ประมาณ 254 เครื่อง
Class D	เป็นการสำรองหมายเลข IP Address ช่วง 224.0.0.0 ถึง 239.255.255.255	ใช้สำหรับ Multicast โดย 255 สำหรับการส่งข้อมูลแบบ Multicast ซึ่งจะไม่มีการแจกจ่ายใช้งานทั่วไปสำหรับบุคคลทั่วไป
Class E	เป็นการสำรองหมายเลข IP Address ช่วง 240.0.0.05 ถึง 255.255.255.255	สำหรับการทดสอบ และพัฒนา

อย่างไรก็ตาม ปัจจุบันระบบเครือข่ายนิยมใช้การแบ่งแบบ CIDR (Classless Inter-Domain Routing) แทนการแบ่งแบบ class เนื่องจากมีความยืดหยุ่นและใช้ทรัพยากร IP ได้มีประสิทธิภาพมากกว่า

6.4.3 ส่วนประกอบของ IPv4 Address

IPv4 address ประกอบด้วย 2 ส่วน ได้แก่ network prefix ใช้ระบุเครือข่ายหรือซับเน็ต และ host identifier ใช้ระบุอุปกรณ์ภายในซับเน็ตนั้น

Subnet Mask ใช้กำหนดว่าbitใดเป็นส่วน network และbitใดเป็นส่วน host ตัวอย่างเช่น

192.168.10.25/24 โดยเครื่องหมาย /24 หมายถึง 24 bitแรกเป็น network prefix ซึ่งเทียบเท่ากับ Subnet Mask คือ 255.255.255.0 ดังนั้น

- Network address คือ 192.168.10.0
- ช่วง host โดยทั่วไปคือ 192.168.10.1-192.168.10.254
- Broadcast address คือ 192.168.10.255

การแบ่ง subnet (subnetting) คือการแบ่งเครือข่ายขนาดใหญ่ออกเป็นเครือข่ายย่อย โดยยืม bitจากส่วน host มาใช้เป็นส่วน subnet การแบ่งดังกล่าวช่วยลดขนาด broadcast domain จัดสรร IP address ได้เหมาะสม และแยกระบบตามหน้าที่หรือระดับความปลอดภัย (Forouzan, 2013) จำนวนที่อยู่ทั้งหมดในซับเน็ต IPv4 คำนวณได้จากสมการที่ 6.2

$$\text{จำนวนที่อยู่ทั้งหมดในซับเน็ต} = 2^{(32-\rho)} \qquad (6.2)$$

เมื่อ ρ คือความยาวของ prefix

ตัวอย่าง /26

$$\text{จำนวนที่อยู่ทั้งหมดในซับเน็ต} = 2^{(32-26)}$$
$$= 64$$

จึงมีทั้งหมด 64 ที่อยู่ และโดยทั่วไปใช้งานกับ host ได้ 62 ที่อยู่ เนื่องจากสงวน network address และ broadcast address ตัวอย่างเครือข่าย 192.168.10.0/24 สามารถแบ่งเป็น 4 ซับเน็ตแบบ /26 ได้แก่

ตารางที่ 6.3 ตัวอย่างการแบ่งซับเน็ตแบบ /26 ของ เครือข่าย 192.168.10.0/24

ซับเน็ต	Network Address	ช่วงอุปกรณ์	Broadcast
1	192.168.10.0/26	192.168.10.1-62	192.168.10.63
2	192.168.10.64/26	192.168.10.65-126	192.168.10.127
3	192.168.10.128/26	192.168.10.129-190	192.168.10.191
4	192.168.10.192/26	192.168.10.193-254	192.168.10.255

การเขียน IPv4 address ในรูปแบบเลขฐานสิบคั่นด้วยจุด และการแปลงเป็นเลขฐานสอง โดยหลักการของ IPv4 address คือ IPv4 มีความยาวทั้งหมด 32 bit แบ่งออกเป็น 4 ส่วน เรียกว่า octet โดยแต่ละ octet มีขนาด 8 bit หรือ 1 ไบต์ ตัวอย่างเช่น

➲ **172.16.254.1** แบ่งเป็น 4 octet ดังตารางที่ 6.4

ตารางที่ 6.4 การแบ่งเลข IP 172.16.254.1 เป็น 4 octet

Octet	เลขฐานสิบ	เลขฐานสอง
1	172	10101100
2	16	00010000
3	254	11111110
4	1	00000001

วิธีคำนวณเลขฐานสิบเป็นเลขฐานสอง

เลขฐานสอง 8 bit มีค่าน้ำหนักประจำตำแหน่งดังนี้

bitที่	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
ค่าน้ำหนัก	128	64	32	16	8	4	2	1

ถ้าตำแหน่งใดใช้ ให้ใส่ **1** ถ้าตำแหน่งใดไม่ใช้ ให้ใส่ **0**

1) แปลง 172

172 = 128 + 32 + 8 + 4

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

ดังนั้น **172 = 10101100**

2) แปลง 16

16 = 16

128	64	32	16	8	4	2	1
0	0	0	1	0	0	0	0

ดังนั้น **16 = 00010000**

3) แปลง 254

254 = 128 + 64 + 32 + 16 + 8 + 4 + 2

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	0

ดังนั้น **254 = 11111110**

4) แปลง 1

1 = 1

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	1

ดังนั้น **1 = 00000001**

สรุปดังนั้นการแปลง IPv4 Address **172.16.254.1**

เมื่อเขียนเป็นเลขฐานสองจะได้เป็น

10101100. 00010000. 11111110. 00000001

ข้อควรจำ แต่ละ octet มี 8 bit จึงมีค่าตั้งแต่	**00000000 ถึง 11111111**
หรือเท่ากับเลขฐานสิบ	**0 ถึง 255**
ดังนั้น IPv4 address จึงมีช่วงค่าตั้งแต่	**0.0.0.0 ถึง 255.255.255.255**

การพิจารณาว่าอยู่ในเครือข่ายเดียวกันหรือไม่ การตรวจสอบว่าอุปกรณ์อยู่ในเครือข่ายเดียวกันหรือไม่นั้น จะพิจารณาจาก network ID โดยใช้ค่า Subnet Mask มาช่วยในการแยกส่วนของ network และ host หาก network ID ตรงกัน แสดงว่าอยู่ในเครือข่ายเดียวกัน เช่น

- **IP: 192.168.1.10**
- **IP: 192.168.1.20**

  (Subnet Mask: 255.255.255.0)

ในการออกแบบระบบความปลอดภัยอัจฉริยะอาจกำหนดซับเน็ต เช่น

- 192.168.10.0/24 สำหรับกล้อง IP
- 192.168.20.0/24 สำหรับ access control
- 192.168.30.0/24 สำหรับระบบแจ้งเตือน
- 192.168.40.0/24 สำหรับ server และระบบบริหารจัดการ

การแยกดังกล่าวควรทำร่วมกับ VLAN และนโยบาย firewall หรือ access control list เพราะการแบ่ง subnet เพียงอย่างเดียวไม่ได้ป้องกันการเข้าถึงระหว่างเครือข่ายโดยอัตโนมัติ

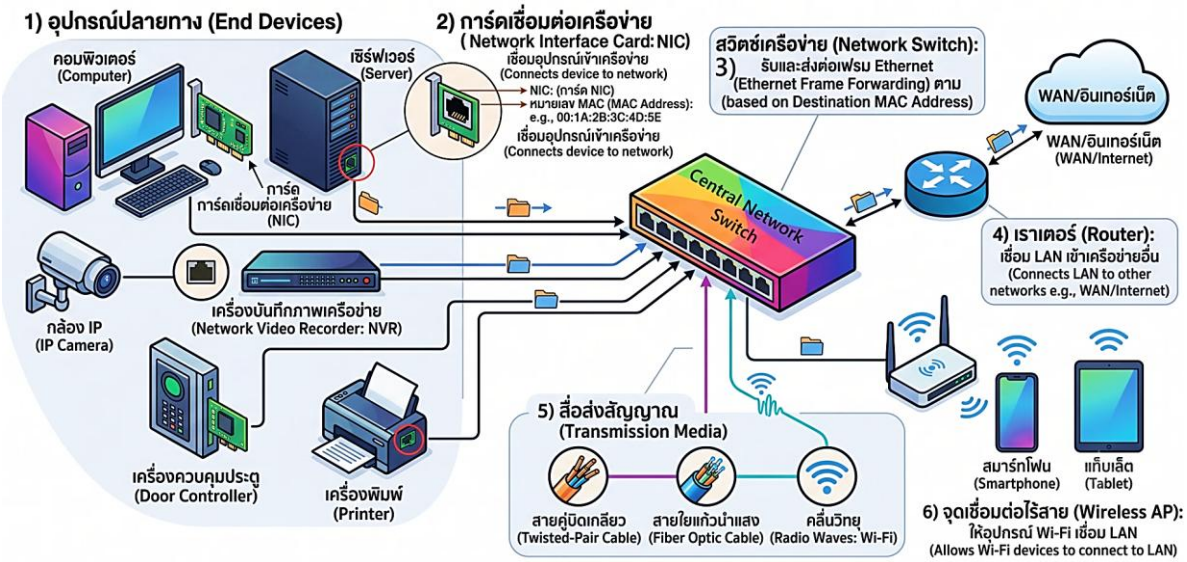
6.5 เครือข่ายท้องถิ่น (Local Area Network: LAN)

เครือข่ายท้องถิ่น คือ เครือข่ายคอมพิวเตอร์ที่เชื่อมต่ออุปกรณ์ภายในพื้นที่ทางภูมิศาสตร์จำกัด เช่น บ้าน สำนักงาน โรงงาน หรือบริเวณมหาวิทยาลัย โดยทั่วไปเครือข่ายชนิดนี้อยู่ภายใต้การบริหารจัดการของบุคคลหรือองค์กรเดียว และใช้สำหรับแลกเปลี่ยนข้อมูล ใช้ทรัพยากรร่วมกัน และเชื่อมต่ออุปกรณ์เข้าสู่ระบบสารสนเทศส่วนกลาง เครือข่าย LAN อาจมีขนาดเล็กเพียงคอมพิวเตอร์สองเครื่องกับเครื่องพิมพ์ หรืออาจประกอบด้วยอุปกรณ์จำนวนมากที่กระจายอยู่หลายชั้นหรือหลายอาคารภายในพื้นที่เดียวกัน (Forouzan, 2013) ในอดีต อุปกรณ์ใน LAN อาจเชื่อมต่อผ่านสื่อกลางร่วม เช่น สายสัญญาณหลักแบบบัส ทำให้ข้อมูลที่ส่งออกจากอุปกรณ์หนึ่งถูกส่งไปถึงอุปกรณ์ทุกตัวบนสื่อกลางเดียวกัน ปัจจุบันใช้สวิตช์เครือข่าย (network switch) เป็นอุปกรณ์ศูนย์กลาง สวิตช์จะตรวจสอบหมายเลขปลายทางในเฟรมและส่งข้อมูลออกเฉพาะพอร์ตที่เชื่อมต่อกับอุปกรณ์ปลายทาง จึงช่วยลดปริมาณข้อมูลที่ไม่เกี่ยวข้องและทำให้อุปกรณ์หลายคู่สามารถสื่อสารพร้อมกันได้ (Forouzan, 2013)

6.5.1 องค์ประกอบของเครือข่าย LAN (Components of a Local Area Network)

เครือข่าย LAN ประกอบด้วยอุปกรณ์และสื่อกลางหลายประเภทที่ทำงานร่วมกันเพื่อให้เกิดการสื่อสารข้อมูลระหว่างอุปกรณ์ภายในเครือข่ายอย่างมีประสิทธิภาพ อุปกรณ์แต่ละชนิดมีหน้าที่เฉพาะ

ในการรับ ส่ง และประมวลผลข้อมูล ตั้งแต่การสร้างข้อมูลที่อุปกรณ์ปลายทาง การส่งข้อมูลผ่านสื่อกลาง การสลับเส้นทางของเฟรมข้อมูล ไปจนถึงการเชื่อมต่อกับเครือข่ายภายนอก เช่น เครือข่ายบริเวณกว้าง (Wide Area Network: WAN) หรืออินเทอร์เน็ต ในระบบรักษาความปลอดภัยอัจฉริยะ องค์ประกอบสำคัญของ LAN ดังรูปที่ 6.7



รูปที่ 6.7 องค์ประกอบของเครือข่าย LAN

1) อุปกรณ์ปลายทาง (End Devices)

อุปกรณ์ปลายทาง คือ อุปกรณ์ที่เป็นต้นทางหรือปลายทางของการรับส่งข้อมูลในเครือข่าย ทำหน้าที่สร้าง รับ ประมวลผล หรือจัดเก็บข้อมูล และเป็นอุปกรณ์ที่ผู้ใช้งานหรือระบบประยุกต์สามารถติดต่อสื่อสารได้โดยตรง อุปกรณ์ปลายทางทุกชนิดจะต้องมีอินเทอร์เฟซเครือข่ายเพื่อเชื่อมต่อเข้าสู่ระบบ LAN และมีหมายเลขประจำอุปกรณ์ในระดับ data link layer หรือ MAC address สำหรับระบุตัวตนภายในเครือข่าย ในระบบรักษาความปลอดภัยอัจฉริยะ อุปกรณ์ปลายทางที่พบได้บ่อย ได้แก่ คอมพิวเตอร์ เซิร์ฟเวอร์ กล้อง IP เครื่องบันทึกวิดีโอผ่านเครือข่าย ระบบบริหารจัดการวิดีโอ เครื่องควบคุมการเข้าออก เครื่องอ่านบัตรและอุปกรณ์ชีวมิติ เกตเวย์สำหรับอุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง หรือเครื่องพิมพ์ อุปกรณ์เหล่านี้สามารถรับส่งข้อมูลผ่านโปรโตคอลมาตรฐาน เช่น Ethernet, IP, TCP, และ UDP โดยข้อมูลจะถูกส่งผ่านสวิตช์เครือข่ายไปยังอุปกรณ์ปลายทางหรือเซิร์ฟเวอร์

2) การ์ดเชื่อมต่อเครือข่าย (Network Interface Card: NIC)

การ์ดเชื่อมต่อเครือข่าย เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่ออุปกรณ์ปลายทางเข้ากับเครือข่าย LAN โดยทำหน้าที่เป็นส่วนเชื่อมต่อระหว่างระบบคอมพิวเตอร์กับสื่อกลางในการสื่อสารข้อมูล NIC ทำงานในชั้น physical layer และ data link layer ของแบบจำลอง OSI และรับผิดชอบการสร้างและรับ Ethernet frame รวมทั้งการแปลงข้อมูลระหว่างรูปแบบดิจิทัลภายในเครื่องกับสัญญาณที่ใช้บนสื่อส่งสัญญาณ โดย NIC ทุกตัวจะมีหมายเลข MAC address (หมายเลขประจำ

อินเทอร์เฟซเครือข่าย) ขนาด 48 bit ใช้สำหรับระบุอุปกรณ์ภายในเครือข่าย Ethernet ใช้ในการส่งต่อ Ethernet frame ภายใน LAN โดยหมายเลข MAC address จะถูกกำหนดโดยผู้ผลิตอุปกรณ์ตามมาตรฐานของ IEEE ปัจจุบัน NIC อาจติดตั้งบนเมนบอร์ดหรือเป็นการ์ดเสริม และรองรับความเร็วหลายระดับ เช่น 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, 10 Gbps และรองรับการเชื่อมต่อผ่านสายใยแก้วนำแสงในระบบเครือข่ายความเร็วสูง

3) สวิตช์เครือข่าย (Network Switch)

สวิตช์เครือข่าย เป็นอุปกรณ์ศูนย์กลางของเครือข่าย LAN ทำหน้าที่รับ วิเคราะห์ และส่งต่อ Ethernet frame ไปยังพอร์ตที่เชื่อมต่อกับอุปกรณ์ปลายทาง โดยพิจารณาจาก destination MAC address และข้อมูลที่จัดเก็บอยู่ใน MAC address table ทำให้สามารถส่งข้อมูลเฉพาะไปยังอุปกรณ์ปลายทางที่ต้องการ ลดปริมาณการกระจายข้อมูลภายในเครือข่าย และเพิ่มประสิทธิภาพในการสื่อสาร สวิตช์สมัยใหม่รองรับการสื่อสารแบบ full-duplex ทำให้สามารถรับและส่งข้อมูลพร้อมกันโดยไม่เกิดการชนกันของข้อมูล (collision) นอกจากนี้ยังรองรับเทคโนโลยีต่าง ๆ เช่น VLAN, link aggregation, QoS, PoE, port security, และ STP

ในระบบรักษาความปลอดภัยอัจฉริยะ สวิตช์มักรองรับมาตรฐาน IEEE 802.3af, IEEE 802.3at หรือ IEEE 802.3bt สำหรับจ่ายพลังงานไฟฟ้าให้กับกล้อง IP จุดเชื่อมต่อไร้สาย และอุปกรณ์ควบคุมการเข้าออกผ่านสาย Ethernet เพียงเส้นเดียว

4) เราเตอร์ (Router)

เราเตอร์ เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่อเครือข่าย IP ที่แตกต่างกัน เช่น การเชื่อม LAN กับ WAN หรืออินเทอร์เน็ต และทำหน้าที่กำหนดเส้นทางของแพ็กเก็ตข้อมูลจากเครือข่ายต้นทางไปยังปลายทาง โดยพิจารณาจาก destination IP address และข้อมูลในตารางเส้นทาง (routing table) เราเตอร์ทำงานในชั้น network layer (layer 3) ในแบบจำลอง OSI และทำหน้าที่เป็น default gateway ของอุปกรณ์ภายใน LAN เพื่อส่งข้อมูลออกไปยังเครือข่ายภายนอก นอกจากนี้เราเตอร์ยังสามารถรองรับการทำงานด้านเครือข่ายและความมั่นคงปลอดภัย เช่น Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), Virtual Private Network (VPN), Dynamic Routing Protocols (DRP), และ Access Control List (ACL)

ในระบบรักษาความปลอดภัยอัจฉริยะ เราเตอร์มีบทบาทสำคัญในการเชื่อมต่อศูนย์ควบคุมกับอาคารหรือสาขาต่าง ๆ รวมถึงการเข้าถึงระบบจากระยะไกลผ่านเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย

5) สื่อส่งสัญญาณ (Transmission Media)

สื่อส่งสัญญาณ คือสื่อกลางที่ใช้ในการส่งข้อมูลระหว่างอุปกรณ์เครือข่าย โดยแบ่งออกเป็น 2 ประเภท ได้แก่ สื่อนำสัญญาณแบบมีตัวนำ (guided media) และ สื่อนำสัญญาณแบบไม่มีตัวนำ (unguided media) สื่อนำสัญญาณแบบมีตัวนำ ประกอบด้วย สายคู่บิดเกลียว เช่น Cat5e, Cat6 และ Cat6A ซึ่งนิยมใช้ในระบบ Ethernet และสายใยแก้วนำแสงซึ่งรองรับการส่งข้อมูลด้วยความเร็วสูงในระยะทางไกล และมีความทนทานต่อสัญญาณรบกวนทางแม่เหล็กไฟฟ้า ส่วนสื่อนำสัญญาณแบบไม่มีตัวนำ ได้แก่ คลื่นวิทยุ (radio waves) ซึ่งใช้ในการสื่อสารแบบไร้สาย เช่น Wi-Fi คลื่นไมโครเวฟ (microwave) หรือ คลื่นอินฟราเรด (infrared) ในบางระบบเฉพาะ

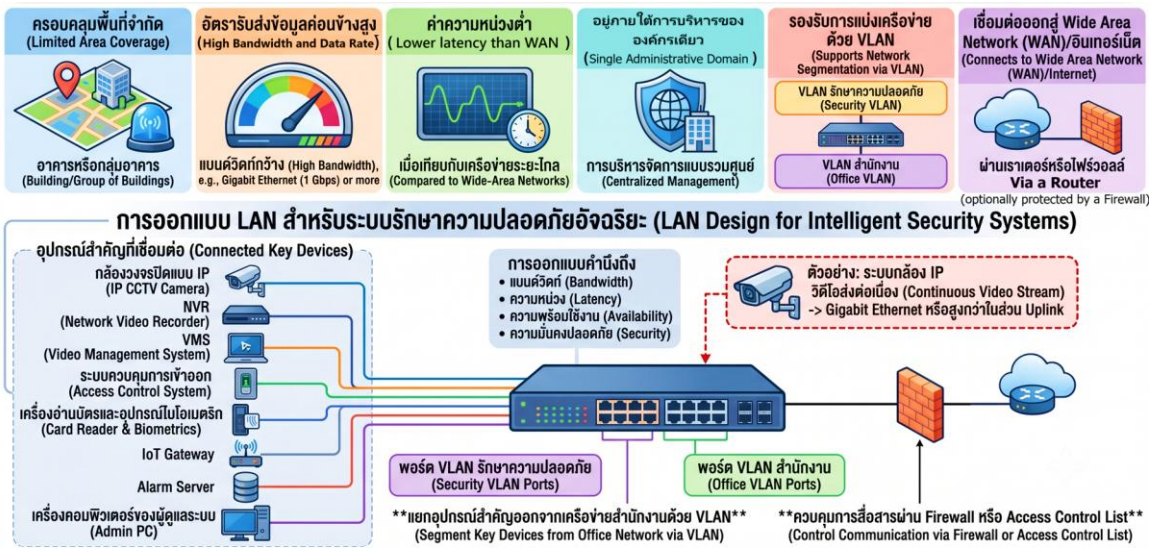
6) จุดเชื่อมต่อไร้สาย (Wireless Access Point: AP)

จุดเชื่อมต่อไร้สาย เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่ออุปกรณ์เครือข่ายไร้สาย (Wireless Local Area Network: WLAN) เข้ากับเครือข่าย LAN แบบใช้สาย โดยทำหน้าที่เป็นสะพานเชื่อม (bridge) ระหว่างเครือข่ายไร้สายกับเครือข่าย Ethernet ทำให้อุปกรณ์ที่รองรับ Wi-Fi เช่น สมาร์ตโฟน แท็บเล็ต คอมพิวเตอร์พกพา และอุปกรณ์ IoT สามารถเข้าถึงทรัพยากรในเครือข่าย ซึ่ง AP ส่วนใหญ่รองรับมาตรฐาน IEEE 802.11 เช่น IEEE 802.11ac (Wi-Fi 5), IEEE 802.11ax (Wi-Fi 6) และ IEEE 802.11be (Wi-Fi 7) พร้อมรองรับเทคโนโลยี Multiple Input Multiple Output (MIMO), Orthogonal Frequency Division Multiple Access (OFDMA) และ beamforming เพื่อเพิ่มประสิทธิภาพของการสื่อสารไร้สาย

ในระบบระบบรักษาความปลอดภัย AP มักใช้สำหรับเชื่อมต่ออุปกรณ์เคลื่อนที่ของเจ้าหน้าที่รักษาความปลอดภัย กล้องวงจรปิดแบบไร้สาย เซนเซอร์ IoT และอุปกรณ์ตรวจสอบภาคสนาม โดยควรกำหนดมาตรการรักษาความปลอดภัย เช่น การใช้ Wi-Fi Protected Access 3 (WPA3) การแยกเครือข่ายด้วย VLAN และการพิสูจน์ตัวตนผ่าน IEEE 802.1X เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

6.5.2 คุณลักษณะของ LAN ในระบบรักษาความปลอดภัย

คุณลักษณะสำคัญของ LAN ได้แก่ ครอบคลุมพื้นที่จำกัด มีอัตรารับส่งข้อมูลค่อนข้างสูง มีค่าความหน่วงต่ำเมื่อเทียบกับเครือข่ายระยะไกล อยู่ภายใต้การควบคุมขององค์กรเดียว รองรับการแบ่งเครือข่ายด้วย VLAN สามารถบริหารจัดการและตรวจสอบอุปกรณ์จากส่วนกลาง และเชื่อมต่อออกสู่ WAN หรืออินเทอร์เน็ตผ่านเราเตอร์หรือไฟร์วอลล์ (firewall) ในระบบรักษาความปลอดภัยอัจฉริยะ โดยมีเครือข่าย LAN เป็นโครงสร้างพื้นฐานที่เชื่อมต่ออุปกรณ์ เช่น กล้องวงจรปิดแบบ IP, NVR, VMS, ระบบควบคุมการเข้าออก, เครื่องอ่านบัตรและอุปกรณ์ไบโอเมตริก, IoT gateway, alarm server, เครื่องคอมพิวเตอร์ของผู้ดูแลระบบ ดังรูปที่ 6.8



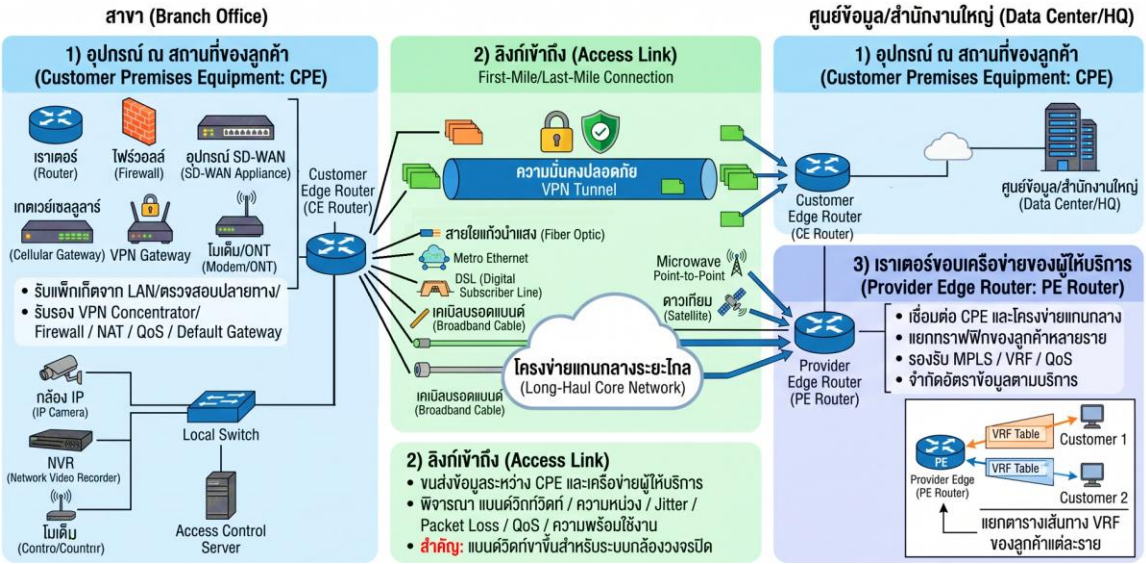
รูปที่ 6.8 คุณลักษณะของ LAN ในระบบรักษาความปลอดภัยอัจฉริยะ

6.6 เครือข่ายบริเวณกว้าง (Wide Area Network: WAN)

เครือข่ายบริเวณกว้าง เป็นเครือข่ายที่ครอบคลุมพื้นที่ทางภูมิศาสตร์กว้างกว่า LAN เช่น ระหว่างอาคารที่อยู่ห่างกัน ระหว่างจังหวัด ระหว่างประเทศ หรือทั่วโลก WAN ทำหน้าที่เชื่อมต่อ LAN หลายเครือข่ายเข้าด้วยกัน โดยข้อมูลมักเดินทางผ่านเราเตอร์ ระบบสื่อสารของผู้ให้บริการ และโครงข่ายแกนกลางที่อาจใช้สายใยแก้วนำแสง ไมโครเวฟ ดาวเทียม หรือเครือข่ายเซลลูลาร์ (Forouzan, 2013) เครือข่าย WAN แตกต่างจาก LAN ตรงที่โครงสร้างพื้นฐานบางส่วนมักไม่ได้เป็นกรรมสิทธิ์ขององค์กรผู้ใช้งานทั้งหมด แต่เช่าใช้บริการจากผู้ให้บริการโทรคมนาคมหรือผู้ให้บริการอินเทอร์เน็ต องค์กรจึงต้องพิจารณาคุณภาพบริการ ความพร้อมใช้งาน ค่าใช้จ่าย และระดับความมั่นคงปลอดภัยของลิงก์ WAN

6.6.1 องค์ประกอบของเครือข่าย WAN

เครือข่าย WAN เป็นระบบสื่อสารที่ใช้เชื่อมต่อเครือข่ายท้องถิ่นหรือระบบเครือข่ายขององค์กรที่อยู่ห่างกันทางภูมิศาสตร์ เช่น การเชื่อมสำนักงานใหญ่กับสำนักงานสาขา ศูนย์ข้อมูล โรงงานหรือระบบคลาวด์ โดยการเชื่อมต่อมักอาศัยโครงสร้างพื้นฐานของผู้ให้บริการโทรคมนาคมหรือผู้ให้บริการอินเทอร์เน็ต ไม่ได้อยู่ภายใต้การควบคุมขององค์กรผู้ใช้ทั้งหมดเช่นเดียวกับ LAN องค์ประกอบของ WAN ทำงานร่วมกันตั้งแต่บริเวณสถานที่ของลูกค้า ลิงก์ที่เชื่อมต่อไปยังผู้ให้บริการ อุปกรณ์ขอบเครือข่ายของผู้ให้บริการ ไปจนถึงโครงข่ายแกนกลางที่ลำเลียงข้อมูลระยะไกล การทำความเข้าใจองค์ประกอบแต่ละส่วนช่วยให้สามารถออกแบบ WAN ให้มีแบนด์วิดท์ ความหน่วง ความพร้อมใช้งาน และระดับความมั่นคงปลอดภัยเหมาะสมกับลักษณะงาน โดยเฉพาะระบบรักษาความปลอดภัยอัจฉริยะที่อาจต้องส่งข้อมูลวิดีโอและเหตุการณ์ระหว่างสถานที่อย่างต่อเนื่อง



รูปที่ 6.9 องค์ประกอบและการทำงานของเครือข่าย WAN สำหรับระบบรักษาความปลอดภัย

1) อุปกรณ์ในสถานที่ของลูกค้า (Customer Premises Equipment: CPE)

อุปกรณ์ CPE หมายถึง อุปกรณ์สื่อสารที่ติดตั้งอยู่ภายในสถานที่ขององค์กรหรือผู้ใช้ และทำหน้าที่เป็นจุดเชื่อมต่อระหว่างเครือข่ายภายในของลูกค้ากับระบบของผู้ให้บริการ อุปกรณ์ CPE อาจเป็นกรรมสิทธิ์ของลูกค้า ผู้ให้บริการ หรืออยู่ภายใต้สัญญาเช่า การบริหารจัดการร่วมกัน ตัวอย่าง CPE เช่น เราเตอร์ (router) ไฟร์วอลล์ (firewall) อุปกรณ์โมเด็มหรือ Optical Network Terminal (ONT) อุปกรณ์ Software-Defined Wide Area Network (SD-WAN) อุปกรณ์ Customer Edge Router (CE router) เกตเวย์สำหรับเครือข่ายเซลลูลาร์ หรือ อุปกรณ์เข้ารหัสหรือ VPN gateway โดยหน้าที่หลักของ CPE คือรับแพ็กเก็ตจาก LAN ภายในองค์กร ตรวจสอบปลายทาง และส่งแพ็กเก็ตออกสู่ WAN ผ่าน access link นอกจากนี้ CPE อาจทำหน้าที่เป็น default gateway, Network Address Translation (NAT), VPN concentrator, firewall และระบบจัดลำดับความสำคัญของข้อมูลด้วย QoS

ในระบบรักษาความปลอดภัยอัจฉริยะ CPE อาจรองรับการเชื่อมต่อระหว่างสาขากับศูนย์ควบคุม เช่น เราเตอร์ที่สาขารับข้อมูลจากกล้อง IP, NVR และ access control server แล้วส่งเฉพาะทราฟฟิกที่ได้รับอนุญาตผ่าน VPN ไปยังศูนย์กลาง หากใช้อุปกรณ์ SD-WAN อุปกรณ์สามารถเลือกใช้ลิงก์หลายชนิด เช่น fiber, broadband และ 4G/5G ตามคุณภาพและนโยบายที่กำหนด อย่างไรก็ตาม firewall ไม่จำเป็นต้องเป็นอุปกรณ์ที่เชื่อม WAN โดยตรงในทุกระบบ บางโครงสร้างใช้ router ต่อกับ WAN แล้ววาง firewall ระหว่าง router กับ LAN ขณะที่ firewall บางรุ่นสามารถทำหน้าที่เป็นทั้ง gateway, router และ firewall ในตัวเดียวกัน

2) ลิงก์เข้าถึง (Access Link)

เป็นลิงก์สื่อสารที่เชื่อมต่ออุปกรณ์ของลูกค้า เช่น CPE หรือเราเตอร์ขององค์กร เข้ากับเครือข่ายของผู้ให้บริการ WAN โดยส่วนนี้มักเรียกว่า last-mile connection เนื่องจากเป็นช่วงเชื่อมต่อระหว่างสถานที่ของผู้ใช้กับโครงข่ายของผู้ให้บริการ access link สามารถใช้เทคโนโลยีได้หลายรูปแบบ เช่น fiber optic, Metro Ethernet, DSL, cable broadband, leased line, microwave point-to-point, เครือข่าย 4G/5G และดาวเทียม การเลือกใช้งานควรพิจารณาปัจจัยสำคัญ เช่น แบนด์วิดท์ (bandwidth) ความหน่วง (latency) ความแปรผันของความหน่วง (jitter) การสูญหายของแพ็กเก็ต (packet loss) ความพร้อมใช้งาน (availability) การรองรับ QoS และลิงก์สำรอง

สำหรับระบบรักษาความปลอดภัยอัจฉริยะ โดยเฉพาะระบบกล้อง IP ที่ส่งวิดีโอจากสาขาไปยังศูนย์กลางหรือระบบ cloud ควรให้ความสำคัญกับ แบนด์วิดท์ขาขึ้น (upload bandwidth) เนื่องจากข้อมูลวิดีโอจำนวนมากถูกส่งออกจากสถานที่ติดตั้งกล้อง หาก access link มีความเร็วขาขึ้นไม่เพียงพอ อาจทำให้ภาพเกิดความล่าช้า สะดุด หรือคุณภาพลดลงได้ เราเตอร์ขอบเครือข่ายของผู้ให้บริการ (Provider Edge Router: PE Router)

6.6.2 โครงข่ายแกนกลางของ WAN (WAN Backbone หรือ Provider Core)

WAN backbone คือ โครงข่ายหลักความเร็วสูงของผู้ให้บริการเครือข่าย ทำหน้าที่รับ-ส่งข้อมูลระหว่างพื้นที่หรือเครือข่ายที่อยู่ห่างไกล และเชื่อมต่ออุปกรณ์ขอบเครือข่ายของผู้ให้บริการ เช่น Provider Edge (PE) router เข้าด้วยกัน โครงข่ายส่วนนี้ประกอบด้วยเราเตอร์ ประสิทธิภาพสูง

ระบบสวิตชิ่ง และลิงก์สื่อสารความจุสูง โดยเฉพาะใยแก้วนำแสง โครงข่ายแกนกลางมักออกแบบให้มีเส้นทางและอุปกรณ์สำรอง (redundancy) เพื่อให้สามารถเปลี่ยนเส้นทางเมื่อเกิดความขัดข้อง และรองรับปริมาณการใช้งานในระบบสื่อสาร (traffic) จำนวนมากด้วยความเร็วและความพร้อมใช้งานสูง เครือข่าย WAN สำหรับการสื่อสารข้อมูลในปัจจุบันใช้หลักการ packet switching เป็นสำคัญ โดยส่งต่อแพ็กเก็ตผ่านอุปกรณ์เครือข่ายไปยังปลายทางตามเส้นทางที่กำหนด (Forouzan, 2013)

สำหรับระบบรักษาความปลอดภัยอัจฉริยะ WAN backbone อาจต้องรองรับข้อมูลหลายประเภท เช่น วิดีโอจากกล้อง IP เสียงจากระบบ intercom ข้อมูล access control และข้อมูลแจ้งเตือน ซึ่งมีความต้องการแตกต่างกัน โดยวิดีโอต้องการแบนด์วิดท์สูง ขณะที่ข้อมูลควบคุมและการแจ้งเตือนควรได้รับการส่งอย่างรวดเร็วและเชื่อถือได้ จึงอาจใช้กลไก QoS เพื่อจัดการและกำหนดลำดับความสำคัญของทราฟฟิกตามความต้องการของระบบ

6.6.3 สื่อส่งสัญญาณที่ใช้ในโครงข่าย WAN (Transmission Media)

สื่อส่งสัญญาณคือช่องทางทางกายภาพหรือคลื่นแม่เหล็กไฟฟ้าที่ใช้ลำเลียงข้อมูลระหว่างองค์ประกอบของ WAN โดยอาจแบ่งเป็นสื่อแบบมีตัวนำและไม่มีตัวนำ

1) สายใยแก้วนำแสง (Fiber Optic Cable)

สายใยแก้วนำแสงเป็นสื่อหลักของ WAN ความเร็วสูง เนื่องจากรองรับแบนด์วิดท์สูง ระยะทางไกล และมีความต้านทานต่อสัญญาณรบกวนทางแม่เหล็กไฟฟ้า เทคโนโลยี Wavelength Division Multiplexing (WDM) และ Dense Wavelength Division Multiplexing (DWDM) ช่วยให้สามารถส่งหลายช่องสัญญาณแสงผ่านเส้นใยแก้วเส้นเดียว ทำให้ใช้ความจุของสายได้มีประสิทธิภาพมากขึ้น (Forouzan, 2013)

2) ไมโครเวฟ (Microwave)

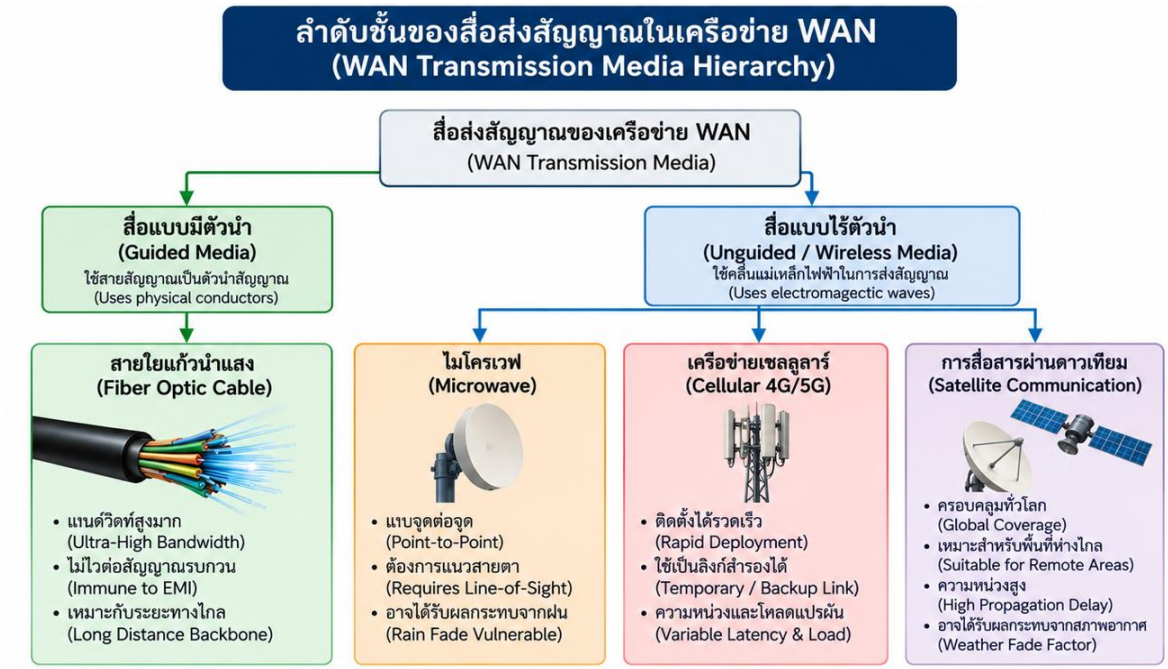
ไมโครเวฟ เป็นการสื่อสารแบบไร้สายระหว่างจุด โดยทั่วไปต้องมีแนวสายตาระหว่างสถานีส่งและรับ เหมาะกับพื้นที่ที่เดินสายใยแก้วได้ยาก เช่น ภูเขา พื้นที่ชนบท หรือการเชื่อมอาคารสองแห่ง ข้อจำกัดสำคัญคือสภาพอากาศ สิ่งกีดขวาง การจัดแนวเสาอากาศ การรบกวนของคลื่น

3) เครือข่ายเซลลูลาร์ (Cellular Network)

เครือข่าย 4G และ 5G ใช้เป็นได้ทั้งลิงก์หลักในสถานที่ชั่วคราวและลิงก์สำรองของ WAN เหมาะสำหรับระบบรักษาความปลอดภัยที่ต้องการความรวดเร็วในการติดตั้ง เช่น กล้องชั่วคราว จุดตรวจเคลื่อนที่ หรือพื้นที่ที่ไม่มีสายสื่อสาร ประสิทธิภาพของเครือข่ายเซลลูลาร์ขึ้นอยู่กับความครอบคลุมของสัญญาณ ปริมาณผู้ใช้งาน และนโยบายของผู้ให้บริการ จึงไม่ควรถือว่ามีความเร็วหรือความหน่วงคงที่

4) ดาวเทียม (Satellite)

การสื่อสารผ่านดาวเทียมเหมาะกับพื้นที่ห่างไกล ทะเล ภูเขา หรือพื้นที่ที่ไม่มีโครงสร้างพื้นฐานภาคพื้นดิน จุดเด่นคือครอบคลุมพื้นที่กว้าง แต่ข้อจำกัดคือความหน่วง ค่าใช้จ่าย และผลกระทบจากสภาพอากาศในบางย่านความถี่ การเลือกสื่อส่งสัญญาณจึงต้องพิจารณาทั้งระยะทาง ปริมาณข้อมูล ความหน่วง ความน่าเชื่อถือ และต้นทุน ไม่ควรพิจารณาเฉพาะอัตราข้อมูลสูงสุดที่ผู้ให้บริการระบุ

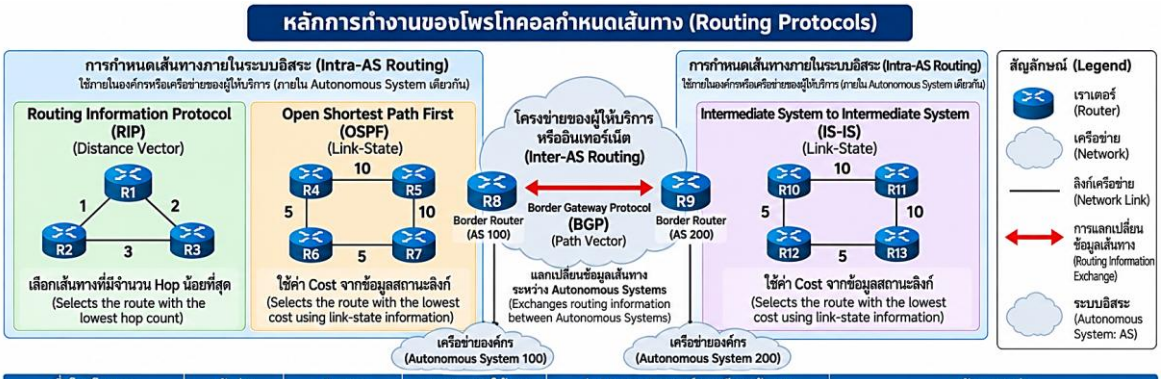


ประเภทสื่อ (Media Type)	ระยะทางโดยทั่วไป (Typical Distance)	แบนด์วิดท์ (Bandwidth)	ความหน่วง (Latency)	ความน่าเชื่อถือ (Reliability)	ต้นทุน (Cost)
สายใยแก้วนำแสง (Fiber Optic)	ไกลมาก (>100 km/span)	สูงมาก (>100 Gbps)	ต่ำมาก (< 5 ms)	สูงมาก (Very High)	สูง (High CAPEX)
ไมโครเวฟ (Microwave)	ปานกลาง (30 – 50 km/hop)	สูง (100 Mbps – 1 Gbps)	ต่ำ (5 – 10 ms)	ปานกลาง (Rain Fade)	ปานกลาง (Medium)
เซลลูลาร์ 4G/5G (Cellular 4G/5G)	ปานกลาง (1 – 10 km/cell)	ปานกลาง – สูง (10 – 1000 Mbps)	ปานกลาง (10 – 50 ms)	ปานกลาง (Load dependent)	ต่ำ – ปานกลาง (OPEX)
ดาวเทียม (GEO/LEO) (Satellite)	ครอบคลุมทั่วโลก (Global)	ปานกลาง (10 – 500 Mbps)	สูง (50 – 600 ms)	ปานกลาง (Weather Fade)	สูงมาก (Very High OPEX)

รูปที่ 6.10 สื่อส่งสัญญาณที่ใช้ในโครงข่าย WAN

6.6.4 โปรโตคอลกำหนดเส้นทาง (Routing Protocols)

โปรโตคอลกำหนดเส้นทาง เป็นกลไกที่เราเตอร์ใช้ แลกเปลี่ยนข้อมูลเส้นทางและคำนวณเส้นทางที่เหมาะสม เพื่อให้สามารถส่งแพ็กเก็ตไปยังเครือข่ายปลายทางได้ โดยแตกต่างจาก routed protocol เช่น IP ซึ่งเป็นโปรโตคอลที่ข้อมูลถูกส่งผ่านเครือข่าย ตัวอย่าง routing protocols ได้แก่ RIP, OSPF, IS-IS และ BGP โดย OSPF และ IS-IS ใช้สำหรับการกำหนดเส้นทางภายใน Autonomous System (AS) ส่วน BGP ใช้แลกเปลี่ยนข้อมูลเส้นทางระหว่าง AS และมีบทบาทสำคัญในการกำหนดเส้นทางบนอินเทอร์เน็ต โดย routing protocol แต่ละชนิดใช้หลักเกณฑ์ในการเลือกเส้นทางแตกต่างกัน เช่น hop count, cost หรือค่าคุณลักษณะของเส้นทาง ขณะที่ BGP สามารถเลือกเส้นทางตามคุณลักษณะและนโยบายการกำหนดเส้นทาง (routing policy) เมื่อเส้นทางเปลี่ยนแปลงหรือเกิดความขัดข้อง โปรโตคอลจะปรับข้อมูลเส้นทางจนเครือข่ายเข้าสู่สถานะสอดคล้องกัน ซึ่งเรียกว่า convergence ส่วนการส่งต่อแพ็กเก็ตจริงจะอาศัยข้อมูลใน forwarding table ของเราเตอร์



ชื่อโพรโทคอล (Protocol Name)	ตัวย่อ (Abbreviation)	ประเภท (Type)	ขอบเขตการใช้งาน (Scope)	ค่า Metric / เกณฑ์การเลือกเส้นทาง (Metric / Selection Criteria)	ลักษณะเด่น (Key Features)
Routing Information Protocol	RIP	Distance Vector	ภายใน AS (Intra-AS)	จำนวน Hop (Hop Count)	• ใช้งานง่าย เหมาะกับเครือข่ายขนาดเล็ก • รองรับสูงสุด 15 Hop
Open Shortest Path First	OSPF	Link-State	ภายใน AS (Intra-AS)	ค่า Cost (โดยทั่วไปสัมพันธ์กับแบนด์วิดท์)	• สร้างฐานข้อมูลสถานะลิงก์ (Link-State Database) • รองรับการแบ่งพื้นที่ (Area) เหมาะกับเครือข่ายขนาดกลาง–ใหญ่
Intermediate System to Intermediate System	IS-IS	Link-State	ภายใน AS (Intra-AS)	ค่า Cost (ตามคุณลักษณะของลิงก์)	• โครงสร้างแบบลำดับชั้น (Level 1 และ Level 2) • นิยมใช้ในเครือข่ายขนาดใหญ่และของผู้ให้บริการ
Border Gateway Protocol	BGP	Path Vector	ระหว่าง AS (Inter-AS)	Path Attributes และนโยบายการกำหนดเส้นทาง (Routing Policy)	• แลกเปลี่ยนเส้นทางระหว่าง Autonomous Systems • เป็นโพรโทคอลสำคัญของอินเทอร์เน็ต

รูปที่ 6.11 หลักการทำงานของโปรโตคอลกำหนดเส้นทาง

จากรูป 6.11 โปรโตคอลกำหนดเส้นทางช่วยให้เราเตอร์เรียนรู้และเลือกเส้นทางสำหรับส่งแพ็กเก็ตไปยังเครือข่ายปลายทาง โดย RIP, OSPF และ IS-IS ใช้สำหรับการกำหนดเส้นทางภายในระบบอิสระ (intra-AS routing) ซึ่ง RIP เลือกเส้นทางโดยพิจารณาจำนวน hop ขณะที่ OSPF และ IS-IS ใช้ข้อมูลสถานะของลิงก์ (link-state) เพื่อคำนวณเส้นทาง ส่วน BGP ใช้แลกเปลี่ยนข้อมูลเส้นทางระหว่างระบบอิสระ (inter-AS routing) โดยพิจารณาคุณลักษณะของเส้นทางและนโยบายการกำหนดเส้นทาง เพื่อให้ข้อมูลสามารถเดินทางระหว่างเครือข่ายต่าง ๆ ได้อย่างเหมาะสม

สรุปองค์ประกอบของ WAN ประกอบด้วยองค์ประกอบสำคัญ เช่น CPE, access link, PE, WAN backbone, transmission media และ routing protocols ซึ่งทำงานร่วมกันเพื่อเชื่อมต่อเครือข่ายที่อยู่ต่างพื้นที่ สำหรับระบบรักษาความปลอดภัยอัจฉริยะ การออกแบบ WAN ควรคำนึงถึง แบนด์วิดท์ ความหน่วง ความพร้อมใช้งาน ความซ้ำซ้อนของเส้นทาง และความมั่นคงปลอดภัย เพื่อรองรับการส่งวิดีโอ ข้อมูลเหตุการณ์ และคำสั่งควบคุมได้อย่างมีประสิทธิภาพและต่อเนื่อง

6.7 เทคโนโลยีเครือข่ายแบบใช้สาย (Wired Local Area Network: Wired LAN)

เทคโนโลยีเครือข่ายแบบใช้สาย (Wired LAN) หรือเรียกว่า Ethernet ได้รับความนิยมและใช้งานอย่างแพร่หลายมากที่สุดในโลก เนื่องจากมีความเรียบง่ายในการติดตั้ง ความน่าเชื่อถือสูง ความสามารถในการขยายระบบ และรองรับการรับส่งข้อมูลด้วยความเร็วตั้งแต่ระดับเมกะbitต่อวินาที (Mbps) ไปจนถึงหลายร้อยกิกะbitต่อวินาที (Gbps) ปัจจุบัน Ethernet เป็นเทคโนโลยีพื้นฐานสำหรับเครือข่ายภายในองค์กร ศูนย์ข้อมูล(data center)ระบบอุตสาหกรรม ระบบอัตโนมัติภายในอาคาร และระบบรักษาความปลอดภัยอัจฉริยะ เช่น ระบบกล้องวงจรปิดผ่านเครือข่าย ระบบควบคุมการเข้าออก ระบบแจ้งเหตุเพลิงไหม้ และระบบบริหารจัดการอาคาร (Forouzan, 2013; IEEE, 2022)

Ethernet ได้รับการพัฒนาให้เป็นมาตรฐาน IEEE 802.3 ซึ่งกำหนดรูปแบบของเฟรม (frame format) วิธีการเข้าถึงสื่อกลาง (MAC) ลักษณะของสัญญาณในชั้นกายภาพ (physical layer) และการทำงานของชั้นเชื่อมโยงข้อมูล (data link layer) เพื่อให้อุปกรณ์จากผู้ผลิตต่างๆ สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ (IEEE, 2022) ในอดีต Ethernet ใช้โครงสร้างเครือข่ายแบบบัส และใช้กลไก Carrier Sense Multiple Access with Collision Detection (CSMA/CD) เพื่อควบคุมการเข้าถึงสื่อกลางร่วมกัน แต่เมื่อเทคโนโลยีสวิตช์เครือข่าย (Ethernet switch) ได้รับการพัฒนา Ethernet ได้เปลี่ยนเป็นโครงสร้างแบบดาว และรองรับการสื่อสารแบบ full-duplex ทำให้ไม่เกิดการชนกันของข้อมูล (collision) และสามารถเพิ่มประสิทธิภาพการรับส่งข้อมูลได้อย่างมาก (Forouzan, 2013; Stallings, 2021)

6.7.1 ความหมายและวิวัฒนาการของ Ethernet

1) ความหมายของ Ethernet

Ethernet คือ เทคโนโลยีเครือข่ายแบบใช้สายสำหรับเครือข่ายเฉพาะที่ (LAN) ซึ่งกำหนดมาตรฐานการรับส่งข้อมูลระหว่างอุปกรณ์เครือข่ายผ่านสายสัญญาณหรือสายใยแก้วนำแสง โดยกำหนดรูปแบบของเฟรม วิธีการระบุที่อยู่ด้วยหมายเลข MAC address กลไกการตรวจสอบความผิดพลาดของข้อมูล และมาตรฐานของชั้นกายภาพและชั้นเชื่อมโยงข้อมูล เพื่อให้อุปกรณ์ต่างๆ สามารถแลกเปลี่ยนข้อมูลได้อย่างถูกต้องและเชื่อถือได้ (Forouzan, 2013)

2) วิวัฒนาการของ Ethernet

Ethernet ได้รับการพัฒนาอย่างต่อเนื่องตั้งแต่ช่วงทศวรรษ 1970 จนถึงปัจจุบัน โดยมีวัตถุประสงค์เพื่อเพิ่มความเร็วในการรับส่งข้อมูล เพิ่มความน่าเชื่อถือของเครือข่าย และรองรับจำนวนอุปกรณ์ที่เพิ่มขึ้น

2.1) ยุคเริ่มต้นของ Ethernet

Ethernet ถูกคิดค้นขึ้นในปี ค.ศ. 1973 โดย Robert Metcalfe และ David Boggs ณ ศูนย์วิจัย Xerox Palo Alto Research Center (Xerox PARC) เพื่อใช้เชื่อมต่อคอมพิวเตอร์และเครื่องพิมพ์ภายในองค์กร งานวิจัยดังกล่าวได้รับแรงบันดาลใจจากระบบเครือข่ายไร้สาย Additive Links On-line Hawaii Area (ALOHAnet) ซึ่งใช้การแบ่งปันสื่อกลางร่วมกันในการรับส่งข้อมูล (Metcalfe & Boggs, 1976) Ethernet รุ่นแรกมีอัตราการรับส่งข้อมูลประมาณ 2.94 Mbps ใช้สายโคแอกเชียล (coaxial cable) เป็นสื่อกลางร่วมกัน

2.2) มาตรฐาน DIX Ethernet

ในปี ค.ศ. 1980 บริษัท Digital Equipment Corporation (DEC), Intel, และ Xerox ได้ร่วมกันพัฒนามาตรฐาน Ethernet เวอร์ชันเชิงพาณิชย์ ซึ่งเรียกว่า DIX Ethernet โดยกำหนดอัตราการรับส่งข้อมูล 10 Mbps และกำหนดรูปแบบของ Ethernet frame ที่กลายเป็นพื้นฐานของ Ethernet ในเวลาต่อมา มาตรฐาน DIX Ethernet มีบทบาทสำคัญในการผลักดันให้ Ethernet กลายเป็นเทคโนโลยีเครือข่ายที่ได้รับการยอมรับในอุตสาหกรรมคอมพิวเตอร์

2.3) มาตรฐาน IEEE 802.3

ปี ค.ศ.1983 สถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers: IEEE) ได้ประกาศใช้มาตรฐาน IEEE 802.3 เพื่อกำหนดมาตรฐานกลางของ Ethernet สำหรับการสื่อสารข้อมูลในเครือข่าย LAN มาตรฐาน IEEE 802.3 กำหนดรายละเอียดเกี่ยวกับ ชั้นกายภาพ (physical layer) ชั้นเชื่อมโยงข้อมูล (data link layer) รูปแบบของ Ethernet frame การเข้าถึงสื่อกลาง และการตรวจสอบความผิดพลาดของข้อมูล มาตรฐานดังกล่าวได้รับการปรับปรุงอย่างต่อเนื่องเพื่อรองรับความเร็วที่สูงขึ้น

2.4) จาก Shared Ethernet สู่ Switched Ethernet

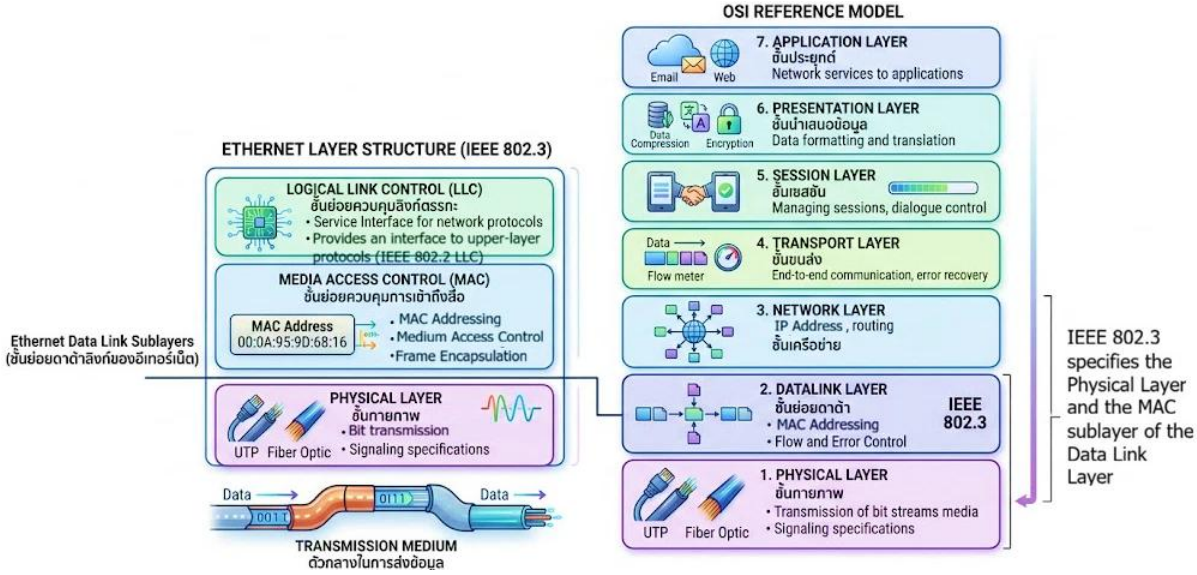
ในช่วงแรก Ethernet ใช้อุปกรณ์ hub เป็นศูนย์กลางของเครือข่าย โดยอุปกรณ์ทุกเครื่องใช้สื่อกลางร่วมกัน ทำให้เกิดปัญหาการชนกันของข้อมูล เมื่อหลายอุปกรณ์ส่งข้อมูลพร้อมกัน จึงต้องใช้กลไก CSMA/CD ในการตรวจจับและหลีกเลี่ยงการชนกันของข้อมูลเมื่อเทคโนโลยี Ethernet switch ได้รับการพัฒนา เครือข่าย Ethernet เปลี่ยนมาใช้การเชื่อมต่อแบบจุดต่อจุด (point-to-point connection) ระหว่างอุปกรณ์กับสวิตช์ ทำให้อุปกรณ์แต่ละเครื่องมีช่องสัญญาณเฉพาะของตนเอง ลดการเกิด collision และเพิ่มประสิทธิภาพของเครือข่ายอย่างมาก นอกจากนี้ Ethernet switch ยังสามารถเรียนรู้หมายเลข MAC address ของอุปกรณ์แต่ละเครื่อง และส่งต่อ Ethernet frame ไปยังพอร์ตปลายทางที่ถูกต้อง ส่งผลให้ลดปริมาณ broadcast ภายในเครือข่ายและเพิ่มประสิทธิภาพการใช้แบนด์วิดท์

6.7.2 สถาปัตยกรรมของ Ethernet (Ethernet Architecture)

Ethernet เป็นเทคโนโลยีเครือข่ายท้องถิ่นแบบใช้สาย (Wired LAN) ที่พัฒนาภายใต้มาตรฐาน IEEE 802.3 ซึ่งกำหนดคุณลักษณะของการสื่อสารข้อมูลในชั้นกายภาพ (physical layer) และชั้นเชื่อมโยงข้อมูล (data link layer) ของแบบจำลอง OSI เพื่อให้อุปกรณ์จากผู้ผลิตต่าง ๆ สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ (Forouzan, 2013; IEEE, 2022) มาตรฐานครอบคลุมข้อกำหนดเกี่ยวกับรูปแบบของ Ethernet frame วิธีการเข้าถึงสื่อกลาง (MAC) ประเภทของสื่อส่งสัญญาณ ความเร็วในการรับส่งข้อมูล ระยะทางในการเชื่อมต่อ และคุณสมบัติของอุปกรณ์เครือข่าย เช่น การ์ดเชื่อมต่อเครือข่าย (NIC) สวิตช์เครือข่าย (network switch) และอุปกรณ์รับส่งสัญญาณ (transceiver) ปัจจุบัน Ethernet เป็นเทคโนโลยีหลักของระบบเครือข่ายองค์กร ศูนย์ข้อมูล ระบบอุตสาหกรรม และระบบรักษาความปลอดภัยอัจฉริยะ เนื่องจากรองรับการสื่อสารที่มีความเร็วสูง มีความเสถียร สามารถขยายระบบได้ง่าย

1) สถาปัตยกรรมของ Ethernet

สถาปัตยกรรมของ Ethernet อ้างอิงแบบจำลอง OSI โดยทำงานใน 2 ชั้นล่าง ได้แก่ชั้นกายภาพ (physical layer) และ ชั้นเชื่อมโยงข้อมูล (data Link layer) โดยชั้นเชื่อมโยงข้อมูลแบ่งออกเป็นสองชั้นย่อย ได้แก่ Logical Link Control (LLC) Sublayer และ MAC sublayer ดังแสดงในรูปที่ 6.12



รูปที่ 6.12 ความสัมพันธ์ระหว่างมาตรฐาน IEEE 802.3 กับ OSI Model

1.1) LLC เป็นชั้นย่อยส่วนบนของ data link layer ซึ่งกำหนดโดยมาตรฐาน IEEE 802.2 ทำหน้าที่เป็นตัวเชื่อมระหว่าง network layer กับ MAC sublayer หน้าที่สำคัญของ LLC ได้แก่ จัดเตรียมบริการให้กับ network layer ระบุชนิดของโปรโตคอลชั้นบน ควบคุมการไหลของข้อมูลในบางระบบ ตรวจสอบความถูกต้องของบริการเชื่อมโยงข้อมูล ซึ่งในระบบ Ethernet สมัยใหม่หน้าที่ของ LLC ลดลงอย่างมาก เนื่องจากการระบุชนิดของโปรโตคอลสามารถทำได้ผ่านฟิลด์ Ether type ภายใน Ethernet frame

1.2) MAC เป็นชั้นย่อยที่สำคัญที่สุดของ Ethernet ที่ควบคุมการเข้าถึงสื่อกลางและกำหนดรูปแบบของ Ethernet frame หน้าที่ของ MAC คือ กำหนดหมายเลข MAC address สร้างและถอด Ethernet frame ควบคุมการเข้าถึงสื่อกลาง ตรวจสอบความผิดพลาดด้วย Frame Check Sequence (FCS) ส่งและรับเฟรมระหว่างอุปกรณ์ภายใน LAN MAC address ซึ่งมี 48 bit (6 ไบต์) ถูกกำหนดโดยผู้ผลิตอุปกรณ์ตามมาตรฐาน IEEE registration authority ทำให้อินเทอร์เฟซเครือข่ายแต่ละตัวมีหมายเลขประจำที่ไม่ซ้ำกันในระดับสากล

1.3) Physical layer ทำหน้าที่ส่งข้อมูลในรูปของbitผ่านสื่อส่งสัญญาณ โดยกำหนดคุณสมบัติทางไฟฟ้า ทางแสง และทางกล ในระบบสื่อสาร หน้าที่ physical layer ได้แก่ แปลงข้อมูลดิจิทัลเป็นสัญญาณ ส่งและรับสัญญาณผ่านสื่อกลาง กำหนดชนิดของสายสัญญาณ กำหนดอัตราการรับส่งข้อมูล และ กำหนดระยะทางสูงสุดของการเชื่อมต่อ Ethernet รองรับสื่อส่งสัญญาณหลายประเภท เช่น สายคู่บิดเกลียว สายใยแก้วนำแสง สายโคแอกเชียล

2) มาตรฐาน IEEE 802.3

IEEE 802.3 เป็นมาตรฐานสากลที่กำหนดรายละเอียดของ Ethernet ได้รับการปรับปรุงอย่างต่อเนื่องเพื่อรองรับเทคโนโลยีใหม่ โดยมาตรฐานนี้กำหนดรูปแบบ Ethernet frame, MAC address วิธีการเข้าถึงสื่อกลาง physical layer ชนิดของสายสัญญาณ ความเร็วในการรับส่งข้อมูล และ ระยะทางในการเชื่อมต่อ ตัวอย่างมาตรฐานที่ใช้งานแพร่หลายแสดงในตารางที่ 6.5

ตารางที่ 6.5 ตัวอย่างมาตรฐาน ความเร็ว และสื่อในการสื่อสารสัญญาณ

มาตรฐาน	ความเร็ว	สื่อส่งสัญญาณ
10BASE-T	10 Mbps	UTP
100BASE-TX	100 Mbps	Cat5/Cat5e UTP
1000BASE-T	1 Gbps	Cat5e/Cat6 UTP
10GBASE-T	10 Gbps	Cat6A/Cat7 UTP
10GBASE-SR	10 Gbps	Multimode Fiber
10GBASE-LR	10 Gbps	Single-mode Fiber

ปัจจุบัน IEEE 802.3 ยังรองรับมาตรฐานความเร็วสูง เช่น 25, 40, 100, 200 และ 400 Gigabit Ethernet สำหรับศูนย์ข้อมูลและระบบ cloud computing

6.7.3 Ethernet Frame Format

Ethernet ใช้ frame เป็นหน่วยข้อมูล (Protocol Data Unit: PDU) ของชั้นเชื่อมโยงข้อมูล (data link layer) โดยเฟรมทำหน้าที่บรรจุข้อมูลที่ได้รับจากชั้นเครือข่าย พร้อมทั้งเพิ่มข้อมูลควบคุม เช่น หมายเลข MAC ต้นทางและปลายทาง รวมถึงข้อมูลตรวจสอบความผิดพลาด ก่อนส่งผ่าน Physical Layer ไปยังอุปกรณ์ปลายทาง (Forouzan, 2013) รูปแบบของ Ethernet Frame ถูกกำหนดโดยมาตรฐาน IEEE 802.3 เพื่อให้ทุกอุปกรณ์สามารถสร้างและตีความเฟรมได้ในรูปแบบเดียวกัน โครงสร้างของ Ethernet Frame รายละเอียด ดังตารางที่ 6.6

ตารางที่ 6.6 ส่วนสำคัญของ Ethernet Frame

ฟิลด์	ขนาด	หน้าที่
Preamble (bitนำสัญญาณ)	7 Bytes	ซิงโครไนซ์สัญญาณระหว่างอุปกรณ์ผู้ส่งผู้รับ
Start Frame Delimiter: SFD (ตัวคั่นเริ่มต้นเฟรม)	1 Byte	ระบุจุดเริ่มต้นของ Ethernet frame
Destination MAC Address (หมายเลข MAC ปลายทาง)	6 Bytes	ระบุอินเทอร์เฟซเครือข่ายปลายทาง
Source MAC Address (หมายเลข MAC ต้นทาง)	6 Bytes	ระบุอินเทอร์เฟซเครือข่ายต้นทาง
Type/Length (ชนิด/ความยาว)	2 Bytes	ระบุชนิดของโปรโตคอลชั้นบน (Ether type) หรือความยาวของข้อมูล ตามรูปแบบเฟรม
Data and Padding (ข้อมูลและbitเติมเต็ม)	46-1500 Bytes	บรรจุข้อมูลจากชั้นเครือข่าย และเติมbitเมื่อข้อมูลมีขนาดต่ำกว่า 46 ไบต์
Frame Check Sequence: FCS (ลำดับตรวจสอบเฟรม)	4 Bytes	ตรวจสอบความผิดพลาดของเฟรมด้วยวิธี Cyclic Redundancy Check (CRC-32)

หมายเหตุ: Preamble และ SFD ใช้สำหรับการซิงโครไนซ์ในชั้นกายภาพ และโดยทั่วไปไม่นับรวมอยู่ในความยาวของ Ethernet Frame ตามมาตรฐาน IEEE 802.3

6.7.4 หลักการทำงานของ CSMA/CD

อุปกรณ์ทุกเครื่องในเครือข่ายใช้สื่อกลางร่วมกัน (shared medium) เช่น สายโคแอกเชียล หรือฮับส่งผลให้อุปกรณ์หลายเครื่องสามารถพยายามส่งข้อมูลผ่านสายสัญญาณเส้นเดียวกันในเวลาเดียวกัน หากไม่มีการควบคุมการเข้าถึงสื่อกลาง การส่งข้อมูลพร้อมกันจะทำให้เกิด การชนกันของข้อมูล ส่งผลให้เฟรมข้อมูลเสียหายและไม่สามารถรับข้อมูลได้อย่างถูกต้อง (Forouzan, 2013) เพื่อแก้ไขปัญหาดังกล่าว Ethernet จึงใช้กลไก CSMA/CD ซึ่งเป็นวิธีการควบคุมการเข้าถึงสื่อกลาง MAC protocol ที่กำหนดให้ทุกอุปกรณ์ตรวจสอบสถานะของสื่อกลางก่อนส่งข้อมูล และสามารถตรวจจับการชนกันของข้อมูลระหว่างการส่งได้ (IEEE, 2022) ปัจจุบัน แม้ว่าเครือข่าย Ethernet ส่วนใหญ่จะใช้ Ethernet Switch และการสื่อสารแบบ Full-Duplex ซึ่งไม่เกิดการชนกันของข้อมูล และเทคโนโลยี CSMA/CD รายละเอียดดังนี้

1) ความหมายของ CSMA/CD

CSMA/CD ย่อมาจาก Carrier Sense Multiple Access with Collision Detection ซึ่งสามารถอธิบายได้ดังนี้

1.1) Carrier Sense (CS) หมายถึง การตรวจสอบสื่อกลางก่อนส่งข้อมูล หากตรวจพบว่ามีอุปกรณ์อื่นกำลังส่งข้อมูลอยู่ จะต้องรอจนกว่าสื่อกลางจะว่าง

1.2) Multiple Access (MA) หมายถึง อุปกรณ์หลายเครื่องสามารถใช้สื่อกลางเดียวกันในการรับส่งข้อมูลได้

1.3) Collision Detection (CD) หมายถึง การตรวจจับการชนกันของข้อมูลในระหว่างการส่ง หากเกิดการชนกัน อุปกรณ์จะหยุดส่งข้อมูลทันทีและส่งใหม่ในภายหลัง

ดังนั้น CSMA/CD จึงเป็นกลไกที่ช่วยลดความเสียหายจากการส่งข้อมูลพร้อมกันบนสื่อกลางร่วมกัน และเพิ่มประสิทธิภาพของเครือข่าย Ethernet ในยุคแรก

2) หลักการทำงานของ CSMA/CD

การทำงานของ CSMA/CD ประกอบด้วย 6 ขั้นตอนหลัก ดังนี้

2.1) ขั้นตอนที่ 1 ตรวจสอบสื่อกลาง (carrier sense) ก่อนเริ่มส่งข้อมูล การ์ดเชื่อมต่อเครือข่าย (NIC) จะตรวจสอบว่าสายสัญญาณกำลังถูกใช้งานอยู่หรือไม่ (1) หากสื่อกลางว่าง (idle) จะเริ่มส่งข้อมูลได้ทันที และ (2) หากสื่อกลางไม่ว่าง (busy) จะรอจนกว่าสื่อกลางจะว่าง การตรวจสอบนี้ช่วยลดโอกาสที่อุปกรณ์หลายเครื่องจะเริ่มส่งข้อมูลพร้อมกัน

2.2) ขั้นตอนที่ 2 เริ่มส่งข้อมูล เมื่อสื่อกลางว่าง อุปกรณ์จะเริ่มส่ง Ethernet frame ผ่านสายสัญญาณ โดยในขณะเดียวกันยังคงตรวจสอบสัญญาณบนสายอย่างต่อเนื่อง

2.3) ขั้นตอนที่ 3 ตรวจจับการชนกันของข้อมูล (collision detection) หากมีอุปกรณ์อีกเครื่องเริ่มส่งข้อมูลในเวลาใกล้เคียงกัน สัญญาณทั้งสองจะซ้อนทับกัน ทำให้เกิด collision NIC จะตรวจสอบระดับแรงดันไฟฟ้าบนสายสัญญาณ หากพบว่าสัญญาณที่ได้รับแตกต่างจากสัญญาณที่ตนเองกำลังส่ง แสดงว่าเกิดการชนกันของข้อมูล

2.4) ขั้นตอนที่ 4 ส่งสัญญาณ jam signal เมื่อพบ collision อุปกรณ์ที่ตรวจพบจะส่ง jam signal ซึ่งเป็นลำดับbitพิเศษเพื่อแจ้งให้อุปกรณ์ทุกเครื่องในเครือข่ายทราบว่าเฟรมดังกล่าวไม่สมบูรณ์และต้องถูกยกเลิก หลังจากส่ง jam signal แล้ว ทุกอุปกรณ์จะหยุดส่งข้อมูลทันที

2.5) ขั้นตอนที่ 5 รอแบบสุ่ม (backoff) เพื่อป้องกันไม่ให้อุปกรณ์ทั้งสองเริ่มส่งข้อมูลใหม่พร้อมกันอีกครั้ง Ethernet ใช้วิธี binary exponential backoff แต่ละอุปกรณ์จะสุ่มระยะเวลารอก่อนเริ่มส่งข้อมูลใหม่ โดยจำนวนช่วงเวลาที่สุ่มจะเพิ่มขึ้นตามจำนวนครั้งที่เกิด Collision ติดต่อกัน ตัวอย่างดังตารางที่ 6.7 วิธีนี้ช่วยลดโอกาสที่อุปกรณ์จะเกิด collision ซ้ำ

ตารางที่ 6.7 จำนวนช่วงเวลาที่สุ่ม

จำนวนครั้งที่ชนกัน	ช่วงเวลาที่สุ่มรอ
ครั้งที่ 1	0-1 Slot Time
ครั้งที่ 2	0-3 Slot Time
ครั้งที่ 3	0-7 Slot Time
ครั้งที่ 4	0-15 Slot Time

2.6) ขั้นตอนที่ 6 ส่งข้อมูลใหม่ หลังจากครบเวลาที่สุ่มไว้ อุปกรณ์จะกลับไปตรวจสอบสื่อกลางอีกครั้ง หากสื่อกลางว่าง จะเริ่มส่งข้อมูลใหม่ แต่หากยังไม่ว่าง จะรอต่อไปจนกว่าจะสามารถส่งข้อมูลได้

3) Collision Domain

Collision domain คือ ขอบเขตของเครือข่ายที่อุปกรณ์มีโอกาสเกิดการชนกันของข้อมูลร่วมกัน ในเครือข่ายที่ใช้ hub ทุกพอร์ตจะอยู่ใน collision domain เดียวกัน ดังนั้นยิ่งมีอุปกรณ์มากโอกาสเกิด collision ก็ยิ่งสูง ส่งผลให้ประสิทธิภาพของเครือข่ายลดลง เมื่อเปลี่ยนมาใช้ Ethernet Switch แต่ละพอร์ตของสวิตช์จะเป็น collision domain แยกจากกัน ทำให้การชนกันของข้อมูลแทบไม่เกิดขึ้น

4) ข้อจำกัดของ CSMA/CD

แม้ CSMA/CD จะเป็นกลไกที่มีประสิทธิภาพสำหรับ Ethernet แบบดั้งเดิม แต่ก็มีข้อจำกัดหลายประการ ได้แก่

4.1) ประสิทธิภาพลดลงเมื่อจำนวนอุปกรณ์เพิ่มขึ้น

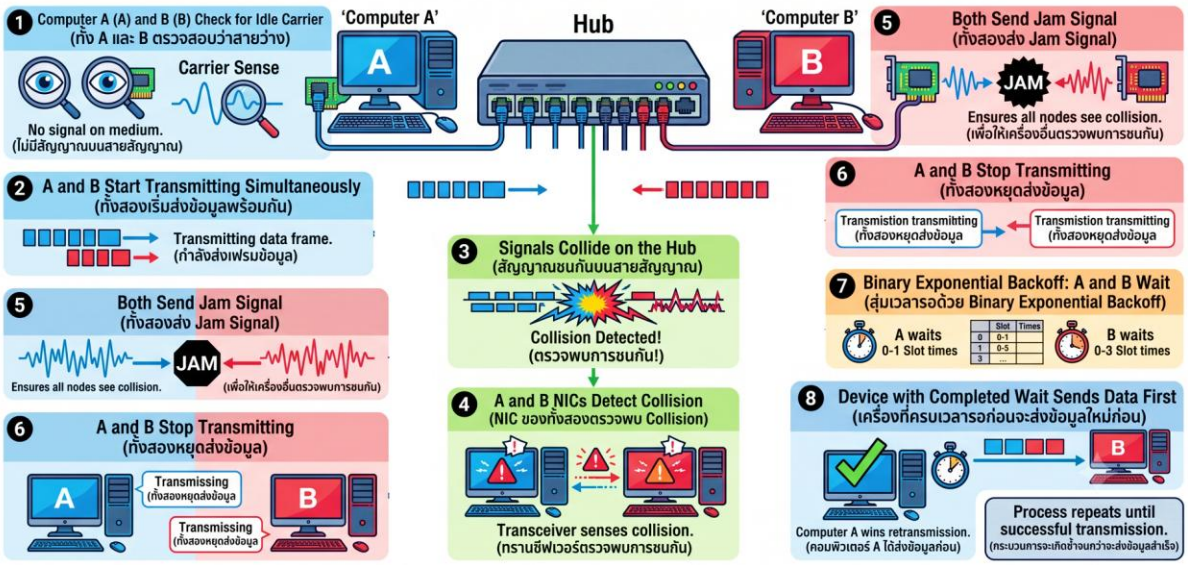
4.2) เกิดการชนกันของข้อมูลบ่อยในช่วงที่มีการรับส่งข้อมูลหนาแน่น

4.3) ต้องเสียเวลาในการส่ง jam signal และรอแบบสุ่ม

4.4) ไม่เหมาะกับการสื่อสารที่ต้องการเวลาตอบสนองคงที่ (real-time communication)

4.5) ไม่รองรับความเร็วสูงในเครือข่ายขนาดใหญ่

ข้อจำกัดเหล่านี้เป็นสาเหตุสำคัญที่ทำให้ Ethernet พัฒนาไปสู่การใช้ Ethernet switch และการสื่อสารแบบ full-duplex



รูปที่ 6.13 กระบวนการทำงานของ CSMA/CD

จากรูปที่ 6.13 ลำดับการทำงานของกลไก CSMA/CD ซึ่งเป็นวิธีการควบคุมการเข้าถึงสื่อกลางที่ใช้ในระบบ Ethernet แบบดั้งเดิมตามมาตรฐาน IEEE 802.3 ที่ใช้อุปกรณ์ Hub หรือสายโคแอกเชียลเป็นสื่อกลางร่วมกัน โดยอุปกรณ์ทุกเครื่องใช้ช่องสัญญาณเดียวกันในการรับส่งข้อมูล จึงมีโอกาสเกิดการชนกันของข้อมูล หากมีการส่งข้อมูลพร้อมกัน

ขั้นตอนแรก คอมพิวเตอร์ A และ B ตรวจสอบว่าสื่อกลางว่างหรือไม่ (carrier sense) หากไม่พบสัญญาณจากอุปกรณ์อื่น ทั้งสองเครื่องจะถือว่าสายสัญญาณอยู่ในสถานะว่าง (idle) และสามารถเริ่มส่งข้อมูลได้ ดังแสดงในขั้นตอนที่ 1 และ 2 ของภาพ อย่างไรก็ตาม เนื่องจากทั้งสองเครื่องเริ่มส่งข้อมูลเกือบพร้อมกัน สัญญาณข้อมูลจึงเดินทางมาพบกันภายใน hub ทำให้เกิด การชนกันของข้อมูลดังในขั้นตอนที่ 3

เมื่อเกิด collision การ์ดเชื่อมต่อเครือข่าย NIC ของทั้งสองเครื่องจะตรวจพบความผิดปกติของสัญญาณบนสายสื่อสาร (collision detection) ดังแสดงในขั้นตอนที่ 4 จากนั้น NIC ของทั้งสองเครื่องจะส่ง jam signal ซึ่งเป็นลำดับbitพิเศษเพื่อแจ้งให้อุปกรณ์ทุกเครื่องในเครือข่ายทราบว่าเฟรมข้อมูลเกิดความเสียหายและไม่สามารถใช้งานได้ ดังแสดงในขั้นตอนที่ 5 หลังจากส่ง jam signal แล้ว ทั้งสองเครื่องจะ ยุติการส่งเฟรมที่กำลังส่งทันที (abort frame transmission) ดังแสดงในขั้นตอนที่ 6

เพื่อหลีกเลี่ยงการเกิด collision ซ้ำคอมพิวเตอร์แต่ละเครื่องจะเข้าสู่กระบวนการ binary exponential backoff โดยสุ่มระยะเวลารอก่อนเริ่มส่งข้อมูลใหม่ ดังแสดงในขั้นตอนที่ 7 ช่วงเวลาที่สุ่มจะเพิ่มขึ้นตามจำนวนครั้งที่เกิด collision ติดต่อกัน ทำให้โอกาสที่อุปกรณ์ทั้งสองจะเริ่มส่งข้อมูลพร้อมกันอีกครั้งลดลง เมื่อครบเวลาที่สุ่มไว้ อุปกรณ์ที่หมดเวลารอก่อนจะกลับมาตรวจสอบสื่อกลางอีกครั้ง หากสายสัญญาณว่างก็จะเริ่มส่งข้อมูลใหม่ก่อน ดังแสดงในขั้นตอนที่ 8 ส่วนอุปกรณ์อีกเครื่องจะรอจนกว่าสื่อกลางจะว่างจึงจึงเริ่มส่งข้อมูลต่อไป

5) CSMA/CD กับ Ethernet ในปัจจุบัน

ในเครือข่าย Ethernet สมัยใหม่ อุปกรณ์ส่วนใหญ่เชื่อมต่อผ่าน Ethernet switch โดยแต่ละพอร์ตของสวิตช์เป็นการเชื่อมต่อแบบ point-to-point และรองรับการรับส่งข้อมูลแบบ full-duplex ซึ่งสามารถส่งและรับข้อมูลพร้อมกันได้ จึงไม่เกิดการชนกันของข้อมูลและไม่จำเป็นต้องใช้ CSMA/CD อีกต่อไป ดังนั้นมาตรฐาน Gigabit Ethernet (IEEE 802.3ab), 10 Gigabit Ethernet (IEEE 802.3an) และมาตรฐานที่มีความเร็วสูงกว่าทั้งหมด จึงทำงานโดยไม่ใช้กลไก CSMA/CD อย่างไรก็ตาม ความรู้เกี่ยวกับ CSMA/CD ยังคงมีความสำคัญสำหรับการศึกษาพื้นฐานของ Ethernet การวิเคราะห์เครือข่ายแบบดั้งเดิม และการทำความเข้าใจวิวัฒนาการของมาตรฐาน IEEE 802.3

6.7.5 Ethernet Switching

1) ความหมายของ Ethernet Switching

การพัฒนาเทคโนโลยี Ethernet จากระบบเครือข่ายแบบใช้สื่อกลางร่วมกัน (shared Ethernet) ไปสู่ระบบเครือข่ายแบบสวิตช์ (switched Ethernet) ถือเป็นการเปลี่ยนแปลงที่สำคัญที่สุดประการหนึ่งของเครือข่ายคอมพิวเตอร์ เนื่องจากสามารถเพิ่มประสิทธิภาพในการรับส่งข้อมูล ลดการชนกันของข้อมูล และรองรับอุปกรณ์จำนวนมากได้อย่างมีประสิทธิภาพ (Forouzan, 2013)

ในระบบรักษาความปลอดภัยอัจฉริยะ Ethernet switch เป็นอุปกรณ์โครงสร้างพื้นฐานที่สำคัญ เนื่องจากใช้เชื่อมต่ออุปกรณ์เครือข่าย เช่น กล้อง IP NVR ระบบควบคุมการเข้าออก เซิร์ฟเวอร์ และอุปกรณ์ IoT เข้าด้วยกัน ทำให้สามารถรับส่งข้อมูลแบบเวลาจริงได้อย่างมีประสิทธิภาพ (IEEE, 2022)

2) หลักการทำงานของ Ethernet switch

Ethernet Switch ทำหน้าที่รับเฟรมข้อมูลจากอุปกรณ์ต้นทาง วิเคราะห์หมายเลข destination MAC address ที่อยู่ภายใน Ethernet frame จากนั้นค้นหาปลายทางใน MAC address table หากพบข้อมูลของปลายทาง สวิตช์จะส่งเฟรมออกเฉพาะพอร์ตที่เชื่อมต่อกับอุปกรณ์ปลายทางเท่านั้น แต่หากไม่พบข้อมูล สวิตช์จะส่งเฟรมออกทุกพอร์ตยกเว้นพอร์ตต้นทาง ซึ่งเรียกว่า flooding เพื่อค้นหาอุปกรณ์ปลายทาง กระบวนการทำงานของ Ethernet Switch (Forouzan, 2013) ประกอบด้วย 4 ขั้นตอนหลัก ได้แก่

2.1) Learning เรียนรู้หมายเลข MAC address จากเฟรมที่รับเข้ามาและบันทึกไว้ใน MAC address table

2.2) Forwarding ส่งต่อเฟรมไปยังพอร์ตปลายทางเมื่อทราบตำแหน่งอุปกรณ์

2.3) Filtering ไม่ส่งเฟรมไปยังพอร์ตอื่นที่ไม่เกี่ยวข้อง ช่วยลดปริมาณทราฟฟิกในเครือข่าย

2.4) Flooding ส่งเฟรมไปยังทุกพอร์ต (ยกเว้นพอร์ตต้นทาง) เมื่อไม่พบ MAC address ของปลายทาง

การทำงานดังกล่าวช่วยเพิ่มประสิทธิภาพของเครือข่าย ลดการใช้แบนด์วิดท์โดยไม่จำเป็น และลดโอกาสเกิดการชนกันของข้อมูล

3) MAC Address Table

MAC address table หรือ Content Addressable Memory (CAM) table เป็นฐานข้อมูลภายใน Ethernet switch ที่ใช้เก็บความสัมพันธ์ระหว่างหมายเลข MAC address กับหมายเลขพอร์ตของสวิตช์ ตัวอย่าง MAC address table ดังตารางที่ 6.8

ตารางที่ 6.8 MAC Address กับหมายเลขพอร์ตของสวิตช์

MAC Address	Switch Port
00:1A:2B:3C:4D:01	Port 1
00:1A:2B:3C:4D:02	Port 2
00:1A:2B:3C:4D:03	Port 5
00:1A:2B:3C:4D:04	Port 8

เมื่อสวิตช์ได้รับเฟรมข้อมูล จะอ่าน source MAC address ก่อน แล้วบันทึกหมายเลขดังกล่าวพร้อมหมายเลขพอร์ตที่รับข้อมูลเข้ามา จากนั้นจึงตรวจสอบ Destination MAC address เพื่อค้นหาพอร์ตปลายทาง หากพบข้อมูลในตาราง สวิตช์จะส่งเฟรมออกเฉพาะพอร์ตนั้น หากไม่พบจะใช้วิธี Flooding เพื่อค้นหาอุปกรณ์ปลายทาง

4) วิธีการส่งต่อเฟรม (Frame Forwarding Methods)

Ethernet switch มีวิธีการส่งต่อเฟรมหลัก 3 วิธี ดังนี้

4.1) Store-and-forward switching เป็นวิธีที่ได้รับความนิยมมากที่สุด โดยสวิตช์จะรับ Ethernet frame ทั้งหมดก่อน จากนั้นตรวจสอบค่า FCS หากไม่พบข้อผิดพลาดจึงส่งเฟรมไปยังปลายทาง ข้อดี คือ ตรวจจับข้อผิดพลาดได้ ลดการส่งเฟรมที่เสียหาย เหมาะกับเครือข่ายองค์กรและระบบรักษาความปลอดภัย ส่วน ข้อเสีย คือ มีค่าหน่วงเวลา (latency) สูงกว่าวิธีอื่นเล็กน้อย

4.2) Cut-through switching สวิตช์จะเริ่มส่งเฟรมทันทีหลังจากอ่าน Destination MAC Address โดยไม่รอรับเฟรมทั้งหมด ข้อดี คือ หน่วงเวลาต่ำมาก เหมาะกับงานที่ต้องการความเร็วสูง ส่วนข้อเสีย อาจส่งต่อเฟรมที่มีข้อผิดพลาด

4.3) Fragment-free switching เป็นวิธีผสมระหว่าง store-and-forward และ cut-through สวิตช์จะรับข้อมูลประมาณ 64 ไบต์แรก ซึ่งเป็นขนาดขั้นต่ำของ Ethernet frame ก่อนเริ่มส่งต่อ เพื่อหลีกเลี่ยงการส่งเฟรมที่เสียหายจาก collision ปัจจุบัน switch ส่วนใหญ่เลือกใช้ store-and-forward เนื่องจากมีความน่าเชื่อถือสูงและรองรับการตรวจสอบข้อผิดพลาดได้ดีกว่า

5) การเรียนรู้ MAC address

Ethernet switch จะสร้าง MAC address table โดยอัตโนมัติผ่านกระบวนการ MAC learning กล่าวคือ ทุกครั้งที่สวิตช์ได้รับเฟรมจะอ่านค่า source MAC address แล้วบันทึกหมายเลขดังกล่าวพร้อมหมายเลขพอร์ตที่รับข้อมูลเข้า หากอุปกรณ์มีการย้ายพอร์ต สวิตช์จะอัปเดตข้อมูลใหม่โดยอัตโนมัติ นอกจากนี้หากไม่มีการใช้งาน MAC address ใดเป็นระยะเวลาหนึ่ง รายการดังกล่าวจะถูกลบออกจากตาราง (MAC aging) เพื่อเพิ่มประสิทธิภาพการจัดเก็บข้อมูล

6) Flooding และ Filtering

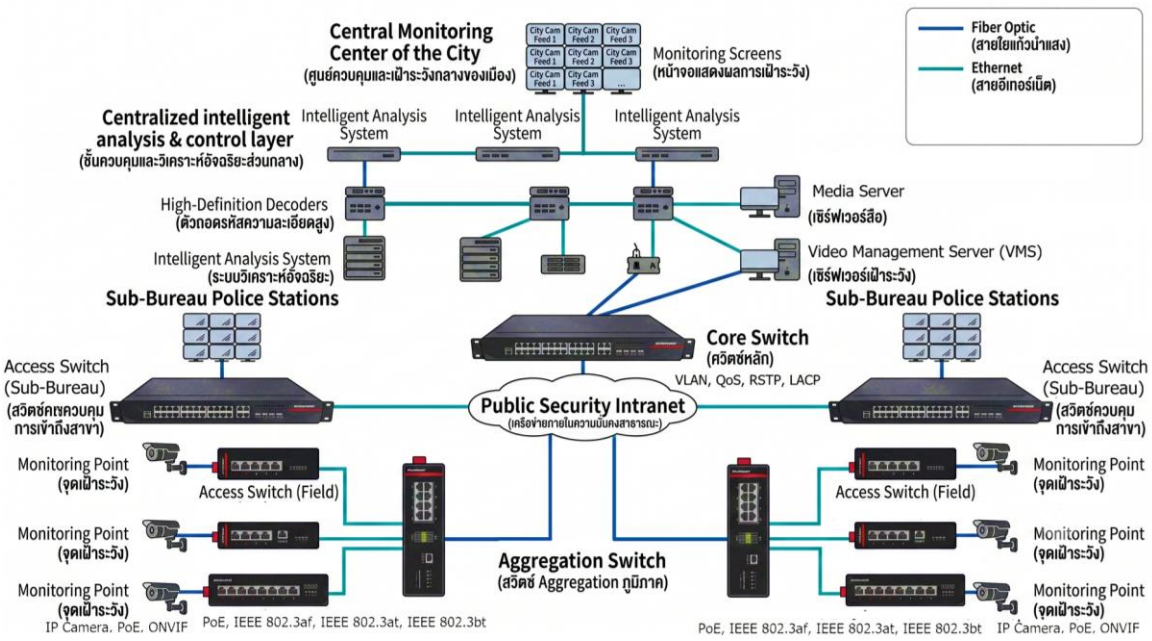
เมื่อสวิตช์ไม่ทราบตำแหน่งของปลายทาง จะใช้วิธี flooding โดยส่งเฟรมออกทุกพอร์ต ยกเว้นพอร์ตที่รับข้อมูลเข้ามา เพื่อค้นหาอุปกรณ์ปลายทาง หลังจากเรียนรู้ตำแหน่งของอุปกรณ์แล้ว สวิตช์จะใช้วิธี filtering โดยส่งเฟรมเฉพาะพอร์ตที่ต้องการเท่านั้น ส่งผลให้ลดทราฟฟิกภายในเครือข่ายและเพิ่มประสิทธิภาพการรับส่งข้อมูล

7) Collision Domain และ Broadcast Domain

การใช้ Ethernet switch ทำให้แต่ละพอร์ตของสวิตช์เป็น collision domain แยกจากกัน ส่งผลให้ไม่เกิดการชนกันของข้อมูลระหว่างอุปกรณ์ที่เชื่อมต่อคนละพอร์ต และรองรับการสื่อสารแบบ full-duplex ได้อย่างมีประสิทธิภาพ อย่างไรก็ตามหากไม่มีการแบ่งเครือข่ายด้วย VLAN ทุกพอร์ตของสวิตช์จะยังคงอยู่ภายใน broadcast domain เดียวกัน ซึ่งหมายความว่าเฟรมประเภท broadcast จะถูกส่งไปยังทุกพอร์ตของสวิตช์ ดังนั้นการกำหนด VLAN จึงเป็นวิธีสำคัญในการลดปริมาณ broadcast traffic และเพิ่มความมั่นคงปลอดภัยของระบบเครือข่ายในระบบ smart security ที่มีการใช้งานกล้อง IP และอุปกรณ์เครือข่ายจำนวนมาก

8) Ethernet switching ในระบบรักษาความปลอดภัยอัจฉริยะ

ในระบบรักษาความปลอดภัยอัจฉริยะ Ethernet switch ทำหน้าที่เป็นศูนย์กลางของการสื่อสารข้อมูล โดยเชื่อมต่ออุปกรณ์ต่าง ๆ เช่น กล้อง IP, NVR, ระบบควบคุมการเข้าออก, เซิร์ฟเวอร์, และอุปกรณ์ IoT เข้าด้วยกัน



รูปที่ 6.14 สถาปัตยกรรมเครือข่าย Ethernet ระบบรักษาความปลอดภัยแบบรวมศูนย์

รูปที่ 6.14 สถาปัตยกรรมเครือข่าย Ethernet สำหรับระบบเฝ้าระวังและรักษาความปลอดภัยแบบรวมศูนย์ ซึ่งประกอบด้วย core layer, aggregation layer และ access layer โดย core

switch ทำหน้าที่เป็นศูนย์กลางในการรับส่งข้อมูลระหว่างศูนย์ควบคุมกลาง (central monitoring center) เซิร์ฟเวอร์ และเครือข่ายสาขา ขณะที่ aggregation switch ทำหน้าที่รวบรวมข้อมูลจาก access switch หลายจุดก่อนส่งเข้าสู่เครือข่ายหลัก ส่วน access switch เชื่อมต่อกับอุปกรณ์ภาคสนาม เช่น กล้องวงจรปิด และจุดเฝ้าระวัง ผ่านสาย Ethernet และรองรับการเชื่อมต่อแบบ PoE การเชื่อมต่อระหว่างอุปกรณ์หลักใช้ สายใยแก้วนำแสง เพื่อรองรับการรับส่งข้อมูลปริมาณมากและระยะทางไกล ส่วนการเชื่อมต่อภายในพื้นที่ใช้ สาย Ethernet สำหรับเชื่อมต่ออุปกรณ์ปลายทาง ระบบดังกล่าวสนับสนุนการประมวลผลด้วย intelligent analysis system และการบริหารจัดการข้อมูลผ่าน media server และ VMS ทำให้สามารถเฝ้าระวัง วิเคราะห์เหตุการณ์ และบริหารจัดการระบบรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ เหมาะสำหรับการประยุกต์ใช้ในระบบรักษาความปลอดภัยขนาดใหญ่ (Forouzan, 2013; Stallings, 2021; IEEE, 2022)

6.8 ไวไฟ (Wi-Fi)

Wi-Fi เป็นเทคโนโลยีเครือข่ายท้องถิ่นแบบไร้สาย (WLAN) ที่พัฒนาขึ้นตามมาตรฐาน IEEE 802.11 เพื่อให้อุปกรณ์อิเล็กทรอนิกส์สามารถรับส่งข้อมูลผ่านคลื่นวิทยุได้โดยไม่ต้องใช้สายสัญญาณ เทคโนโลยีดังกล่าวช่วยเพิ่มความสะดวกในการเชื่อมต่อเครือข่ายและรองรับการสื่อสารของอุปกรณ์หลากหลายประเภท เช่น คอมพิวเตอร์ สมาร์ตโฟน แท็บเล็ต กล้องวงจรปิดไร้สาย และอุปกรณ์ IoT (IEEE, 2020) คำว่า Wi-Fi เดิมเป็นชื่อทางการค้าที่จัดตั้งโดยองค์กร Wi-Fi alliance เพื่อใช้รับรองว่าอุปกรณ์เครือข่ายไร้สายสามารถทำงานร่วมกันได้ตามมาตรฐาน IEEE 802.11 เมื่ออุปกรณ์ผ่านการทดสอบความเข้ากันได้ (interoperability) จะได้รับเครื่องหมาย Wi-Fi certified ซึ่งแสดงว่าอุปกรณ์สามารถสื่อสารกับผลิตภัณฑ์ของผู้ผลิตรายอื่นที่ผ่านการรับรองมาตรฐานเดียวกันได้อย่างมีประสิทธิภาพ

6.8.1 Wi-Fi และ Wireless

คำว่า Wi-Fi และ wireless มักถูกใช้แทนกันในชีวิตประจำวัน แต่ทั้งสองคำมีความหมายแตกต่างกัน โดย wireless เป็นคำทั่วไปที่หมายถึงเทคโนโลยีการสื่อสารทุกประเภทที่ไม่ใช้สายสัญญาณ เช่น Bluetooth, Zigbee, LoRaWAN, cellular network และ Wi-Fi ส่วน Wi-Fi หมายถึงเทคโนโลยีเครือข่ายไร้สายที่ทำงานตามมาตรฐาน IEEE 802.11 โดยเฉพาะ ดังนั้น Wi-Fi จึงถือเป็นเทคโนโลยีหนึ่งภายใต้กลุ่มของระบบสื่อสารแบบไร้สาย

มาตรฐาน IEEE 802.11ได้รับการประกาศใช้อย่างเป็นทางการครั้งแรกในปี ค.ศ. 1997 โดยสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) มาตรฐานที่ได้รับความนิยมในช่วงเริ่มต้น ได้แก่ IEEE 802.11a, IEEE 802.11b และ IEEE 802.11g (Forouzan, 2013; IEEE, 2020) มีคุณลักษณะดังนี้

1) IEEE 802.11a

ทำงานในย่านความถี่ 5 GHz รองรับอัตราการรับส่งข้อมูลสูงสุด 54 Mbps มีข้อดีคือมีสัญญาณรบกวนน้อยและให้ประสิทธิภาพในการสื่อสารสูง อย่างไรก็ตาม ไม่สามารถทำงานร่วมกับอุปกรณ์ที่ใช้มาตรฐาน IEEE 802.11b ซึ่งทำงานบนย่านความถี่ 2.4 GHz ได้

2) IEEE 802.11b

ทำงานในย่านความถี่ 2.4 GHz รองรับอัตราการรับส่งข้อมูลสูงสุดที่11 Mbpsเนื่องจากใช้งานบนย่านความถี่ที่ได้รับความนิยม จึงมีโอกาสเกิดสัญญาณรบกวนจากอุปกรณ์อื่น เช่น ไมโครเวฟ โทรศัพท์ไร้สาย และอุปกรณ์ Bluetooth ได้มากกว่ามาตรฐานที่ใช้ย่านความถี่ 5 GHz

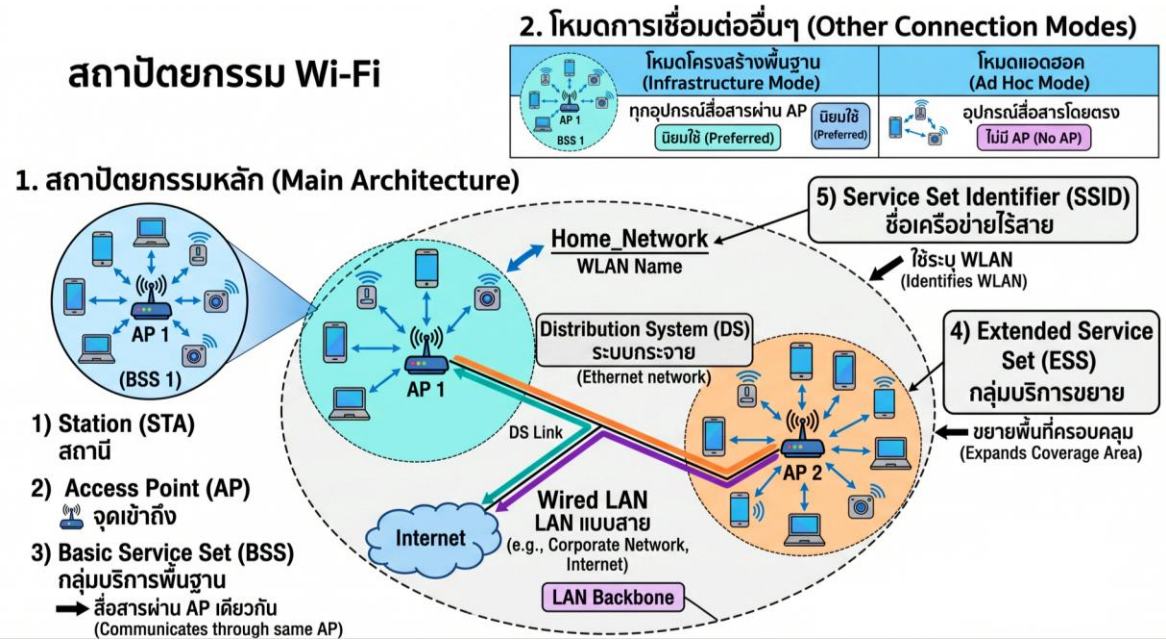
3) IEEE 802.11g

ทำงานในย่านความถี่ 2.4 GHz เช่นเดียวกับ IEEE 802.11b แต่เพิ่มอัตราการรับส่งข้อมูลสูงสุดเป็น 54 Mbps พร้อมทั้งรองรับการทำงานร่วมกับอุปกรณ์ IEEE 802.11b จึงได้รับความนิยมอย่างแพร่หลายในเครือข่ายไร้สายภายในบ้านและสำนักงาน

มาตรฐาน IEEE 802.11 การพัฒนาต่อเนื่อง มาตรฐานรุ่นใหม่ เช่น IEEE 802.11n (Wi-Fi4), IEEE 802.11ac (Wi-Fi5), IEEE 802.11ax (Wi-Fi 6/6E) และ IEEE 802.11be (Wi-Fi 7) ซึ่งรองรับอัตราการรับส่งข้อมูลที่สูงขึ้น ลดความหน่วงของเครือข่าย และเพิ่มประสิทธิภาพในการรองรับอุปกรณ์จำนวนมาก

6.8.2 สถาปัตยกรรม Wi-Fi

โครงสร้างแบบ infrastructure mode เป็นรูปแบบที่นิยมใช้ อุปกรณ์ทุกตัวสื่อสารผ่าน AP ขณะที่ Ad Hoc mode อนุญาตให้อุปกรณ์สื่อสารกันโดยตรงโดยไม่มี AP ดังรูปที่ 6.15



รูปที่ 6.15 สถาปัตยกรรม Wi-Fi

รูปที่ 6.15 องค์ประกอบหลักของเครือข่าย Wi-Fi ประกอบด้วย (1) Station (STA) อุปกรณ์ที่เชื่อมต่อผ่าน Wi-Fi (2) Access Point (AP) อุปกรณ์ที่เชื่อมสถานีไร้สายเข้าสู่ LAN (3) Basic Service Set (BSS) กลุ่มสถานีที่สื่อสารผ่าน AP เดียวกัน (4) Extended Service Set (ESS) การเชื่อมหลาย BSS ผ่าน distribution system เพื่อขยายพื้นที่ครอบคลุม และ (5) Service Set Identifier (SSID) ชื่อเครือข่ายไร้สายที่ใช้ระบุ WLAN

6.8.3 วิธีเข้าถึงสื่อของ Wi-Fi

Wi-Fi ไม่ใช้ CSMA/CD เพราะอุปกรณ์ไร้สายไม่สามารถส่งข้อมูลและตรวจจับ collision ได้อย่างมีประสิทธิภาพในเวลาเดียวกัน จึงใช้ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) กระบวนการพื้นฐานประกอบด้วย (1) ตรวจสอบว่าช่องสัญญาณว่างหรือไม่ (2) รอช่วงเวลาที่กำหนด (3) สุ่มเวลาหน่วงหรือ backoff (4) ส่งเฟรมเมื่อช่องสัญญาณว่าง และ (5) รอ acknowledgment จากผู้รับ ในบางกรณีอาจใช้ Request to Send (RTS) และ Clear to Send (CTS) เพื่อลดปัญหา hidden station

6.8.4 การรักษาความมั่นคงปลอดภัยของ Wi-Fi

แนวทางสำคัญการรักษาความมั่นคงปลอดภัย ได้แก่ (1) ใช้ WPA3 หรืออย่างน้อย WPA2 ที่ใช้ Advanced Encryption Standard (AES) (2) เปลี่ยนรหัสผ่านและบัญชีผู้ดูแลเริ่มต้น (3) ปิด Wi-Fi Protected Setup (WPS) เมื่อไม่จำเป็น (4) แยกเครือข่ายอุปกรณ์ smart security ออกจากเครือข่ายผู้ใช้ทั่วไป (5) กำหนด VLAN ให้กับ SSID แต่ละกลุ่ม (6) ใช้ IEEE 802.1X และระบบ Remote Authentication Dial-In User Service (RADIUS) ในเครือข่ายองค์กร (7) อัปเดต firmware ของ AP และอุปกรณ์ปลายทาง (8) จำกัดการเข้าถึงหน้า management และ (9) ตรวจสอบ rogue access point และอุปกรณ์ที่เชื่อมต่อผิดปกติ

ตารางที่ 6.9 สรุปเปรียบเทียบเครือข่าย LAN, WAN, Ethernet, และ Wi-Fi

หัวข้อ	LAN	WAN	Ethernet	Wi-Fi
ลักษณะ	เครือข่ายพื้นที่จำกัด	เชื่อมเครือข่ายระยะไกล	เทคโนโลยี LAN แบบใช้สาย	เทคโนโลยี LAN แบบไร้สาย
มาตรฐานหลัก	Ethernet/Wi-Fi	หลายเทคโนโลยี	IEEE 802.3	IEEE 802.11
สื่อกลาง	สายหรือไร้สาย	Fiber, Cellular, Microwave, Satellite	Copper/Fiber	คลื่นวิทยุ
อุปกรณ์หลัก	Switch, AP, Router	Router, Firewall, Provider Network	Switch, NIC	Access Point, Wireless Client
ความเสถียร	สูงภายในพื้นที่จำกัด	ขึ้นกับผู้ให้บริการและระยะทาง	สูง	ขึ้นกับสัญญาณและการรบกวน
การใช้งาน Smart Security	เชื่อมอุปกรณ์ภายในสถานที่	เชื่อมหลายสาขาหรือคลาวด์	กล้อง NVR Server Controller	กล้องไร้สายและอุปกรณ์เคลื่อนที่

6.9 Zigbee

Zigbee เป็นเทคโนโลยีการสื่อสารไร้สายสำหรับเครือข่ายส่วนบุคคลแบบใช้พลังงานต่ำ (Low-Rate Wireless Personal Area Network: LR-WPAN) พัฒนาขึ้นบนมาตรฐาน IEEE 802.15.4 มีวัตถุประสงค์เพื่อรองรับการสื่อสารของอุปกรณ์ตรวจวัด และอุปกรณ์ควบคุม ที่ต้องการอัตราการรับส่งข้อมูลต่ำ ใช้พลังงานต่ำ มีต้นทุนต่ำ และสามารถทำงานด้วยแบตเตอรี่ได้นานหลายปี (IEEE, 2020; Gavra et al., 2023) เทคโนโลยี Zigbee ได้รับการพัฒนาโดย Zigbee alliance (ปัจจุบันคือ Connectivity Standards Alliance: CSA) เพื่อสร้างมาตรฐานกลางสำหรับระบบ IoT และระบบอัตโนมัติ โดยกำหนดชั้น network layer, application layer และระบบรักษาความปลอดภัยเพิ่มเติมจากมาตรฐาน IEEE 802.15.4 ทำให้อุปกรณ์จากผู้ผลิตหลายรายสามารถทำงานร่วมกันได้ (Gavra et al., 2023; AlShuhail et al., 2022) เมื่อเปรียบเทียบกับเทคโนโลยี Wi-Fi และ Bluetooth แล้ว Zigbee มีจุดเด่นด้านการใช้พลังงานต่ำ ความสามารถในการสร้างเครือข่ายที่รองรับอุปกรณ์จำนวนมาก และรองรับการสื่อสารแบบ mesh network จึงเหมาะสำหรับระบบ smart home, smart building, ระบบรักษาความปลอดภัย และเครือข่ายเซ็นเซอร์ไร้สาย (Wireless Sensor Networks: WSN) มากกว่าการรับส่งข้อมูลความเร็วสูง เช่น วิดีโอหรือมัลติมีเดีย

6.9.1 ย่านความถี่และอัตราการรับส่งข้อมูล

1) ย่านความถี่และอัตราการรับส่งข้อมูลของ Zigbee

มาตรฐาน IEEE 802.15.4 รองรับการทำงานในย่านความถี่ที่ไม่ต้องขอใบอนุญาต (license-free frequency bands) จำนวน 3 ช่วง ได้แก่ 868 MHz, 902-928 MHz และ 2.4 GHz โดยแต่ละย่านมีจำนวนช่องสัญญาณและอัตราการรับส่งข้อมูลแตกต่างกัน ดังตาราง 6.10 โดยย่านความถี่ 2.4 GHz เป็นย่านที่นิยมใช้งานมากที่สุด เนื่องจากสามารถใช้งานได้ทั่วโลกและรองรับอัตราการรับส่งข้อมูลสูงสุด 250 kbps ซึ่งเพียงพอสำหรับการส่งข้อมูลจากเซ็นเซอร์ ระบบควบคุม และอุปกรณ์ IoT ย่านความถี่ อัตราการรับส่งข้อมูลดังตารางที่ 6.10

2) การกระจายสเปกตรัมและเทคนิคการมอดูเลต

เพื่อเพิ่มความทนทานต่อสัญญาณรบกวนและลดผลกระทบจากการแทรกสอดของคลื่นวิทยุ มาตรฐาน IEEE 802.15.4 ใช้เทคนิค Direct Sequence Spread Spectrum (DSSS) สำหรับทุกย่านความถี่ โดยใช้เทคนิคการมอดูเลตแตกต่างกันตามย่านความถี่ ดังนี้

2.1)ย่าน 2.4 GHz ใช้เทคนิค Offset Quadrature Phase Shift Keying (O-QPSK) ร่วมกับรหัสลำดับเทียม (Pseudo Noise Code: PN Code) ความยาว 32 ชิป (32-chip PN sequence) และใช้แบนด์วิดท์ของสัญญาณประมาณ 2 MHz

2.2)ย่าน 868 MHz และ 915 MHz ใช้เทคนิค Binary Phase Shift Keying (BPSK) ร่วมกับรหัส PN ความยาว 15 ชิป (15-chip PN sequence) โดยใช้แบนด์วิดท์ประมาณ 600 kHz ในยุโรป และ 1.2 MHz ในอเมริกาเหนือ

2.3)การเลือกใช้ DSSS ร่วมกับ BPSK หรือ O-QPSK ช่วยเพิ่มความสามารถในการต้านทานสัญญาณรบกวน (noise immunity) ลดผลกระทบจากการเกิดสัญญาณหลายเส้นทาง

(multipath fading) และทำให้การสื่อสารมีความน่าเชื่อถือมากขึ้น แม้ในสภาพแวดล้อมที่มีคลื่นวิทยุจากอุปกรณ์อื่นจำนวนมาก

ตารางที่ 6.10 คุณลักษณะของย่านความถี่และอัตราการรับส่งข้อมูลของ Zigbee ตามมาตรฐาน IEEE 802.15.4

ย่านความถี่ (Frequency Band)	ช่องสัญญาณ (Channels)	อัตราชิป (Chip Rate)	อัตราการรับ-ส่งข้อมูล (Max Data Rate)	อัตราสัญลักษณ์ (Symbol Rate)	เทคนิคการมอดูเลต (Modulation)	พื้นที่การใช้งาน
868-870 MHz	0 (1 ช่อง)	300 kchip/s	20 kb/s	20 kbaud	BPSK	ยุโรป
902-928 MHz	1-10 (10 ช่อง)	600 kchip/s	40 kb/s	40 kbaud	BPSK	อเมริกาเหนือ ออสเตรเลีย และ นิวซีแลนด์
2.4-2.4835 GHz	11-26 (16 ช่อง)	2.0 Mchip/s	250 kb/s	62.5 kbaud	O-QPSK (16-ary Orthogonal Modulation)	ใช้งานได้ทั่วโลก

3) บทบาทของชั้น PHY และ MAC

มาตรฐาน IEEE 802.15.4 กำหนดหน้าที่ของสองชั้นหลัก ได้แก่

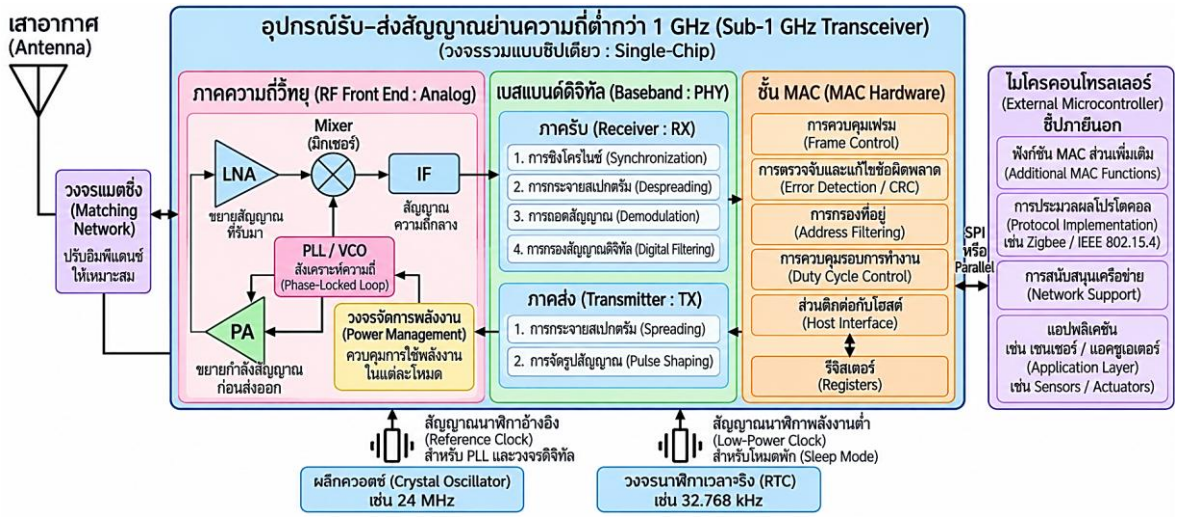
3.1) PHY ทำหน้าที่เกี่ยวกับการรับ-ส่งสัญญาณวิทยุ การเลือกช่องสัญญาณ (channel selection) การมอดูเลตและดีมอดูเลตสัญญาณ การตรวจจับระดับพลังงานของช่องสัญญาณ (Energy Detection: ED) และการประเมินคุณภาพของลิงก์ (Link Quality Indication: LQI)

3.2) MAC ทำหน้าที่ควบคุมการเข้าถึงสื่อกลาง การสร้างและจัดการเฟรมข้อมูล การกำหนดที่อยู่ของอุปกรณ์ การตรวจสอบความถูกต้องของข้อมูล การหลีกเลี่ยงการชนกันของข้อมูลด้วยเทคนิค CSMA/CA รวมถึงการจัดการการเชื่อมต่อและการยกเลิกการเชื่อมต่อของอุปกรณ์ภายในเครือข่าย

กล่าวโดยสรุป IEEE 802.15.4 เป็นมาตรฐาน ที่ออกแบบเพื่อรองรับการสื่อสารไร้สายที่ใช้พลังงานต่ำ ความซับซ้อนต่ำ และมีต้นทุนต่ำ โดยมุ่งเน้นการใช้งานด้านเซ็นเซอร์และการควบคุมมากกว่าการรับส่งข้อมูลความเร็วสูง จึงเป็นรากฐานเครือข่าย IoT ในปัจจุบัน

6.9.2 การออกแบบวงจรความถี่วิทยุสำหรับอุปกรณ์ Zigbee

การออกแบบวงจรความถี่วิทยุ (Radio Frequency: RF) ที่มีผลต่อประสิทธิภาพของอุปกรณ์ Zigbee ระบบจะต้องสามารถรับ–ส่งข้อมูลได้อย่างมีประสิทธิภาพ พร้อมกับใช้พลังงานต่ำ ขนาดเล็ก ต้นทุนไม่สูง ให้เหมาะกับเซนเซอร์และอุปกรณ์ IoT ที่ใช้พลังงานจากแบตเตอรี่ ดังนั้นอุปกรณ์รับ–ส่งสัญญาณสมัยใหม่จึงมักใช้ วงจรรวมแบบชิปเดี่ยว (single-chip transceiver) รวมวงจร RF และวงจรดิจิทัลที่เกี่ยวข้องไว้ภายในชิป เพื่อลดจำนวนอุปกรณ์ภายนอกและลดความซับซ้อนของวงจร ตัวอย่างโครงสร้างของ อุปกรณ์รับ–ส่งสัญญาณย่านต่ำกว่า 1 GHz (sub-1 GHz transceiver) อาจรวมวงจร PHY และฟังก์ชันบางส่วนที่เกี่ยวข้องกับ MAC ไว้ภายในชิป และเชื่อมต่อกับไมโครคอนโทรลเลอร์สำหรับประมวลผลโปรโตคอลและแอปพลิเคชัน อุปกรณ์ภายนอกที่สำคัญอาจประกอบด้วย ผลึกควอตซ์ (crystal) เพื่อสร้างความถี่อ้างอิงให้วงจร เช่น Phase-Locked Loop (PLL) และระบบนาฬิกาดิจิทัล รวมถึง Real-Time Clock (RTC) สำหรับการทำงานที่ใช้พลังงานต่ำ ตัวอย่างโครงสร้างของ sub-1 GHz transceiver (Bhosale& Rajireddy, 2007) ดังรูปที่ 6.16



รูปที่ 6.16 อุปกรณ์รับส่งสัญญาณที่ทำงานในย่านความถี่ต่ำกว่า 1 GHz

6.9.3 หลักการทำงานของ Zigbee

Zigbee ทำงานโดย PHY และ MAC ขณะที่ Zigbee alliance ได้พัฒนา Network Layer (NWK) และ Application Layer (APL) เพิ่ม รองรับการกำหนดเส้นทาง การบริหารเครือข่าย และการทำงานร่วมกันของอุปกรณ์จากผู้ผลิตหลายราย (Gavra et al., 2023) การดังนี้

1) Coordinator สร้างเครือข่ายและกำหนดค่าเครือข่าย

2) Router ทำหน้าที่ขยายระยะทางและกำหนดเส้นทางข้อมูล

3) End device เชื่อมต่อกับ router หรือ coordinator เพื่อส่งข้อมูลจากเซ็นเซอร์หรือรับคำสั่งควบคุม

4) ข้อมูลถูกส่งผ่าน network layer ด้วยเส้นทางที่เหมาะสมที่สุด

5) หากเส้นทางหนึ่งขัดข้อง ระบบ mesh จะค้นหาเส้นทางใหม่โดยอัตโนมัติ (self-healing)

กลไกดังกล่าวทำให้ Zigbee มีความทนทานต่อความเสียหายของโหนดและเพิ่มความน่าเชื่อถือของระบบเครือข่าย (Paul & Singh, 2015; Gavra et al., 2023)

6.9.4 คุณลักษณะของเครือข่าย Zigbee

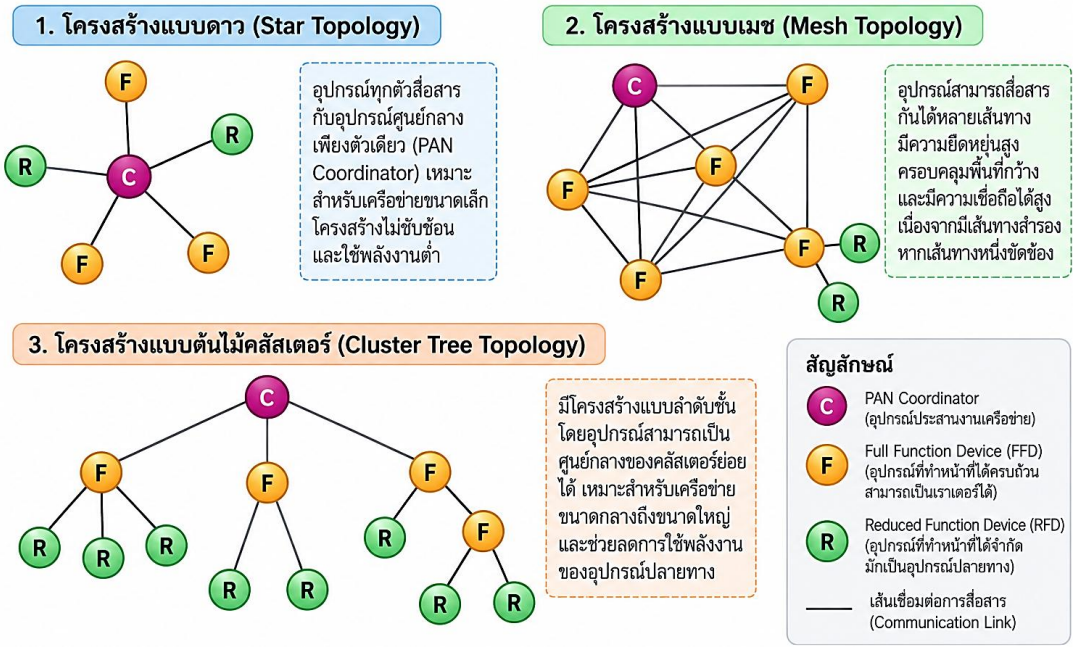
คุณสมบัติเด่นของ Zigbee ได้แก่ ทำงานบนมาตรฐาน IEEE 802.15.4

1) ใช้พลังงานต่ำมาก (ultra-low power)
2) อัตราการรับส่งข้อมูลสูงสุด 250 kbps
3) รองรับอุปกรณ์มากกว่า 65,000 โหนดต่อเครือข่าย
4) รองรับการสื่อสารแบบ star, tree และ mesh network
5) รองรับการทำงานด้วยแบตเตอรี่เป็นเวลาหลายปี
6) มีระบบรักษาความปลอดภัยด้วย AES-128 encryption
7) รองรับการค้นหาอุปกรณ์ (discovery) และการเชื่อมต่ออัตโนมัติ (self-forming network)
8) มีความสามารถในการซ่อมแซมเส้นทางการสื่อสารอัตโนมัติ (self-healing network)

เครือข่าย Zigbee มีคุณสมบัติหลายประการที่ช่วยเพิ่มประสิทธิภาพของการสื่อสารข้อมูล โดยในชั้น PHY มีฟังก์ชันสำคัญ ได้แก่ (1) Energy Detection (ED) สำหรับตรวจวัดระดับพลังงานของช่องสัญญาณ (2) Link Quality Indication (LQI) สำหรับประเมินคุณภาพของลิงก์สื่อสาร และ (3) Clear Channel Assessment (CCA) สำหรับตรวจสอบว่าช่องสัญญาณว่างก่อนเริ่มส่งข้อมูล ในชั้น MAC รองรับทั้งการเข้าถึงสื่อกลางแบบมีการแข่งขัน (contention-based access) และแบบไม่มีการแข่งขัน (contention-free access) โดยกำหนดขนาดเฟรมข้อมูลสูงสุด 128 ไบต์ ซึ่งสามารถบรรจุข้อมูล (payload) ได้สูงสุด 104 ไบต์ นอกจากนี้ยังรองรับการกำหนดหมายเลขอุปกรณ์ทั้งแบบ IEEE address ขนาด 64 bit และ short address ขนาด 16 bit ทำให้สามารถรองรับอุปกรณ์ได้มากกว่า 65,000 โหนด ภายในเครือข่ายเดียว การเข้าถึงสื่อกลางใช้เทคนิค CSMA/CA ซึ่งช่วยลดโอกาสการชนกันของข้อมูล และเพิ่มประสิทธิภาพของการสื่อสารในเครือข่ายไร้สาย คุณสมบัติเหล่านี้ทำให้ Zigbee เหมาะสำหรับงานควบคุมและตรวจวัดที่ต้องการความน่าเชื่อถือสูงและใช้พลังงานต่ำ (Gavra et al., 2023; AlShuhail et al., 2022)

6.9.5 รูปแบบโครงสร้างเครือข่ายของ Zigbee (Zigbee Network Topologies)

Zigbee รองรับโครงสร้างเครือข่ายหลัก 3 รูปแบบ ได้แก่ star topology, mesh topology และ cluster tree topology ซึ่งผู้ใช้งานสามารถเลือกใช้ให้เหมาะสมกับลักษณะของระบบและพื้นที่ติดตั้ง (Bhosale& Rajireddy, 2007; AlShuhail et al., 2022; Gavra et al., 2023)



รูปที่ 6.17 โครงสร้างเครือข่ายของ Zigbee (ดัดแปลงจาก Bhosale& Rajireddy, 2007)

1) Star Topology

Star topology เป็นโครงสร้างเครือข่ายที่อุปกรณ์ทุกตัวติดต่อสื่อสารกับ Zigbee coordinator ตัวเดียว โดยไม่มีการรับส่งข้อมูลผ่านอุปกรณ์อื่น มีโครงสร้างเรียบง่าย ติดตั้งและบริหารจัดการได้ง่าย อีกทั้งอุปกรณ์ปลายทางสามารถเข้าสู่โหมดพัก (sleep mode) ได้เป็นเวลานาน ส่งผลให้ใช้พลังงานต่ำ เหมาะสำหรับเครือข่ายเซ็นเซอร์ที่มีจำนวนอุปกรณ์ไม่มาก

2) Mesh Topology

Mesh topology เป็นโครงสร้างที่อุปกรณ์สามารถสื่อสารผ่านหลายเส้นทาง (multi-hop communication) โดยแต่ละโหนดสามารถทำหน้าที่เป็นตัวส่งต่อข้อมูล (router) ได้ หากเส้นทางหลักเกิดความขัดข้อง ระบบจะค้นหาเส้นทางใหม่โดยอัตโนมัติ ซึ่งช่วยให้เครือข่ายสามารถสร้างเส้นทางการสื่อสารได้โดยอัตโนมัติ และหากโหนดหรือเส้นทางใดเกิดความเสียหายระบบจะเลือกเส้นทางใหม่โดยอัตโนมัติ ทำให้การรับส่งข้อมูลยังคงดำเนินได้อย่างต่อเนื่อง เพิ่มความครอบคลุมของเครือข่ายและความน่าเชื่อถือ ด้านความปลอดภัย Zigbee มีชุดกลไก (security toolbox) สำหรับปกป้องข้อมูล ประกอบด้วยการควบคุมสิทธิ์การเข้าถึง (Access Control List: ACL) การตรวจสอบความสดใหม่ของแพ็กเก็ตข้อมูล (packet freshness) การเข้ารหัสข้อมูลด้วย Advanced Encryption Standard (AES) ขนาด 128 bit กลไกเหล่านี้ช่วยป้องกันการดักฟัง การปลอมแปลงข้อมูล และการโจมตีจากบุคคลที่ไม่ได้รับอนุญาต ทำให้ Zigbee เหมาะสำหรับระบบที่ต้องการความมั่นคงปลอดภัยของข้อมูลสูง

3) Cluster Tree Topology

Cluster tree topology เป็นโครงสร้างแบบผสมระหว่าง star และ mesh โดยแบ่งเครือข่ายออกเป็นหลายกลุ่ม แต่ละกลุ่มมี coordinator หรือ router ทำหน้าที่ควบคุมอุปกรณ์ภายใน

กลุ่ม ข้อมูลสามารถส่งต่อระหว่างคลัสเตอร์ผ่าน router สามารถขยายพื้นที่ครอบคลุมของเครือข่ายได้ง่าย พร้อมทั้งยังคงสามารถรักษาการใช้พลังงานต่ำของอุปกรณ์ปลายทาง

6.9.6 ประเภทของเครือข่าย Zigbee

ในระดับการทำงานของ Zigbee อุปกรณ์สามารถแบ่งออกเป็น 3 ประเภท ได้แก่

1) Zigbee Coordinator

เป็นอุปกรณ์หลักของเครือข่าย ทำหน้าที่ สร้างเครือข่าย (network formation) กำหนดหมายเลขเครือข่าย (PAN ID) บริหารจัดการอุปกรณ์ทั้งหมด เก็บข้อมูลของโหนดภายในเครือข่าย และดูแลความปลอดภัยของเครือข่าย โดยเครือข่าย Zigbee หนึ่งเครือข่ายจะมี coordinator ได้เพียง 1 ตัว

2) Zigbee Router

Router ทำหน้าที่รับและส่งต่อข้อมูลระหว่างโหนดต่าง ๆ ภายในเครือข่าย พร้อมทั้งช่วยขยายระยะครอบคลุมของเครือข่าย และสร้างเส้นทางสำรองเมื่อเกิดความขัดข้องของเส้นทางหลัก

3) Zigbee End Device

End device เป็นอุปกรณ์ปลายทาง เช่น เซ็นเซอร์ สวิตช์ อุปกรณ์ตรวจวัดต่าง ๆ โดยสามารถเป็น RFD หรือ FFD ก็ได้ อุปกรณ์ประเภทนี้ไม่ทำหน้าที่กำหนดเส้นทางข้อมูล และสามารถเข้าสู่โหมดพักเพื่อประหยัดพลังงานได้เป็นเวลานาน

6.9.7 ประเภทของอุปกรณ์ในเครือข่าย Zigbee

มาตรฐาน IEEE 802.15.4 แบ่งอุปกรณ์ออกเป็น 2 ประเภท ได้แก่ Reduced Function Device (RFD) และ Full Function Device (FFD) ซึ่ง Zigbee ใช้เป็นพื้นฐานในการกำหนดบทบาทของอุปกรณ์ภายในเครือข่าย

1) RFD

RFD เป็นอุปกรณ์ที่ออกแบบให้มีโครงสร้างเรียบง่าย ใช้หน่วยความจำ RAM และ ROM ขนาดเล็ก จึงมีต้นทุนต่ำและใช้พลังงานต่ำ โดยทั่วไปจะใช้แบตเตอรี่เป็นแหล่งพลังงาน ทำหน้าที่เป็นอุปกรณ์ปลายทาง เช่น เซ็นเซอร์ตรวจจับอุณหภูมิ เซ็นเซอร์ตรวจจับควัน หรือสวิตช์ไร้สาย โดยอุปกรณ์ RFD สามารถ ค้นหาเครือข่ายที่พร้อมใช้งาน ส่งข้อมูลจากเซ็นเซอร์ ตรวจสอบว่ามีข้อมูลรอรับหรือไม่ ขอรับข้อมูลจาก coordinator เข้าสู่โหมดพักเป็นเวลานานเพื่อลดการใช้พลังงาน อย่างไรก็ตาม RFD ไม่สามารถทำหน้าที่กำหนดเส้นทางข้อมูล (routing) และสามารถติดต่อสื่อสารได้เฉพาะกับอุปกรณ์ประเภท FFD เท่านั้น

2) FFD

FFD เป็นอุปกรณ์ที่มีทรัพยากรระบบมากกว่า RFD จึงสามารถทำหน้าที่เป็น Zigbee coordinator, Zigbee router หรืออุปกรณ์สื่อสารทั่วไป FFD สามารถติดต่อสื่อสารได้ทั้งกับอุปกรณ์ประเภท FFD และ RFD รวมทั้งสามารถกำหนดเส้นทางข้อมูลและบริหารจัดการเครือข่ายได้ โดยทั่วไปมักใช้แหล่งจ่ายไฟถาวร (line powered) ที่รองรับการทำงานต่อเนื่อง

6.10 Z-Wave

Z-Wave เป็นเทคโนโลยีการสื่อสารไร้สายสำหรับระบบควบคุมอัตโนมัติ (wireless home automation protocol) ที่ออกแบบมาโดยเฉพาะสำหรับงาน smart home, building automation และ smart security systems โดยเน้นการใช้พลังงานต่ำ (low power consumption) ความหน่วงต่ำ (low latency) และการสื่อสารที่มีความน่าเชื่อถือสูง เทคโนโลยีนี้เหมาะสำหรับอุปกรณ์ที่ใช้แบตเตอรี่ เช่น เซ็นเซอร์ตรวจจับความเคลื่อนไหว เซ็นเซอร์ประตูหน้าต่าง เซ็นเซอร์ควัน กลอนประตูอัจฉริยะ สวิตช์ไฟอัจฉริยะ และเทอร์โมสแตตอัจฉริยะ แตกต่างจาก Wi-Fi และ Zigbee ที่ทำงานในย่านความถี่ 2.4 GHz เป็นหลัก Z-Wave ใช้งานในย่าน Sub-GHz ISM band (ประมาณ 868 MHz ในยุโรป และ 908 MHz ในสหรัฐอเมริกา) จึงช่วยลดการรบกวนจากอุปกรณ์ Wi-Fi และ Bluetooth ที่ใช้งานอยู่ในย่านความถี่เดียวกัน ส่งผลให้การสื่อสารมีเสถียรภาพมากขึ้นภายในอาคาร

6.10.1 คุณลักษณะของ Z-Wave

Z-Wave ได้รับการออกแบบเพื่อรองรับการสื่อสารข้อมูลปริมาณไม่มาก แต่ต้องการความเชื่อถือได้สูงและประหยัดพลังงาน จึงมีคุณลักษณะที่สำคัญดังนี้

1) ใช้พลังงานต่ำ (low power consumption) เหมาะสำหรับอุปกรณ์ที่ใช้แบตเตอรี่ ซึ่งสามารถทำงานได้เป็นเวลาหลายปีโดยไม่จำเป็นต้องเปลี่ยนแบตเตอรี่บ่อย

2) ทำงานในย่านความถี่ Sub-GHz โดยใช้ความถี่ประมาณ 868 MHz (ยุโรป) และ 908 MHz (สหรัฐอเมริกา) ช่วยลดปัญหาการรบกวนจาก Wi-Fi, Bluetooth และ Zigbee ที่ทำงานในย่าน 2.4 GHz

3) Mesh networking

4) ทุกอุปกรณ์ที่เชื่อมต่อไฟฟ้าสามารถทำหน้าที่เป็น repeater หรือ router เพื่อส่งต่อข้อมูลไปยังอุปกรณ์อื่น ทำให้ขยายระยะการสื่อสาร เพิ่มความน่าเชื่อถือของเครือข่ายได้

5) รองรับการทำงานร่วมกัน (interoperability)

6) อุปกรณ์จากผู้ผลิตหลายรายทำงานร่วมกัน ผ่านมาตรฐาน Z-Wave alliance

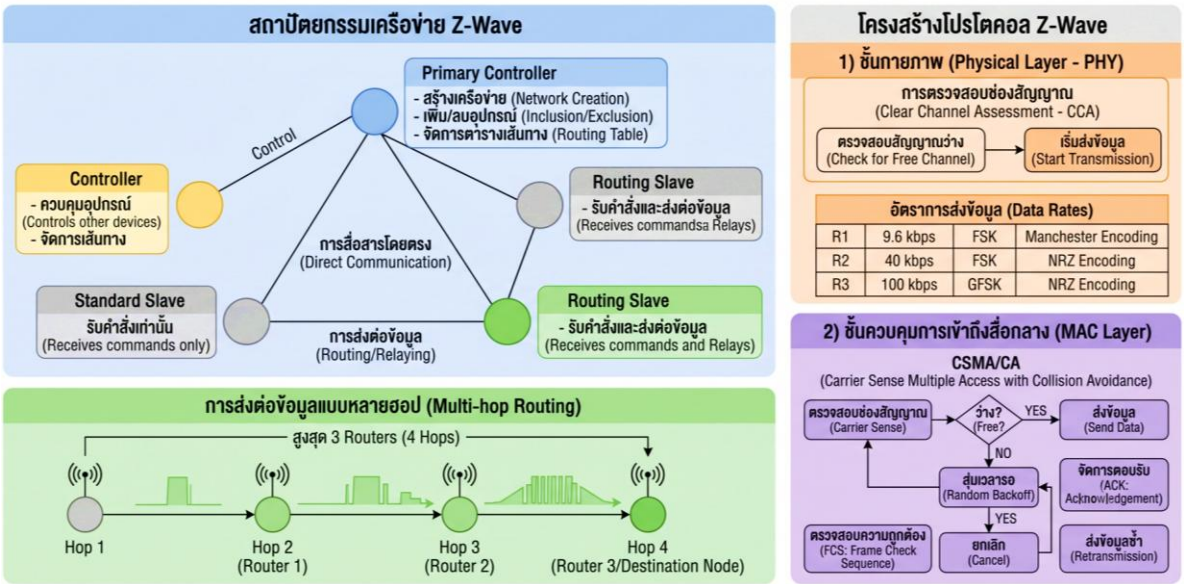
7) ความปลอดภัยสูง

8) รองรับการเข้ารหัสข้อมูล (encryption) และกลไกการยืนยันตัวตนของอุปกรณ์ ช่วยเพิ่มความปลอดภัยให้กับระบบ smart home และระบบรักษาความปลอดภัย

6.10.2 สถาปัตยกรรมเครือข่าย Z-Wave

เครือข่าย Z-Wave ประกอบด้วย controller และ slave nodes ภายในแต่ละเครือข่ายจะมี primary controller ทำหน้าที่สร้างเครือข่ายเพิ่ม (inclusion) และลบ (exclusion) อุปกรณ์ รวมทั้งจัดการตารางเส้นทาง (routing table) ของเครือข่าย อุปกรณ์ในเครือข่ายแบ่งออกเป็น(1) controller ทำหน้าที่ควบคุมอุปกรณ์อื่นและจัดการเส้นทางการสื่อสาร (2) standard slave รับคำสั่งจาก controller เท่านั้น และ (3) routing slave สามารถรับคำสั่งและทำหน้าที่ส่งต่อข้อมูล (relay) ไปยังอุปกรณ์อื่นในเครือข่าย ซึ่งการส่งต่อข้อมูลแบบหลายฮอป (multi-hop routing) เป็นจุดเด่น

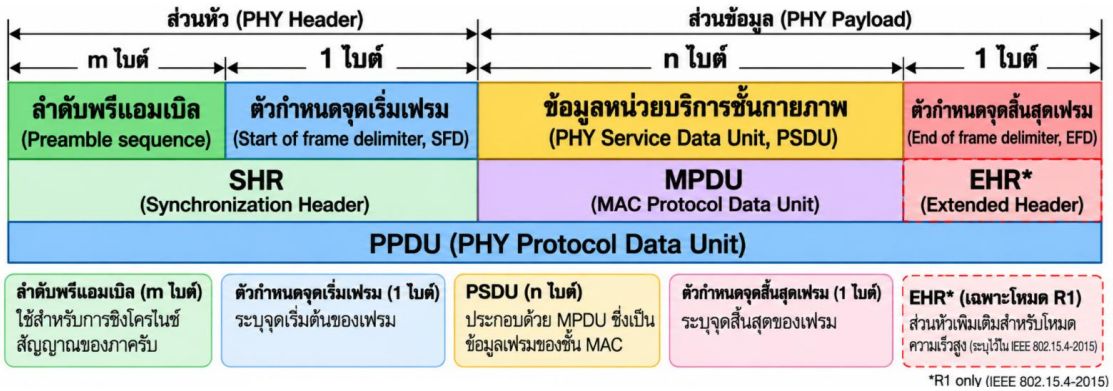
ของ Z-Wave โดยใน Z-Wave แบบดั้งเดิมสามารถส่งต่อข้อมูลผ่าน router ได้สูงสุด 3 ตัว (4 hops) ทำให้สามารถครอบคลุมพื้นที่ภายในบ้านหรืออาคารได้กว้างขึ้น แม้ว่าบางอุปกรณ์จะอยู่นอกระยะของ controller โดยตรงก็ตาม



รูปที่ 6.18 สถาปัตยกรรมเครือข่ายและลำดับชั้นโปรโตคอลของ Z-Wave

1) ชั้นกายภาพ (Physical Layer)

ชั้น PHY ทำหน้าที่ควบคุมการรับ-ส่งข้อมูลผ่านคลื่นวิทยุ โดยการเลือกความถี่ การเปิด-ปิดวงจร RF และการส่งเฟรมข้อมูล ก่อนเริ่มส่งข้อมูลจะมีการตรวจสอบว่าช่องสัญญาณว่างหรือไม่ (clear channel assessment) เพื่อลดการชนกันของข้อมูล



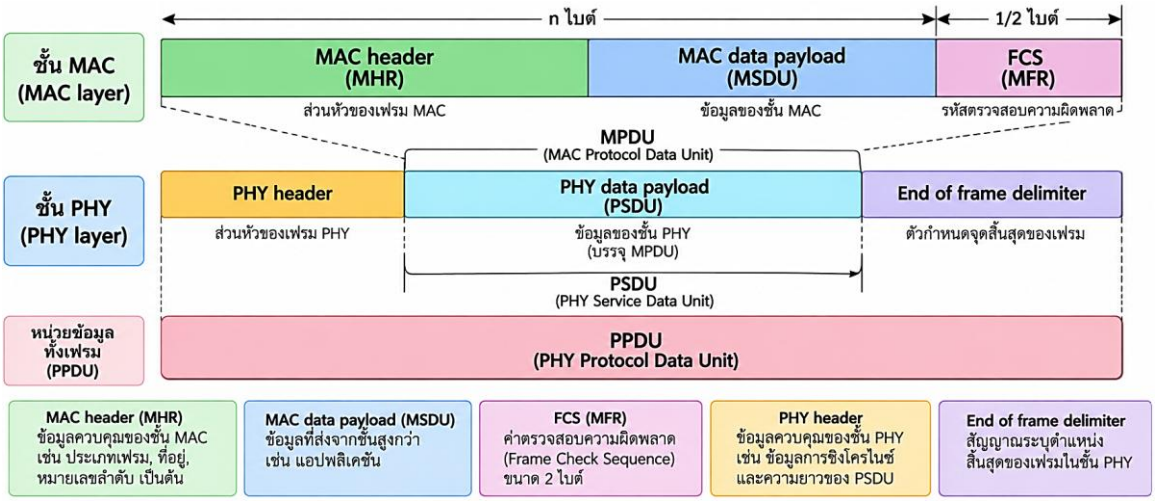
รูปที่ 6.19 รูปแบบทั่วไปของ physical เฟรม

Z-Wave รองรับอัตราการรับส่งข้อมูล 3 ระดับ ได้แก่ (1) R1 ที่ความเร็ว 9.6 kbps (2) R2 ที่ความเร็ว 40 kbps และ (3) R3 ที่ความเร็ว 100 kbps ซึ่งใช้การมอดูเลตประกอบด้วย

(1) FSK สำหรับ R1 และ R2 (2) GFSK (Gaussian Frequency Shift Keying) สำหรับ R3 โดยใช้การเข้ารหัสข้อมูลแบบ Manchester encoding และ Non-Return-to-Zero (NRZ) ตามอัตราการรับส่งข้อมูลแต่ละระดับ

2) ชั้นควบคุมการเข้าถึงสื่อกลาง (MAC Layer)

MAC layer ทำหน้าที่ควบคุมการเข้าถึงช่องสัญญาณ ตรวจสอบความถูกต้องของข้อมูล (FCS) จัดการการตอบรับ (ACK) และการส่งข้อมูลซ้ำ (retransmission) โดย Z-wave ใช้วิธี CSMA/CA โดยจะตรวจสอบว่าช่องสัญญาณว่างก่อนส่งข้อมูล หากช่องสัญญาณไม่ว่าง ระบบจะสุ่มเวลารอ (random backoff) ก่อนเริ่มส่งใหม่ ซึ่งช่วยลดโอกาสการชนกันของข้อมูลและเพิ่มความน่าเชื่อถือของการสื่อสาร



รูปที่ 6.20 รูปแบบทั่วไปของ MAC เฟรม

6.10.3 โหนดในเครือข่าย Z-Wave (Z-Wave Nodes)

ภายในเครือข่าย Z-Wave อุปกรณ์ทุกชนิดที่เข้าร่วมการสื่อสารเรียกว่า โหนด (node) โดยแต่ละโหนดจะได้รับ Node ID ซึ่งเป็นหมายเลขประจำตัวที่ไม่ซ้ำกันภายในเครือข่าย เพื่อใช้ในการระบุอุปกรณ์และรับ-ส่งข้อมูลระหว่างกัน โหนดทั้งหมดภายในเครือข่ายเดียวกันจะใช้ Home ID เดียวกัน ซึ่งทำหน้าที่เป็นหมายเลขประจำเครือข่าย ทำให้อุปกรณ์สามารถสื่อสารได้เฉพาะกับอุปกรณ์ที่อยู่ในเครือข่ายเดียวกันเท่านั้น โหนดในระบบ Z-Wave มีบทบาทแตกต่างกันตามหน้าที่และลักษณะการใช้พลังงาน โดยสามารถแบ่งออกเป็นหลายประเภท ดังนี้

1) Controller Node

Controller node เป็นโหนดที่ทำหน้าที่ควบคุมและบริหารจัดการเครือข่าย Z-Wave ทั้งหมด โดยทำหน้าที่สร้างเครือข่าย กำหนด home ID และ node ID เพิ่มหรือลบอุปกรณ์ รวมทั้งกำหนดเส้นทางการรับส่งข้อมูล ระหว่างโหนดต่าง ๆ controller แบ่งออกเป็น 2 ประเภท ได้แก่

1.1) Primary controller เป็นตัวควบคุมหลักที่สร้างเครือข่ายและบริหารจัดการอุปกรณ์ทั้งหมด

1.2) Secondary controller เป็นตัวควบคุมรองที่ได้รับข้อมูลเครือข่ายจาก primary controller และสามารถควบคุมอุปกรณ์ภายในเครือข่ายได้ แต่ไม่สามารถสร้างเครือข่ายใหม่ได้

ในระบบ smart home ปัจจุบัน controller มักอยู่ในรูปของ smart home hub, gateway หรือ central controller ซึ่งเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อให้ผู้ใช้สามารถควบคุมอุปกรณ์ผ่านสมาร์ตโฟนหรือระบบ cloud ได้

2) Slave Node

Slave node เป็นโหนดที่ทำหน้าที่รับคำสั่งจาก controller และดำเนินการตามคำสั่งที่ได้รับ โดยไม่สามารถควบคุมอุปกรณ์อื่นได้โดยตรง ตัวอย่างของ slave node ได้แก่ smart plug, smart switch, smart bulb, smart door lock, thermostat, หรือ curtain controller โดย slave node จะตอบสนองต่อคำสั่งจาก controller เช่น เปิด-ปิดอุปกรณ์ ปรับระดับความสว่าง ล็อกหรือปลดล็อกประตู

3) Routing Slave Node

Routing slave node เป็น slave node ที่มีความสามารถเพิ่มเติมในการทำหน้าที่เป็น router หรือ repeater สำหรับส่งต่อข้อมูลระหว่างโหนดต่าง ๆ ภายในเครือข่ายโดยทั่วไป routing slave เป็นอุปกรณ์ที่ได้รับพลังงานจากแหล่งจ่ายไฟหลัก (mains powered devices) เช่น smart switch, smart plug, wall controller, หรือ smart dimmer เมื่อมีการรับข้อมูลจาก controller หรือโหนดอื่น อุปกรณ์ประเภทนี้สามารถส่งต่อข้อมูลไปยังโหนดปลายทาง ทำให้เครือข่ายสามารถสื่อสารแบบหลายฮอป (multi-hop communication) ได้ ส่งผลให้ครอบคลุมพื้นที่ได้กว้างขึ้นและเพิ่มความน่าเชื่อถือของเครือข่าย

4) End Node หรือ Battery-powered Node

End node หรือ battery-powered node เป็นอุปกรณ์ที่ใช้พลังงานจากแบตเตอรี่ จึงได้รับการออกแบบให้ใช้พลังงานต่ำที่สุด ตัวอย่างอุปกรณ์ ได้แก่ motion sensor, door/window sensor, smoke detector, gas sensor, flood sensor, หรือ temperature sensor เพื่อประหยัดพลังงาน อุปกรณ์เหล่านี้จะเข้าสู่ sleep mode เป็นส่วนใหญ่ และจะตื่นขึ้น (wake up) เฉพาะเมื่อถึงรอบเวลาที่กำหนดหรือเมื่อเกิดเหตุการณ์สำคัญ เช่น การตรวจพบการเคลื่อนไหว การเปิดประตู หรือการตรวจพบควัน จากนั้นจึงส่งข้อมูลไปยัง Controller ก่อนกลับเข้าสู่โหมดพักอีกครั้ง เนื่องจากต้องประหยัดพลังงาน end node จึงไม่ทำหน้าที่ routing node และไม่ส่งต่อข้อมูลให้กับอุปกรณ์อื่น

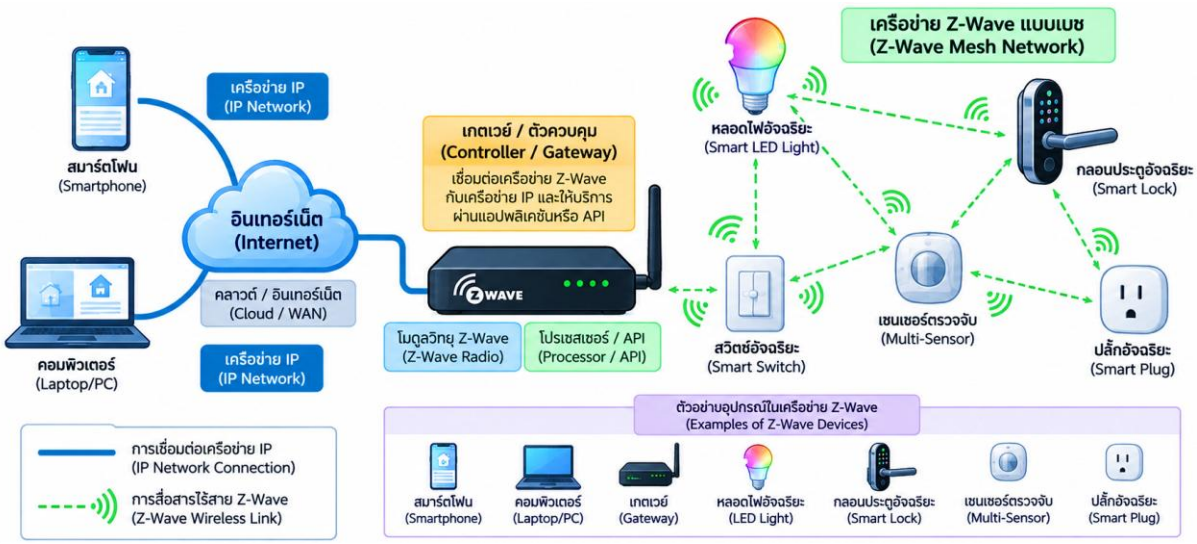
5) Frequently Listening Routing Slave (FLiRS)

อุปกรณ์บางประเภท เช่น smart door lock, battery-powered siren เป็นต้องตอบสนองต่อคำสั่งอย่างรวดเร็ว แม้ว่าจะใช้พลังงานจากแบตเตอรี่ จึงใช้กลไก FLiRS จะไม่เปิดตัวรับสัญญาณตลอดเวลา แต่จะตื่นขึ้นเป็นช่วงสั้น ๆ เพื่อฟังสัญญาณจาก controller หากพบคำสั่ง ระบบจะเปิดการทำงานทันที วิธีการนี้ช่วยลดการใช้พลังงาน ขณะเดียวกันยังคงสามารถตอบสนองต่อคำสั่งได้รวดเร็วกว่าการใช้ sleep mode แบบปกติ

6) Virtual Node

Virtual node เป็นโหนดเสมือนที่ไม่มีฮาร์ดแวร์จริง แต่ถูกสร้างขึ้นภายใน controller หรือ gateway เพื่อใช้จัดกลุ่มอุปกรณ์หลายตัวเข้าด้วยกัน เช่น การสร้างกลุ่มไฟส่องสว่างทั้งชั้น หรือ

กลุ่มอุปกรณ์รักษาความปลอดภัย เพื่อให้สามารถควบคุมอุปกรณ์หลายตัวพร้อมกันได้ด้วยคำสั่งเดียว



รูปที่ 6.21 โทโพโลยีของโหนดในเครือข่ายบ้านอัจฉริยะ Z-Wave

ความสัมพันธ์ระหว่างโหนดในเครือข่าย Z-Wave คือ เมื่อมีการส่งคำสั่งจาก controller ไปยังอุปกรณ์ปลายทาง หากอุปกรณ์ดังกล่าวอยู่นอกระยะการสื่อสารโดยตรง controller จะเลือกเส้นทางผ่าน routing slave node ที่เหมาะสมที่สุด เพื่อส่งข้อมูลไปยังปลายทาง เมื่ออุปกรณ์ปลายทางได้รับคำสั่งแล้ว จะส่งข้อมูลตอบกลับ (ACK) ผ่านเส้นทางเดียวกันหรือเส้นทางอื่นที่มีประสิทธิภาพกว่า ทำให้เครือข่ายมีความยืดหยุ่นและสามารถทำงานได้แม้บางโหนดจะไม่พร้อมใช้งาน

6.10.4 รูปแบบการทำงานของอุปกรณ์เครือข่าย Z-Wave

Z-Wave รองรับโหมดการทำงานหลัก 2 รูปแบบ ได้แก่

1) Always Listening (AL)

อุปกรณ์เปิดตัวรับสัญญาณตลอดเวลา จึงมีค่าความหน่วงต่ำ เหมาะสำหรับอุปกรณ์ที่ใช้ไฟฟ้าจากแหล่งจ่ายหลัก เช่น สวิตช์ไฟอัจฉริยะ

2) Frequently Listening (FL)

ตัวรับสัญญาณจะเปิดเป็นช่วง ๆ ตามเวลาที่กำหนดเพื่อตรวจสอบว่ามีข้อมูลส่งเข้ามาหรือไม่ ช่วยลดการใช้พลังงาน เหมาะสำหรับเซ็นเซอร์ที่ใช้แบตเตอรี่ เช่น เซ็นเซอร์ประตู เซ็นเซอร์ควัน และเซ็นเซอร์ตรวจจับความเคลื่อนไหว

6.11 LoRaWAN (Long Range Wide Area Network)

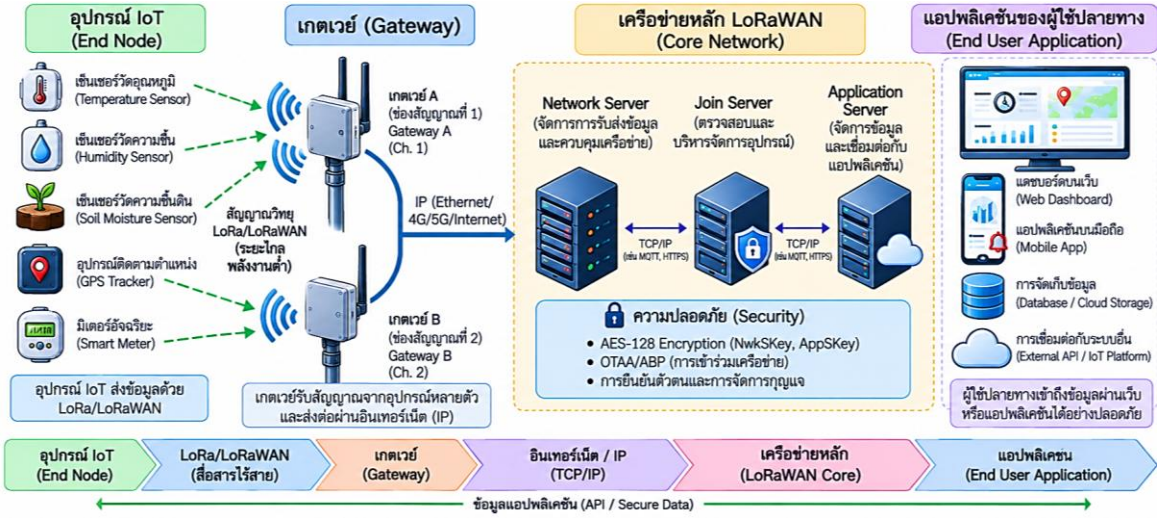
6.11.1 ความหมายของ LoRaWAN

LoRaWAN เป็นโปรโตคอลการสื่อสารสำหรับเครือข่าย Low-Power Wide Area Network (LPWAN) ที่ได้รับการออกแบบมาเพื่อรองรับอุปกรณ์ IoT ซึ่งต้องการสื่อสารข้อมูลในระยะไกลโดยใช้พลังงานต่ำ โปรโตคอลดังกล่าวได้รับการกำหนดมาตรฐานโดย LoRa alliance เพื่อให้สามารถเชื่อมต่ออุปกรณ์จากผู้ผลิตหลายรายเข้าด้วยกันได้อย่างมีประสิทธิภาพและเกิดความสามารถในการทำงานร่วมกัน (interoperability) ระหว่างอุปกรณ์ (LoRa alliance, 2024) LoRaWAN ทำงานบนชั้น MAC layer และกำหนดรูปแบบการสื่อสารระหว่างอุปกรณ์ปลายทาง (end devices) เกตเวย์ (gateway) และเซิร์ฟเวอร์เครือข่าย (network server) โดยใช้เทคนิคการมอดูเลชัน LoRa Chirp Spread Spectrum (CSS) ในชั้นกายภาพ (PHY) ซึ่งช่วยให้สามารถส่งข้อมูลได้ในระยะไกล มีความทนทานต่อสัญญาณรบกวน และใช้พลังงานต่ำ เหมาะสำหรับงานที่ต้องการส่งข้อมูลเป็นช่วงเวลาห่างกัน เช่น การวัดค่าจากเซ็นเซอร์ การติดตามทรัพย์สิน และระบบสมาร์ตซิตี้

6.11.2 หลักการทำงานของ LoRaWAN

สถาปัตยกรรมของ LoRaWAN ประกอบด้วยองค์ประกอบสำคัญ ได้แก่ end device, gateway, network server และ application server โดย end device จะรับข้อมูลจากเซ็นเซอร์และส่งผ่านการสื่อสารวิทยุที่ใช้ LoRa modulation ไปยัง gateway ซึ่งทำหน้าที่เป็นตัวกลางส่งต่อแพ็กเก็ตระหว่างเครือข่ายวิทยุกับเครือข่าย IP จากนั้นข้อมูลจะถูกส่งไปยัง network server เพื่อจัดการเครือข่าย เช่น ตรวจสอบความถูกต้องและความมั่นคงปลอดภัยของแพ็กเก็ต การกำจัดแพ็กเก็ตซ้ำ และจัดการเส้นทางการส่งข้อมูล ก่อนส่งข้อมูลที่เกี่ยวข้องไปยัง application server สำหรับประมวลผล จัดเก็บ และนำไปใช้ในแอปพลิเคชัน เช่น dashboard หรือ cloud platform (LoRa Alliance, 2024; Bonilla et al., 2023)

LoRaWAN ใช้สถาปัตยกรรมแบบ star-of-stars ซึ่งแตกต่างจากเครือข่ายแบบ mesh เช่น Zigbee ที่โหนดบางประเภทสามารถส่งต่อข้อมูลให้โหนดอื่นเพื่อขยายพื้นที่ครอบคลุม ใน LoRaWAN end device ไม่ทำหน้าที่เป็น relay แต่จะส่งสัญญาณโดยตรงไปยัง gateway ที่อยู่ในระยะรับสัญญาณ ดังนั้นแพ็กเก็ตเดียวกันอาจถูกรับโดย gateway หลายตัวและส่งต่อไปยัง Network Server ซึ่งจะทำหน้าที่กำจัดข้อมูลซ้ำและจัดการการสื่อสารของเครือข่าย วิธีนี้ช่วยลดความซับซ้อนและภาระการประมวลผลของ end device นอกจากนี้ end device สามารถเข้าสู่ sleep mode ตามรูปแบบการทำงานของอุปกรณ์และคลาสของ LoRaWAN เพื่อลดการใช้พลังงาน ทำให้ LoRaWAN เหมาะสำหรับระบบ IoT ที่ต้องการ การสื่อสารระยะไกล ใช้พลังงานต่ำ รองรับอุปกรณ์จำนวนมาก ใช้งานในพื้นที่กว้าง เช่น ระบบตรวจวัดสิ่งแวดล้อม เกษตรอัจฉริยะ และตรวจสอบความปลอดภัยจากระยะไกล



รูปที่ 6.22 สถาปัตยกรรมเครือข่ายและการสื่อสารของ LoRaWAN สำหรับระบบ IoT

6.11.3 คุณลักษณะของ LoRaWAN

LoRaWAN มีคุณสมบัติสำคัญ ได้แก่

1) รองรับการสื่อสารระยะไกลประมาณ 2-5 km ในเมือง และ 10-20 km ในพื้นที่ชนบท ทั้งนี้ขึ้นอยู่กับสภาพแวดล้อม เสาอากาศ และกำลังส่ง

2) ใช้พลังงานต่ำมาก ทำให้อุปกรณ์สามารถใช้แบตเตอรี่ได้นานหลายปี

3) รองรับอุปกรณ์จำนวนหลายหมื่นตัวต่อ gateway

4) ใช้ย่านความถี่ ISM band ที่ไม่ต้องขอใบอนุญาต เช่น 433 MHz, 470 MHz, 868 MHz (Europe), 915 MHz (North America), 923 MHz (Asia)

5) รองรับ Adaptive Data Rate (ADR)

6) มีความสามารถในการทะลุผ่านสิ่งกีดขวางได้ดีกว่าระบบสื่อสารระยะสั้น

7) เหมาะกับการส่งข้อมูลปริมาณน้อยเป็นระยะ ๆ มากกว่าการสื่อสารแบบ real-time หรือการส่งภาพและวิดีโอ (LoRa Alliance, 2024; Bonilla et al., 2023)

6.11.4 คลาสของอุปกรณ์ LoRaWAN

LoRaWAN กำหนดการทำงานของอุปกรณ์ปลายทางออกเป็น 3 คลาส ได้แก่

1) Class A

เป็นคลาสพื้นฐานที่อุปกรณ์ทุกตัวต้องรองรับ ใช้พลังงานต่ำที่สุด เปิดหน้าต่างรับข้อมูล (receive windows) หลังจากส่งข้อมูลขึ้น (uplink) เท่านั้น และ เหมาะสำหรับเซ็นเซอร์ที่ส่งข้อมูลเป็นช่วงเวลา

2) Class B

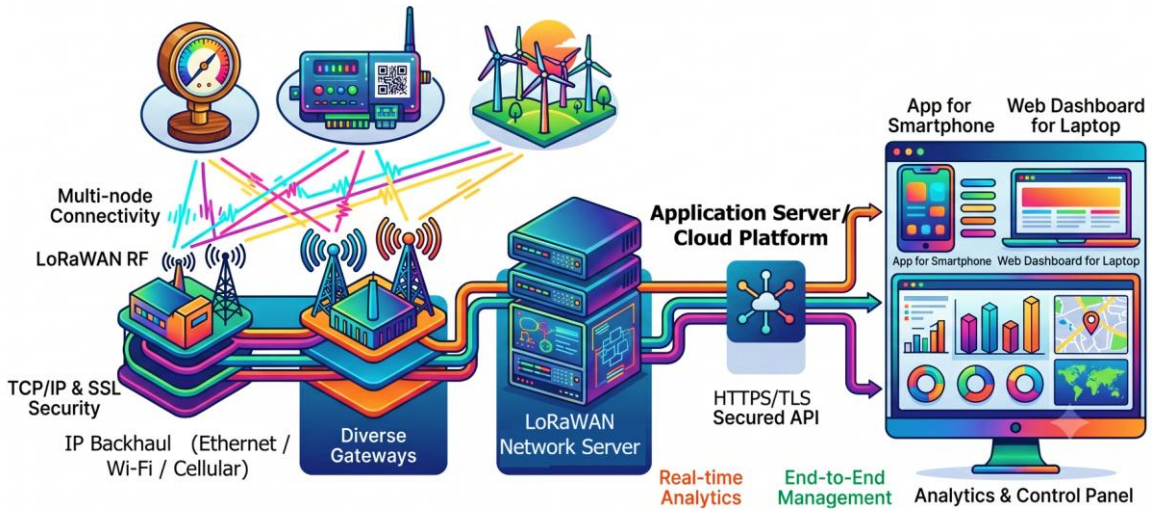
เพิ่ม receive window ตาม beacon จาก gateway โดยลดเวลาในการรอ downlink ใช้พลังงานมากกว่า class A และเหมาะสำหรับระบบควบคุมอุปกรณ์

3) Class C

เปิดรับข้อมูลตลอดเวลา จะมีความหน่วงเวลาต่ำที่สุด ใช้พลังงานสูงที่สุด เหมาะสำหรับอุปกรณ์ที่ใช้ไฟเลี้ยงตลอดเวลา เช่น smart controller หรือ industrial controller

6.11.5 สถาปัตยกรรมเครือข่าย LoRaWAN

LoRaWAN ใช้โครงสร้างเครือข่ายแบบ star-of-stars topology ซึ่งแตกต่างจาก Zigbee ที่ใช้ mesh network โดยอุปกรณ์ปลายทางจะสื่อสารกับ gateway โดยตรง ไม่จำเป็นต้องส่งข้อมูลผ่านอุปกรณ์ตัวกลาง ทำให้ลดความซับซ้อนของระบบและลดการใช้พลังงานของอุปกรณ์ปลายทาง องค์ประกอบของเครือข่ายประกอบด้วย end devices, LoRa gateway, IP backhaul, network server, join server, และ application server ในระบบเดียวกัน ข้อมูลจาก end device อาจถูก gateway หลายตัวรับพร้อมกัน จากนั้น network server จะเลือกแพ็กเก็ตที่มีคุณภาพดีที่สุดเพื่อนำไปประมวลผล ซึ่งช่วยเพิ่มความน่าเชื่อถือของการรับส่งข้อมูล (LoRa Alliance, 2024)



รูปที่ 6.23 สถาปัตยกรรมของเครือข่าย LoRaWAN และการเชื่อมต่อกับระบบ cloud

รูปที่ 6.23 สถาปัตยกรรมของเครือข่าย LoRaWAN โดยอุปกรณ์ end devices ส่งข้อมูลผ่านสัญญาณ LoRa ไปยัง gateway จากนั้นข้อมูลจะถูกส่งผ่านเครือข่าย IP (Ethernet, Wi-Fi หรือ Cellular) ไปยัง LoRaWAN network server และ application server/cloud platform เพื่อประมวลผล จัดเก็บ และแสดงผลผ่านแอปพลิเคชันบนสมาร์ตโฟนหรือ Web dashboard โดยการสื่อสารกับผู้ใช้งานใช้โปรโตคอล HTTPS/TLS เพื่อรักษาความปลอดภัยของข้อมูล

6.11.6 โครงสร้างพื้นฐานของเครือข่าย LoRaWAN

โครงสร้างเครือข่ายพื้นฐานของระบบ LoRaWAN สำหรับการประมวลผลและแสดงผลแก่ผู้ใช้งาน มีดังนี้

1) เครือข่ายสาธารณะ (Public Networks)

เครือข่ายแบบสาธารณะ ให้บริการโดยผู้ให้บริการโทรคมนาคมหรือผู้ให้บริการเครือข่ายสื่อสาร (telecommunication operators หรือ communication providers) ซึ่งใช้ประโยชน์

จากโครงสร้างพื้นฐานด้านการสื่อสารที่มีอยู่เดิม เพื่อให้บริการเครือข่าย LoRaWAN แก่ผู้ใช้งานในรูปแบบการสมัครสมาชิก (subscription-based service) เช่นเดียวกับบริการเครือข่ายโทรศัพท์เคลื่อนที่ เครือข่ายลักษณะนี้มักครอบคลุมพื้นที่ระดับประเทศ ทำให้บริษัทหรือองค์กรที่พัฒนาโซลูชัน IoT สามารถสมัครใช้บริการได้โดยไม่จำเป็นต้องลงทุนติดตั้งโครงสร้างพื้นฐานด้วยตนเอง

2) เครือข่ายชุมชน (Community-Based Networks)

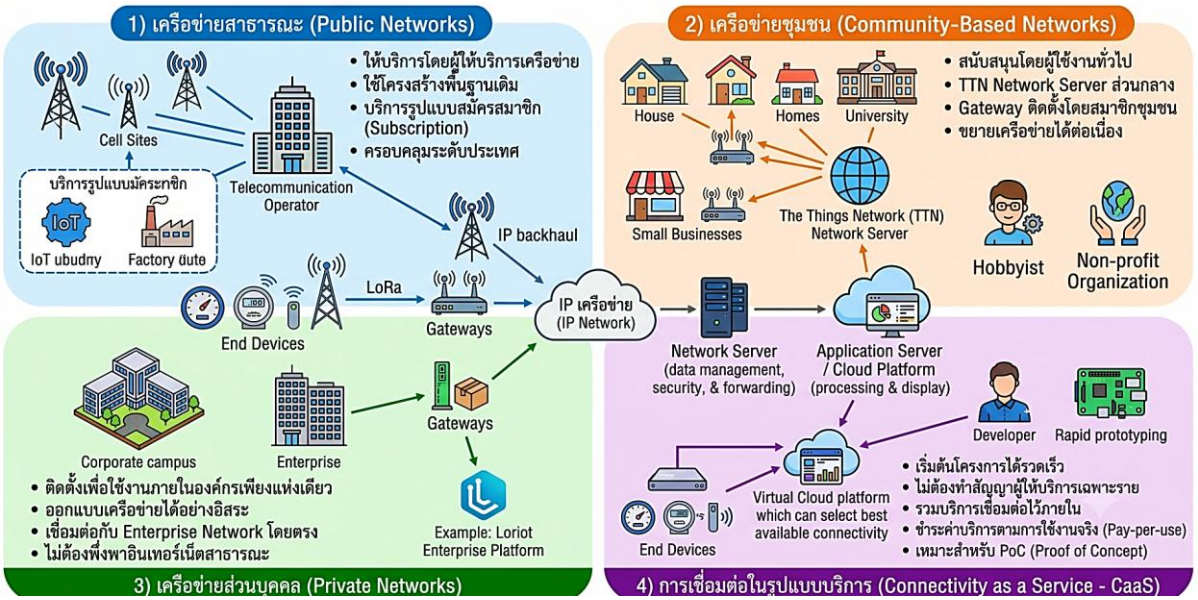
เครือข่ายชุมชนเป็นเครือข่ายที่ได้รับการสนับสนุนจากผู้ใช้งานทั่วไป เช่น นักพัฒนาสมัครเล่น (hobbyists) องค์กรไม่แสวงหากำไร และธุรกิจขนาดเล็ก ตัวอย่างที่ได้รับความนิยมคือ The Things Network (TTN) ซึ่งให้บริการโครงสร้างพื้นฐานของ network server สำหรับชุมชนผู้ใช้งาน LoRaWAN ทั่วโลก ในขณะที่ gateway จะถูกติดตั้งโดยสมาชิกของชุมชนเองตามพื้นที่ที่ต้องการเพิ่มความครอบคลุมของสัญญาณ ทำให้เครือข่ายสามารถขยายตัวได้อย่างต่อเนื่องตามความต้องการของผู้ใช้งาน

3) เครือข่ายส่วนบุคคล (Private Networks)

เครือข่ายส่วนบุคคลเป็นเครือข่ายที่องค์กรหรือหน่วยงานติดตั้งขึ้น เพื่อรองรับการใช้งานภายในองค์กรเพียงแห่งเดียว ไม่ได้ให้บริการแก่ผู้ใช้งานภายนอก ข้อดีของเครือข่ายประเภทนี้คือ ผู้ดูแลระบบสามารถออกแบบและกำหนดค่าการทำงานของเครือข่ายให้เหมาะสมกับอุปกรณ์ IoT ขององค์กรได้อย่างอิสระ อีกทั้งยังสามารถเชื่อมต่อเครือข่าย LoRaWAN เข้ากับระบบเครือข่ายภายใน (enterprise network) ได้โดยไม่จำเป็นต้องพึ่งพาเครือข่ายอินเทอร์เน็ตสาธารณะ ตัวอย่างผู้ให้บริการระบบเครือข่ายส่วนบุคคล ได้แก่ Loriot ซึ่งให้บริการแพลตฟอร์ม LoRaWAN ระดับองค์กร (enterprise-grade LoRaWAN) ที่สามารถติดตั้งและบริหารจัดการเครือข่ายขององค์กรได้อย่างมีประสิทธิภาพ และยังสามารถนำไปพัฒนาเป็นบริการเชิงพาณิชย์ได้

4) การเชื่อมต่อในรูปแบบบริการ (Connectivity as a Service: CaaS)

CaaS เป็นรูปแบบการให้บริการที่ช่วยให้ผู้พัฒนาระบบ IoT สามารถเริ่มต้นโครงการที่ใช้ LoRaWAN ได้อย่างรวดเร็ว โดยไม่จำเป็นต้องทำสัญญาใช้บริการกับผู้ให้บริการเครือข่ายรายใดรายหนึ่ง ในรูปแบบนี้ แพลตฟอร์ม IoT จะรวมบริการด้านการเชื่อมต่อเครือข่ายไว้ภายใน ผู้ใช้งานสามารถเลือกใช้เครือข่ายที่เหมาะสมและเชื่อมต่ออุปกรณ์เข้าสู่ Cloud ได้โดยตรง ทำให้สามารถพัฒนาโครงการต้นแบบ (Proof of Concept: PoC) ได้อย่างรวดเร็ว ลดภาระในการลงทุนโครงสร้างพื้นฐาน และชำระค่าบริการตามการใช้งานจริง เช่น จำนวนอุปกรณ์ที่เชื่อมต่อกับระบบ Cloud ในแต่ละเดือน จึงมีความยืดหยุ่นสูงและเหมาะสำหรับการทดลองหรือการพัฒนาระบบในระยะเริ่มต้น



รูปที่ 6.24 โครงสร้างพื้นฐานของเครือข่าย LoRaWAN

6.11.7 ความปลอดภัยของ LoRaWAN

LoRaWAN ได้รับการออกแบบให้มีระบบรักษาความปลอดภัยแบบ end-to-end โดยใช้ AES-128 encryption, Message Integrity Code (MIC), Network Session Key (NwkSKey), Application Session Key (AppSKey) การเข้ารหัสข้อมูลแบ่งออกเป็นสองระดับ ได้แก่

1) Network security สำหรับตรวจสอบความถูกต้องของแพ็กเก็ตและป้องกันการปลอมแปลงข้อมูล

2) Application security สำหรับเข้ารหัสข้อมูลตั้งแต่เซ็นเซอร์จนถึง application server ทำให้ gateway และผู้ให้บริการเครือข่ายไม่สามารถอ่านข้อความภายในได้

LoRaWAN รองรับการเข้าร่วมเครือข่ายสองรูปแบบ ได้แก่ Over-the-Air Activation (OTAA) และ Activation by Personalization (ABP) โดย OTAA เป็นวิธีที่แนะนำ เนื่องจากสามารถสร้าง session keys ใหม่ทุกครั้งที่เชื่อมต่อ ทำให้มีความปลอดภัยสูงกว่า ABP ซึ่งใช้คีย์เดิมตลอดอายุการใช้งาน

6.11.8 การประยุกต์ใช้ LoRaWAN ในระบบรักษาความปลอดภัยอัจฉริยะ

LoRaWAN ถูกนำมาใช้อย่างแพร่หลายในงานระบบรักษาความปลอดภัยอัจฉริยะและ ระบบเมืองอัจฉริยะเนื่องจากรองรับการสื่อสารระยะไกลและใช้พลังงานต่ำ โดยตัวอย่างการประยุกต์ใช้ได้แก่ระบบแจ้งเตือนการบุกรุกพื้นที่ห่างไกล ระบบตรวจจับควันและไฟไหม้ ระบบตรวจจับการเปิด-ปิดประตู ระบบตรวจวัดอุณหภูมิและความชื้นในห้องเซิร์ฟเวอร์ ระบบติดตามทรัพย์สิน (asset tracking) ระบบติดตามยานพาหนะ ระบบตรวจสอบสถานะอุปกรณ์ไฟฟ้า ระบบตรวจสอบคุณภาพอากาศ ระบบ smart meter ระบบ smart agriculture ระบบ smart building ระบบ smart parking และระบบ smart healthcare

6.12 เครือข่ายท้องถิ่นเสมือน (Virtual Local Area Network: VLAN)

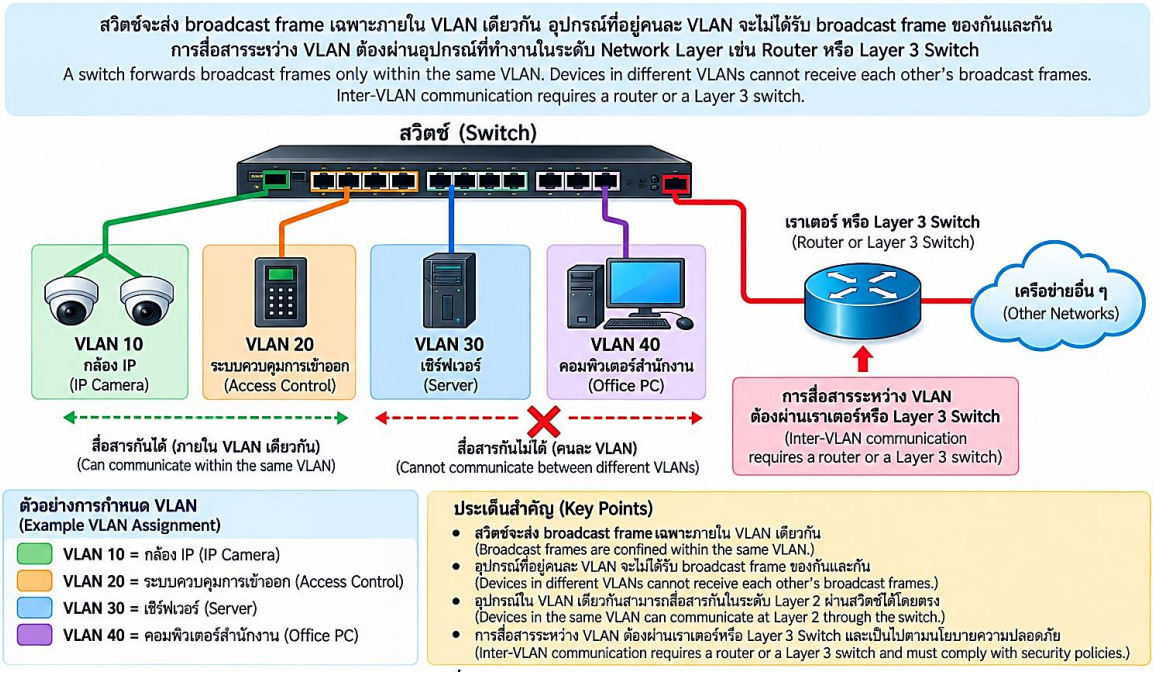
เครือข่ายท้องถิ่นเสมือน (VLAN) เป็นเทคโนโลยีที่ใช้แบ่งเครือข่ายท้องถิ่นทางกายภาพออกเป็นเครือข่ายย่อยเชิงตรรกะ ด้วยการกำหนดค่าบนสวิตช์ โดยไม่จำเป็นต้องแยกสายสัญญาณหรือจัดหาอุปกรณ์เครือข่ายคนละชุดให้แก่ทุกระบบ อุปกรณ์ที่เป็นสมาชิกของ VLAN เดียวกัน จะสื่อสารกันเสมือนเชื่อมต่ออยู่ในเครือข่าย LAN เดียวกัน แม้อุปกรณ์เหล่านั้นจะติดตั้งอยู่คนละชั้นคนละอาคาร หรือเชื่อมต่อกับสวิตช์คนละตัวก็ตาม (Forouzan, 2013) ในระบบรักษาความปลอดภัยอัจฉริยะ VLAN มีบทบาทสำคัญต่อการแบ่งส่วนเครือข่าย (network segmentation) เนื่องจากระบบหนึ่งอาจประกอบด้วยกล้อง IP เครื่องบันทึกภาพเครือข่าย ระบบควบคุมการเข้าออก ระบบโทรศัพท์ผ่านเครือข่าย อุปกรณ์แจ้งเตือน เซิร์ฟเวอร์บริหารจัดการ และเครื่องคอมพิวเตอร์ของผู้ใช้งาน หากอุปกรณ์ทั้งหมดอยู่ในเครือข่ายเดียวกัน การส่งข้อมูลแบบ broadcast อาจกระจายไปยังอุปกรณ์ทุกตัว และอุปกรณ์ที่ถูกบุกรุกเพียงตัวเดียวอาจเข้าถึงหรือโจมตีอุปกรณ์อื่นในเครือข่ายได้ง่ายขึ้น การแบ่งระบบออกเป็น VLAN จึงช่วยจำกัดขอบเขตการสื่อสาร ลดปริมาณ broadcast traffic และเปิดโอกาสให้ผู้ดูแลระบบกำหนดนโยบายควบคุมการเข้าถึงระหว่างระบบได้อย่างละเอียด อย่างไรก็ตาม VLAN เป็นเพียงกลไกการแบ่งเครือข่ายเชิงตรรกะในระดับ data link layer ไม่ใช่ระบบรักษาความปลอดภัยที่สมบูรณ์ในตัวเอง การป้องกันที่มีประสิทธิภาพต้องใช้ VLAN ร่วมกับ router, layer 3 switch, firewall, access control list และพิสูจน์ตัวตนอื่น ๆ

6.12.1 หลักการทำงานของ VLAN

เครือข่าย LAN ทั่วไป สวิตช์จะส่ง broadcast frame ออกไปยังทุกพอร์ตที่อยู่ใน broadcast domain เดียวกัน แต่เมื่อมีการกำหนด VLAN สวิตช์จะจำกัดการส่ง broadcast ให้อยู่ภายใน VLAN ของต้นทางเท่านั้น อุปกรณ์ที่อยู่คนละ VLAN จะไม่ได้รับ broadcast frame ของกันและกัน ดังนั้น VLAN แต่ละชุดจึงถือเป็น broadcast domain ที่แยกจากกัน อุปกรณ์ใน VLAN เดียวกันสามารถสื่อสารในระดับ layer 2 ผ่านสวิตช์ได้โดยตรง ส่วนการสื่อสารระหว่าง VLAN ต้องผ่านอุปกรณ์ที่ทำงานใน network layer เช่น router หรือ layer 3 switch (Forouzan, 2013) ตัวอย่างเช่น หากกำหนดให้

- กล้อง IP อยู่ใน VLAN 10
- ระบบควบคุมการเข้าออกอยู่ใน VLAN 20
- เซิร์ฟเวอร์บริหารจัดการอยู่ใน VLAN 30
- คอมพิวเตอร์สำนักงานอยู่ใน VLAN 40

กล้องใน VLAN 10 จะไม่สามารถส่งข้อมูลไปยังคอมพิวเตอร์ใน VLAN 40 ได้โดยตรง แม้ทั้งสองอุปกรณ์จะเชื่อมต่ออยู่กับสวิตช์ตัวเดียวกัน การสื่อสารจะเกิดขึ้นได้ก็ต่อเมื่อผ่าน inter-VLAN Routing และได้รับอนุญาตจากนโยบายของ router, layer 3 switch หรือ firewall



รูปที่ 6.25 หลักการทำงานของ VLAN

6.12.2 VLAN กับ Subnet

VLAN และ subnet เป็นแนวคิดที่เกี่ยวข้องกันแต่ทำงานต่างระดับกัน

1) VLAN ทำงานใน data link layer หรือ layer 2

2) IP subnet ทำงานใน network layer หรือ layer 3

ในการออกแบบเครือข่ายโดยทั่วไป VLAN หนึ่งควรสัมพันธ์กับ IP subnet หนึ่ง เพื่อให้การบริหารจัดการและการกำหนดเส้นทางมีความชัดเจน ตัวอย่างดังตารางที่ 6.11 การจับคู่ VLAN กับ subnet ช่วยให้สามารถกำหนด default gateway, DHCP scope, access control list และ firewall policy แยกตามประเภทของอุปกรณ์ได้อย่างเป็นระบบ

ตารางที่ 6.11 ตัวอย่างการบริหารจัดการและการกำหนดเส้นทางของ VLAN

VLAN	ระบบ	IP Subnet
VLAN 10	กล้อง IP	192.168.10.0/24
VLAN 20	ระบบควบคุมการเข้าออก	192.168.20.0/24
VLAN 30	ระบบแจ้งเตือนและ IoT Gateway	192.168.30.0/24
VLAN 40	NVR และ VMS Server	192.168.40.0/24
VLAN 50	ผู้ดูแลระบบ	192.168.50.0/24
VLAN 60	ผู้ใช้งานทั่วไป	192.168.60.0/24
VLAN 70	เครือข่ายสำหรับผู้มาติดต่อ	192.168.70.0/24

6.12.3 การกำหนดสมาชิกของ VLAN

สมาชิกของ VLAN สามารถกำหนดโดยใช้เกณฑ์หลายรูปแบบ ได้แก่ หมายเลขพอร์ตของสวิตช์ MAC address, IP address, multicast IP address หรือใช้หลายเกณฑ์ร่วมกัน (Forouzan, 2013)

1) การกำหนดตามพอร์ตของสวิตช์

เป็นวิธีที่นิยมมากที่สุดในการติดตั้งระบบรักษาความปลอดภัย ผู้ดูแลระบบกำหนดให้พอร์ตหนึ่งเป็นสมาชิกของ VLAN ที่ต้องการ เช่น

- พอร์ต 1-16 เป็น VLAN 10 สำหรับกล้อง IP
- พอร์ต 17-20 เป็น VLAN 20 สำหรับ access controller
- พอร์ต 21-22 เป็น VLAN 30 สำหรับระบบแจ้งเตือน

อุปกรณ์ที่ต่อเข้ากับพอร์ตนั้นจะถูกจัดให้อยู่ใน VLAN ตามที่กำหนด วิธีนี้ติดตั้งง่าย ควบคุมได้ชัดเจน และเหมาะกับอุปกรณ์ที่ติดตั้งประจำตำแหน่ง

2) การกำหนดตาม MAC address

สวิตช์หรือระบบควบคุมเครือข่ายสามารถพิจารณา MAC address ของอุปกรณ์เพื่อกำหนด VLAN วิธีนี้ช่วยให้อุปกรณ์ยังคงอยู่ใน VLAN เดิมแม้ย้ายไปเชื่อมต่อที่พอร์ตอื่น แต่ต้องบริหารรายการ MAC address ให้ถูกต้องและไม่ควรใช้เป็นมาตรการพิสูจน์ตัวตนเพียงอย่างเดียว เนื่องจาก MAC address สามารถถูกปลอมแปลงได้

3) การกำหนดตาม IP address

บางระบบสามารถกำหนดสมาชิกตาม IP address หรือ IP subnet อย่างไรก็ตาม การพิจารณา IP address เป็นกระบวนการระดับ layer 3 และต้องอาศัยสวิตช์หรือระบบควบคุมที่รองรับคุณสมบัติดังกล่าว

4) การกำหนดแบบอัตโนมัติ

ระบบเครือข่ายสมัยใหม่อาจใช้การพิสูจน์ตัวตน เช่น IEEE 802.1X หรือระบบ network access control เพื่อกำหนด VLAN ตามตัวตน ประเภทอุปกรณ์ หรือสิทธิ์ของผู้ใช้งาน การกำหนดแบบอัตโนมัติเหมาะกับเครือข่ายขนาดใหญ่หรือพื้นที่ที่มีอุปกรณ์เคลื่อนย้ายบ่อย

6.12.4 Access Port และ Trunk Port

พอร์ตของ managed switch ที่เกี่ยวข้องกับ VLAN แบ่งได้เป็น 2 ลักษณะสำคัญ ได้แก่

1) Access Port

Access port เป็นพอร์ตที่เชื่อมต่อกับอุปกรณ์ปลายทางและเป็นสมาชิกของ VLAN เดียว เช่น กล้อง IP, access controller, เครื่องอ่านบัตร, NVR, เครื่องคอมพิวเตอร์ผู้ดูแลระบบ โดยเฟรมที่ส่งระหว่างอุปกรณ์ปลายทางกับ access port โดยทั่วไปจะไม่มี VLAN tag อุปกรณ์ปลายทางจึงไม่จำเป็นต้องรับรู้ว่าตนเองอยู่ใน VLAN หมายเลขใด สวิตช์จะกำหนด VLAN ให้ตามค่าที่ตั้งไว้บนพอร์ต ตัวอย่างเช่น หากพอร์ต 5 ถูกกำหนดเป็น access port ของ VLAN 10 กล้องที่เชื่อมต่อกับพอร์ตนี้จะถูกจัดให้อยู่ใน VLAN 10 โดยอัตโนมัติ

2) Trunk Port

Trunk port เป็นพอร์ตที่ใช้ส่งข้อมูลหลาย VLAN ผ่านลิงก์เดียวกัน ใช้เชื่อมต่อสวิตช์กับสวิตช์ สวิตช์กับ router สวิตช์กับ firewall สวิตช์กับ server ที่รองรับหลาย VLAN และสวิตช์กับ wireless access point ที่มีหลาย SSID เพื่อให้สวิตช์ปลายทางทราบว่าเฟรมหนึ่งเป็นสมาชิกของ VLAN ใด จะมีการเพิ่ม VLAN tag ลงใน Ethernet frame ก่อนส่งผ่าน trunk link

6.12.5 มาตรฐาน IEEE 802.1Q

IEEE 802.1Q เป็นมาตรฐานสำหรับการกำหนด VLAN tag ใน Ethernet frame เพื่อให้เฟรมของหลาย VLAN สามารถเดินทางผ่าน trunk link เดียวกันได้ มาตรฐานดังกล่าวช่วยให้อุปกรณ์เครือข่ายจากผู้ผลิตหลายรายสามารถทำงานร่วมกันได้ (Forouzan, 2013) 802.1Q tag มีขนาด 4 ไบต์ และประกอบด้วยข้อมูลสำคัญ ได้แก่

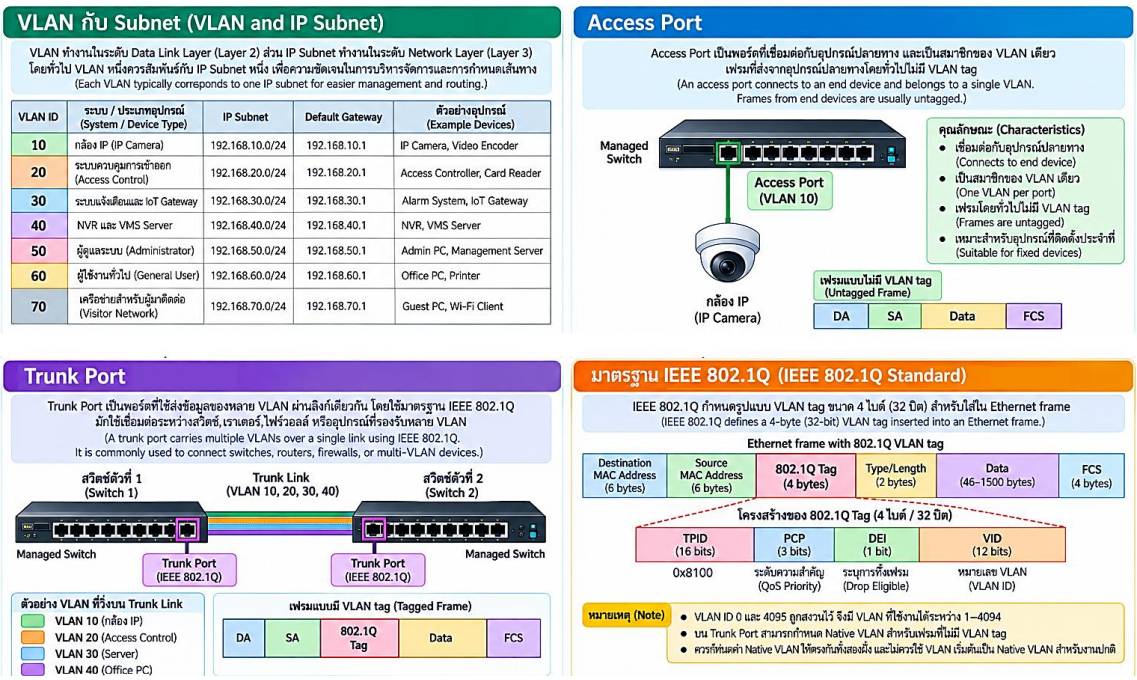
1) Tag Protocol Identifier (TPID) ใช้ระบุว่าเฟรมมี 802.1Q tag

2) Priority Code Point (PCP) มีขนาด 3 bit ใช้กำหนดระดับความสำคัญของเฟรมตามแนวคิด QoS

3) Drop Eligible Indicator (DEI) ใช้ระบุว่าเฟรมสามารถถูกพิจารณาทิ้งก่อนเมื่อเครือข่ายแออัดหรือไม่

4) VLAN Identifier (VID) มีขนาด 12 bit ใช้ระบุหมายเลข VLAN

5) ค่า VLAN ID มีช่วงตัวเลขตามฟิลด์ 12 bit แต่ VLAN ID 0 และ 4095 ถูกสงวนไว้ จึงมี VLAN ที่ใช้ระบุเครือข่ายได้ตามปกติระหว่าง 1-4094 ทั้งนี้ ความสามารถของสวิตช์แต่ละรุ่นในการรองรับจำนวน VLAN อาจแตกต่างกัน



รูปที่ 6.26 หลักการแบ่งเครือข่าย และการเชื่อมต่อของ VLAN ตามมาตรฐาน IEEE 802.1Q

6.12.6 การประยุกต์ใช้ VLAN ในระบบรักษาความปลอดภัยอัจฉริยะ

1) VLAN สำหรับกล้องวงจรปิด

กล้อง IP ควรแยกออกจากเครือข่ายสำนักงาน เนื่องจากกล้องจำนวนมากสร้างข้อมูลวิดีโอต่อเนื่องและอาจมีช่องโหว่จาก firmware หรือบริการเครือข่ายที่เปิดใช้งาน การแยกกล้องไว้ใน VLAN เฉพาะช่วยจำกัดการเข้าถึงและลดโอกาสที่กล้องซึ่งถูกบุกรุกจะโจมตีคอมพิวเตอร์ของผู้ใช้งาน ควรกำหนดให้กล้องติดต่อได้เฉพาะ NVR หรือ VMS server, NTP server, DNS server, management server และ update server ที่ได้รับอนุญาต และไม่ควรอนุญาตให้กล้องเข้าถึงอินเทอร์เน็ตโดยตรงโดยไม่มีเหตุผลและไม่มีการควบคุม

2) VLAN สำหรับระบบควบคุมการเข้าออก

Access controller, door controller, biometric reader และ management server ควรอยู่ใน VLAN ที่แยกจากผู้ใช้งานทั่วไป เนื่องจากระบบดังกล่าวเกี่ยวข้องกับข้อมูลตัวตนและการควบคุมประตู ควรกำหนดนโยบายให้ access controller ติดต่อได้เฉพาะ server ที่จำเป็น และป้องกันไม่ให้เครื่องคอมพิวเตอร์ทั่วไปเข้าถึงหน้าเว็บหรือพอร์ตบริหารของ controller โดยตรง

3) VLAN สำหรับระบบแจ้งเตือนและ IoT Gateway

ระบบเซนเซอร์ gateway, alarm controller และอุปกรณ์ IoT ควรแยกออกจากกล้องและเครือข่ายสำนักงาน เนื่องจากอุปกรณ์เหล่านี้มักมีทรัพยากรจำกัดและอาจไม่รองรับมาตรการความมั่นคงปลอดภัยระดับสูง

4) VLAN สำหรับเซิร์ฟเวอร์รักษาความปลอดภัย

NVR, VMS server, access control server และฐานข้อมูลควรอยู่ใน server VLAN หรือ management VLAN ที่ได้รับการควบคุมเป็นพิเศษ อนุญาตให้เฉพาะอุปกรณ์และผู้ดูแลที่จำเป็นเข้าถึงได้

5) VLAN สำหรับผู้ดูแลระบบ

ควรมี management VLAN สำหรับบริหารสวิตช์ router, firewall, NVR และอุปกรณ์รักษาความปลอดภัย ม่ควรใช้ VLAN เดียวกับผู้ใช้งานทั่วไป และควรจำกัดการเข้าถึงตาม IP address, user account หรือระบบพิสูจน์ตัวตนของผู้ดูแล

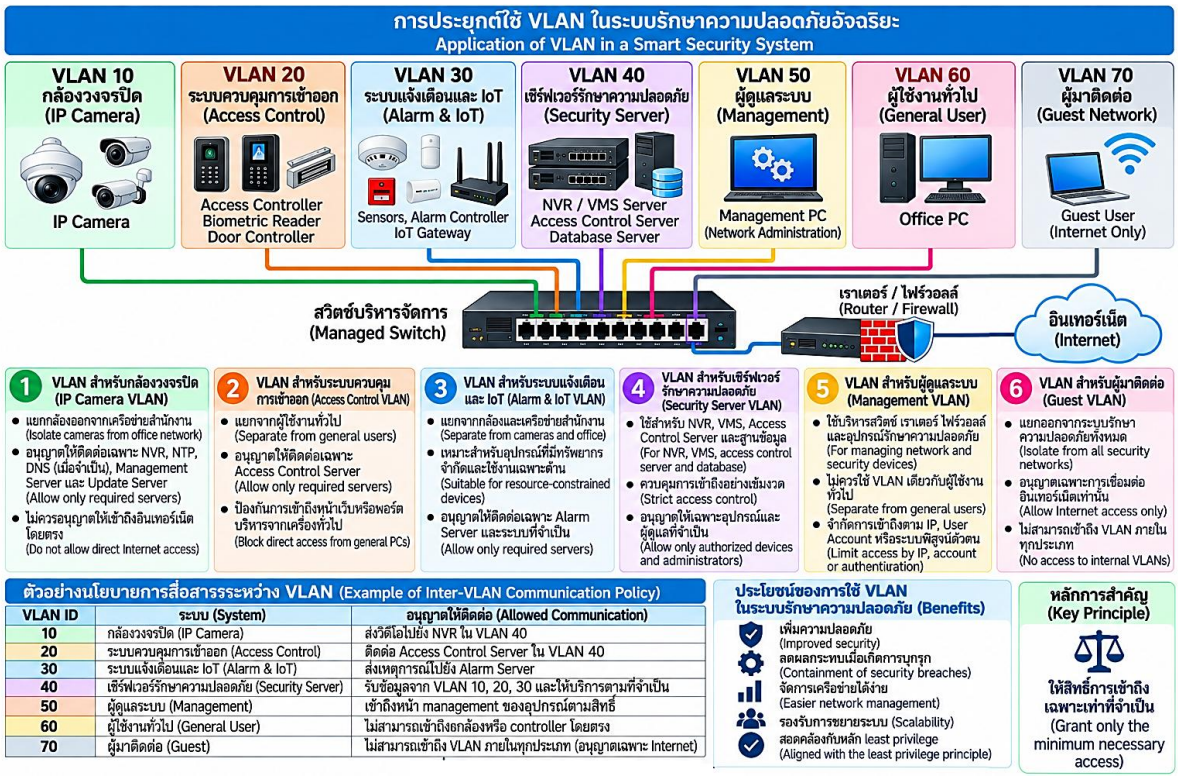
6) VLAN สำหรับผู้มาติดต่อ

Guest VLAN ควรแยกออกจากระบบรักษาความปลอดภัยทั้งหมด และอนุญาตเฉพาะการเชื่อมต่อสู่อินเทอร์เน็ตเท่านั้น แนวคิดการสร้างเครือข่ายเฉพาะกลุ่มหรือเครือข่ายเสมือนที่แยกจากกันช่วยลดการเข้าถึงทรัพยากรที่ไม่เกี่ยวข้องและสนับสนุนการควบคุมสิทธิ์

โครงสร้าง VLAN ในระบบรักษาความปลอดภัยอัจฉริยะ ตัวอย่างนโยบายการสื่อสาร ดังนี้

- VLAN 10 อนุญาตให้ส่งวิดีโอไปยัง NVR ใน VLAN 40
- VLAN 20 อนุญาตให้ติดต่อ access control server ใน VLAN 40
- VLAN 30 อนุญาตให้ส่งเหตุการณ์ไปยัง alarm server
- VLAN 60 ไม่สามารถเข้าถึงกล้องหรือ controller โดยตรง
- VLAN 70 ไม่สามารถเข้าถึง VLAN ภายในทุกประเภท
- VLAN 50 จะเข้าถึงหน้า management ของอุปกรณ์ตามสิทธิ์ของผู้ดูแล

แนวทางดังกล่าวสอดคล้องกับหลัก least privilege ซึ่งกำหนดให้อุปกรณ์ได้รับอนุญาตให้ติดต่อเฉพาะระบบที่จำเป็นต่อหน้าที่เท่านั้น



รูปที่ 6.27 การประยุกต์ใช้ VLAN ในระบบรักษาความปลอดภัยอัจฉริยะ

ตารางที่ 6.12 ตัวอย่างโครงสร้าง VLAN สำหรับ Smart Security

VLAN ID	ชื่อ VLAN	อุปกรณ์	IP Subnet	สิทธิ์หลัก
10	CCTV-CAMERA	กล้อง IP	192.168.10.0/24	ส่งข้อมูลไปยัง NVR/VMS
20	ACCESS-CONTROL	Access Controller และเครื่องอ่าน	192.168.20.0/24	ติดต่อ Access Server
30	ALARM-IOT	Alarm Gateway และ IoT Gateway	192.168.30.0/24	ติดต่อ Alarm Server
40	SECURITY-SERVER	NVR, VMS และฐานข้อมูล	192.168.40.0/24	รับข้อมูลจากระบบที่อนุญาต
50	MANAGEMENT	เครื่องผู้ดูแลและอุปกรณ์บริหาร	192.168.50.0/24	บริหารอุปกรณ์ทุกระบบตามสิทธิ์
60	OFFICE	คอมพิวเตอร์สำนักงาน	192.168.60.0/24	เข้าถึงเฉพาะบริการที่อนุญาต
70	GUEST	ผู้มาติดต่อ	192.168.70.0/24	อินเทอร์เน็ตเท่านั้น

6.12.7 ประโยชน์ของ VLAN ต่อระบบรักษาความปลอดภัยอัจฉริยะ

1) ลด broadcast traffic

2) Broadcast frame จะถูกจำกัดอยู่ภายใน VLAN จึงช่วยลดปริมาณข้อมูลที่ไม่จำเป็นในเครือข่ายและลดภาระของอุปกรณ์ปลายทาง

3) แยกประเภทอุปกรณ์

4) สามารถแยกกล้อง IP ระบบควบคุมการเข้าออก เซิร์ฟเวอร์ และผู้ใช้งานทั่วไปออกจากกันโดยไม่ต้องใช้สวิตช์คนละตัวทั้งหมด

5) เพิ่มความยืดหยุ่น

6) การย้ายอุปกรณ์จาก VLAN หนึ่งไปยังอีก VLAN สามารถดำเนินการโดยเปลี่ยนค่าบนสวิตช์ ไม่จำเป็นต้องเปลี่ยนสายหรือโครงสร้างทางกายภาพ Forouzan (2013) ระบุว่า VLAN ช่วยลดเวลาและค่าใช้จ่ายในการเปลี่ยนกลุ่มของอุปกรณ์ เพราะการกำหนดสมาชิกดำเนินการผ่านซอฟต์แวร์

7) เพิ่มการควบคุมด้านความมั่นคงปลอดภัย

8) อุปกรณ์ใน VLAN หนึ่งจะไม่ได้รับ broadcast ของ VLAN อื่น และการสื่อสารข้าม VLAN สามารถควบคุมผ่าน firewall หรือ ACL ได้

9) VLAN สามารถใช้ร่วมกับ QoS เพื่อจัดลำดับความสำคัญของทราฟฟิก เช่น ให้ความสำคัญกับวิดีโอสดหรือข้อมูลแจ้งเตือนมากกว่าข้อมูลทั่วไป งานด้านเครือข่ายเสมือนและ Network Slicing ยังแสดงให้เห็นว่าการแบ่งทราฟฟิกเชิงตรรกะช่วยกำหนดคุณลักษณะและลำดับความสำคัญของบริการแต่ละกลุ่มได้

6.12.8 ข้อจำกัดของ VLAN

แม้ VLAN จะช่วยแบ่งเครือข่าย แต่ไม่ควรถือว่า VLAN เป็นกลไกรักษาความปลอดภัยที่เพียงพอ เนื่องจากมีข้อจำกัดดังนี้

1) VLAN ไม่ได้เข้ารหัสข้อมูล

2) อุปกรณ์ใน VLAN เดียวกันยังสามารถโจมตีกันได้

3) การตั้งค่า trunk ผิดพลาดอาจทำให้ทราฟฟิกข้าม VLAN โดยไม่ตั้งใจ

4) การเปิด Inter-VLAN Routing โดยไม่มี ACL อาจทำให้ทุก VLAN ติดต่อกันได้

5) ผู้โจมตีอาจใช้เทคนิค VLAN Hopping หากสวิตช์ถูกตั้งค่าไม่เหมาะสม

6) VLAN ไม่สามารถแทนที่ firewall, authentication หรือ intrusion detection system ได้

7) ความผิดพลาดของผู้ดูแล เช่น การกำหนดพอร์ตผิด VLAN อาจเปิดเผยระบบสำคัญ VLAN จึงควรเป็นส่วนหนึ่งของแนวทาง defense in depth ใช้มาตรการป้องกันหลายชั้น

6.12.9 แนวทางการออกแบบ VLAN อย่างปลอดภัย

แนวทางที่เหมาะสมสำหรับระบบ smart security ได้แก่

1) แยก VLAN ตามหน้าที่และระดับความสำคัญของอุปกรณ์

2) กำหนด VLAN หนึ่งให้สัมพันธ์กับ IP subnet หนึ่ง

3) ใช้ access port สำหรับอุปกรณ์ปลายทาง

4) อนุญาต VLAN บน trunk เฉพาะรายการที่จำเป็น

5) หลีกเลี่ยงการใช้ VLAN 1 สำหรับอุปกรณ์หรือการบริหารระบบ

6) เปลี่ยน native VLAN เป็น VLAN ที่ไม่ได้ใช้กับอุปกรณ์ปลายทาง

7) ปิดพอร์ตสวิตช์ที่ไม่ได้ใช้งานและย้ายไปยัง VLAN ที่ไม่ใช้งาน

8) ปิดการเจรจา trunk อัตโนมัติบนพอร์ตที่ไม่จำเป็น

9) ใช้ ACL หรือ firewall ควบคุม inter-VLAN traffic

10) จำกัด management VLAN ให้เข้าถึงได้เฉพาะเครื่องของผู้ดูแล

11) ใช้ IEEE 802.1X หรือ port security เมื่ออุปกรณ์รองรับ

12) ตรวจสอบ log, MAC address table และเหตุการณ์การเปลี่ยนแปลงพอร์ต

13) สำรอง configuration ของสวิตช์และจัดทำเอกสาร VLAN อย่างเป็นระบบ

14) ใช้ SNMP เวอร์ชันที่มีการพิสูจน์ตัวตนและการเข้ารหัสสำหรับการบริหารอุปกรณ์

กล่าวโดยสรุป VLAN เป็นเทคโนโลยีที่แบ่ง LAN ทางกายภาพออกเป็น broadcast domain เชิงตรรกะหลายกลุ่มผ่านการกำหนดค่าบน managed switch สมาชิกของ VLAN สามารถกำหนดตามพอร์ต MAC address, IP address หรือเกณฑ์อื่น และข้อมูลของหลาย VLAN สามารถส่งผ่าน trunk link ด้วยมาตรฐาน IEEE 802.1Q สำหรับระบบรักษาความปลอดภัย VLAN ช่วยแยกกล้อง IP ระบบควบคุมการเข้าออก ระบบแจ้งเตือน เซิร์ฟเวอร์ และผู้ใช้งานทั่วไปออกจากกัน ลด broadcast traffic และช่วยให้สามารถกำหนดนโยบายการเข้าถึงระหว่างระบบได้ละเอียดขึ้น อย่างไรก็ตาม VLAN ไม่ได้เข้ารหัสข้อมูลและไม่ควรใช้เป็นมาตรการป้องกันเพียงอย่างเดียว การออกแบบที่ถูกต้องต้องใช้ร่วมกับ IP subnet, inter-VLAN routing, firewall, access control list, การพิสูจน์ตัวตน และระบบตรวจสอบเครือข่าย เพื่อสร้างความมั่นคงปลอดภัยแบบหลายชั้น

6.13 Power over Ethernet (PoE)

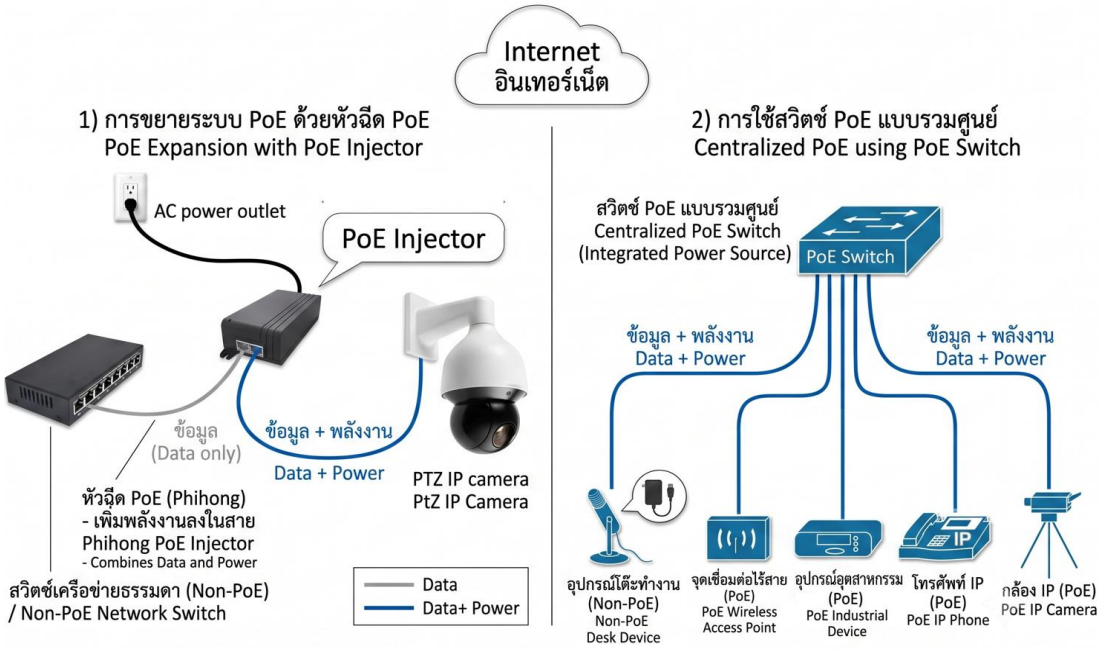
6.13.1 ความหมายของ Power over Ethernet (PoE)

Power over Ethernet (PoE) เป็นเทคโนโลยีที่ช่วยให้สามารถส่ง พลังงานไฟฟ้า (power) และข้อมูล (data) ผ่านสาย Ethernet เส้นเดียวกันได้ ทำให้อุปกรณ์ปลายทางไม่จำเป็นต้องมีแหล่งจ่ายไฟแยกต่างหาก ส่งผลให้การติดตั้งระบบเครือข่ายมีความสะดวก ลดจำนวนสายไฟ ลดค่าใช้จ่ายในการเดินระบบ และเพิ่มความยืดหยุ่นในการติดตั้งอุปกรณ์ในตำแหน่งที่ไม่มีปลั๊กไฟ (IEEE, 2022)

6.13.2 หลักการทำงานของ PoE

หลักการทำงานของ PoE อาศัยการส่งพลังงานไฟฟ้ากระแสตรง (Direct Current: DC) ควบคู่กับการรับส่งข้อมูลผ่านสายคู่บิดเกลียวภายในสาย Ethernet เส้นเดียวกัน โดยก่อนเริ่มจ่ายพลังงาน

อุปกรณ์ PSE จะตรวจสอบก่อนว่าอุปกรณ์ปลายทางรองรับมาตรฐาน PoE หรือไม่ ผ่านกระบวนการ detection และ classification หากตรวจพบว่าอุปกรณ์เป็น Powered Device (PD) ที่รองรับมาตรฐาน IEEE 802.3 PSE จึงจะเริ่มจ่ายพลังงานไฟฟ้าอย่างเหมาะสมตามกำลังไฟที่อุปกรณ์ต้องการ (IEEE, 2022) การตรวจสอบดังกล่าวช่วยป้องกันไม่ให้ PSE จ่ายไฟไปยังอุปกรณ์ที่ไม่รองรับ PoE ซึ่งอาจทำให้เกิดความเสียหายต่ออุปกรณ์หรือระบบเครือข่าย นอกจากนี้ PSE ยังสามารถตรวจสอบสถานะการใช้พลังงานของ PD ได้ตลอดเวลา และจะหยุดจ่ายไฟเมื่ออุปกรณ์ถูกถอดออกหรือเกิดความผิดปกติของระบบ เพื่อเพิ่มความปลอดภัยในการใช้งาน ข้อดีของการนำเทคโนโลยี PoE มาใช้ในระบบเครือข่ายมีข้อดีหลายประการ ได้แก่ ลดจำนวนสายไฟและค่าใช้จ่ายในการติดตั้ง สามารถติดตั้งอุปกรณ์ในตำแหน่งที่ไม่มีปลั๊กไฟ ลดความซับซ้อนของระบบสายสัญญาณ รองรับการบริหารจัดการพลังงานจากส่วนกลาง เพิ่มความสะดวกในการบำรุงรักษาและขยายระบบ และ รองรับระบบสำรองไฟฟ้า (Uninterruptible Power Supply: UPS) ผ่าน PoE switch ทำให้อุปกรณ์ปลายทางยังคงทำงานได้เมื่อไฟฟ้าดับ



รูปที่ 6.28 สถาปัตยกรรมของระบบ PoE

6.13.3 องค์ประกอบของระบบ PoE

ระบบ PoE ประกอบด้วยองค์ประกอบสำคัญ 3 ส่วน (Forouzan, 2013; IEEE, 2022; Odom, 2024) ได้แก่

1) Power Sourcing Equipment (PSE) เป็นอุปกรณ์ต้นทางที่ทำหน้าที่จ่ายพลังงานไฟฟ้าและส่งข้อมูลผ่านสาย Ethernet เช่น PoE switch และ PoE injector

2) Powered Device (PD) เป็นอุปกรณ์ปลายทางที่รับทั้งข้อมูลและพลังงานไฟฟ้าผ่านสาย Ethernet เช่น IP camera, wireless access point, IP phone, video intercom และอุปกรณ์ IoT

3) Ethernet Cabling เป็นสายสัญญาณ เช่น Cat5e, Cat6 หรือ Cat6A ทำหน้าที่ส่งทั้งข้อมูลและพลังงานไฟฟ้าระหว่าง PSE และ PD โดยระยะทางมาตรฐานไม่เกิน 100 m ตามข้อกำหนดของ Ethernet

6.13.4 มาตรฐานของ PoE

มาตรฐาน IEEE ได้พัฒนา PoE อย่างต่อเนื่องเพื่อรองรับอุปกรณ์ที่ต้องการกำลังไฟเพิ่มขึ้น มาตรฐาน PoE ที่ใช้งานในปัจจุบันแสดงดังตารางที่ ตารางที่ 6.13

ตารางที่ 6.13 แสดงการเปรียบเทียบมาตรฐาน PoE ที่ใช้งานในปัจจุบัน

มาตรฐาน IEEE	ชื่อมาตรฐาน	กำลังไฟจาก PSE	กำลังไฟที่ PD ได้รับโดยประมาณ	ตัวอย่างการใช้งาน
IEEE 802.3af	PoE	15.4 W	12.95 W	IP Phone, IP Camera, Access Point
IEEE 802.3at	PoE+	30 W	25.5 W	PTZ Camera, Wi-Fi Access Point
IEEE 802.3bt Type 3	PoE++	60 W	51 W	Multi-radio AP, Video Conference
IEEE 802.3bt Type 4	PoE++	90-100 W	71-90 W	LED Lighting, Digital Signage, Thin Client

การพัฒนามาตรฐาน PoE ทำให้สามารถรองรับอุปกรณ์ที่ต้องใช้พลังงานสูง เช่น กล้องวงจรปิดแบบหมุนซูม (Pan-Tilt-Zoom: PTZ camera) จอแสดงผลอัจฉริยะ และอุปกรณ์ Smart Building ได้อย่างมีประสิทธิภาพ

6.13.5 การประยุกต์ใช้ PoE ในระบบรักษาความปลอดภัยอัจฉริยะ

PoE เป็นเทคโนโลยีที่มีบทบาทสำคัญในระบบรักษาความปลอดภัยอัจฉริยะ เนื่องจากช่วยให้การติดตั้งอุปกรณ์เครือข่ายเป็นไปอย่างสะดวกและมีประสิทธิภาพ ตัวอย่างการประยุกต์ใช้งานได้แก่ กล้อง IP กล้อง PTZ, wireless access point ระบบควบคุมการเข้าออก เครื่องอ่านบัตร RFID และเครื่องอ่านชีวมิติ video intercom เซนเซอร์ IoT สำหรับระบบรักษาความปลอดภัย หรือระบบไฟส่องสว่างอัจฉริยะ (smart lighting) สำหรับระบบกล้องวงจรปิด PoE ช่วยให้สามารถติดตั้งกล้องในตำแหน่งที่เหมาะสมได้โดยไม่ต้องเดินสายไฟเพิ่มเติม เพียงเชื่อมต่อสาย Ethernet จาก PoE switch ไปยังกล้องก็สามารถรับส่งข้อมูลและจ่ายพลังงานได้พร้อมกัน ส่งผลให้ลดต้นทุนการติดตั้งและเพิ่มความน่าเชื่อถือของระบบ

กว่าวโดยสรุป PoE เป็นเทคโนโลยีที่รวมการส่งข้อมูลและพลังงานไฟฟ้าไว้ในสาย Ethernet เส้นเดียวกัน ช่วยลดต้นทุนและความซับซ้อนในการติดตั้งระบบเครือข่าย พร้อมทั้งเพิ่มความ

ยืดหยุ่นในการติดตั้งอุปกรณ์ปลายทาง มาตรฐาน IEEE 802.3af, IEEE 802.3at และ IEEE 802.3bt รองรับการจ่ายพลังงานในระดับที่แตกต่างกันเพื่อให้เหมาะสมกับอุปกรณ์แต่ละประเภท ปัจจุบัน PoE ได้กลายเป็นองค์ประกอบสำคัญของระบบ Smart security systems โดยเฉพาะการเชื่อมต่อกล้อง IP ระบบควบคุมการเข้าออก จุดกระจายสัญญาณไร้สาย และอุปกรณ์ IoT ทำให้ระบบเครือข่ายมีความสะดวกในการติดตั้ง มีความน่าเชื่อถือ และสามารถบริหารจัดการจากศูนย์กลางได้อย่างมีประสิทธิภาพ

บรรณานุกรมบทที่ 6

AlShuhail, A. S., Bhatia, S., Kumar, A., & Bhushan, B. (2022). Zigbee-based low power consumption wearables device for voice data transmission. *Sustainability, 14*(17), 10847. https://doi.org/10.3390/su141710847.

Bhosale, S., & Rajireddy, S. (2007). *ZigBee technology*. In Proceedings of TECTRIX-2K7 National Conference (P.E.S. College of Engineering, Aurangabad, India.

Bonilla, V., Campoverde, B., & Yoo, S. G. (2023). A systematic literature review of LoRaWAN: Sensors and applications. *Sensors, 23*(20), 8440. https://doi.org/10.3390/s23208440.

Boussard, M., Bui, D. T., Douville, R., Justen, P., Le Sauze, N., Peloso, P., Vandeputte, F., & Verdot, V. (2018). Future spaces: Reinventing the home network for better security and automation in the IoT era. *Sensors, 18*(9), 2986. https://doi.org/10.3390/s18092986.

Forouzan, B. A. (2013). *Data communications and networking* (5th ed.). McGraw-Hill Education.

Gavra, V., Pop, O. A., & Dobra, I. (2023). A comprehensive analysis: Evaluating security characteristics of XBee devices against Zigbee protocol. *Sensors, 23*(21), 8736. https://doi.org/10.3390/s23218736.

Gupta, P. C. (2013). *Data communications and computer networks (2nd ed.)*. PHI Learning.

IEEE. (2020). *IEEE Standard for Low-Rate Wireless Networks (IEEE Std 802.15.4-2020).* Institute of Electrical and Electronics Engineers.

IEEE. (2022). *IEEE Std 802.3™-2022: IEEE Standard for Ethernet*. Institute of Electrical and Electronics Engineers.

LoRa Alliance. (2024). *What is LoRaWAN?* https://lora-alliance.org/.

Metcalfe, R. M., & Boggs, D. R. (1976). Ethernet: Distributed packet switching for local computer networks. *Communications of the ACM, 19*(7), 395–404. https://doi.org/10.1145/360248.360253.

Odom, W. (2024). *CCNA 200-301 Official Cert Guide, Volume 1* (2nd ed.). Cisco Press.

Paul, Y., & Singh, R. (2015). Zigbee technology: A comprehensive review of protocol, applications, and advancements. *IJRDO Journal of Computer Science and Engineering.*

Serror, M., Henze, M., Hack, S., Schuba, M., & Wehrle, K. (2018). *Towards in-network security for smart homes*. In Proceedings of the 13th International Conference on Availability, Reliability and Security. Association for Computing Machinery. https://doi.org/10.1145/3230833.3232802.

Stallings, W. (2017). *Data and computer communications* (10th ed.). Pearson.

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. *Electronics, 13*(16), 3343. https://doi.org/10.3390/electronics13163343.

Yin, Y. (2024). Information security and risk control model based on Plan-Do-Check-Action for digital libraries. *Journal of Cyber Security and Mobility, 13*(02), 305–326. https://doi: 10.13052/jcsm2245-1439.1326.

สรุปสาระสำคัญของบทที่ 6
ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัย

ความรู้เบื้องต้นเกี่ยวกับเครือข่ายในระบบรักษาความปลอดภัย

ระบบเครือข่ายเป็นโครงสร้างพื้นฐานสำคัญของระบบรักษาความปลอดภัยอัจฉริยะ ทำหน้าที่เชื่อมโยงอุปกรณ์ปลายทาง อุปกรณ์ควบคุม เซิร์ฟเวอร์ ระบบคลาวด์ และแอปพลิเคชันเข้าด้วยกัน เพื่อให้สามารถรับส่งข้อมูล ตรวจสอบสถานะ แจ้งเตือน และตอบสนองต่อเหตุการณ์ได้แบบเวลาจริง องค์ประกอบสำคัญของระบบประกอบด้วยอุปกรณ์อัจฉริยะ เครือข่ายสื่อสาร อุปกรณ์เครือข่าย ระบบประมวลผลส่วนกลาง ระบบคลาวด์ ส่วนติดต่อผู้ใช้งาน และระบบรักษาความมั่นคงปลอดภัย เครือข่ายที่ดีควรมีความพร้อมใช้งานสูง มีความน่าเชื่อถือ มีความหน่วงต่ำ รองรับอุปกรณ์จำนวนมาก สามารถขยายระบบได้ และรองรับมาตรฐานการสื่อสารหลายประเภท นอกจากนี้ยังต้องมีมาตรการพิสูจน์ตัวตน การเข้ารหัส การกำหนดสิทธิ์ และการตรวจสอบความผิดปกติของทราฟฟิก เพื่อป้องกันการโจมตีทางไซเบอร์และการเข้าถึงระบบโดยไม่ได้รับอนุญาต

โครงสร้างการเชื่อมต่อเครือข่าย (Network Topology)

โทโพโลยีเครือข่ายเป็นรูปแบบการเชื่อมต่อระหว่างอุปกรณ์ โหนด และสายสัญญาณภายในระบบ ซึ่งพิจารณาได้ทั้งในเชิงกายภาพและเชิงตรรกะ รูปแบบสำคัญ ได้แก่ แบบบัส แบบดาว แบบวงแหวน แบบตาข่าย และแบบผสม โทโพโลยีแบบดาวเป็นรูปแบบที่นิยมใช้กับอุปกรณ์ปลายทาง เช่น กล้อง IP ที่เชื่อมต่อกับ PoE switch เนื่องจากติดตั้ง บริหารจัดการ และแยกจุดขัดข้องได้ง่าย ส่วนแบบวงแหวนและตาข่ายเหมาะสำหรับโครงข่ายแกนกลางที่ต้องการเส้นทางสำรองและความต่อเนื่องในการทำงาน ขณะที่ระบบขนาดใหญ่มักใช้โทโพโลยีแบบผสม โดยใช้แบบดาวกับอุปกรณ์ปลายทาง แบบวงแหวนหรือ partial mesh กับเครือข่ายแกนกลาง และแบบ mesh กับเซ็นเซอร์ไร้สาย การเลือกโทโพโลยีต้องพิจารณาความน่าเชื่อถือ ความสามารถในการขยายระบบ ค่าใช้จ่าย ความสะดวกในการซ่อมบำรุง และผลกระทบเมื่ออุปกรณ์บางส่วนขัดข้อง

ชุดโปรโตคอล TCP/IP

TCP/IP เป็นชุดโปรโตคอลพื้นฐานที่ใช้ในการสื่อสารผ่านเครือข่ายและอินเทอร์เน็ต โดยแบ่งหน้าที่การสื่อสารออกเป็นหลายชั้น ได้แก่ physical, data link, network, transport และ application layer การแบ่งชั้นช่วยให้แต่ละส่วนทำหน้าที่เฉพาะ เช่น การส่งสัญญาณ การสร้างเฟรม การกำหนด IP address การเลือกเส้นทาง การควบคุมการรับส่งข้อมูล และการให้บริการแก่แอปพลิเคชัน ในการส่งข้อมูลจะเกิดกระบวนการห่อหุ้มข้อมูลจากชั้นบนลงสู่ชั้นล่าง และถอดห่อหุ้มเมื่อถึงปลายทาง TCP เหมาะกับข้อมูลที่ต้องการความครบถ้วนและถูกต้อง เช่น การดาวน์โหลดวิดีโอหลักฐานหรือการตั้งค่าระบบ ส่วน UDP เหมาะกับการสตรีมวิดีโอสดและข้อมูลเวลาจริงที่ต้องการความหน่วงต่ำ นอกจากนี้ยังครอบคลุมโปรโตคอลระดับแอปพลิเคชัน เช่น HTTPS, DHCP, DNS, MQTT, RTSP และ ONVIF ซึ่งสนับสนุนการบริหารจัดการ การแจ้งเตือน และการทำงานร่วมกันของอุปกรณ์รักษาความปลอดภัยจากผู้ผลิตหลายราย

IP Address และ Subnet

IP address เป็นที่อยู่เชิงตรรกะที่ใช้ระบุอุปกรณ์และอินเทอร์เฟซในเครือข่าย โดย IPv4 มีขนาด 32 bitและ IPv6 มีขนาด 128 bit การกำหนด IP address สำหรับกล้อง IP, NVR, access controller และ server ควรจัดทำอย่างเป็นระบบ และอุปกรณ์ที่ต้องมีตำแหน่งเครือข่ายแน่นอนควรใช้ static IP หรือ DHCP reservation เพื่อป้องกันหมายเลขเปลี่ยนแปลง การใช้ Subnet Mask หรือ prefix length ช่วยแบ่งส่วน network และ host รวมทั้งใช้แบ่งเครือข่ายขนาดใหญ่ออกเป็นเครือข่ายย่อย การทำ subnetting ช่วยลด broadcast domain จัดสรรหมายเลข IP ได้อย่างเหมาะสม และแยกระบบตามหน้าที่ เช่น เครือข่ายกล้อง ระบบควบคุมการเข้าออก ระบบแจ้งเตือน และเซิร์ฟเวอร์ อย่างไรก็ตาม การแบ่ง subnet เพียงอย่างเดียวไม่สามารถป้องกันการเข้าถึงข้ามเครือข่ายได้ จึงควรใช้ร่วมกับ VLAN, firewall และ access control list

เครือข่ายท้องถิ่น (Local Area Network: LAN)

LAN เป็นเครือข่ายที่ครอบคลุมพื้นที่จำกัด เช่น บ้าน อาคาร สำนักงาน โรงงาน หรือมหาวิทยาลัย และอยู่ภายใต้การบริหารจัดการขององค์กรเดียว องค์ประกอบสำคัญประกอบด้วยอุปกรณ์ปลายทาง NIC, network switch, router, สื่อส่งสัญญาณ และ wireless access point ในระบบรักษาความปลอดภัย LAN ใช้เชื่อมต่อกล้อง IP, NVR, VMS, access controller, IoT gateway, alarm server และคอมพิวเตอร์ของผู้ดูแลระบบ จุดเด่นของ LAN คือมีอัตรารับส่งข้อมูลสูง ความหน่วงต่ำ และบริหารจัดการได้จากส่วนกลาง การออกแบบต้องคำนวณแบนด์วิดท์ให้เพียงพอกับวิดีโอจากกล้อง ใช้ Gigabit Ethernet หรือความเร็วสูงกว่าสำหรับ Uplink และควรแยกอุปกรณ์สำคัญออกจากเครือข่ายสำนักงานด้วย VLAN พร้อมควบคุมการสื่อสารผ่าน firewall หรือ ACL

เครือข่ายบริเวณกว้าง (Wide Area Network: WAN)

WAN เป็นเครือข่ายที่ใช้เชื่อมต่อ LAN หลายแห่งในพื้นที่ห่างไกล เช่น ระหว่างอาคาร สาขา จังหวัด ประเทศ หรือระบบคลาวด์ โดยอาศัยโครงสร้างพื้นฐานของผู้ให้บริการโทรคมนาคม องค์ประกอบสำคัญ ได้แก่ customer premises equipment, access link, provider Edge router และโครงข่ายแกนกลางของผู้ให้บริการ เทคโนโลยีที่ใช้ ได้แก่ fiber optic, metro Ethernet, leased line, microwave, 4G/5G และ satellite ในระบบรักษาความปลอดภัย WAN รองรับการส่งภาพวิดีโอ เหตุการณ์แจ้งเตือน และข้อมูลควบคุมจากสาขาไปยังศูนย์กลาง จึงต้องพิจารณาแบนด์วิดท์ขาขึ้น ความหน่วง jitter การสูญหายของแพ็กเก็ต และความพร้อมใช้งาน ควรใช้ VPN หรือ SD-WAN เพื่อเพิ่มความปลอดภัยและเลือกเส้นทางสำรอง รวมทั้งใช้ QoS เพื่อจัดลำดับความสำคัญของข้อมูลแจ้งเตือนและวิดีโอที่สำคัญ

Ethernet

Ethernet เป็นเทคโนโลยีเครือข่ายแบบใช้สายตามมาตรฐาน IEEE 802.3 ซึ่งทำงานในphysical layer และ data link layer ข้อมูลถูกจัดรูปแบบเป็น Ethernet frame ซึ่งประกอบด้วย destination MAC address, source MAC address, type/length, data และ frame check

sequence สวิตช์จะเรียนรู้ MAC address และส่งต่อเฟรมไปยังพอร์ตปลายทางที่เหมาะสม ทำให้การรับส่งข้อมูลมีประสิทธิภาพ Ethernet สมัยใหม่ใช้โครงสร้างแบบดาวและการสื่อสารแบบ full-duplex จึงไม่เกิดการชนกันของข้อมูลเหมือนระบบ shared Ethernet ในอดีต เทคโนโลยีนี้เหมาะกับระบบกล้อง IP, NVR, server และ access controller เพราะมีความเร็ว ความเสถียร และความปลอดภัยสูง ส่วนระบบขนาดใหญ่ควรใช้ fiber optic เป็น backbone และใช้สายคู่บิดเกลียวเชื่อมต่ออุปกรณ์ปลายทาง

ไวไฟ (Wi-Fi)

Wi-Fi เป็นเทคโนโลยี WLAN ตามมาตรฐาน IEEE 802.11 ใช้คลื่นวิทยุเชื่อมต่ออุปกรณ์โดยไม่ต้องเดินสาย เหมาะสำหรับสมาร์ตโฟน แท็บเล็ต กล้องไร้สาย และอุปกรณ์ IoT คำว่า wireless มีความหมายกว้างกว่าคำว่า Wi-Fi เพราะรวมถึง Bluetooth, Zigbee, Z-Wave, LoRaWAN และเครือข่ายเซลลูลาร์ด้วย ประสิทธิภาพของ Wi-Fi ขึ้นอยู่กับย่านความถี่ ระยะห่าง สิ่งกีดขวาง การรบกวน จำนวนอุปกรณ์ และตำแหน่งของ Access Point การออกแบบควรสำรวจพื้นที่และวาง AP ให้มีความครอบคลุมเพียงพอ พร้อมแยกเครือข่ายผู้ใช้ทั่วไป อุปกรณ์รักษาความปลอดภัย และผู้มาติดต่อออกจากกัน ด้านความมั่นคงปลอดภัยควรใช้ WPA2 หรือ WPA3 รหัสผ่านที่รัดกุม การพิสูจน์ตัวตน IEEE 802.1X การปิดฟังก์ชันที่ไม่จำเป็น และการอัปเดตเฟิร์มแวร์สม่ำเสมอ

Zigbee

Zigbee เป็นเทคโนโลยีเครือข่ายส่วนบุคคลไร้สายกำลังต่ำตามมาตรฐาน IEEE 802.15.4 เหมาะกับเซ็นเซอร์และอุปกรณ์ควบคุมที่ส่งข้อมูลปริมาณไม่มากและต้องทำงานด้วยแบตเตอรี่เป็นเวลานาน รองรับโทโพโลยีแบบ star, tree และ mesh โดยประกอบด้วย Coordinator, Router และ End Device การใช้ Mesh ช่วยให้อุปกรณ์ส่งต่อข้อมูลผ่านโหนดอื่น ขยายระยะการสื่อสาร และสร้างเส้นทางใหม่เมื่อเส้นทางเดิมขัดข้อง Zigbee รองรับอุปกรณ์จำนวนมาก อัตรารับส่งข้อมูลสูงสุดประมาณ 250 kbps และใช้ AES-128 เพื่อรักษาความปลอดภัย เหมาะสำหรับเซ็นเซอร์ตรวจจับการเคลื่อนไหว เซ็นเซอร์ประตูและหน้าต่าง เครื่องตรวจจับควัน ระบบไฟอัจฉริยะ และระบบแจ้งเตือน อย่างไรก็ตาม ต้องวางแผนการใช้ช่องสัญญาณเพื่อลดการรบกวนกับ Wi-Fi ในย่าน 2.4 GHz

Z-Wave

Z-Wave เป็นเทคโนโลยีไร้สายกำลังต่ำที่ออกแบบสำหรับ smart home, building automation และระบบรักษาความปลอดภัย โดยทั่วไปทำงานในย่าน Sub-GHz จึงมีการรบกวนจาก Wi-Fi และ Bluetooth น้อยกว่าเทคโนโลยีที่ใช้ย่าน 2.4 GHz เครือข่ายใช้โครงสร้างแบบ Mesh ประกอบด้วย controller และโหนดอุปกรณ์ โดยอุปกรณ์ที่ต่อกับแหล่งจ่ายไฟสามารถช่วยส่งต่อข้อมูลเพื่อเพิ่มระยะทางและความน่าเชื่อถือ Z-Wave เหมาะกับเซ็นเซอร์ประตู-หน้าต่าง อุปกรณ์ตรวจจับการเคลื่อนไหว กลอนประตูอัจฉริยะ ไซเรน และอุปกรณ์ควบคุมภายในอาคาร จุดเด่นคือใช้พลังงานต่ำ มีความสามารถในการทำงานร่วมกันระหว่างผลิตภัณฑ์ และมีระบบเข้ารหัสกับการพิสูจน์ตัวตน อย่างไรก็ตาม ความถี่ที่ใช้งานแตกต่างกันตามภูมิภาค จึงต้องเลือกอุปกรณ์ให้ตรงกับข้อกำหนดของประเทศที่ติดตั้ง

LoRaWAN

LoRaWAN เป็นโปรโตคอลเครือข่ายบริเวณกว้างกำลังต่ำที่เหมาะกับอุปกรณ์ IoT ซึ่งต้องส่งข้อมูลขนาดเล็กในระยะไกลและใช้พลังงานต่ำ ใช้สถาปัตยกรรมแบบ star-of-stars ประกอบด้วย end device, gateway, network server, join server และ application server อุปกรณ์ปลายทางส่งข้อมูลผ่าน LoRa ไปยัง gateway หลายตัว จากนั้น gateway ส่งต่อแพ็กเก็ตผ่านเครือข่าย IP ไปยัง network server เพื่อกำจัดข้อมูลซ้ำ ตรวจสอบความถูกต้อง จัดการเส้นทาง และควบคุมความปลอดภัย LoRaWAN รองรับอุปกรณ์ class A, B และ C ซึ่งแตกต่างกันด้านการใช้พลังงานและความพร้อมรับข้อมูลขาลง ใช้การเข้ารหัส AES-128 และรองรับการเชื่อมต่อแบบ OTAA และ ABP เหมาะสำหรับการเฝ้าระวังพื้นที่กว้าง ระบบติดตามทรัพย์สิน เซ็นเซอร์รั้ว ระบบตรวจจับน้ำท่วม ควัน หรือสภาพแวดล้อมในพื้นที่ที่ไม่มีโครงสร้างพื้นฐานเครือข่ายหนาแน่น

เครือข่ายท้องถิ่นเสมือน (Virtual Local Area Network: VLAN)

VLAN เป็นเทคโนโลยีที่ใช้แบ่งเครือข่าย LAN ทางกายภาพออกเป็นเครือข่ายย่อยเชิงตรรกะในระดับ Data Link Layer อุปกรณ์ใน VLAN เดียวกันจะอยู่ใน Broadcast Domain เดียวกัน แม้เชื่อมต่อกับสวิตช์คนละตัว การใช้งาน VLAN ในระบบรักษาความปลอดภัยช่วยแยกกล้อง IP, access control, alarm/IoT, server, management, office และ guest network ออกจากกัน เพื่อลด broadcast และจำกัดการแพร่กระจายของภัยคุกคาม พอร์ตที่เชื่อมต่ออุปกรณ์ปลายทางมักกำหนดเป็น access port ส่วนลิงก์ระหว่างสวิตช์ใช้ trunk port และ IEEE 802.1Q tag การสื่อสารข้าม VLAN ต้องผ่าน router หรือ layer 3 switch และควรกำหนดนโยบายด้วย firewall หรือ ACL ตามหลัก least privilege ทั้งนี้ VLAN ไม่ใช่มาตรการรักษาความปลอดภัยที่สมบูรณ์โดยลำพัง แต่ต้องใช้ร่วมกับการพิสูจน์ตัวตน การควบคุมสิทธิ์ และการตรวจสอบเครือข่าย

Power over Ethernet (PoE)

PoE เป็นเทคโนโลยีที่ส่งข้อมูลและพลังงานไฟฟ้าผ่านสาย Ethernet เส้นเดียวกัน โดยอุปกรณ์จ่ายไฟเรียกว่า power sourcing equipment เช่น PoE switch หรือ PoE injector ส่วนอุปกรณ์รับไฟเรียกว่า powered device เช่น IP camera, wireless access point, IP phone และ access controller ก่อนจ่ายไฟ PSE จะตรวจสอบว่าอุปกรณ์ปลายทางรองรับ PoE หรือไม่ เพื่อป้องกันความเสียหาย มาตรฐานสำคัญ ได้แก่ IEEE 802.3af, IEEE 802.3at และ IEEE 802.3bt ซึ่งรองรับกำลังไฟเพิ่มขึ้นตามลำดับ การเลือกใช้งานต้องตรวจสอบกำลังไฟรวมของสวิตช์หรือ power budget ให้เพียงพอ รวมถึงคำนึงถึงการสูญเสียในสาย ระยะทาง และความต้องการกำลังไฟสูงสุดของอุปกรณ์ PoE ช่วยลดจำนวนสาย ลดค่าใช้จ่ายในการติดตั้ง และช่วยให้อุปกรณ์ทั้งหมดสามารถสำรองพลังงานจาก UPS ที่จุดศูนย์กลางได้ เหมาะสำหรับกล้อง IP กล้อง PTZ, wireless AP, video intercom, เครื่องอ่าน RFID และอุปกรณ์ IoT ในระบบรักษาความปลอดภัยอัจฉริยะ

แบบฝึกหัดท้ายบทที่ 6
ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัย

ตอนที่ 1 คำถามปรนัย

คำชี้แจง: จงเลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียว

1. ข้อใดอธิบายบทบาทของระบบเครือข่ายในระบบรักษาความปลอดภัยอัจฉริยะได้ถูกต้องที่สุด
   ก. ใช้สำหรับจ่ายพลังงานให้กับอุปกรณ์เท่านั้น
   ข. ใช้เชื่อมโยงอุปกรณ์เพื่อรับส่งข้อมูล ควบคุม และแจ้งเตือน
   ค. ใช้สำหรับจัดเก็บภาพจากกล้องเท่านั้น
   ง. ใช้แทนระบบควบคุมการเข้าออกทั้งหมด
2. คุณลักษณะใดมีความสำคัญต่อเครือข่ายของระบบรักษาความปลอดภัยที่ต้องแจ้งเตือนแบบเวลาจริง
   ก. ความหน่วงต่ำ ข. จำนวนสายสัญญาณมาก
   ค. การใช้ IP Address ซ้ำกัน ง. การปิดระบบเครือข่ายเป็นระยะ
3. โทโพโลยีใดนิยมใช้เชื่อมต่อกล้อง IP แต่ละตัวเข้ากับ PoE Switch
   ก. Bus Topology ข. Star Topology
   ค. Ring Topology ง. Full Mesh Topology
4. ข้อใดเป็นข้อเสียสำคัญของ Star Topology
   ก. ใช้กับ Ethernet ไม่ได้ ข. ไม่สามารถเพิ่มอุปกรณ์ได้
   ค. หากอุปกรณ์ศูนย์กลางขัดข้อง อุปกรณ์ที่เชื่อมต่ออาจไม่สามารถสื่อสารได้
   ง. อุปกรณ์ทุกตัวต้องส่งต่อข้อมูลให้กัน
5. โทโพโลยีใดเหมาะสำหรับสร้างเส้นทางสำรองระหว่างสวิตช์ในอาคารขนาดใหญ่
   ก. Ring หรือ Partial Mesh ข. Bus เพียงอย่างเดียว
   ค. Point-to-Point เพียงเส้นทางเดียว ง. Star ที่ไม่มีอุปกรณ์สำรอง
6. อุปกรณ์ใดทำงานหลักใน Data Link Layer และส่งต่อข้อมูลโดยพิจารณา MAC Address
   ก. Router ข. Network Switch
   ค. Application Server ง. Firewall เท่านั้น
7. อุปกรณ์ใดทำหน้าที่เลือกเส้นทางของ IP Packet ระหว่างเครือข่าย
   ก. Hub ข. Repeater
   ค. Router ง. NIC
8. ข้อใดเป็นหน้าที่ของ Transport Layer
   ก. กำหนดแรงดันไฟฟ้าของสายสัญญา ข. กำหนด MAC Address
   ค. สื่อสารระหว่างกระบวนการโดยใช้หมายเลขพอร์ต ง. จ่ายไฟให้กล้อง IP

9. โปรโตคอลใดเหมาะกับการดาวน์โหลดไฟล์วิดีโอหลักฐานที่ต้องการข้อมูลครบถ้วน

ก. UDP ข. TCP

ค. ARP ง. ICMP

10. โปรโตคอลใดเหมาะกับการสตรีมวิดีโอสดที่ต้องการความหน่วงต่ำ

ก. UDP ข. FTP

ค. SMTP ง. DNS

11. หน่วยข้อมูลใน Network Layer เรียกว่าอะไร

ก. Bit ข. Frame

ค. Segment ง. IP Packet หรือ Datagram

12. ข้อใดเป็นลำดับการห่อหุ้มข้อมูลที่ถูกต้อง

ก. Data > Frame > Segment > Packet > Bit

ข. Data > Segment > Packet > Frame > Bit

ค. Bit > Data > Packet > Segment > Frame

ง. Packet > Data > Frame > Bit > Segment

13. IPv4 Address มีความยาวกี่bit

ก. 16 bit ข. 32 bit

ค. 48 bit ง. 128 bit

14. เครือข่าย 192.168.10.0/24 มี Subnet Mask ตรงกับข้อใด

ก. 255.0.0.0 ข. 255.255.0.0

ค. 255.255.255.0 ง. 255.255.255.252

15. การแบ่ง Subnet มีประโยชน์อย่างไร

ก. เพิ่ม Broadcast Domain ให้ใหญ่ขึ้น

ข. ลด Broadcast Domain และจัดสรร IP Address ได้เหมาะสม

ค. ทำให้อุปกรณ์ทุกตัวใช้ IP เดียวกัน

ง. ยกเลิกการใช้งาน Router

16. ข้อใดเป็นอุปกรณ์ปลายทางในเครือข่ายรักษาความปลอดภัย

ก. IP Camera ข. Router

ค. Core Switch ง. Firewall

17. อุปกรณ์ใดทำหน้าที่เชื่อม WLAN เข้ากับ LAN แบบใช้สาย

ก. Wireless Access Point ข. NVR

ค. Media Converter ง. Join Server

18. ข้อใดเหมาะสำหรับใช้เป็นสื่อกลางของ Backbone ระหว่างอาคาร

ก. สายโทรศัพท์ภายใน ข. สายใยแก้วนำแสง

ค. สาย USB ง. สายสัญญาณสัญญาณเตือน

19. ข้อใดเป็นปัจจัยสำคัญในการเลือกบริการ WAN สำหรับระบบกล้องวงจรปิด

ก. แบนด์วิดท์ขาขึ้น ข. สีของเราเตอร์

ค. จำนวนปลั๊กไฟในห้อง ง. ขนาดหน้าจอของผู้ใช้

20. Ethernet ทำงานเกี่ยวข้องกับชั้นใดเป็นหลัก

ก. Physical และ Data Link Layer ข. Network และ Application Layer

ค. Session และ Presentation Layer ง. Application Layer เพียงชั้นเดียว

21. Wi-Fi เป็นมาตรฐานในกลุ่มใด

ก. IEEE 802.3 ข. IEEE 802.11

ค. IEEE 802.15.4 ง. IEEE 802.1Q

22. ข้อใดเป็นมาตรการรักษาความปลอดภัยของ Wi-Fi ที่เหมาะสม

ก. ใช้ WEP ข. ใช้ WPA3 และแยกเครือข่ายด้วย VLAN

ค. เปิดเครือข่ายโดยไม่ใช้รหัสผ่าน ง. ใช้รหัสผ่านเดียวกับอุปกรณ์ทุกระบบตลอดเวลา

23. Zigbee เหมาะกับงานลักษณะใดมากที่สุด

ก. การส่งวิดีโอความละเอียดสูง ข. เซ็นเซอร์พลังงานต่ำและข้อมูลปริมาณน้อย

ค. การเชื่อมต่อ WAN ระหว่างประเทศ ง. การสำรองไฟให้เซิร์ฟเวอร์

24. ข้อใดเป็นอุปกรณ์หลักในเครือข่าย Zigbee

ก. Coordinator, Router และ End Device ข. Server, Hub และ Repeater

ค. Modem, Firewall และ NVR ง. CPE, PE Router และ Core Router

25. Z-Wave มีข้อดีเด่นเมื่อเปรียบเทียบกับเทคโนโลยีที่ใช้ย่าน 2.4 GHz คือข้อใด

ก. ส่งวิดีโอได้เร็วกว่า Ethernet ข. มีโอกาสถูกรบกวนจาก Wi-Fi น้อยกว่า

ค. ไม่ต้องใช้ Controller ง. ใช้ได้โดยไม่ต้องคำนึงถึงความถี่ของแต่ละประเทศ

26. LoRaWAN ใช้สถาปัตยกรรมเครือข่ายแบบใด

ก. Bus ข. Star-of-Stars

ค. Ring ง. Full Mesh ระหว่าง End Devices

27. องค์ประกอบใดทำหน้าที่กำจัดแพ็กเก็ตซ้ำใน LoRaWAN

ก. End Device ข. Gateway

ค. Network Server ง. Mobile Application

28. VLAN ทำหน้าที่สำคัญอย่างไร

ก. เพิ่มแรงดันไฟฟ้าในสาย Ethernet

ข. แบ่งเครือข่ายเชิงตรรกะออกเป็น Broadcast Domain

ค. แทนที่ Firewall ได้ทั้งหมด

ง. แปลง IPv4 เป็น IPv6

29. พอร์ตที่ใช้เชื่อมต่ออุปกรณ์ปลายทางเข้าสู่ VLAN เดียวโดยทั่วไปเรียกว่าอะไร

ก. Trunk Port ข. Access Port

ค. WAN Port ง. Console Port

30. อุปกรณ์ที่จ่ายพลังงานในระบบ PoE เรียกว่าอะไร

ก. Powered Device ข. Power Sourcing Equipment

ค. End Device ง. Application Server

31. กล้อง IP ที่รับพลังงานจาก PoE Switch จัดเป็นอุปกรณ์ประเภทใด

ก. PSE ข. PD

ค. PE ง. CPE

32. ข้อใดเป็นมาตรฐาน PoE ที่รองรับกำลังไฟสูงกว่ามาตรฐาน IEEE 802.3af

ก. IEEE 802.3at และ IEEE 802.3bt ข. IEEE 802.11ax

ค. IEEE 802.15.4 ง. IEEE 802.1X

ตอนที่ 2 คำถามอัตนัยด้านความรู้และความเข้าใจ

33. อธิบายความสำคัญของระบบเครือข่ายต่อการทำงานของระบบรักษาความปลอดภัยอัจฉริยะ

---

34. อธิบายองค์ประกอบหลักของเครือข่ายระบบรักษาความปลอดภัยทั้ง 7 ส่วน พร้อมยกตัวอย่างอุปกรณ์ในแต่ละส่วน

---

35. เปรียบเทียบ Physical Topology และ Logical Topology พร้อมยกตัวอย่างในระบบกล้องวงจรปิด

---

36. เปรียบเทียบข้อดีและข้อจำกัดของ Bus, Star, Ring, Mesh และ Hybrid Topology

---

---

37. อธิบายเหตุผลที่ระบบรักษาความปลอดภัยขนาดใหญ่ควรใช้เส้นทางเครือข่ายและแหล่งจ่ายไฟสำรอง

---

38. อธิบายหน้าที่ของ Physical, Data Link, Network, Transport และ Application Layer โดยเชื่อมโยงกับการส่งภาพจาก IP Camera ไปยัง NVR

---

39. เปรียบเทียบการสื่อสารแบบ End-to-End และ Hop-to-Hop

---

40. อธิบายความแตกต่างระหว่าง TCP และ UDP พร้อมยกตัวอย่างการใช้งานในระบบรักษาความปลอดภัยอย่างละสองกรณี

---

41. อธิบายกระบวนการ Encapsulation และ Decapsulation ตั้งแต่ต้นทางถึงปลายทาง

---

42. อธิบายความแตกต่างระหว่าง IP Address และ MAC Address

---

43. อธิบายเหตุผลที่กล้อง IP, NVR และ Access Controller ควรใช้ Static IP หรือ DHCP Reservation

---

---

44. อธิบายประโยชน์ของ Subnetting ในการออกแบบระบบรักษาความปลอดภัย

---

45. อธิบายหน้าที่ของ NIC, Switch, Router และ Wireless Access Point ภายใน LAN

---

46. อธิบายความแตกต่างระหว่าง LAN และ WAN ในด้านพื้นที่ ความเป็นเจ้าของโครงสร้างพื้นฐาน ความหน่วง และการบริหารจัดการ

---

47. อธิบายบทบาทของ CPE, Access Link, PE Router และ WAN Backbone

---

---

48. อธิบายเหตุผลที่ระบบกล้องวงจรปิดจากสาขาต้องให้ความสำคัญกับแบนด์วิดท์ขาขึ้นของ WAN

---

49. อธิบายโครงสร้างของ Ethernet Frame และหน้าที่ของ Frame Check Sequence

---

---

50. อธิบายความแตกต่างระหว่าง Switch Layer 2 และ Router หรือ Layer 3 Switch

---

---

51. อธิบายปัจจัยที่มีผลต่อคุณภาพสัญญาณ Wi-Fi ในอาคาร

---

52. เปรียบเทียบ Wi-Fi, Zigbee, Z-Wave และ LoRaWAN ในด้านระยะทาง อัตรารับส่งข้อมูล การใช้พลังงาน และลักษณะงานที่เหมาะสม

---

53. อธิบายการทำงานของ Mesh Network ใน Zigbee และ Z-Wave รวมทั้งข้อดีและข้อจำกัด

---

54. อธิบายองค์ประกอบและการไหลของข้อมูลในสถาปัตยกรรม LoRaWAN ตั้งแต่ End Device ไปจนถึง End User Application

---

---

55. อธิบายเหตุผลที่ LoRaWAN End Device สามารถประหยัดพลังงานได้มากกว่าโหนดในเครือข่าย Mesh บางประเภท

---

56. อธิบายหลักการทำงานของ VLAN และความแตกต่างระหว่าง Access Port กับ Trunk Port

---

---

57. เพราะเหตุใด VLAN เพียงอย่างเดียวจึงไม่เพียงพอสำหรับการรักษาความมั่นคงปลอดภัยของเครือข่าย

---

58. อธิบายหลักการทำงานของ PoE และความแตกต่างระหว่าง PSE กับ PD

---

59. อธิบายปัจจัยที่ต้องพิจารณาในการคำนวณ PoE Power Budget

ตอนที่ 3 แบบฝึกหัดการคำนวณและการวิเคราะห์

60. ให้ออกแบบเครือข่ายสำหรับอาคารสำนักงาน

อาคารสำนักงานสูง 8 ชั้นต้องติดตั้งกล้อง IP ชั้นละ 12 ตัว ระบบควบคุมการเข้าออกชั้นละ 4 จุด และ Wireless Access Point ชั้นละ 2 ตัว จงออกแบบโครงสร้างเครือข่ายโดยระบุ

1. รูปแบบ Network Topology
2. ประเภทและจำนวนสวิตช์โดยประมาณ
3. การใช้ PoE
4. สื่อส่งสัญญาณสำหรับอุปกรณ์ปลายทางและ Backbone
5. แนวทางสำรองระบบเมื่อสวิตช์หรือสาย Backbone ขัดข้อง
6. แนวทางแบ่ง VLAN

7 อินเทอร์เน็ตของสรรพสิ่งสำหรับระบบรักษาความปลอดภัย

71

พื้นฐานของ INTERNET OF THINGS

7.1.1 องค์ประกอบพื้นฐานของระบบ IoT

7.1.2 หลักการทำงานของระบบ IoT

7.1.3 ความสำคัญของ IoT ในระบบรักษาความปลอดภัยอัจฉริยะ

72

ไมโครคอนโทรลเลอร์ ARDUINO

7.2.1 แพลตฟอร์ม Arduino

7.2.2 สถาปัตยกรรมของ Arduino Uno R3

7.2.3 ซอฟต์แวร์ Arduino IDE

7.2.4 การเชื่อมต่อโมดูล RC522 RFID กับไมโครคอนโทรลเลอร์ Arduino

7.2.5 การติดตั้งไลบรารี MFRC522

7.2.6 การตรวจสอบการเชื่อมต่อและการอ่านข้อมูลของ MFRC522

7.2.7 การประยุกต์ใช้แท็ก RFID ควบคุมการเปิดปิดอุปกรณ์

73

NODEMCU ESP8266

7.3.1 ประเภทของโมดูลและบอร์ดพัฒนา ESP8266

7.3.2 โครงสร้างของ ESP8266

7.3.3 การเชื่อมต่อ ESP8266 กับโปรแกรม Arduino IDE

7.3.4 การเชื่อมต่อโมดูล RFID RC522 กับ ESP8266

7.3.5 การพัฒนาเว็บเซิร์ฟเวอร์ด้วย ESP8266

74

RASPBERRY PI

7.4.1 ความหมายและวิวัฒนาการของ Raspberry Pi

7.4.2 สถาปัตยกรรมและองค์ประกอบของ Raspberry Pi

7.4.3 คุณสมบัติของ Raspberry Pi

7.4.3 GPIO ของ Raspberry Pi

75 **แพลตฟอร์มคลาวด์เพื่อใช้ในระบบความปลอดภัยอัจฉริยะ**

7.5.1 ความหมายของ Cloud Platform

7.5.2 องค์ประกอบของ Cloud Platform

7.5.3 รูปแบบการให้บริการของ Cloud Platform

7.5.4 บทบาทของ Cloud Platform ในระบบความปลอดภัยอัจฉริยะ

76 **REST API**

7.6.1 หลักการทำงานของ REST API

7.6.2 LINE Messaging API

7.6.3 การเชื่อมต่อ Google Cloud และ Google Sheets

บทที่ 7 อินเทอร์เน็ตของสรรพสิ่งสำหรับระบบรักษาความปลอดภัย

Internet of Things (IoT) for Smart Security

ระบบรักษาความปลอดภัยอัจฉริยะ (smart security system) ในปัจจุบันได้พัฒนาจากระบบรักษาความปลอดภัยแบบแยกส่วน (standalone security system) ไปสู่ระบบที่สามารถเชื่อมโยงอุปกรณ์หลากหลายชนิดผ่านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต โดยอาศัยเทคโนโลยี Internet of Things (IoT) ทำให้อุปกรณ์ เช่น กล้องวงจรปิด (IP camera) ระบบควบคุมการเข้าออก (access control system) เซนเซอร์ตรวจจับการบุกรุก (intrusion detection sensors) เซนเซอร์ตรวจจับควันและก๊าซ ระบบแจ้งเตือนอัคคีภัย และระบบบริหารจัดการอาคาร สามารถสื่อสาร แลกเปลี่ยนข้อมูล และทำงานร่วมกันแบบอัตโนมัติผ่านเครือข่ายเดียวกันได้

7.1 พื้นฐานของ Internet of Things (IoT)

IoT หรือ อินเทอร์เน็ตของสรรพสิ่ง เป็นแนวคิดของการเชื่อมโยงอุปกรณ์ วัตถุ เครื่องจักร และระบบต่าง ๆ เข้ากับเครือข่ายอินเทอร์เน็ต เพื่อให้สามารถรับรู้สภาพแวดล้อม (sensing) แลกเปลี่ยนข้อมูล (data exchange) วิเคราะห์ข้อมูล (data analytics) และสั่งงานหรือควบคุมอุปกรณ์ได้โดยอัตโนมัติหรือกึ่งอัตโนมัติผ่านระบบเครือข่าย โดยมีเป้าหมายเพื่อเพิ่มประสิทธิภาพในการทำงาน ลดการใช้ทรัพยากร และสนับสนุนการตัดสินใจบนพื้นฐานของข้อมูล (data-driven decision making) (Atzori et al., 2010; Al-Fuqaha et al., 2015) แนวคิดของ IoT เกิดขึ้นจากการพัฒนาของเทคโนโลยีอินเทอร์เน็ต เซ็นเซอร์ ระบบสมองกลฝังตัว (embedded systems) ระบบสื่อสารไร้สาย การประมวลผลแบบคลาวด์ (cloud computing) และปัญญาประดิษฐ์ (Artificial Intelligence: AI) ซึ่งทำให้อุปกรณ์ต่าง ๆ สามารถเชื่อมต่อกันได้อย่างต่อเนื่องและสามารถสื่อสารกันแบบ Machine-to-Machine (M2M) โดยไม่จำเป็นต้องอาศัยการควบคุมจากมนุษย์ตลอดเวลา

กล่าวโดยสรุป IoT คือระบบที่ทำให้อุปกรณ์ทางกายภาพ (physical objects) กลายเป็นอุปกรณ์อัจฉริยะ (smart objects) ผ่านการติดตั้งเซ็นเซอร์ ตัวกระตุ้น (actuator) หน่วยประมวลผล และโมดูลสื่อสารเครือข่าย ทำให้อุปกรณ์สามารถเก็บข้อมูล วิเคราะห์สถานการณ์ และตอบสนองต่อเหตุการณ์ต่าง ๆ ได้อย่างชาญฉลาด (Ayeni, 2020)

7.1.1 องค์ประกอบพื้นฐานของระบบ IoT

ระบบ IoTประกอบด้วยองค์ประกอบสำคัญหลายส่วนที่ทำงานร่วมกัน ดังนี้

1) อุปกรณ์ตรวจวัด (sensors)

เซ็นเซอร์เป็นองค์ประกอบสำคัญที่สุดของ IoT ทำหน้าที่ตรวจวัดข้อมูลจากสภาพแวดล้อม เช่น อุณหภูมิ ความชื้น แสงสว่าง ความดัน ควัน ก๊าซ การเคลื่อนไหว หรือตำแหน่ง โดยข้อมูลที่เซ็นเซอร์ตรวจวัดได้จะถูกแปลงเป็นสัญญาณดิจิทัลและส่งต่อไปยังระบบประมวลผลเพื่อวิเคราะห์และตัดสินใจ (Al-Fuqaha et al., 2015)

2) ตัวกระตุ้น (Actuators)

actuator เป็นอุปกรณ์ที่รับคำสั่งจากระบบประมวลผลแล้วเปลี่ยนเป็นการกระทำทางกายภาพ เช่น เปิดหรือปิดไฟ เปิดหรือปิดวาล์ว หมุนมอเตอร์ เปิดระบบระบายอากาศ เปิดสัญญาณ

เตือนภัย กล่าวคือ เซ็นเซอร์ทำหน้าที่ "รับข้อมูล" ส่วน actuator ทำหน้าที่ "ตอบสนอง" ต่อข้อมูลดังกล่าว

3) หน่วยประมวลผล (Processing Unit)

หน่วยประมวลผลทำหน้าที่ควบคุมการทำงานของอุปกรณ์ IoT ประมวลผลข้อมูลจากเซ็นเซอร์ และส่งคำสั่งไปยัง actuator โดยอาจเป็น microcontroller, microprocessor, หรือ embedded computer เช่น Arduino, ESP32, ESP8266, Raspberry Pi, STM32 หน่วยประมวลผลบางระบบสามารถประมวลผลข้อมูลภายในอุปกรณ์ (Edge computing) เพื่อลดภาระการส่งข้อมูลไปยัง cloud และลดเวลาตอบสนองของระบบ

4) ระบบสื่อสาร (Communication Network)

ข้อมูลจากอุปกรณ์ IoT จะถูกส่งผ่านเครือข่ายสื่อสารไปยัง gateway หรือ cloud โดยเลือกใช้เทคโนโลยีที่เหมาะสมกับระยะทาง อัตราการรับส่งข้อมูล และการใช้พลังงาน เช่นEthernet, Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, NB-IoT, 4G/5G การเลือกเทคโนโลยีสื่อสารขึ้นอยู่กับลักษณะของงาน เช่น ระบบ smart home มักใช้ Wi-Fi หรือ Zigbee ขณะที่ smart agriculture นิยมใช้ LoRaWAN เนื่องจากครอบคลุมระยะทางไกลและใช้พลังงานต่ำ (Raja et al., 2023)

5) Gateway

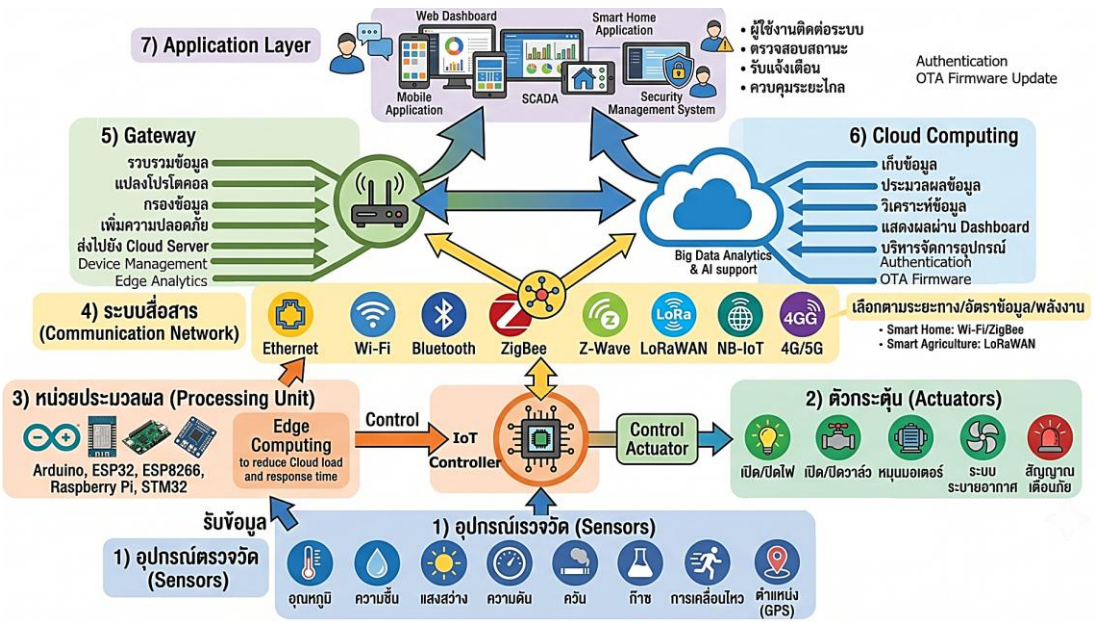
IoT gateway เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์ IoT กับเครือข่ายอินเทอร์เน็ต โดยทำหน้าที่ รวบรวมข้อมูลจากอุปกรณ์หลายตัว แปลงโปรโตคอลการสื่อสาร กรองข้อมูล เพิ่มความปลอดภัย และส่งข้อมูลไปยัง cloud server โดย gateway มีบทบาทสำคัญในระบบที่มีอุปกรณ์จำนวนมาก หรือมีการใช้โปรโตคอลหลายประเภทในระบบเดียวกัน

6) Cloud Computing

Cloud เป็นศูนย์กลางสำหรับ เก็บข้อมูล ประมวลผลข้อมูล วิเคราะห์ข้อมูล แสดงผลผ่าน Dashboard และ บริหารจัดการอุปกรณ์ IoT cloud computing ช่วยให้สามารถจัดเก็บข้อมูลจำนวนมหาศาลและรองรับการขยายตัวของระบบได้อย่างมีประสิทธิภาพ อีกทั้งยังสนับสนุนการวิเคราะห์ข้อมูลด้วยเทคนิค big data analytics และ Artificial Intelligence (AI) เพื่อเพิ่มความแม่นยำในการตัดสินใจ (Al-Fuqaha et al., 2015)

7) Application Layer

Application คือส่วนที่ผู้ใช้งานติดต่อกับระบบ เช่น mobile application, Web dashboard, Supervisory Control and Data Acquisition (SCADA), smart home application, security management system ผู้ใช้งานสามารถตรวจสอบสถานะอุปกรณ์ รับการแจ้งเตือน และควบคุมอุปกรณ์จากระยะไกลผ่านอินเทอร์เน็ตได้



รูปที่ 7.1 องค์ประกอบพื้นฐานของระบบ IoT

7.1.2 หลักการทำงานของระบบ IoT

โดยทั่วไป ระบบ IoT ทำงานเป็นลำดับขั้น ดังนี้

1) เซ็นเซอร์ตรวจวัดข้อมูลจากสภาพแวดล้อม
2) หน่วยประมวลผลรวบรวมและประมวลผลข้อมูลเบื้องต้น
3) ส่งข้อมูลผ่านเครือข่ายสื่อสารไปยัง gateway หรือ cloud
4) Cloud วิเคราะห์ข้อมูลและจัดเก็บฐานข้อมูล
5) ระบบประมวลผลสร้างคำสั่งหรือแจ้งเตือน
6) ส่งคำสั่งกลับมายังอุปกรณ์ IoT
7) Actuator ดำเนินการตามคำสั่ง เช่น เปิดไฟ เปิดพัดลม หรือแจ้งเตือนผู้ใช้งาน

กระบวนการดังกล่าวช่วยให้ระบบสามารถทำงานแบบอัตโนมัติ (automation) ติดตามสถานะได้แบบเวลาจริง (real-time monitoring) และควบคุมจากระยะไกล (remote control) ซึ่งเป็นคุณลักษณะสำคัญของระบบ IoT ในงานด้าน smart home, smart building, smart factory และ smart security system ซึ่งระบบ IoT มีคุณลักษณะสำคัญหลายประการ ได้แก่ (1) การเชื่อมต่อ (connectivity) คือ อุปกรณ์สามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลผ่านเครือข่ายอินเทอร์เน็ตได้อย่างต่อเนื่อง (2) การรับรู้สภาพแวดล้อม (sensing) ใช้เซ็นเซอร์ในการเก็บข้อมูลจากสภาพแวดล้อมจริง (3) ระบบอัตโนมัติ (automation) สามารถดำเนินการตอบสนองต่อเหตุการณ์ได้โดยอัตโนมัติ (4) การประมวลผลอัจฉริยะ (intelligence) เป็นการผสานการทำงานร่วมกับ AI และ machine learning เพื่อเพิ่มความสามารถในการวิเคราะห์และคาดการณ์ (5) การขยายระบบได้ (scalability) เพื่อให้รองรับการเพิ่มจำนวนอุปกรณ์โดยไม่กระทบต่อประสิทธิภาพของระบบ และ (6) การทำงานร่วมกัน (interoperability) รองรับการสื่อสารระหว่างอุปกรณ์จากผู้ผลิตและมาตรฐานที่แตกต่างกันผ่านโปรโตคอลที่เหมาะสม (Ayeni, 2020; Ayeni et al., 2025; Raja et al., 2023)

7.1.3 ความสำคัญของ IoT ในระบบรักษาความปลอดภัยอัจฉริยะ

IoT เป็นเทคโนโลยีพื้นฐานของระบบรักษาความปลอดภัยอัจฉริยะในปัจจุบัน โดยทำให้อุปกรณ์ต่าง ๆ เช่น กล้อง IP camera เครื่องตรวจจับควัน เครื่องตรวจจับก๊าซ เซ็นเซอร์ตรวจจับการเคลื่อนไหว ระบบควบคุมประตู และระบบแจ้งเตือน สามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลผ่านเครือข่ายได้แบบเวลาจริง ผู้ดูแลระบบสามารถติดตามสถานะ แจ้งเตือนเหตุการณ์ผิดปกติ และควบคุมอุปกรณ์จากระยะไกลผ่านสมาร์ตโฟนหรือศูนย์ควบคุมได้อย่างมีประสิทธิภาพ นอกจากนี้การผสาน IoT กับ cloud computing, Edge computing และ AI ยังช่วยให้ระบบสามารถวิเคราะห์เหตุการณ์ คาดการณ์ความเสี่ยง และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและแม่นยำ ส่งผลให้ระบบรักษาความปลอดภัยมีประสิทธิภาพ ความน่าเชื่อถือ และความสามารถในการขยายระบบสูงขึ้น

7.2 ไมโครคอนโทรลเลอร์ Arduino

Arduino เป็นแพลตฟอร์มสำหรับพัฒนาต้นแบบทางอิเล็กทรอนิกส์แบบเปิด (open-source electronics prototyping platform) ประกอบด้วยฮาร์ดแวร์บอร์ดไมโครคอนโทรลเลอร์และซอฟต์แวร์สำหรับพัฒนาโปรแกรม จุดเด่นของ Arduino คือมีโครงสร้างที่ยืดหยุ่น ใช้งานได้ไม่ซับซ้อน และรองรับการเชื่อมต่อกับเซ็นเซอร์ อุปกรณ์แสดงผล โมดูลสื่อสาร และแอกชูเอเตอร์ได้หลากหลาย จึงเหมาะสำหรับการศึกษา การทดลอง การสร้างต้นแบบระบบสมองกลฝังตัว ระบบอัตโนมัติ หุ่นยนต์ และระบบอินเทอร์เน็ตของสรรพสิ่ง Arduino สามารถรับข้อมูลจากเซ็นเซอร์ทั้งแบบดิจิทัลและแอนะล็อก นำข้อมูลมาประมวลผลตามโปรแกรมที่กำหนด และส่งสัญญาณไปควบคุมอุปกรณ์เอาต์พุต เช่น หลอดไฟ LED รีเลย์ มอเตอร์ และจอแสดงผล นอกจากนี้ยังสามารถเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายเพื่อรับส่งและบันทึกข้อมูลได้ ความสามารถดังกล่าวทำให้ Arduino เหมาะสำหรับการสร้างอุปกรณ์ต้นแบบที่ต้นทุนไม่สูงและสามารถปรับเปลี่ยนให้สอดคล้องกับวัตถุประสงค์ (Gubsky, 2023; Kim et al., 2020)

7.2.1 แพลตฟอร์ม Arduino

ผู้เริ่มต้นไม่จำเป็นต้องศึกษาสถาปัตยกรรมภายในของไมโครคอนโทรลเลอร์อย่างละเอียดทั้งหมดก่อนใช้งาน แต่ควรมีความรู้พื้นฐานเกี่ยวกับชนิดของบอร์ด คุณสมบัติทางไฟฟ้า หมายเลขขาอินพุตและเอาต์พุต ข้อจำกัดด้านแรงดันและกระแส ตลอดจนวิธีเชื่อมต่อวงจรอย่างปลอดภัย ความรู้ดังกล่าวมีความสำคัญต่อการป้องกันความเสียหายของบอร์ดและอุปกรณ์ที่นำมาเชื่อมต่อ แพลตฟอร์ม Arduino ประกอบด้วยสองส่วนสำคัญ ได้แก่ ฮาร์ดแวร์ และ ซอฟต์แวร์

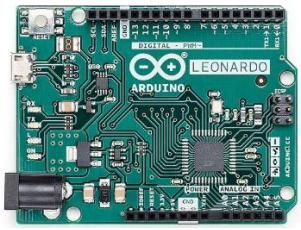
1) ฮาร์ดแวร์ Arduino

ฮาร์ดแวร์ Arduino เป็นบอร์ดวงจรพิมพ์ที่มีไมโครคอนโทรลเลอร์เป็นส่วนประกอบหลัก พร้อมวงจรสนับสนุนที่ช่วยให้ผู้ใช้สามารถจ่ายไฟ อัปโหลดโปรแกรม และเชื่อมต่ออุปกรณ์ภายนอกได้สะดวก บอร์ดแต่ละรุ่นแตกต่างกันในด้านชนิดของไมโครคอนโทรลเลอร์ จำนวนขาอินพุตและเอาต์พุต ขนาดหน่วยความจำ แรงดันไฟฟ้าทำงาน ความเร็วสัญญาณนาฬิกา ขนาดของบอร์ด และอินเทอร์เฟซการสื่อสาร ตัวอย่างบอร์ดที่นิยมใช้ ได้แก่ Arduino Uno R3, Arduino Mega ใช้

ไมโครคอนโทรลเลอร์ ATmega2560 มีขาอินพุตและเอาต์พุต รวมถึงหน่วยความจำมากกว่า Arduino Uno จึงเหมาะสำหรับระบบที่ต้องเชื่อมต่ออุปกรณ์จำนวนมาก ตัวอย่างบอร์ด Arduino แสดงดังรูปที่ 7.2 และรายละเอียดดังตารางที่ 7.1

(ก) Arduino UNO R3

(ข) Arduino UNO R4 Minima



(ค) Arduino Leonardo

(ง) Arduino UNO WIFI

(จ) Arduino Zero

(ฉ) Arduino Mega

(ช) Arduino Due

(ซ) Arduino UNO R4 WiFi

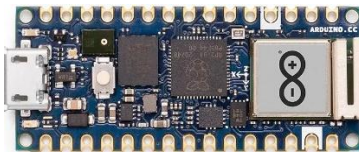
(ฌ) Arduino MKR Zero

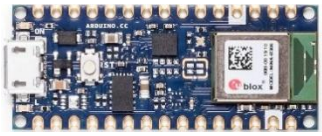
(ญ) Arduino Nano

(ฎ) Arduino Micro

(ฏ) Arduino Nano Every

(ฐ) Arduino GIGA R1 WiFi

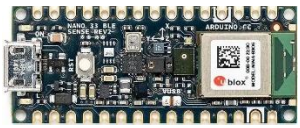

(ฑ) Arduino Nano RP


(ฒ) Arduino Nano 33 BLE

(ณ) Arduino Nano 33 IoT

(ด) Arduino MKR WiFi

(ต) Arduino Nano ESP32


(ถ) Arduino Nano BLE

(ท) Arduino MKR Vidor

(ธ) Arduino MKR NB

(น) Nicla Sense ME

(บ) Nicla Voice

(ป) Nicla Vision

(ผ) Portenta H7

(ฝ) Portenta X8

(พ) Portenta C33

รูปที่ 7.2 ตัวอย่างบอร์ด Arduino รุ่นต่าง ๆ

ตารางที่ 7.1 ตัวอย่างบอร์ด Arduino รุ่นต่าง ๆ

บอร์ด	การใช้งาน	การเชื่อมต่อ	หน่วยประมวลผล	งานที่เหมาะสม	จุดเด่นสำคัญ
Arduino Uno R3	ระดับเริ่มต้น	ไม่มีการสื่อสารไร้สายในตัว	8 bit	การเรียนรู้และโครงงานพื้นฐาน	ใช้งานง่ายและมีแหล่งสนับสนุนจำนวนมาก
Arduino UNO R4 WiFi	IoT	Wi-Fi และ BLE	32 bit	อุปกรณ์อัจฉริยะ	มีระบบสื่อสารไร้สายในตัว
Arduino Nano	ขนาดกะทัดรัด	ไม่มีการสื่อสารไร้สายในตัว	8 bit	โครงงานบนเบรดบอร์ด	มีขนาดเล็ก
Arduino Nano Every	ขนาดกะทัดรัด	ไม่มีการสื่อสารไร้สายในตัว	8 bit	โครงงานที่ต้องการประสิทธิภาพสูงกว่า Nano รุ่นเดิม	มีหน่วยความจำมากขึ้น
Arduino Nano ESP32	IoT	Wi-Fi และ BLE	32 bit	โครงงานไร้สาย	ประสิทธิภาพสูง
Arduino Mega 2560	ระดับสูง	ไม่มีการสื่อสารไร้สายในตัว	8 bit	หุ่นยนต์และระบบที่ใช้เซ็นเซอร์จำนวนมาก	มีขา I/O จำนวนมาก

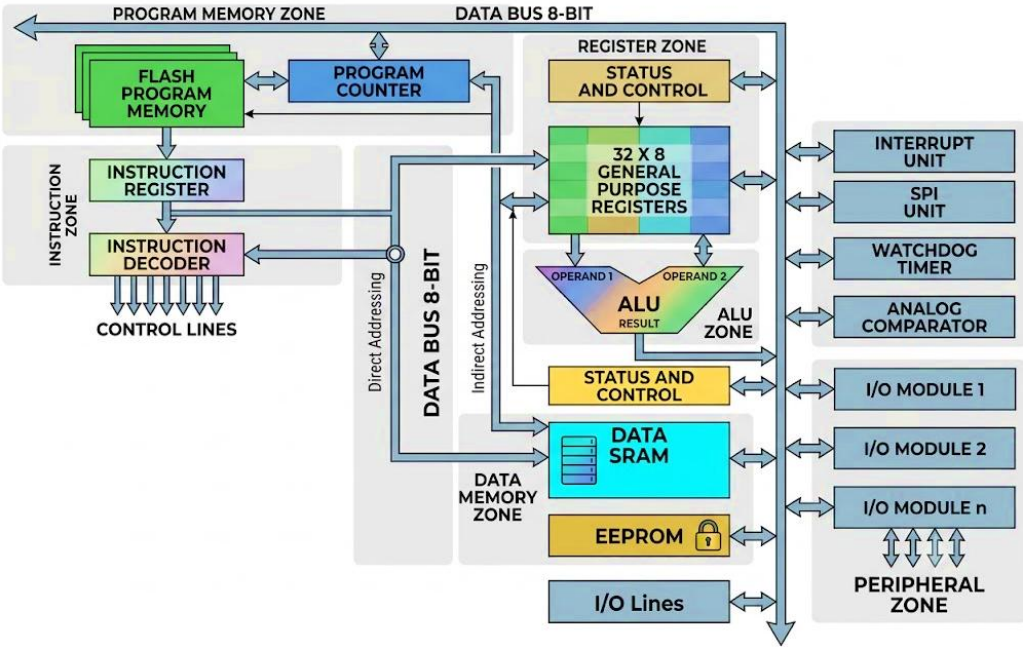
ตารางที่ 7.1 ตัวอย่างบอร์ด Arduino รุ่นต่าง ๆ (ต่อ)

บอร์ด	การใช้งาน	การเชื่อมต่อ	หน่วยประมวลผล	งานที่เหมาะสม	จุดเด่นสำคัญ
Arduino Leonardo	งานด้าน USB	ไม่มีการสื่อสารไร้สายในตัว	8 bit	อุปกรณ์ HID	ทำงานเลียนแบบแป้นพิมพ์หรือเมาส์ได้
Arduino Due	ประสิทธิภาพสูง	ไม่มีการสื่อสารไร้สายในตัว	32 bit	ระบบที่มีความซับซ้อน	ประมวลผลได้รวดเร็ว
Arduino Zero	ระดับสูง	ไม่มีการสื่อสารไร้สายในตัว	32 bit	ระบบประหยัดพลังงานและงาน 32 bit	ออกแบบให้ใช้พลังงานอย่างมีประสิทธิภาพ
Arduino Nano 33 BLE	AI/IoT	BLE	32 bit	อุปกรณ์สวมใส่และการเรียนรู้ของเครื่อง	มีหน่วยวัดความเฉื่อยในตัว
Arduino Nano 33 IoT	IoT	Wi-Fi และ BLE	32 bit	อุปกรณ์เชื่อมต่อเครือข่าย	รองรับการสื่อสารที่มีความปลอดภัย
Arduino GIGA R1 WiFi	ระดับมืออาชีพ	Wi-Fi และ BLE	แบบสองแกนประมวลผล	หุ่นยนต์และระบบเวลาจริง	มีสมรรถนะสูงมาก
Portenta H7	ระดับอุตสาหกรรม	Wi-Fi และ BLE	แบบสองแกนประมวลผล	AI และ Edge Computing	ออกแบบสำหรับงานอุตสาหกรรม
Portenta C33	IoT ระดับมืออาชีพ	Wi-Fi และ BLE	32 bit	ระบบ IoT ที่ต้องการความปลอดภัย	ให้ความสำคัญกับความมั่นคงปลอดภัย

7.2.2 สถาปัตยกรรมของ Arduino Uno R3 (Architecture of Arduino Uno R3)

Arduino Uno R3 เป็นบอร์ดไมโครคอนโทรลเลอร์ที่ออกแบบตามแนวคิดของระบบสมองกลฝังตัว มีไมโครคอนโทรลเลอร์ ATmega328P เป็นหน่วยประมวลผลกลาง (Central Processing Unit: CPU) ทำหน้าที่รับข้อมูลจากอุปกรณ์อินพุต ประมวลผลคำสั่งตามโปรแกรมและส่งผลลัพธ์ไปควบคุมอุปกรณ์เอาต์พุต สถาปัตยกรรมของ Arduino มีองค์ประกอบหลัก ได้แก่ หน่วยประมวลผลกลาง หน่วยความจำ วงจรจ่ายไฟ วงจรสร้างสัญญาณนาฬิกา วงจรแปลงสัญญาณ USB เป็น UART ชุดขาอินพุต เอาต์พุต สำหรับเชื่อมต่อกับอุปกรณ์ภายนอก บอร์ดสามารถรับสัญญาณจากเซ็นเซอร์ทั้งแอนะล็อกและดิจิทัล (Gubsky, 2023) ในเชิงสถาปัตยกรรม Arduino ทำหน้าที่เป็นตัวควบคุม (controller) ที่อยู่ระหว่างอุปกรณ์ตรวจจับ (sensors) และอุปกรณ์ตอบสนอง (actuators) โดย

ข้อมูลที่รับจากเซ็นเซอร์จะถูกประมวลผลตามอัลกอริทึมที่กำหนดไว้ในโปรแกรม จากนั้นจึงส่งคำสั่งไปควบคุมอุปกรณ์ปลายทางหรือส่งข้อมูลไปยังระบบเครือข่ายผ่านโมดูลสื่อสาร ทำให้พัฒนาระบบที่มีความยืดหยุ่นและง่าย



รูปที่ 7.3 สถาปัตยกรรมภายในโดยสังเขปของไมโครคอนโทรลเลอร์ AVR แบบ 8 bit

รูปที่ 7.3 สถาปัตยกรรมภายในของไมโครคอนโทรลเลอร์ AVR มีหลักการทำงานดังนี้

1) หน่วยความจำโปรแกรม (Flash Program Memory)

ในส่วนนี้จะใช้เก็บโปรแกรมที่ผู้ใช้อัปโหลดเข้าสู่ไมโครคอนโทรลเลอร์ เช่น โปรแกรม Arduino Sketch ข้อมูลในหน่วยความจำแฟลชยังคงอยู่แม้ตัดแหล่งจ่ายไฟ โดย program counter ทำหน้าที่เก็บตำแหน่งของคำสั่งถัดไปที่จะถูกอ่านจาก flash program memory โดยค่าของ program counter จะเพิ่มขึ้นตามลำดับคำสั่ง หรือเปลี่ยนไปยังตำแหน่งใหม่เมื่อพบคำสั่งกระโดด การเรียกฟังก์ชัน หรือการขัดจังหวะ

2) การรับและถอดรหัสคำสั่ง

คำสั่งที่อ่านจากหน่วยความจำโปรแกรมจะถูกส่งเข้าสู่ instruction register เพื่อเก็บคำสั่งปัจจุบัน จากนั้น instruction decoder จะวิเคราะห์ว่าคำสั่งนั้นต้องดำเนินการใด เช่นการย้ายข้อมูล การบวกหรือลบ การเปรียบเทียบค่า การอ่านหรือเขียนขา I/O หรือการกระโดดไปยังตำแหน่งอื่นของโปรแกรม เมื่อถอดรหัสแล้ว วงจรควบคุมจะสร้าง control lines เพื่อควบคุมส่วนต่าง ๆ ภายในไมโครคอนโทรลเลอร์ให้ทำงานตามคำสั่ง

3) ชุดรีจิสเตอร์ทั่วไป (General-Purpose Registers)

ส่วน 32×8 general-purpose registers หมายถึง รีจิสเตอร์ทั่วไปจำนวน 32 ตัว โดยแต่ละตัวมีขนาด 8 bit รีจิสเตอร์เหล่านี้ใช้เก็บข้อมูลชั่วคราวที่ต้องนำไปคำนวณหรือประมวลผล รีจิสเตอร์ทั่วไปเชื่อมต่อโดยตรงกับ ALU จึงสามารถนำข้อมูลสองค่าเข้าสู่ ALU และรับผลลัพธ์กลับ

ได้อย่างรวดเร็ว ลักษณะดังกล่าวเป็นจุดเด่นของสถาปัตยกรรม AVR และช่วยให้คำสั่งจำนวนมากดำเนินการได้ภายในหนึ่งรอบสัญญาณนาฬิกา

4) หน่วยคำนวณและตรรกะ (Arithmetic Logic Unit: ALU)

ALU ทำหน้าที่คำนวณทางคณิตศาสตร์และตรรกะ เช่นการบวกและการลบ การเพิ่มหรือลดค่า การเปรียบเทียบ การ AND, OR และ XOR การเลื่อนbit และการทดสอบค่าbit ข้อมูลจากรีจิสเตอร์จะเข้าสู่ ALU ในรูปของ operand 1 และ operand 2 หลังจากประมวลผลแล้ว ผลลัพธ์จะถูกส่งกลับไปยังรีจิสเตอร์หรือหน่วยความจำที่เกี่ยวข้อง

5) รีจิสเตอร์สถานะและควบคุม (Status and Control Register)

ส่วน status and control register ใช้เก็บสถานะที่เกิดจากการประมวลผลของ ALU เช่นผลลัพธ์เป็นศูนย์ เกิดตัวทด ผลลัพธ์ติดลบ เกิดการล้นของข้อมูล สถานะการอนุญาตให้เกิด interrupt สำหรับ AVR สถานะเหล่านี้สัมพันธ์กับ Status Register (SREG) โปรแกรมสามารถใช้ตรวจสอบผลลัพธ์ของการคำนวณและควบคุมการตัดสินใจของโปรแกรมได้

6) หน่วยความจำ Static Random Access Memory (SRAM)

SRAM เป็นหน่วยความจำชั่วคราวที่ใช้เก็บตัวแปร ข้อมูลจากเซ็นเซอร์ stack และข้อมูลระหว่างการทำงานของโปรแกรม ข้อมูลใน SRAM จะสูญหายเมื่อหยุดจ่ายไฟการเข้าถึง SRAM สามารถทำได้ทั้งแบบ (1) direct addressing คือระบุตำแหน่งหน่วยความจำโดยตรง และ (2) indirect addressing คือเข้าถึงหน่วยความจำผ่านรีจิสเตอร์ตัวชี้ตำแหน่งใน ATmega328P มี SRAM ขนาด 2 kB

7) หน่วยความจำ Electrically Erasable Programmable Read-Only Memory (EEPROM)

EEPROM เป็นหน่วยความจำแบบไม่ลบเลือน ใช้เก็บข้อมูลที่ต้องคงอยู่หลังจากตัดไฟ เช่น รหัสผ่าน ค่าการปรับเทียบเซ็นเซอร์ หมายเลขประจำอุปกรณ์ ค่าตั้งต้นของระบบ โดย EEPROM แตกต่างจาก flash program memory ตรงที่มักใช้เก็บข้อมูลของผู้ใช้งาน ไม่ใช่คำสั่งโปรแกรมหลัก สำหรับ ATmega328P มี EEPROM ขนาด 1 kB

8) บัสข้อมูลขนาด 8 bit (Data Bus 8-bit)

Data Bus 8-bit เป็นเส้นทางภายในสำหรับรับส่งข้อมูลระหว่างรีจิสเตอร์ SRAM, EEPROM, ALU และอุปกรณ์ต่อพ่วง โดยสามารถส่งข้อมูลครั้งละ 8 bit ซึ่งสอดคล้องกับการเป็นไมโครคอนโทรลเลอร์ AVR แบบ 8 bit

9) หน่วยขัดจังหวะ (Interrupt Unit)

ทำหน้าที่ตอบสนองต่อเหตุการณ์ที่ต้องจัดการทันที เช่น การเปลี่ยนสถานะขาอินพุต การควบคุมเวลาเมื่อครบ การรับข้อมูลผ่าน serial ADC โดยเมื่อเกิด interrupt ไมโครคอนโทรลเลอร์จะหยุดการทำงานหลักชั่วคราว บันทึกตำแหน่งปัจจุบัน แล้วกระโดดไปทำงานใน interrupt service routine จากนั้นจึงกลับมาทำงานต่อจากตำแหน่งเดิม

10) โมดูล Serial Peripheral Interface (SPI)

SPI เป็นโปรโตคอลการสื่อสารข้อมูลอนุกรม แบบซิงโครนัส (synchronous) ที่มีความเร็วสูง ใช้เชื่อมกับอุปกรณ์ เช่น หน่วยความจำภายนอก จอแสดงผล RFID เซ็นเซอร์ และโมดูลสื่อสาร SPI มีอัตราการรับส่งข้อมูลสูง ใช้สายสัญญาณ SCK, MOSI, MISO และ SS

11) Watchdog Timer

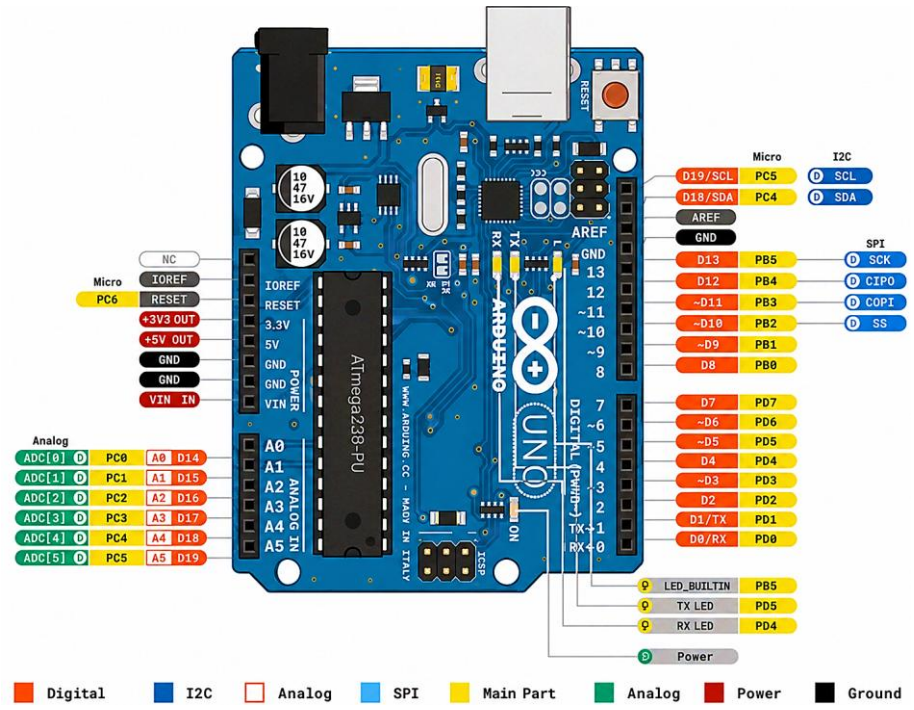
Watchdog Timer เป็นวงจรตรวจสอบความผิดปกติของโปรแกรม หากโปรแกรมค้างหรือไม่รีเซต Watchdog ภายในเวลาที่กำหนด วงจรจะรีเซตไมโครคอนโทรลเลอร์โดยอัตโนมัติ ส่วนนี้มีความสำคัญในระบบรักษาความปลอดภัยและระบบ IoT เพราะช่วยให้ระบบสามารถกลับมาทำงานได้เองเมื่อเกิดความผิดพลาดของซอฟต์แวร์

12) Analog Comparator

ทำหน้าที่เปรียบเทียบแรงดันแอนะล็อกสองค่า และให้ผลลัพธ์ว่าค่าใดสูงกว่า ใช้ตรวจจับระดับแรงดัน หรือเหตุการณ์ interrupt ได้ โดยไม่ต้องใช้ ADC ในบางกรณี analog comparator ไม่ใช่สิ่งเดียวกับ ADC โดย ADC ทำหน้าที่แปลงแรงดันแอนะล็อกเป็นค่าดิจิทัลหลายระดับ ส่วน comparator ให้ผลลัพธ์เพียงสองสถานะ

13) โมดูล I/O และอุปกรณ์ต่อพ่วง

กล่อง I/O module 1, 2 และ n เป็นการแทนอุปกรณ์ต่อพ่วงชนิดต่าง ๆ ภายในไมโครคอนโทรลเลอร์ สำหรับ ATmega328P สามารถหมายถึง GPIO, timer/counter, PWM, ADC, USART, SPI, TWI หรือ I²C, external interrupt, pin change interrupt อุปกรณ์เหล่านี้เชื่อมต่อกับบัสข้อมูลภายใน และบางส่วนเชื่อมต่อออกไปยังขาภายนอกผ่าน I/O lines



รูปที่ 7.4 โครงสร้างของ Arduino Uno R3

7.2.3 ซอฟต์แวร์ Arduino IDE

Arduino Integrated Development Environment (Arduino IDE) ทำหน้าที่เขียนและแก้ไขรหัสโปรแกรม ตรวจไวยากรณ์ คอมไพล์โปรแกรม และอัปโหลดโปรแกรมเข้าสู่บอร์ด Arduino โปรแกรมที่เขียนใน Arduino IDE เรียกว่า สเก็ตช์ (sketch) ภาษาโปรแกรมของ Arduino IDE มีพื้นฐานมา

จากภาษา C/C++ และเพิ่มเติมฟังก์ชันกับไลบรารีที่ช่วยให้ควบคุมฮาร์ดแวร์ได้ง่ายขึ้น เช่น pinMode(), digitalRead(), digitalWrite(), analogRead() และ delay() โดย Arduino IDE ใช้งานได้บนระบบปฏิบัติการ Windows, macOS และ Linux และรองรับการเพิ่มไลบรารีเพื่อใช้งานร่วมกับเซ็นเซอร์ จอแสดงผล และโมดูลสื่อสารชนิดต่าง ๆ (Gubsky, 2023; Kim et al., 2020)

1) โครงสร้างพื้นฐานของโปรแกรม Arduino IDE

โปรแกรม Arduino IDE ทั่วไปต้องมีฟังก์ชันหลักอย่างน้อยสองฟังก์ชัน ได้แก่ setup() และ loop() โดยทั้งสองฟังก์ชันมีชนิดข้อมูลส่งกลับเป็น void หมายถึง ไม่มีการส่งค่ากลับ

1.1) ฟังก์ชัน setup()

ฟังก์ชัน setup() จะทำงานหนึ่งครั้งหลังจากเปิดจ่ายไฟให้บอร์ด กดปุ่มรีเซต หรืออัปโหลดโปรแกรมใหม่ ใช้สำหรับกำหนดค่าเริ่มต้นของระบบ เช่น กำหนดขาให้เป็นอินพุตหรือเอาต์พุต เริ่มต้นการสื่อสารแบบอนุกรม เริ่มต้นไลบรารี และกำหนดค่าเริ่มต้นให้เซ็นเซอร์หรือจอแสดงผล

```
void setup()
  {
     // คำสั่งในส่วนนี้ทำงานหนึ่งครั้งเมื่อเริ่มต้นระบบ
  }
```

1.2) ฟังก์ชัน loop()

เมื่อฟังก์ชัน setup() ทำงานเสร็จแล้ว โปรแกรมจะเข้าสู่ฟังก์ชัน loop() และดำเนินคำสั่งภายในฟังก์ชันนี้ซ้ำอย่างต่อเนื่องตราบเท่าที่บอร์ดยังได้รับไฟเลี้ยง ลักษณะการทำงานทั่วไปคือรับข้อมูลจากอินพุต ประมวลผลข้อมูล และส่งผลลัพธ์ไปยังเอาต์พุต

```
void loop()
  {
     // คำสั่งในส่วนนี้ทำงานวนซ้ำอย่างต่อเนื่อง
  }
```

โครงสร้างดังกล่าวสอดคล้องกับหลักการทำงานของระบบสมองกลฝังตัว ซึ่งต้องตรวจสอบอินพุตและตอบสนองต่อสถานการณ์ต่าง ๆ อย่างต่อเนื่อง

1.3) ตัวดำเนินการในโปรแกรม Arduino

1.3.1) ตัวดำเนินการทางคณิตศาสตร์

ตัวดำเนินการทางคณิตศาสตร์ใช้สำหรับคำนวณค่าของตัวแปรหรือข้อมูล ได้แก่

- + การบวก `z = x + y;`
- - การลบ `z = x - y;`
- * การคูณ `z = x * y;`
- / การหาร `z = x / y;`
- % การหารเอาเศษ `z = x % y;`

การหารจำนวนเต็มจะให้ผลลัพธ์เป็นจำนวนเต็ม เช่น 5/2 ได้ผลลัพธ์เป็น 2 หากต้องการผลลัพธ์เป็นเลขทศนิยม ตัวถูกดำเนินการอย่างน้อยหนึ่งค่าต้องเป็นชนิดเลขทศนิยม เช่น 5.0/2.0

1.3.2) ตัวเพิ่มและตัวลดค่า

- x++ เพิ่มค่า x ขึ้น 1 `x = x + 1;`
- x-- ลดค่า x ลง 1 `x = x - 1;`

ในต้นฉบับที่เขียน x - เพื่อหมายถึงการลดค่าครั้งละหนึ่งนั้นไม่ถูกต้อง ตัวดำเนินการที่ถูกต้องคือ x--

1.3.3) ตัวดำเนินการกำหนดค่าแบบประกอบ

- += x += 2; `x = x + 2;`
- -= x -= 2; `x = x - 2;`
- *= x *= 2; `x = x * 2;`
- /= x /= 2; `x = x / 2;`
- %= x %= 2; `x = x % 2;`

1.3.4) ตัวดำเนินการระดับbit

ตัวดำเนินการระดับbitใช้กับข้อมูลจำนวนเต็ม โดยดำเนินการกับแต่ละbit ของข้อมูล เช่น &=, `, ^=, <<=, และ >>= ซึ่งตัวดำเนินการเหล่านี้แตกต่างจากตัวดำเนินการตรรกะ เช่น && และ || ซึ่งใช้ตรวจสอบเงื่อนไขแบบจริงหรือเท็จ

2) พื้นฐานการเขียนโปรแกรมเบื้องต้น

การเขียนโปรแกรมควบคุม LED ให้กระพริบเป็นการตรวจสอบพื้นฐานว่าบอร์ด การเชื่อมต่อ USB การเลือกพอร์ต และกระบวนการอัปโหลดโปรแกรมทำงานถูกต้อง บอร์ด Arduino Uno R3 และ Arduino Mega 2560 มี LED บนบอร์ดเชื่อมต่อกับขาดิจิทัล D13 โดยสามารถอ้างถึงขาดังกล่าวด้วยค่าคงที่ LED_BUILTIN เพื่อให้โปรแกรมรองรับบอร์ดได้เหมาะสมมากขึ้น

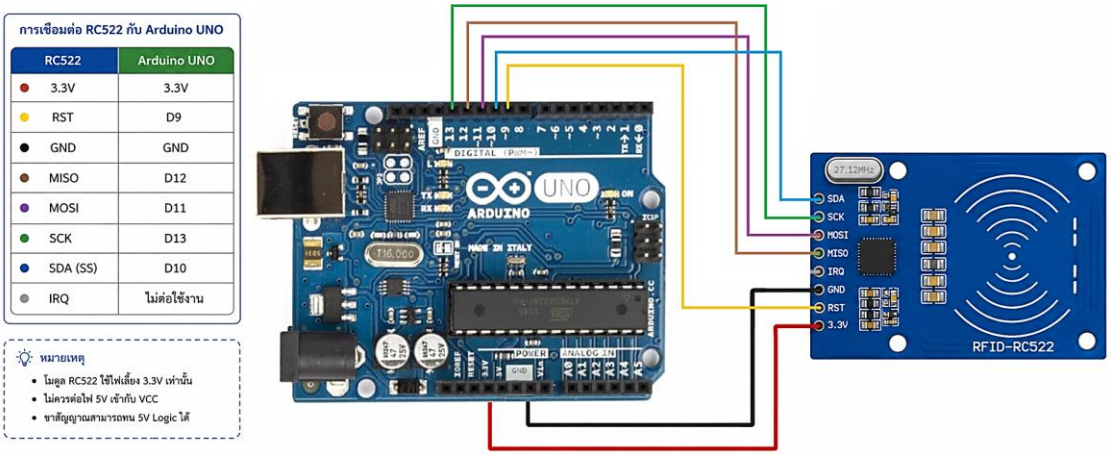
```
void setup()
{
    pinMode(LED_PIN, OUTPUT);
}

void loop()
{
    digitalWrite(LED_PIN, HIGH);
    delay(250);

    digitalWrite(LED_PIN, LOW);
    delay(250);
}
```

การทำงานของโปรแกรมโดยคำสั่ง pinMode(LED_PIN, OUTPUT) เป็นการกำหนดให้ขาที่เชื่อมต่อกับ LED ทำหน้าที่เป็นเอาต์พุต ส่วน digitalWrite() ใช้กำหนดระดับลอจิกให้กับขาดิจิทัล โดย HIGH ทำให้ LED ติด และ LOW ทำให้ LED ดับ คำสั่ง delay(250) ทำให้โปรแกรมหยุดรอเป็นเวลา 250 ms ในหนึ่งรอบ LED จะติด 250 ms และดับ 250 ms

7.2.4 การเชื่อมต่อโมดูล RC522 RFID กับไมโครคอนโทรลเลอร์ Arduino

การเชื่อมต่อโมดูลเข้ากับบอร์ด Arduino เพื่อเริ่มต้นใช้งาน เริ่มต้นด้วยการเชื่อมต่อขา VCC ของโมดูลเข้ากับขา 3.3V ของ Arduino และเชื่อมต่อขา GND เข้ากับกราวด์ (GND) ของ Arduino สำหรับขา RST (Reset) สามารถเชื่อมต่อกับขาดิจิทัลใดก็ได้ของ Arduino โดยในตัวอย่างนี้เชื่อมต่อกับขาดิจิทัลหมายเลข 5 (Digital Pin 5) ส่วนขา IRQ (Interrupt Request) จะไม่ถูกใช้งานในการเชื่อมต่อนี้ เนื่องจากไลบรารี Arduino ที่นิยมใช้กับ RC522 ยังไม่รองรับการทำงานของขาอินเทอร์รัปต์ดังกล่าว

หลังจากนั้นจะเหลือเฉพาะขาที่ใช้สำหรับการสื่อสารแบบ SPI ซึ่งเป็นโปรโตคอลหลักในการรับส่งข้อมูลระหว่าง RC522 กับไมโครคอนโทรลเลอร์ เนื่องจากโมดูล RC522 มีการรับส่งข้อมูลจำนวนมาก จึงควรเชื่อมต่อเข้ากับขา Hardware SPI ของไมโครคอนโทรลเลอร์โดยตรง เพราะ Hardware SPI มีความเร็วสูงกว่าการจำลอง SPI ด้วยซอฟต์แวร์ (Bit-Banging) ผ่านขาดิจิทัลทั่วไป การเชื่อมต่อโมดูล RC522 RFID กับไมรโครคอนโทรลเลอร์ Arduino UNO ดังรูปที่ 7.5 และตารางที่ 7.2 การเชื่อมต่อโมดูล RC522 RFID กับ Arduino



รูปที่ 7.5 การเชื่อมต่อสายโมดูล RFID RC522 กับ Arduino UNO

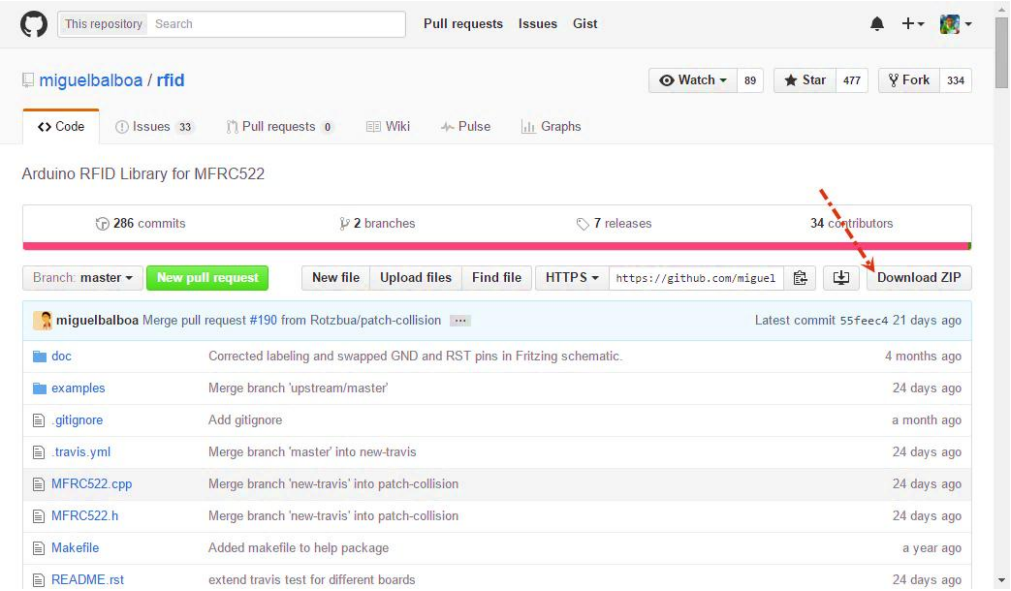
ตารางที่ 7.2 การเชื่อมต่อโมดูล RC522 RFID กับ Arduino

RC522	Arduino UNO/Nano	Arduino Mega
SDA (SS)	D10	D53
SCK	D13	D52
MOSI	D11	D51
MISO	D12	D50
RST	D5	D5
GND	GND	GND
VCC	3.3V	3.3V

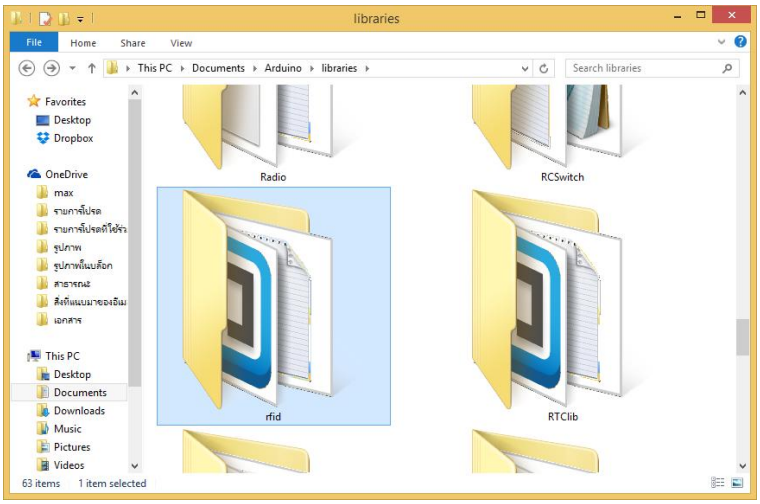
7.2.5 การติดตั้งไลบรารี MFRC522

การสื่อสารกับโมดูล RC522 RFID โดยผ่านไลบรารีชื่อว่า MFRC522 Library ซึ่งช่วยให้การอ่านและเขียนข้อมูลบนแท็ก RFID ทำได้ง่ายขึ้น โดยไลบรารีนี้พัฒนาโดย Miguel Balboa ขั้นแรกให้ดาวน์โหลดไลบรารีจาก GitHub Repository หรือดาวน์โหลดไฟล์ ZIP ของไลบรารีโดยตรงได้ที่ลิงค์ https://github.com/miguelbalboa/rfid หลังจากดาวน์โหลดแล้ว ให้ติดตั้งไลบรารีใน Arduino IDE โดยมีขั้นตอนติดตั้งไลบรารีดังนี้

1) เปิดโปรแกรม Arduino IDE
2) ไปที่เมนู Sketch > Include Library > Add .ZIP Library
3) เลือกไฟล์ rfid-master.zip ที่ดาวน์โหลดไว้



รูปที่ 7.6 ดาวน์โหลดไลบรารี MFRC522

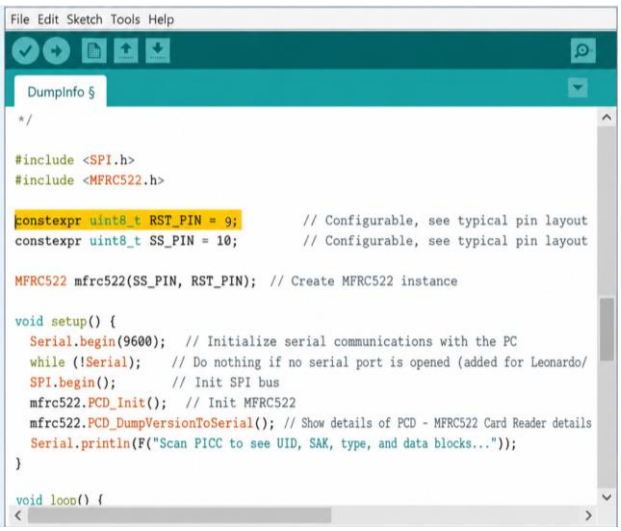


รูปที่ 7.7 การติดตั้งไลบรารี MFRC522

เมื่อติดตั้งไลบรารีเรียบร้อยแล้ว ให้เปิดตัวอย่างโปรแกรมโดยไปที่ File > Examples > MFRC522 > DumpInfo โดยโปรแกรมตัวอย่างนี้ จะไม่ทำการเขียนข้อมูลลงบนแท็ก RFID แต่จะใช้สำหรับตรวจสอบว่าโมดูลสามารถอ่านแท็กได้หรือไม่ พร้อมทั้งแสดงข้อมูลของแท็ก

รูปที่ 7.8 การตรวจสอบการอ่านแท็กของโมดูล RC522

การกำหนดขา RST ในโปรแกรม ให้ตรวจสอบว่ามีการกำหนดค่าขา RST_PIN ถูกต้องหรือไม่ เช่น หากเชื่อมต่อขา RST ของ RC522 เข้ากับขา D9 ของ Arduino จะต้องกำหนดคือ #define RST_PIN 9 (โปรแกรมดังภาคผนวก ข Arduino Code: 1)

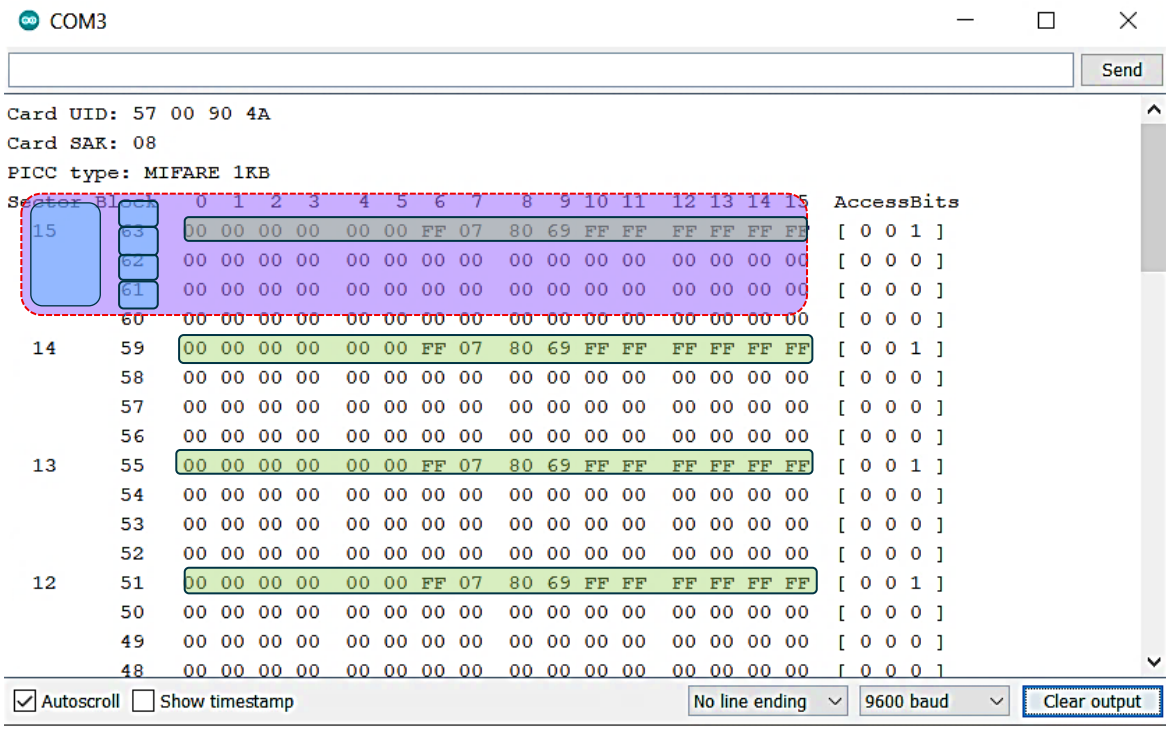


รูปที่ 7.9 การการกำหนดขา RST

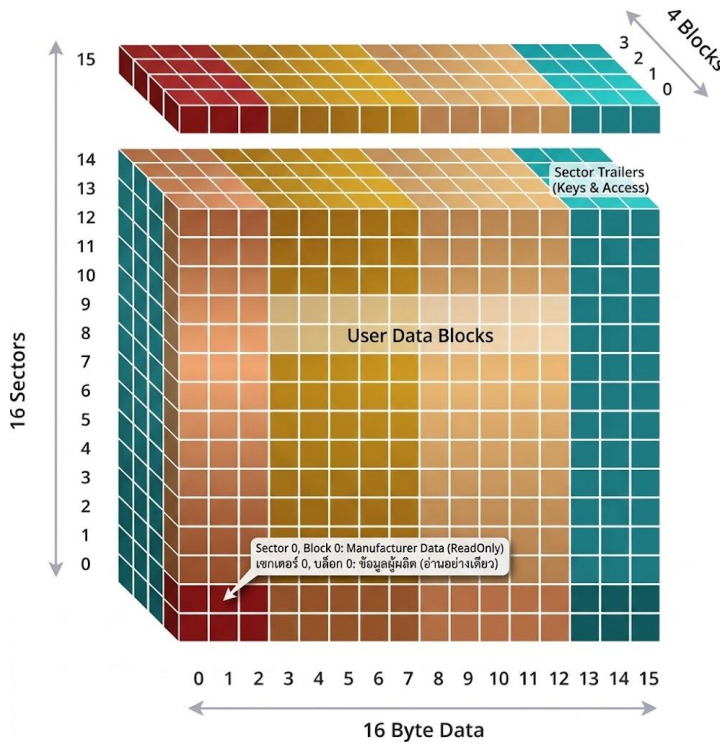
7.2.6 การตรวจสอบการเชื่อมต่อและการอ่านข้อมูลของ MFRC522

เมื่อเขียนโปรแกรมแล้ว ให้อัปโหลดโปรแกรมไปยัง Arduino และเปิดหน้าต่าง Serial Monitor ให้แตะแท็ก RFID เข้าใกล้โมดูล RC522 ระบบจะแสดงข้อมูลของแท็กบน Serial Monitor ข้อมูลที่แสดงประกอบด้วย (1) หมายเลข UID (2) ขนาดหน่วยความจำ และ (3) โครงสร้างหน่วยความจำ จะเห็นได้ว่า Block 3 ของแต่ละ Sector เรียกว่า Sector Trailer ซึ่งใช้เก็บข้อมูลสำคัญที่เรียกว่า Access Bits สำหรับกำหนดสิทธิ์ในการอ่านและเขียนข้อมูลของ Block อื่น ๆ ภายใน Sector เดียวกัน

ดังนั้น Block ที่สามารถใช้เก็บข้อมูลของผู้ใช้ได้จริงจะมีเพียง 3 Block แรกของแต่ละ Sector ได้แก่ Block 0, Block 1 และ Block 2 เนื่องจากแต่ละ Block มีขนาด 16 byte ทำให้ในแต่ละ Sector ซึ่งมีขนาดรวม 64 byte จะมีพื้นที่สำหรับจัดเก็บข้อมูลผู้ใช้จริงจำนวน 3 x 16 เท่ากับ 48 byte ส่วนอีก 16 byte สุดท้ายจะถูกใช้เป็น Sector Trailer สำหรับข้อมูลด้านความปลอดภัยและการกำหนดสิทธิ์การเข้าถึง นอกจากนี้ Block 0 ของ Sector 0 ยังถูกเรียกว่า Manufacturer Block หรือ manufacturer data ซึ่งใช้เก็บข้อมูลจากผู้ผลิตชิป รวมถึงหมายเลขประจำตัวเฉพาะของบัตร หรือ UID โดยทั่วไป Manufacturer Block จะถูกกำหนดค่ามาจากโรงงานผู้ผลิต และไม่สามารถแก้ไขได้ในบัตร MIFARE มาตรฐานทั่วไป โดยสามารถเขียนโปรแกรมควบคุมระบบ ดังภาคผนวก ข (Arduino Code: 1) รูปที่ 7.9 แสดงรูปแบบ ของ Memory Map แบบสามมิติ (Prabhu, 2026)



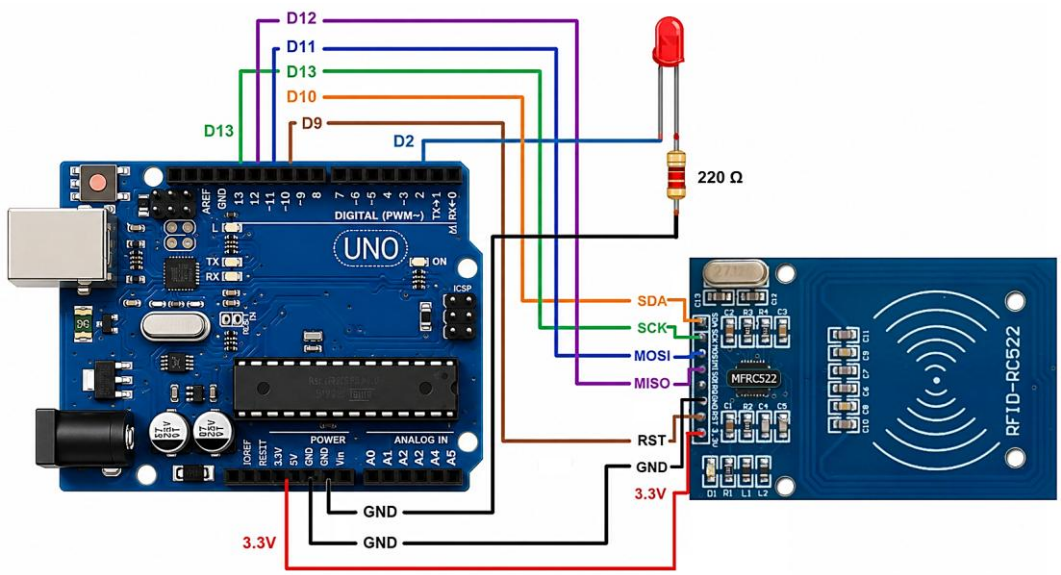
รูปที่ 7.10 ค่า UID และข้อมูลในแต่ละ data blocks



รูปที่ 7.11 รูปแบบ Memory Layout แบบสามมิติ

7.2.7 การประยุกต์ใช้แท็ก RFID ควบคุมการเปิดปิดอุปกรณ์

จากการติดตั้งโมดูล MFRC522 ร่วมกับ Arduino Uno สามารถอ่านค่า UID ของแท็ก RFID ได้แล้ว จากนั้นนำค่าที่อ่านได้มาใช้เป็นเงื่อนไขในการควบคุมอุปกรณ์ภายนอก เช่น LED โดยวงจรเพิ่มเติมจะประกอบด้วยหลอด LED และตัวต้านทาน ต่อเข้ากับขา A0 ของ Arduino เพื่อใช้เป็นขาสัญญาณควบคุมการติด-ดับของอุปกรณ์ ดังรูปที่ 7.12



รูปที่ 7.12 วงจร RFID RC522 เพื่อควบคุมการติด ดับ LED

จากรูปที่ 7.12 การทำงานของวงจร RFID ควบคุม LED วงจรประกอบด้วยบอร์ด Arduino Uno โมดูล RFID RC522 หลอด LED และตัวต้านทาน 220 Ω เพื่อใช้ทดลองอ่านค่าแท็ก RFID และควบคุมการติด ดับของหลอด LED โดย Arduino จะจ่ายแรงดันไฟฟ้า 3.3 V ให้กับโมดูล RC522 และเชื่อมต่อกราวด์ร่วมกัน จากนั้นโมดูล RFID จะสื่อสารกับ Arduino ผ่านระบบ SPI โดยใช้ขา SDA/SS, SCK, MOSI, MISO, และ RST ในการรับส่งข้อมูล จากนั้นเมื่อมีแท็ก RFID เข้าใกล้โมดูล RC522 ระบบจะอ่านค่า UID ของแท็กและส่งข้อมูลไปยัง Arduino โปรแกรมจะนำค่า UID ที่อ่านได้เก็บไว้ในตัวแปร strID แล้วเปรียบเทียบกับ UID ที่กำหนดไว้ หากข้อมูลตรงกัน Arduino จะสั่งให้ขา A0 ส่งสัญญาณไปยัง LED ทำให้หลอด LED ติด แต่หาก UID ไม่ตรงกัน LED จะดับ ตัวต้านทาน 220 โอห์ม ทำหน้าที่จำกัดกระแสไฟฟ้าที่ไหลผ่าน LED เพื่อป้องกันความเสียหายของอุปกรณ์ โดยสามารถเขียนโปรแกรมควบคุมระบบ ดังภาคผนวก ข (Arduino Code: 2)

7.3 NodeMCU ESP8266

ESP8266 เป็นระบบบนชิปสำหรับการสื่อสารไร้สายที่รวมหน่วยประมวลผลแบบ 32 bit วงจร Wi-Fi และชุดโปรโตคอล TCP/IP ไว้ภายในอุปกรณ์เดียว จึงสามารถทำหน้าที่เป็นทั้งหน่วยควบคุมของระบบสมองกลฝังตัวและอุปกรณ์เชื่อมต่อเครือข่ายได้โดยไม่จำเป็นต้องใช้ไมโครคอนโทรลเลอร์ภายนอกในงานทั่วไป คุณสมบัติดังกล่าวทำให้ ESP8266 เหมาะสำหรับการพัฒนาอุปกรณ์ IoT ระบบบ้านอัจฉริยะ ระบบตรวจวัดจากระยะไกล และระบบรักษาความปลอดภัยอัจฉริยะที่ต้องรับข้อมูลจากเซ็นเซอร์ ประมวลผล และส่งข้อมูลผ่านเครือข่าย Wi-Fi (Santos & Santos, 2016; Ayeni et al., 2025) สามารถนำ ESP8266 มาสร้างเว็บเซิร์ฟเวอร์สำหรับควบคุมเอาต์พุตผ่านเว็บเบราว์เซอร์ โดยใช้บอร์ด ESP-12E NodeMCU เป็นตัวอย่างหลัก โดยสามารถเข้าถึงหน้าเว็บผ่านคอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ตที่อยู่ในเครือข่ายเดียวกัน แล้วสั่งเปิด–ปิดขา GPIO ซึ่งสามารถนำไปควบคุม LED รีเลย์ หรืออุปกรณ์ภายนอกอื่นได้ แนวคิดนี้เป็นพื้นฐานสำคัญของระบบควบคุมอุปกรณ์ผ่านเครือข่ายภายในและระบบ IoT ขนาดเล็ก

7.3.1 ประเภทของโมดูลและบอร์ดพัฒนา ESP8266

ESP8266 มีการพัฒนาออกมาหลายรูปแบบเพื่อรองรับการใช้งานที่หลากหลาย ทั้งในรูปแบบโมดูล (ESP modules) และบอร์ดพัฒนา (development boards) ซึ่งแต่ละรุ่นมีความแตกต่างกันในด้านจำนวนขา GPIO หน่วยความจำแฟลช วงจรสนับสนุน และความสะดวกในการพัฒนาโปรแกรม ผู้พัฒนาสามารถเลือกใช้งานให้เหมาะสมกับลักษณะของโครงการ โดยรุ่นที่ได้รับความนิยมแบ่งออกเป็น 2 กลุ่ม ดังนี้

1) โมดูลตระกูล ESP (ESP Modules)

โมดูลตระกูล ESP ใช้ชิป ESP8266EX เป็นหน่วยประมวลผลหลัก และมีหลายรุ่นที่แตกต่างกันในด้านจำนวนขา GPIO และรูปแบบของเสาอากาศ

1.1) ESP-01

เป็นโมดูลรุ่นแรกที่มีขนาดเล็กที่สุด มีขาพิน 8 ขา และ GPIO สำหรับใช้งานเพียง 2 ขา (GPIO0 และ GPIO2) เหมาะสำหรับงานควบคุมอุปกรณ์พื้นฐาน เช่น รีเลย์ หลอดไฟ หรือการเชื่อมต่อ Wi-Fi ร่วมกับไมโครคอนโทรลเลอร์ภายนอก

1.2) ESP-07

พัฒนาต่อยอดจาก ESP-01 โดยเพิ่มจำนวนขา GPIO และรองรับทั้งเสาอากาศแบบ PCB และขั้วต่อเสาอากาศภายนอก (IPEX/U.FL) จึงเหมาะสำหรับงานที่ต้องการระยะการสื่อสารไกลหรือสภาพแวดล้อมที่มีสิ่งกีดขวาง

1.3) ESP-12E และ ESP-12F

เป็นโมดูลที่ได้รับความนิยมมากที่สุด มีขาพิน 32 ขา และหน่วยความจำแฟลชขนาด 4 MB รองรับการเชื่อมต่ออุปกรณ์ต่อพ่วงได้หลากหลาย จึงถูกนำมาใช้เป็นโมดูลหลักของบอร์ดพัฒนา เช่น NodeMCU และ WeMos D1Mini

2) บอร์ดพัฒนา (Development Boards)

บอร์ดพัฒนาเป็นแผงวงจรที่ติดตั้งโมดูล ESP8266 พร้อมวงจรสนับสนุน เช่น วงจรควบคุมแรงดันไฟฟ้า วงจร USB-to-UART และปุ่มรีเซต ทำให้สามารถพัฒนาและอัปโหลดโปรแกรมผ่านพอร์ต USB ได้โดยตรง

2.1) NodeMCU V2 (Amica Version)

ใช้โมดูล ESP-12E ขนาดกะทัดรัด สามารถเสียบบน breadboard ได้สะดวก และมีวงจร USB-to-UART ในตัว จึงเหมาะสำหรับการพัฒนาโครงงาน IoT

2.2) NodeMCU V3 (Lolin Version)

พัฒนาต่อจาก NodeMCU V2 โดยใช้ชิป USB-to-UART รุ่น CH340 ตัวบอร์ดมีขนาดกว้างขึ้นและแข็งแรงกว่าเดิม แต่ยังรองรับการพัฒนาโปรแกรมผ่าน Arduino IDE ได้เช่นเดียวกัน

2.3) WeMos D1 Mini

เป็นบอร์ดพัฒนาขนาดเล็กที่ใช้โมดูล ESP-12F มีขนาดกะทัดรัดกว่า NodeMCU เหมาะสำหรับงานที่มีข้อจำกัดด้านพื้นที่ เช่น ระบบบ้านอัจฉริยะและอุปกรณ์ IoT แม้จะมีจำนวนขา GPIO น้อยกว่า แต่ยังรองรับการเชื่อมต่อ Wi-Fi และสามารถใช้งานร่วมกับบอร์ดเสริม (shields) ได้หลายประเภท เช่น Relay shield, OLED shield และ battery shield

7.3.2 โครงสร้างของ ESP8266

โครงสร้างภายนอกและตำแหน่งขาต่อใช้งานของบอร์ด NodeMCU ESP8266 ดังรูปที่ 7.13 มีรายละเอียด ดังนี้

1) ขาจ่ายไฟ (Power Pins)

บอร์ด NodeMCU ESP8266 มีขาสำหรับจ่ายไฟและรับไฟเลี้ยงที่สำคัญ ได้แก่ VIN, 3.3V และ GND

1.1) VIN (Voltage Input) เป็นขาสำหรับรับแรงดันไฟฟ้าภายนอกเพื่อจ่ายให้กับบอร์ด NodeMCU และอุปกรณ์ต่อพ่วง โดยแรงดันที่ป้อนเข้าขา VIN จะผ่านวงจรควบคุมแรงดันไฟฟ้า (voltage regulator) บนบอร์ดก่อนจ่ายให้กับไมโครคอนโทรลเลอร์ ESP8266 ดังนั้นจึงสามารถจ่ายแรงดันไฟฟ้ากระแสตรงประมาณ 5 V เข้าที่ขา VIN ได้อย่างปลอดภัย

1.2) ขา 3.3V เป็นขาเอาต์พุตของวงจรควบคุมแรงดันบอร์ด ให้แรงดันไฟฟ้า 3.3 V สำหรับจ่ายไฟให้กับเซ็นเซอร์ โมดูล หรืออุปกรณ์อิเล็กทรอนิกส์ภายนอกที่ทำงานด้วยแรงดัน 3.3 V

1.3) ขา GND ขากราวด์ (Ground) หรือจุดอ้างอิงศักย์ไฟฟ้า ใช้เป็นจุดเชื่อมต่อกราวด์ร่วมของวงจรทั้งหมด

2) ขาสื่อสารแบบ I²C (I²C Pins)

บอร์ด NodeMCU ESP8266 รองรับการสื่อสารแบบ Inter-Integrated Circuit (I²C) สำหรับเชื่อมต่อกับเซ็นเซอร์และอุปกรณ์ต่อพ่วงที่ใช้บัส I²C เช่น จอ OLED, RTC, EEPROM และเซ็นเซอร์ต่าง ๆ ESP8266 รองรับการทำงานทั้งในโหมด Master และ Slave โดยการกำหนดขาสัญญาณและการทำงานสามารถกำหนดได้ผ่านซอฟต์แวร์ (software I²C) ความถี่สัญญาณนาฬิกาสูงสุดประมาณ 100 kHz ทั้งนี้ ความถี่ของสัญญาณนาฬิกาที่กำหนดควรสูงกว่าหรือเท่ากับความถี่ที่อุปกรณ์ slave รองรับ เพื่อให้การสื่อสารเป็นไปอย่างถูกต้องและมีประสิทธิภาพ

3) ขาอินพุต/เอาต์พุตทั่วไป (GPIO Pins)

ESP8266 มีขา GPIO (General Purpose Input/Output) จำนวน 17 ขา ซึ่งสามารถกำหนดหน้าที่การทำงานได้ด้วยโปรแกรม เช่น อินพุตและเอาต์พุตดิจิทัล (digital input/output), การสื่อสารแบบ I²C, การสื่อสารแบบ I2S, UART, PWM, การรับ–ส่งสัญญาณอินฟราเรด (IR), การควบคุมหลอด LED, การรับสัญญาณจากปุ่มกด (push button) โดยขา GPIO ทุกขาที่รองรับการทำงานแบบดิจิทัลสามารถกำหนดให้มีตัวต้านทาน pull-up หรือ pull-down ภายในไมโครคอนโทรลเลอร์ หรือกำหนดให้เป็นสถานะ High Impedance (Hi-Z) ได้ เมื่อกำหนดให้เป็นอินพุต ขา GPIO ยังสามารถตั้งค่าให้ตรวจจับเหตุการณ์แบบ edge trigger หรือ level trigger เพื่อสร้างสัญญาณขัดจังหวะ (interrupt) ให้กับหน่วยประมวลผลได้

4) ช่องรับสัญญาณแอนะล็อก (ADC Channel)

NodeMCU ESP8266 มีวงจร Successive Approximation Register Analog-to-Digital Converter (SAR ADC) ความละเอียด 10-bit ADC สามารถนำไปใช้งานได้สองลักษณะ ได้แก่ (1) วัดแรงดันไฟเลี้ยงของชิป (VDD3P3) และ (2) วัดแรงดันไฟฟ้าจากขาอินพุตแอนะล็อก (TOUT หรือ A0) อย่างไรก็ตาม ทั้งสองฟังก์ชัน ไม่สามารถใช้งานพร้อมกันได้ ผู้ใช้งานต้องเลือกใช้เพียงฟังก์ชันใดฟังก์ชันหนึ่งตามลักษณะการประยุกต์ใช้งาน

5) ขาสื่อสารแบบ UART (UART Pins)

ESP8266 มีวงจรสื่อสารแบบอนุกรม UART (Universal Asynchronous Receiver/Transmitter) จำนวน 2 ชุด ได้แก่ UART0 และ UART1

5.1) UART0 ประกอบด้วยขา TXD0, RXD0, RTS0 และ CTS0 ใช้สำหรับรับ–ส่งข้อมูลกับคอมพิวเตอร์หรือไมโครคอนโทรลเลอร์อื่น รองรับความเร็วในการรับส่งข้อมูลได้สูงสุดประมาณ 4.5 Mbps

5.2) UART1 มีเฉพาะขาส่งข้อมูล TXD1 เท่านั้น จึงไม่สามารถรับข้อมูลได้ โดยทั่วไปนิยมใช้สำหรับแสดงข้อความสถานะของโปรแกรม (debug หรือ log messages)

UART สามารถประยุกต์ใช้ในการสื่อสารกับอุปกรณ์ต่าง ๆ เช่น GPS, RFID reader, fingerprint sensor, GSM module และไมโครคอนโทรลเลอร์อื่น ๆ

6) ขาสื่อสารแบบ SPI (SPI Pins)

ESP8266 รองรับวงจรสื่อสารแบบ Serial Peripheral Interface (SPI) จำนวน 2 ชุด ได้แก่ SPI และ HSPI โดยทั้งสองชุดสามารถทำงานได้ทั้งในโหมด master และ slaveคุณสมบัติของ

SPI ได้แก่ (1) รองรับรูปแบบการรับส่งข้อมูล (SPI mode) จำนวน 4 รูปแบบ (2) รองรับความถี่สัญญาณนาฬิกาสูงสุด 80 MHz และ (3) มีหน่วยความจำแบบ First In-First Out (FIFO) ขนาด 64 byte เพื่อเพิ่มประสิทธิภาพในการรับส่งข้อมูล SPI เหมาะสำหรับเชื่อมต่อกับอุปกรณ์ที่ต้องการรับส่งข้อมูลความเร็วสูง เช่น จอ TFT จอ OLED หน่วยความจำ flash SD card โมดูล RFID และเซ็นเซอร์ความเร็วสูง

7) ขาสื่อสารแบบ SDIO (SDIO Pins)

ESP8266 รองรับการสื่อสารแบบ Secure Digital Input/Output (SDIO) สำหรับเชื่อมต่อกับหน่วยความจำแบบ SD card โดยตรง รองรับมาตรฐาน (1) SDIO version 1.1 แบบ 4-bit ความถี่ 25 MHz และ (2) SDIO version 2.0 แบบ 4-bit ความถี่ 50 MHz ซึ่งการเชื่อมต่อแบบ SDIO มีความเร็วสูงกว่าการใช้งาน SD Card ผ่าน SPI จึงเหมาะสำหรับระบบที่ต้องรับส่งข้อมูลปริมาณมาก

8) ขา PWM (Pulse Width Modulation)

NodeMCU ESP8266 รองรับสัญญาณ PWM จำนวน 4 ช่อง สามารถสร้างสัญญาณ PWM ผ่านซอฟต์แวร์เพื่อนำไปใช้ควบคุมอุปกรณ์ต่าง ๆ เช่น การปรับความสว่างของLED การควบคุมความเร็วของมอเตอร์กระแสตรง หรือการควบคุมอุปกรณ์อิเล็กทรอนิกส์กำลัง โดยความกว้างของพัลส์สามารถกำหนดได้ในช่วงประมาณ 1,000–10,000 μs หรือคิดเป็นช่วงความถี่ประมาณ 100–1,000 H_z ทั้งนี้ ความถี่ PWM ที่ใช้งานจริงสามารถกำหนดได้ผ่านไลบรารีและซอฟต์แวร์ที่ใช้พัฒนาโปรแกรม

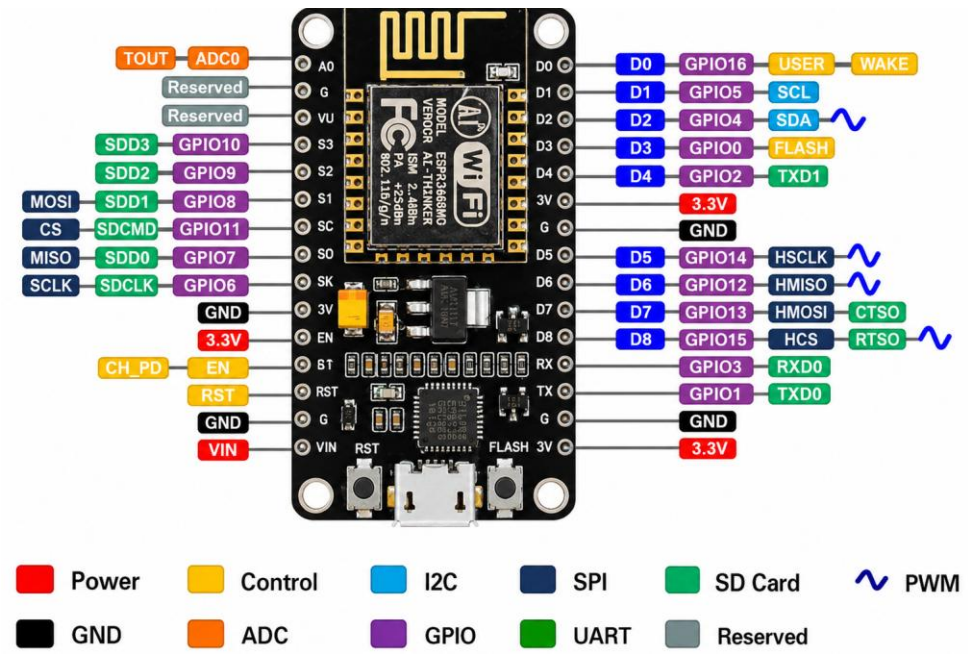
9) ขาควบคุมระบบ (Control Pins)

ESP8266 มีขาควบคุมการทำงานของระบบที่สำคัญ ได้แก่ EN, RST และ WAKE

9.1) EN (Chip Enable) โดยขา (1) เมื่อขา EN อยู่ในระดับลอจิก HIGH ไมโครคอนโทรลเลอร์จะทำงานตามปกติ และ (2) เมื่อขา EN อยู่ในระดับลอจิก LOW ชิปจะเข้าสู่โหมดใช้พลังงานต่ำ (power-down Mode)

9.2) RST (Reset) ขา RST (Reset) ใช้สำหรับรีเซตไมโครคอนโทรลเลอร์ ทำให้โปรแกรมเริ่มทำงานใหม่ตั้งแต่ต้น เหมาะสำหรับการรีสตาร์ตระบบเมื่อเกิดความผิดพลาดหรือเมื่อผู้ใช้งานต้องการเริ่มต้นการทำงานใหม่

9.3) WAKE (Wake-up) ขา WAKE ใช้สำหรับปลุกไมโครคอนโทรลเลอร์ให้กลับมาทำงานจากโหมด deep sleep ซึ่งเป็นโหมดประหยัดพลังงาน โดยมักเชื่อมต่อกับวงจรตั้งเวลาหรือขา GPIO16 เพื่อให้ระบบสามารถตื่นขึ้นมาตามช่วงเวลาที่กำหนด และกลับเข้าสู่โหมดประหยัดพลังงานอีกครั้ง เหมาะสำหรับระบบ IoT ที่ใช้พลังงานจากแบตเตอรี่ เช่น ระบบตรวจวัดสภาพแวดล้อมหรือระบบเฝ้าระวังระยะไกล



รูปที่ 7.13 ขาต่อใช้งานของบอร์ด NodeMCU ESP8266

7.3.3 การเชื่อมต่อ ESP8266 กับโปรแกรม Arduino IDE

1) ดาวโหลด Arduino IDE

ดาวน์โหลดโปรแกรม Arduino IDE ที่ https://www.arduino.cc/en/Main/Softwareเลือกระบบปฏิบัติการของเครื่องที่ใช้ และทำการติดตั้งโปรแกรม (Santos & Santos,2016)

2) การติดตั้งบอร์ด ESP8266

การติดตั้งบอร์ด ESP8266 ในโปรแกรม Arduino IDE ให้ทำตามขั้นตอน ดังนี้

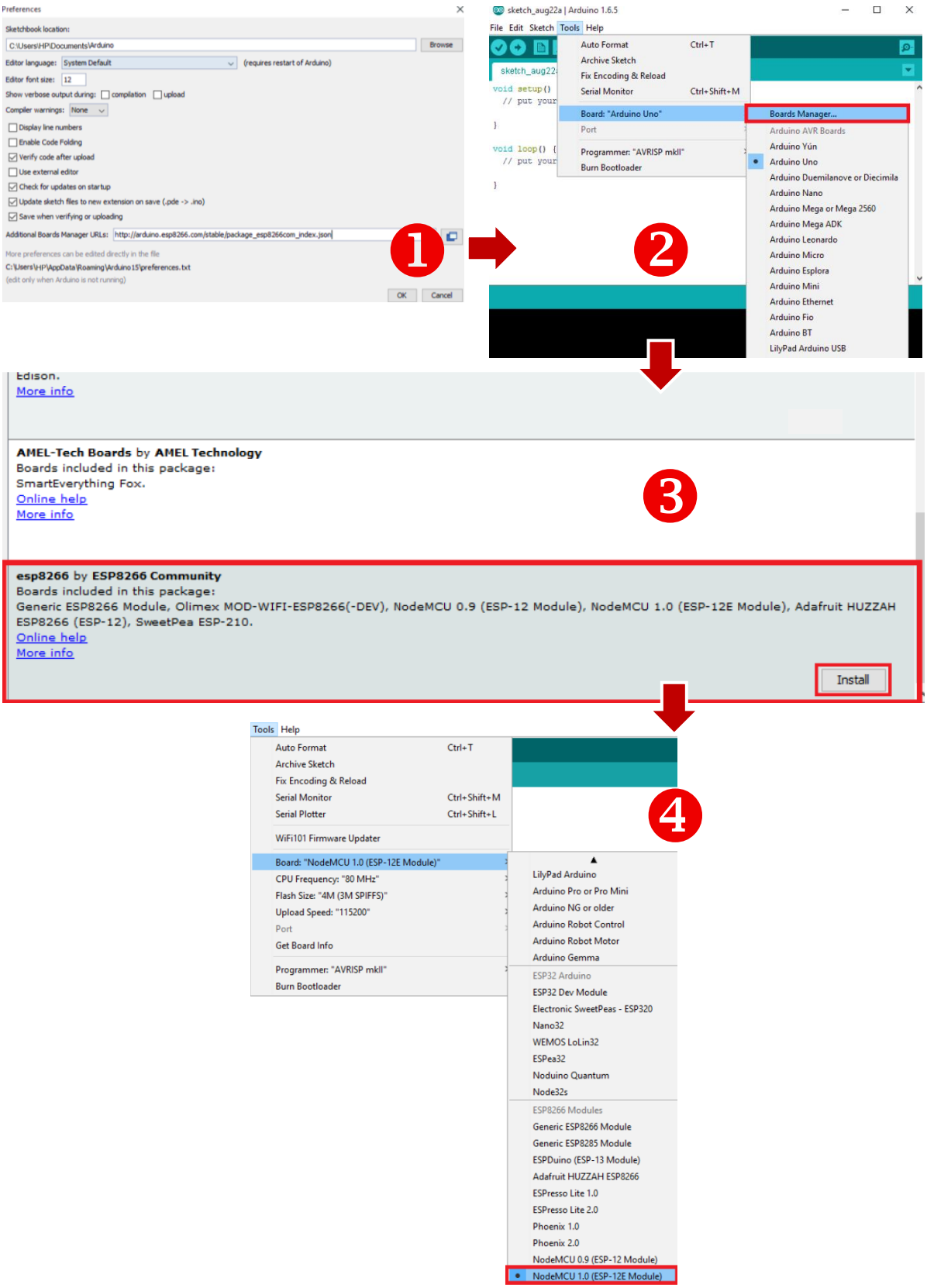
2.1) เปิดหน้าต่างการตั้งค่าจาก Arduino IDE ไปที่ ไฟล์ > การตั้งค่า

2.2) ป้อน http://arduino.esp8266.com/stable/package_esp8266com_index.json ลงในช่อง URL ของตัวจัดการบอร์ดเพิ่มเติม แล้วกดปุ่ม “ตกลง”

2.3) ไปที่ Tools > Board > Boards Manager

2.4) เลือกเมนูบอร์ด ESP8266 แล้วติดตั้ง esp8266 โดย “ESP8266 Community”

2.5) ไปที่ เครื่องมือ > บอร์ด > NodeMCU 1.0 (โมดูล ESP-12E)



รูปที่ 7.14 ขั้นตอนการเชื่อมต่อ ESP8266 กับโปรแกรม Arduino IDE (ดัดแปลงจาก Santos & Santos, 2016)

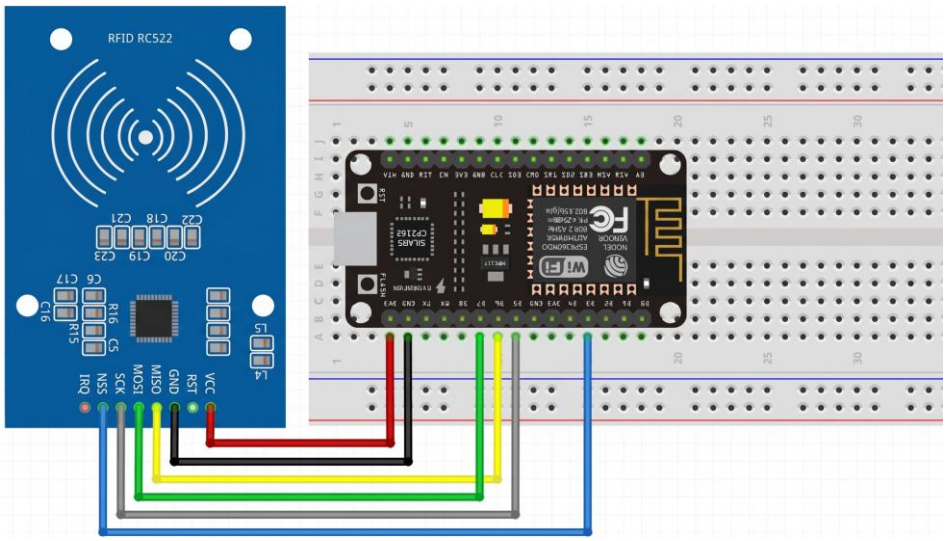
7.3.4 การเชื่อมต่อโมดูล RFID RC522 กับ ESP8266

1) การทำงานของวงจรโมดูล RFID ร่วมกับ NodeMCU ESP8266

วงจรเชื่อมต่อโมดูล RFID RC522 เข้ากับบอร์ดไมโครคอนโทรลเลอร์ NodeMCU ESP8266 เพื่อใช้สำหรับอ่านข้อมูลจากบัตร RFID โมดูล RC522 จะทำหน้าที่เป็นตัวอ่านบัตร ส่วน NodeMCU จะทำหน้าที่ประมวลผลข้อมูลที่อ่านได้ โมดูล RFID RC522 โดยใช้แรงดันไฟฟ้า 3.3 V ดังนั้นขา VCC ของ RC522 จึงต่อเข้ากับขา 3V3 ของ NodeMCU และขา GND ของ RC522 ต่อเข้ากับขา GND ของ NodeMCU เพื่อให้วงจรมีกราวด์ร่วมกัน หากต่อไฟเลี้ยงผิด เช่น ต่อเข้ากับ 5 V อาจทำให้โมดูล RC522 เสียหายได้การสื่อสารระหว่าง RC522 กับ NodeMCU ใช้การสื่อสารแบบ SPI ซึ่งเป็นการรับและส่งข้อมูลผ่านสายสัญญาณหลายเส้น โดยขาที่สำคัญ ได้แก่ SDA/SS, SCK, MOSI, MISO, และ RST เมื่อมีบัตร RFID เข้าใกล้บริเวณเสาอากาศของโมดูล RC522 โมดูลจะอ่านค่า UID ของบัตร แล้วส่งข้อมูลดังกล่าวไปยัง NodeMCU ผ่านขา SPI เพื่อนำไปตรวจสอบหรือใช้งานต่อ การต่อสายดังตารางที่ 7.3

ตารางที่ 7.3 การเชื่อมต่อระหว่างโมดูล RFID RC522 กับ NodeMCU ESP8266

โมดูล RFID	บอร์ด ESP8266	หน้าที่ของขา
VCC	3V3	จ่ายไฟเลี้ยง 3.3 V ให้โมดูล
GND	GND	กราวด์ร่วมของวงจร
RST	D1 หรือ GPIO5	รีเซ็ต/เริ่มต้นการทำงานของโมดูล
SDA / SS	D2 หรือ GPIO4	เลือกอุปกรณ์ SPI เพื่อเริ่มสื่อสาร
MOSI	D7 หรือ GPIO13	ส่งข้อมูลจาก NodeMCU ไปยัง RC522
MISO	D6 หรือ GPIO12	ส่งข้อมูลจาก RC522 กลับมายัง NodeMCU
SCK	D5 หรือ GPIO14	สัญญาณนาฬิกาสำหรับ SPI
IRQ	ไม่ได้ต่อ	ใช้สำหรับสัญญาณขัดจังหวะ แต่ในการทดลองทั่วไปไม่จำเป็นต้องใช้



รูปที่ 7.15 การต่อวงจรโมดูล RFID RC522 กับ NodeMCU ESP8266

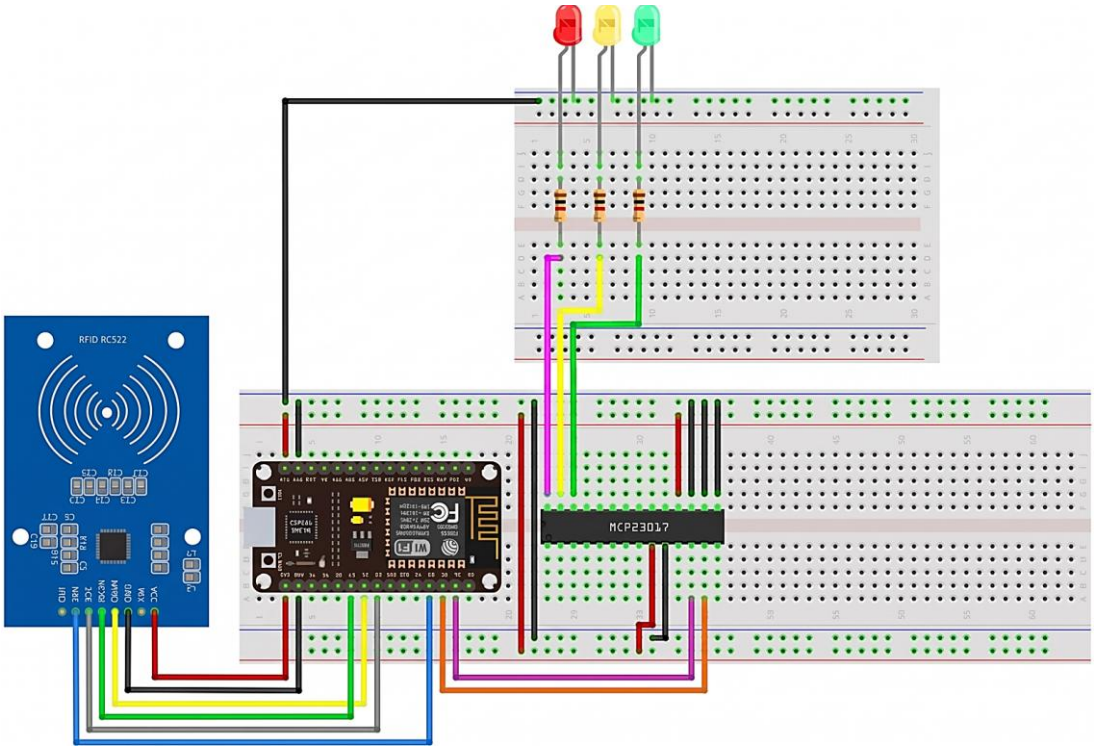
จากรูปที่ 7.15 ลำดับการทำงานของวงจรคือ เมื่อจ่ายไฟให้ NodeMCU และ RC522 แล้ว โปรแกรมใน NodeMCU จะเริ่มต้นระบบ SPI และเริ่มต้นโมดูล RC522 จากนั้น RC522 จะรอการสแกนบัตร RFID เมื่อมีบัตรเข้าใกล้สนามแม่เหล็กไฟฟ้าของโมดูล บัตรจะได้รับพลังงานและส่งข้อมูล UID กลับมายังตัวอ่าน RC522 จากนั้นข้อมูล UID จะถูกส่งต่อไปยัง NodeMCU เพื่อแสดงผลบน Serial Monitor หรือนำไปเปรียบเทียบกับรหัสที่กำหนดไว้ในโปรแกรม หากนำวงจรนี้ไปประยุกต์ใช้ในระบบควบคุมการเข้า ออก NodeMCU สามารถนำค่า UID ที่อ่านได้ไปตรวจสอบกับฐานข้อมูลหรือค่าที่กำหนดไว้ล่วงหน้า หาก UID ตรงกับผู้ที่ได้รับอนุญาต ระบบอาจสั่งเปิดประตู เปิดรีเลย์ เปิดไฟ LED หรือส่งข้อมูลผ่าน Wi-Fi ไปยังระบบออนไลน์ได้ แต่หาก UID ไม่ตรงกัน ระบบสามารถปฏิเสธการเข้าใช้งานหรือแจ้งเตือนได้ การต่อใช้งาน ESP8266 กับโมดูล RFID เพื่ออ่านรหัสแท็ก สามารถเขียนโปรแกรมดังภาคผนวก ข (Arduino Code: 3)

โดยสรุปวงจรนี้เป็นพื้นฐานของระบบอ่านบัตร RFID ด้วย NodeMCU ESP8266 เหมาะสำหรับการเรียนรู้การสื่อสารแบบ SPI และสามารถต่อยอดเป็นระบบเช็กชื่อ ระบบควบคุมประตู ระบบบันทึกเวลา หรือระบบ IoT ที่ต้องการระบุตัวตนด้วยบัตร RFID ได้

2) การทำงานของวงจรโมดูล RFID ร่วมกับไฟ LED และไอซี MCP23017

วงจรนี้เป็นการประยุกต์ใช้งาน โมดูล RFID RC522 ร่วมกับ NodeMCU ESP8266, ไอซี MCP23017, และ หลอด LED เพื่อใช้แสดงสถานะการอ่านแท็ก RFID โดยมี NodeMCU ทำหน้าที่เป็นไมโครคอนโทรลเลอร์หลักในการอ่านข้อมูลจากแท็ก RFID และสั่งงาน LED ผ่านไอซี MCP23017 โมดูล RFID RC522 ทำหน้าที่อ่านข้อมูลจากบัตรหรือแท็ก RFID เมื่อแท็กเข้าใกล้บริเวณเสาอากาศของโมดูล RC522 โมดูลจะอ่านค่า UID ของแท็ก แล้วส่งข้อมูลไปยัง NodeMCU ผ่านการสื่อสารแบบ SPI โดยใช้ขา SDA, SCK, MOSI, MISO, และ RST ส่วนขา VCC ของโมดูล RFID จะต่อเข้ากับแรงดัน 3.3 V และขา GND จะต่อร่วมกับกราวด์ของวงจร

ในวงจรนี้มีการใช้ MCP23017 ซึ่งเป็นไอซีขยายขาอินพุตเอาต์พุต (I/O expander) เพื่อเพิ่มจำนวนขาใช้งานให้กับ NodeMCU เนื่องจาก NodeMCU มีจำนวนขา I/O จำกัด หากต้องเชื่อมต่อทั้งโมดูล RFID, LED, และอุปกรณ์อื่นเพิ่มเติม อาจทำให้ขาไม่เพียงพอ ยกตัวอย่าง เช่น MCP23017 ทำให้สามารถควบคุม LED ได้โดยใช้ขาสื่อสารเพียงไม่กี่ขา ไอซี MCP23017 สื่อสารกับ NodeMCU ผ่านระบบ I^2C โดยใช้ขา SDA และ SCL ในการรับส่งข้อมูล NodeMCU จะส่งคำสั่งไปยัง MCP23017 เพื่อกำหนดให้ขาบางขาเป็นเอาต์พุต จากนั้น MCP23017 จะจ่ายสัญญาณออกไปควบคุม LED แต่ละดวงตามสถานะที่โปรแกรมกำหนดไว้ หลอด LED ในวงจรทำหน้าที่แสดงสถานะการทำงานของระบบ เช่น LED สีเขียวใช้แสดงสถานะว่าอ่านแท็ก RFID สำเร็จหรือแท็กได้รับอนุญาต LED สีแดงใช้แสดงสถานะว่าแท็กไม่ถูกต้องหรือไม่ได้รับอนุญาต และ LED สีเหลืองอาจใช้แสดงสถานะรอการอ่านแท็กหรือกำลังประมวลผล โดย LED แต่ละดวงจะต่อร่วมกับตัวต้านทานเพื่อจำกัดกระแสไฟฟ้า ป้องกันไม่ให้กระแสไหลผ่าน LED มากเกินไปจนทำให้ LED เสียหาย



รูปที่ 7.16 การต่อวงจรโมดูล RFID ร่วมกับไฟ LED และไอซี MCP23017

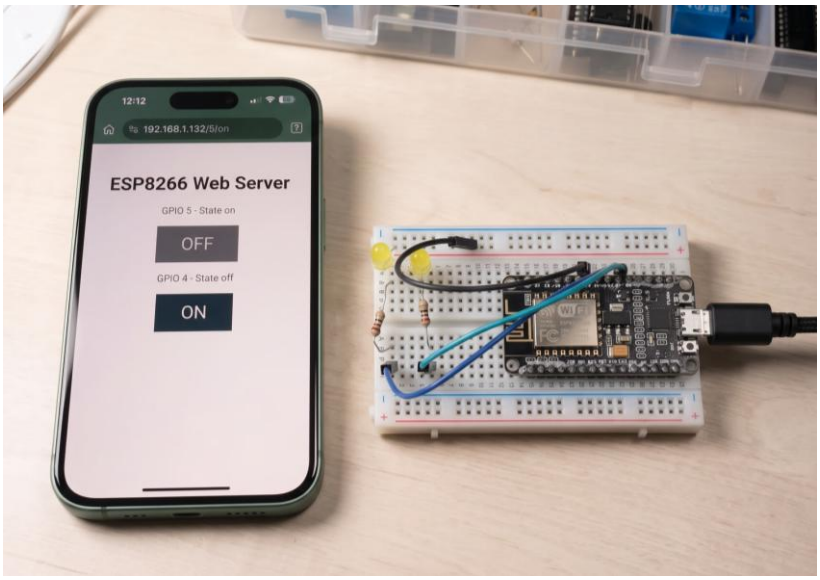
จากรูปที่ 7.16 ลำดับการทำงานของวงจรเริ่มจากการจ่ายไฟให้กับ NodeMCU โมดูล RFID RC522 และไอซี MCP23017 โดยทุกอุปกรณ์ต้องต่อกราวด์ร่วมกันเพื่อให้สามารถสื่อสารกันได้อย่างถูกต้อง จากนั้น NodeMCU จะเริ่มต้นการสื่อสารกับโมดูล RFID และ MCP23017 เมื่อมีแท็ก RFID เข้าใกล้โมดูล RC522 ระบบจะอ่านค่า UID ของแท็กและส่งข้อมูลมายัง NodeMCU เพื่อประมวลผล เมื่อ NodeMCU ตรวจสอบค่า UID แล้ว โปรแกรมจะส่งคำสั่งไปยัง MCP23017 เพื่อควบคุมการติดดับของ LED ตามผลการตรวจสอบ เช่น หากอ่านแท็กสำเร็จและ UID ตรงกับค่าที่กำหนดไว้ LED สีเขียวจะติดเพื่อแสดงว่าอนุญาตให้เข้าใช้งาน แต่หาก UID ไม่ตรงกับค่าที่กำหนด LED สีแดงจะติดเพื่อแสดงว่าปฏิเสธการเข้าใช้งาน ส่วน LED สีเหลืองสามารถใช้เป็นไฟแสดงสถานะพร้อมทำงานหรือรอการสแกนแท็ก การต่อใช้งาน ESP8266 กับโมดูล RFID เพื่ออ่านรหัสในแท็กสามารถเขียนโปรแกรมควบคุมการทำงานดังภาคผนวก ข (Arduino Code: 4)

โดยสรุปวงจรนี้แสดงหลักการนำโมดูล RFID มาประยุกต์ใช้ร่วมกับ LED เพื่อแสดงสถานะการทำงาน และใช้ MCP23017 เพื่อเพิ่มจำนวนขา I/O ให้กับไมโครคอนโทรลเลอร์ ทำให้สามารถขยายระบบไปใช้งานร่วมกับอุปกรณ์อื่น ๆ ได้มากขึ้น เช่น รีเลย์ จอแสดงผล บัซเซอร์ หรือระบบควบคุมประตูอัตโนมัติ

7.3.5 การพัฒนาเว็บเซิร์ฟเวอร์ด้วย ESP8266

หัวข้อนี้อธิบายขั้นตอนการสร้างเว็บเซิร์ฟเวอร์แบบทำงานอิสระด้วย ESP8266 เพื่อควบคุมเอาต์พุตจำนวน 2 ช่อง โดยใช้หลอด LED สองดวงเป็นอุปกรณ์ตัวอย่าง ภายหลังสามารถเปลี่ยนหลอด LED เป็นรีเลย์หรือวงจรขับอุปกรณ์ไฟฟ้าชนิดอื่นได้ตามวัตถุประสงค์ของการใช้งาน เว็บ

เซิร์ฟเวอร์ที่สร้างขึ้นสามารถปรับรูปแบบการแสดงผลให้เหมาะสมกับขนาดหน้าจอของอุปกรณ์เคลื่อนที่ หรือที่เรียกว่า responsive Web design ผู้ใช้สามารถเข้าถึงเว็บเซิร์ฟเวอร์ผ่านอุปกรณ์ใด ๆ ที่มีเว็บเบราว์เซอร์และเชื่อมต่ออยู่ในเครือข่ายท้องถิ่นเดียวกัน เช่น คอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ต โปรแกรมควบคุมทั้งหมดพัฒนาด้วย Arduino IDE (Santos & Santos,2016; Ayeni et al., 2025)



รูปที่ 7.17 การควบคุมเอาต์พุตของ ESP8266 ผ่านเว็บเซิร์ฟเวอร์บนอุปกรณ์เคลื่อนที่

1) การเตรียมโปรแกรม Arduino IDE

ก่อนพัฒนาเว็บเซิร์ฟเวอร์ ต้องติดตั้งโปรแกรม Arduino IDE ที่แพ็กเกจสนับสนุนบอร์ด ESP8266 ตามขั้นตอนต่อไปนี้

1.1)ดาวน์โหลดและติดตั้ง Arduino IDE รุ่นที่รองรับระบบปฏิบัติการของคอมพิวเตอร์ ทั้งนี้ Arduino IDE รุ่นเก่าบางรุ่นอาจไม่รองรับแพ็กเกจ ESP8266 รุ่นปัจจุบัน

1.2) เปิด Arduino IDE แล้วเลือกเมนู

➲ File > Preferences

1.3) ป้อน URL ต่อไปนี้ในช่อง Additional Boards Manager URLs

➲ http://arduino.esp8266.com/stable/package_esp8266com_index.json

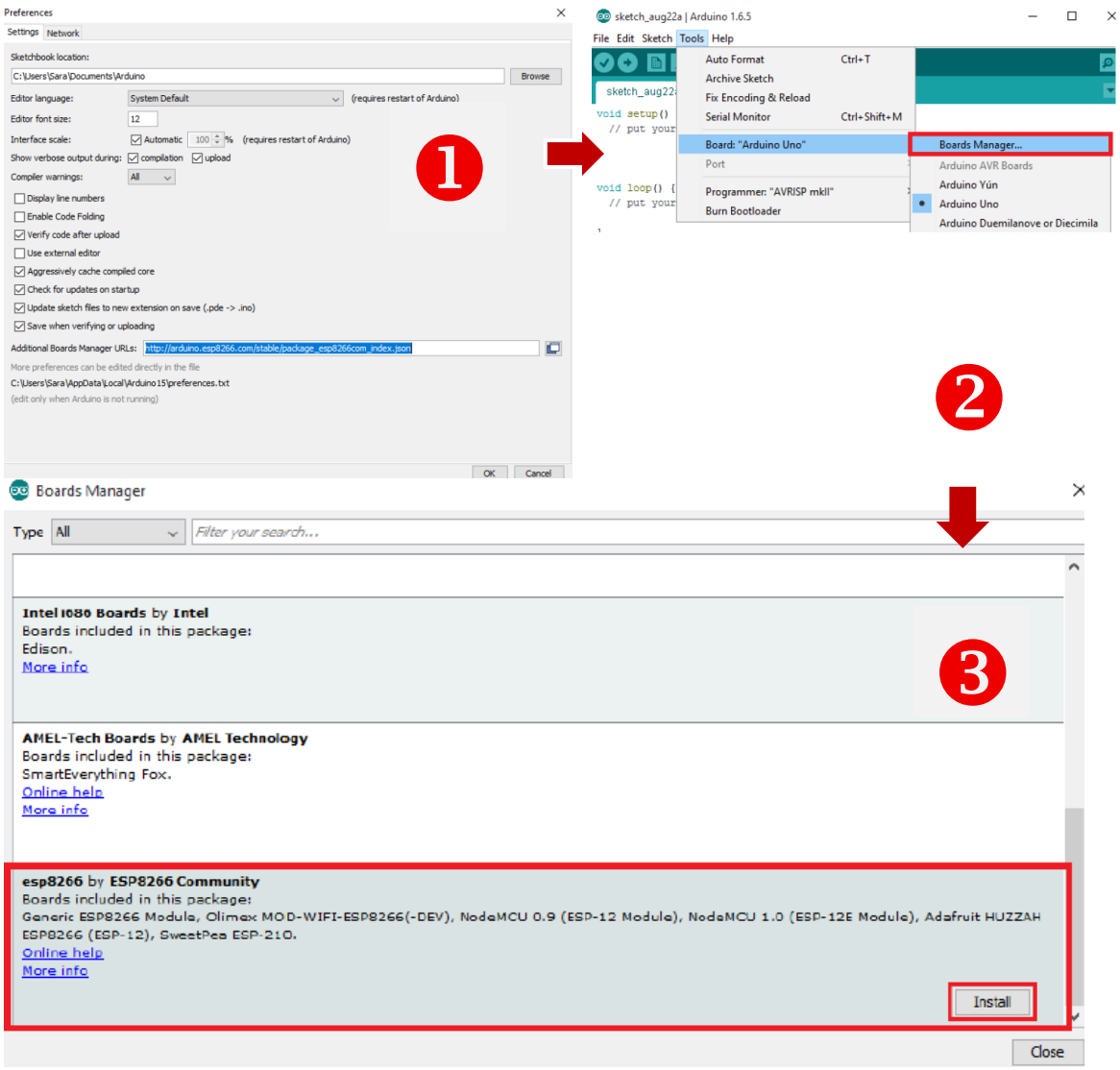
จากนั้นกดปุ่ม **OK**

1.4) ไปที่เมนู

➲ Tools > Board > Boards Manager

1.5) ค้นหาคำว่า esp8266 แล้วติดตั้งแพ็กเกจ esp8266 by ESP8266 Community

1.6) เมื่อการติดตั้งเสร็จสมบูรณ์ ให้เลือกชนิดบอร์ด ESP8266 ที่ใช้งานจริง เช่น Tools > Board > NodeMCU 1.0 (ESP-12E module) จากนั้นเปิด Arduino IDE ใหม่อีกครั้งเพื่อให้การตั้งค่ามีผลอย่างสมบูรณ์



รูปที่ 7.18 การติดตั้งแพ็กเกจ ESP8266 ผ่าน Boards Manager
(ดัดแปลงจาก Santos & Santos, 2016)

2) การเขียนโปรแกรม

จากนั้นทำการโปรแกรมเว็บเซิร์ฟเวอร์ ESP8266 (โปรแกรมดังภาคผนวก ข Arduino Code: 5)

3) การอัปโหลดโปรแกรมเข้าสู่ ESP-12E NodeMCU

การอัปโหลดโปรแกรมเข้าสู่บอร์ด ESP-12E NodeMCU ทำได้สะดวก เนื่องจากบอร์ดมีวงจรแปลง USB เป็น UART และวงจรควบคุมโหมดดาวน์โหลดติดตั้งอยู่ภายใน

ขั้นตอนการอัปโหลดมีดังนี้

3.1) เชื่อมต่อบอร์ด ESP-12E NodeMCU เข้ากับคอมพิวเตอร์ด้วยสาย USB

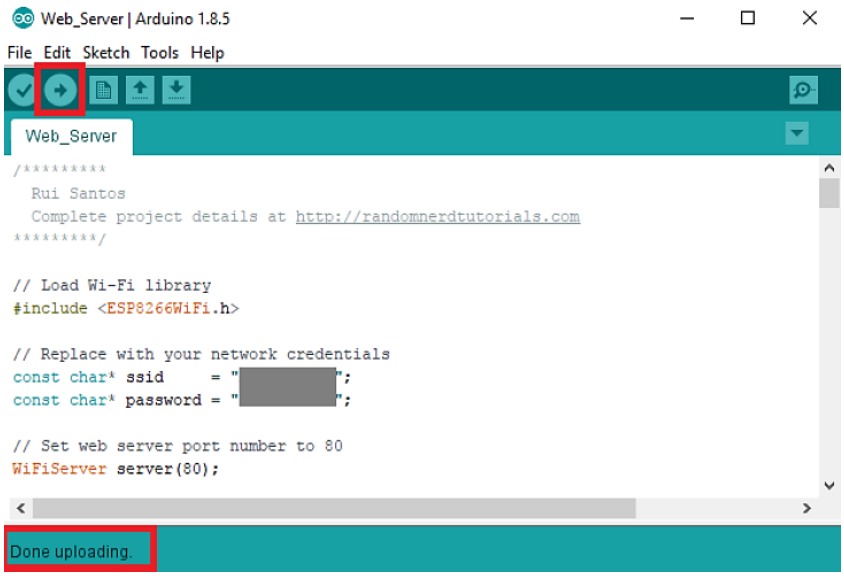
3.2) เลือกชนิดบอร์ดให้ถูกต้อง เช่น NodeMCU 1.0 (ESP-12E module)

3.3) เลือกพอร์ตอนุกรมหรือ COM port ให้ตรงกับบอร์ด

3.4) กดปุ่ม Upload

3.5) รอจนโปรแกรม Arduino IDE แสดงข้อความ “Done uploading”

หมายเลข COM port ของคอมพิวเตอร์แต่ละเครื่องอาจแตกต่างกัน จึงไม่จำเป็นต้องตรงกับตัวอย่าง



รูปที่ 7.19 การอัปโหลดโปรแกรมเว็บเซิร์ฟเวอร์เข้าสู่บอร์ด ESP-12E NodeMCU (ดัดแปลงจาก Santos & Santos, 2016)

4) การอัปโหลดโปรแกรมเข้าสู่ ESP-01

โมดูล ESP-01 ไม่มีวงจร USB-to-UART ในตัว จึงต้องใช้อุปกรณ์แปลงสัญญาณ USB เป็น UART เช่น FTDI programmer เพื่อเชื่อมต่อกับคอมพิวเตอร์ การต่อวงจรระหว่าง ESP-01 และ FTDI programmer ดังตารางที่ 7.4

ตารางที่ 7.4 การต่อวงจรระหว่าง ESP-01 และ FTDI Programmer

ESP8266 ESP-01	FTDI Programmer
RX	TX
TX	RX
CH_PD หรือ EN	3.3 V
GPIO0	GND
VCC	3.3 V
GND	GND

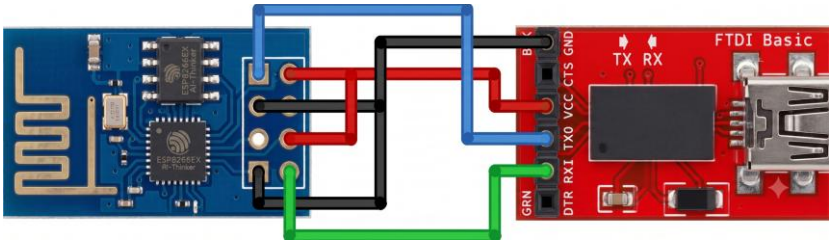
สำหรับการต่อ GPIO0 ลงกราวด์ในระหว่างเปิดเครื่องหรือรีเซต จะทำให้ ESP8266 เข้าสู่ UART download mode หรือโหมดรับโปรแกรมผ่าน UART หลังจากอัปโหลดโปรแกรมเสร็จแล้ว ต้องถอด GPIO0 ออกจากกราวด์ และรีเซตโมดูลอีกครั้งเพื่อให้ ESP8266 เริ่มทำงานในโหมดปกติ โดยมีข้อควรระวัง (Santos & Santos, 2016)

4.1) ESP-01 ต้องใช้แรงดันไฟฟ้า 3.3 V

4.2) ห้ามจ่ายแรงดัน 5 V เข้าขา VCC หรือขาสัญญาณโดยตรง

4.3) แหล่งจ่าย 3.3 V ต้องสามารถจ่ายกระแสได้เพียงพอสำหรับการทำงานของ Wi-Fi

4.4) สาย TX และ RX ต้องต่อไขว้กัน กล่าวคือ TX ของ FTDI ต่อกับ RX ของ ESP-01 และ RX ของ FTDI ต่อกับ TX ของ ESP-01



รูปที่ 7.20 การเชื่อมต่อโมดูล ESP-01 กับอุปกรณ์ USB-to-UART สำหรับอัปโหลดโปรแกรม

5) การประกอบวงจร

อุปกรณ์ที่ใช้ประกอบวงจรเว็บเซิร์ฟเวอร์ ได้แก่

5.1) บอร์ด ESP-12E NodeMCU หรือโมดูล ESP-01

5.1) หลอด LED จำนวน 2 ดวง

5.1) ตัวต้านทานจำกัดกระแส 220 Ω หรือ 330 Ω จำนวน 2 ตัว

5.1) แผ่นทดลอง breadboard

5.1) สายเชื่อมต่อ

5.1) อุปกรณ์ USB-to-UART ในกรณีใช้ ESP-01

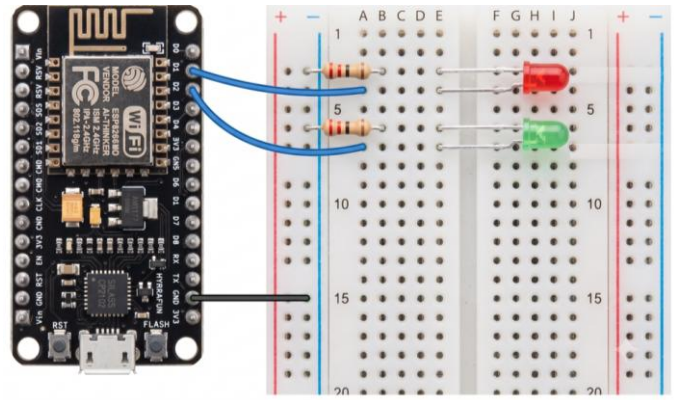
สำหรับบอร์ด NodeMCU ให้เชื่อมต่อ LED ดวงหนึ่งกับ GPIO4 และอีกดวงหนึ่งกับ GPIO5 โดยต่อตัวต้านทานจำกัดกระแสแบบอนุกรมกับ LED แต่ละดวง บนบอร์ด NodeMCU หมายเลขขาที่พิมพ์บนบอร์ดมีความสัมพันธ์กับ GPIO ตัวอย่างการเชื่อมต่อ (Santos & Santos, 2016) ดังนี้

- GPIO5 (D1) > ตัวต้านทาน 220-330 Ω > LED > GND
- GPIO4 (D2) > ตัวต้านทาน 220-330 Ω > LED > GND

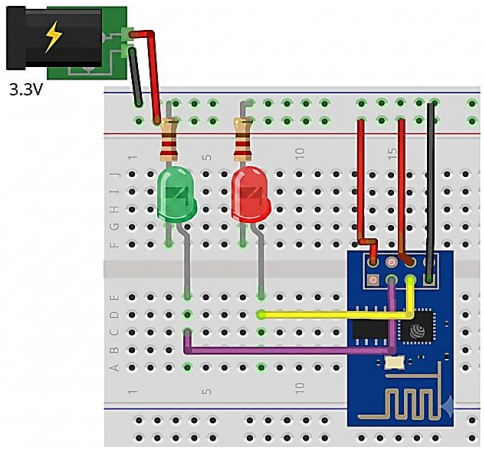
กรณีใช้ ESP-01 จะมี GPIO ที่นำออกมาใช้งานได้จำกัด ดังนั้นต้องเปลี่ยนหมายเลข GPIO ในโปรแกรมจาก GPIO5 และ GPIO4 เป็น GPIO2 และ GPIO0 ตัวอย่างการกำหนดค่าใหม่คือ

```
const int output2 = 2;
const int output0 = 0;
```

อย่างไรก็ตาม GPIO0 และ GPIO2 เป็นขาที่มีผลต่อโหมดการบูต ผู้ใช้จึงต้องระมัดระวังไม่ให้อุปกรณ์ภายนอกดึงขาเหล่านี้เข้าสู่ระดับลอจิกที่ไม่เหมาะสมในช่วงเปิดเครื่องหรือรีเซต เพราะอาจทำให้ ESP8266 ไม่สามารถเริ่มโปรแกรมในโหมดปกติได้



รูปที่ 7.21 การเชื่อมต่อ LED สองดวงกับ GPIO4 และ GPIO5 ของ ESP-12E NodeMCU



รูปที่ 7.22 การเชื่อมต่อ LED สองดวงกับ GPIO0 และ GPIO2 ของโมดูล ESP-01

6) การทดสอบเว็บเซิร์ฟเวอร์

หลังจากแก้ไขชื่อเครือข่ายและรหัสผ่านแล้ว ให้ตรวจสอบชนิดบอร์ดและ COM port จากนั้นอัปโหลดโปรแกรมเข้าสู่ ESP8266

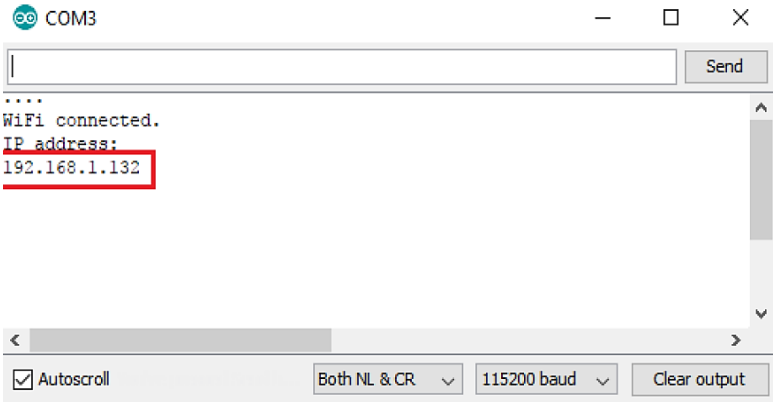
6.1) เปิด Serial Monitor และกำหนดอัตราการสื่อสารเป็น 15200 baud

6.2) การค้นหา IP Address ของ ESP8266

6.3) เมื่อ ESP8266 เชื่อมต่อกับเครือข่าย Wi-Fi สำเร็จ เราเตอร์จะกำหนด IP Address ให้กับบอร์ดผ่าน DHCP โปรแกรมจะแสดง IP Address ดังกล่าวบน Serial Monitorตัวอย่างข้อความที่อาจปรากฏ คือ

- `WiFi connected`
- `IP address: 192.168.1.132`

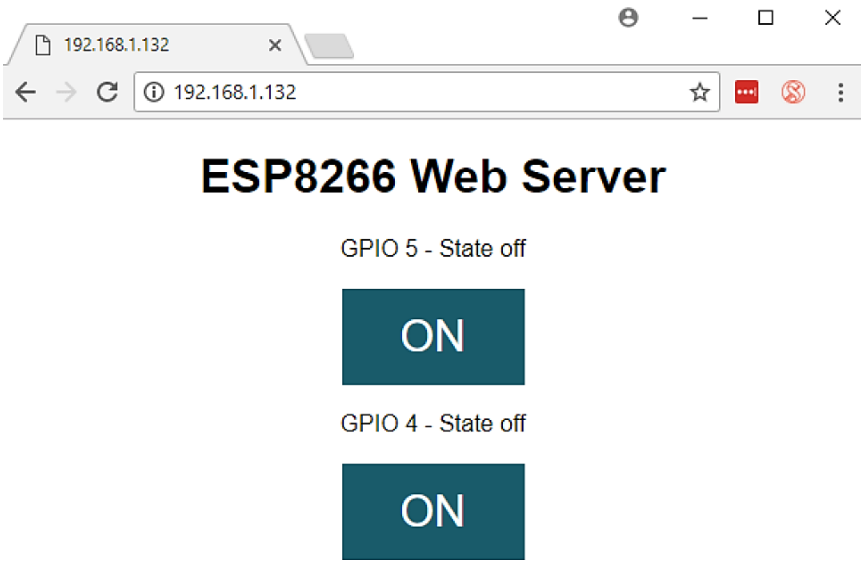
ให้บันทึก IP address นี้ไว้ เนื่องจากต้องใช้สำหรับเข้าถึงเว็บเซิร์ฟเวอร์ หากไม่ปรากฏ IP address ให้กดปุ่ม reset บนบอร์ด และตรวจสอบว่าอัตรา baud ของ Serial Monitor ตรงกับค่าในคำสั่ง `Serial.begin(115200)` (Santos & Santos, 2016)



รูปที่ 7.23 แสดง IP address ของ ESP8266 ผ่าน Serial Monitor (ดัดแปลงจาก Santos & Santos, 2016)

7) การเข้าถึงเว็บเซิร์ฟเวอร์

เปิดเว็บเบราว์เซอร์บนคอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ตที่เชื่อมต่ออยู่ในเครือข่ายเดียวกับ ESP8266 จากนั้นป้อน IP address ของ ESP8266 ลงในแถบที่อยู่ของเว็บเบราว์เซอร์ เช่น http://192.168.1.132 เว็บเบราว์เซอร์จะส่ง HTTP Request ไปยัง ESP8266 และ ESP8266 จะตอบกลับด้วยหน้า HTML ซึ่งแสดงสถานะและปุ่มควบคุม GPIO4 และ GPIO5 หน้าเว็บเริ่มต้นจะแสดงสถานะของ GPIO ทั้งสองเป็น OFF และแสดงปุ่ม ON สำหรับสั่งเปิดเอาต์พุต (Santos & Santos, 2016)



รูปที่ 7.24 หน้าเว็บสำหรับควบคุม GPIO4 และ GPIO5 ของ ESP8266 (ดัดแปลงจาก Santos & Santos, 2016)

8) การทำงานของ HTTP Request

เมื่อเว็บเบราว์เซอร์เชื่อมต่อกับ ESP8266 จะส่งข้อมูลคำขอ HTTP เข้ามา ตัวอย่างเช่น

➲GET / HTTP/1.1
➲Host: 192.168.1.132
➲Connection: keep-alive

ข้อมูลดังกล่าวประกอบด้วยบรรทัดคำขอและ HTTP header fields ใช้ระบุข้อมูลเกี่ยวกับการทำรายการ เช่น (1) วิธีการร้องขอ เช่น GET (2) เส้นทางของทรัพยากร (3) เวอร์ชัน HTTP (4) Host (5) รูปแบบข้อมูลที่ยอมรับ (6) ภาษาที่รองรับ และ (7) ข้อมูลเกี่ยวกับเว็บเบราว์เซอร์ โปรแกรมอ่านข้อมูลเหล่านี้ทีละอักขระ เก็บไว้ในตัวแปร header และตรวจสอบว่าได้รับบรรทัดว่างซึ่งแสดงถึงจุดสิ้นสุดของ HTTP Request Header แล้วหรือไม่

9) การทดสอบปุ่มควบคุม

เมื่อกดปุ่ม ON ของ GPIO5 เว็บเบราว์เซอร์จะเปลี่ยน URL เป็น

➲ http://<ESP_IP_ADDRESS>/5/on

และส่ง HTTP Request ในรูปแบบ

➲ GET /5/on HTTP/1.1

ESP8266 ตรวจสอบข้อความ GET /5/on ภายใน HTTP header หากพบข้อความดังกล่าว โปรแกรมจะดำเนินการดังนี้

9.1) แสดงข้อความ GPIO 5 on บน Serial Monitor
9.2) เปลี่ยนค่าตัวแปร output5State เป็น "on"
9.3) กำหนด GPIO5 เป็นระดับ HIGH
9.4) สร้างหน้าเว็บใหม่เพื่อแสดงสถานะ GPIO5 เป็น on
9.5) เปลี่ยนปุ่มควบคุมจาก ON เป็น OFF หลักการเดียวกันใช้กับ URL อื่น เช่น

ตารางที่ 7.5 ตัวอย่างการทดสอบปุ่มควบคุม

URL	การทำงาน
/5/on	กำหนด GPIO5 เป็น HIGH
/5/off	กำหนด GPIO5 เป็น LOW
/4/on	กำหนด GPIO4 เป็น HIGH
/4/off	กำหนด GPIO4 เป็น LOW

7.4 Raspberry Pi

7.4.1 ความหมายและวิวัฒนาการของ Raspberry Pi

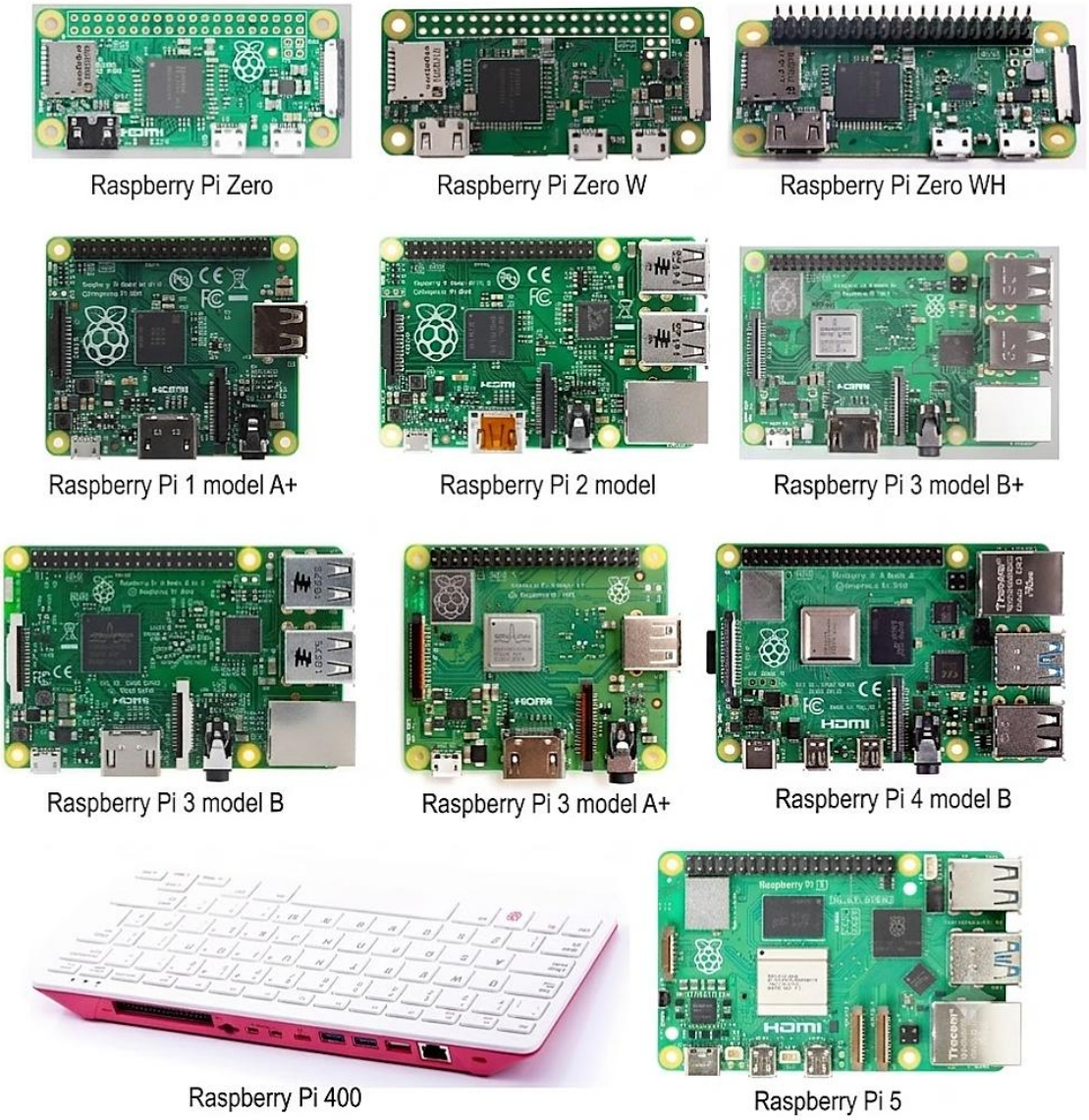
1) ความหมายของ Raspberry Pi

Raspberry Pi เป็นคอมพิวเตอร์บอร์ดเดี่ยว (Single Board Computer: SBC) ที่ได้รับการพัฒนาโดย Raspberry Pi Foundation สหราชอาณาจักร โดยมีวัตถุประสงค์หลักเพื่อส่งเสริมการเรียนรู้ด้านวิทยาการคอมพิวเตอร์ การเขียนโปรแกรม และระบบสมองกลฝังตัว ให้แก่เยาวชนและผู้สนใจทั่วโลก ภายใต้แนวคิดการพัฒนาคอมพิวเตอร์ที่มีต้นทุนต่ำ ขนาดกะทัดรัด ใช้งานง่าย และ

สามารถเชื่อมต่อกับอุปกรณ์อิเล็กทรอนิกส์ภายนอกได้อย่างหลากหลาย (Ghael et al., 2021; Mathe et al., 2024)

Raspberry Pi แตกต่างจากไมโครคอนโทรลเลอร์ทั่วไป เช่น Arduino ตรงที่เป็นคอมพิวเตอร์สมบูรณ์แบบที่สามารถติดตั้งระบบปฏิบัติการได้ โดยส่วนใหญ่ใช้ Raspberry Pi OS ซึ่งพัฒนาบนพื้นฐานของ Debian Linux และรองรับการใช้งานแบบกราฟิก (Graphical User Interface: GUI) รวมถึงการใช้งานผ่านคำสั่ง (Command Line Interface: CLI) นอกจากนี้ยังรองรับภาษาโปรแกรมหลายภาษา เช่น Python, C/C++, Java และ JavaScript ตลอดจนสามารถประมวลผลข้อมูลภาพ วิดีโอ ปัญญาประดิษฐ์ (AI) และการเชื่อมต่อกับบริการคลาวด์ได้อย่างมีประสิทธิภาพ ทำให้ Raspberry Pi ได้รับความนิยมอย่างแพร่หลายในงาน IoT ระบบอัตโนมัติ หุ่นยนต์ ระบบตรวจสอบและเฝ้าระวัง หรือระบบรักษาความปลอดภัยอัจฉริยะ (Halvorsen, 2026; Mathe et al., 2024)

2) วิวัฒนาการของ Raspberry Pi



รูปที่ 7.25 วิวัฒนาการของ Raspberry Pi (ดัดแปลงจาก Mathe et al., 2024)

Raspberry Pi ได้รับการพัฒนาอย่างต่อเนื่องเพื่อเพิ่มประสิทธิภาพด้านการประมวลผล การเชื่อมต่อเครือข่าย และการรองรับงานด้าน IoT และระบบสมองกลฝังตัว โดย Raspberry Pi รุ่นแรกเมื่อปี 2012 ใช้หน่วยประมวลผล ARM11 ความเร็ว 700 MHz และหน่วยความจำ 256–512 MB เหมาะสำหรับการเรียนรู้การเขียนโปรแกรมและการพัฒนาระบบพื้นฐาน (Ghael et al., 2021)

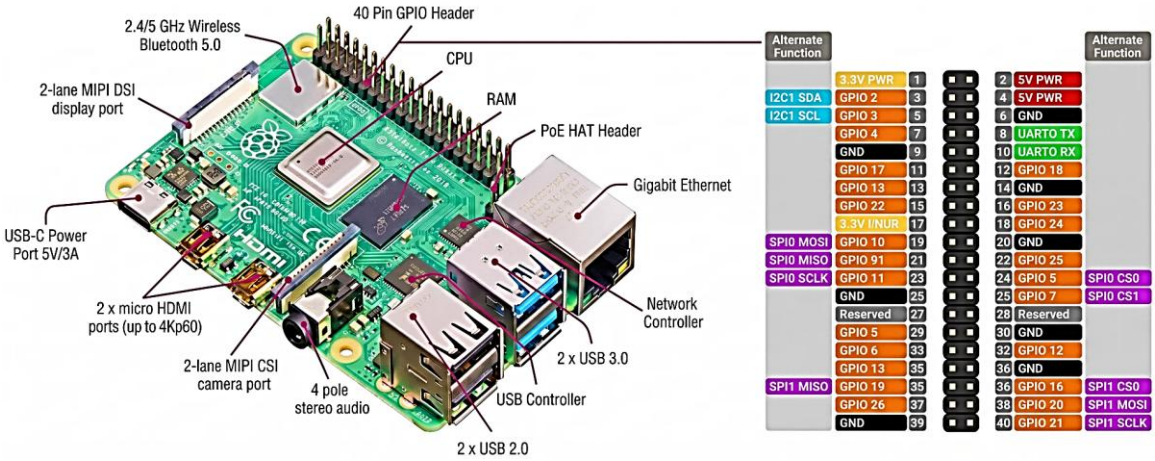
ต่อมา Raspberry Pi 2 ปี 2015 ได้เปลี่ยนมาใช้หน่วยประมวลผลแบบ Quad-core Cortex-A7 พร้อมหน่วยความจำ 1 GB เพื่อเพิ่มประสิทธิภาพในการประมวลผล ขณะที่ Raspberry Pi 3 ปี 2016 ได้เพิ่มการเชื่อมต่อ Wi-Fi และ Bluetooth ภายในบอร์ด พร้อมใช้หน่วยประมวลผล Cortex-A53 ทำให้เหมาะสำหรับงาน IoT และระบบควบคุมอัจฉริยะมากยิ่งขึ้น (Mathe et al., 2024)

ในปี 2019 Raspberry Pi Foundation ได้เปิดตัว Raspberry Pi 4 ซึ่งใช้หน่วยประมวลผล Cortex-A72 รองรับหน่วยความจำสูงสุด 8 GB พร้อมพอร์ต USB 3.0, Gigabit Ethernet และรองรับการแสดงผลแบบ Dual 4k HDMI ส่งผลให้สามารถใช้งานเป็นคอมพิวเตอร์ขนาดเล็กและแพลตฟอร์มสำหรับงาน IoT ได้อย่างมีประสิทธิภาพ (The MagPi, 2019; The MagPi Magazine, 2019)

ล่าสุด Raspberry Pi 5 (2023) ได้รับการพัฒนาให้ใช้หน่วยประมวลผล Quad-core ARM Cortex-A76 ความเร็ว 2.4 GHz พร้อมหน่วยความจำ LPDDR4X รองรับ PCI Express (PCIe), USB 3.0 ความเร็วสูง และตัวควบคุม RP1 I/O Controller ทำให้สามารถรองรับงานด้าน Edge AI, computer vision, การประมวลผลภาพแบบเรียลไทม์ และระบบ IoT อัจฉริยะได้อย่างมีประสิทธิภาพมากกว่ารุ่นก่อน (Joshi & Gawande, 2025)

7.4.2 สถาปัตยกรรมและองค์ประกอบของ Raspberry Pi

Raspberry Pi เป็นคอมพิวเตอร์บอร์ดเดี่ยว (Single Board Computer: SBC) ที่ออกแบบให้มีองค์ประกอบหลักของระบบคอมพิวเตอร์ครบถ้วนบนแผงวงจรเดียว ประกอบด้วยหน่วยประมวลผลกลาง (CPU) หน่วยความจำหลัก (RAM) หน่วยจัดเก็บข้อมูล ระบบเครือข่าย และวงจรอินพุต/เอาต์พุต (I/O) ทำให้สามารถติดตั้งระบบปฏิบัติการและประมวลผลโปรแกรมได้เช่นเดียวกับคอมพิวเตอร์ทั่วไป แต่มีขนาดเล็ก ใช้พลังงานต่ำ เหมาะสำหรับการพัฒนาระบบสมองกลฝังตัวและระบบ IoT (Halvorsen, 2026; Mathe et al., 2024) สถาปัตยกรรมของ Raspberry Pi ประกอบด้วยหน่วยประมวลผลที่ทำหน้าที่ควบคุมการทำงานทั้งหมดของระบบ ร่วมกับหน่วยความจำ RAM สำหรับจัดเก็บข้อมูลและโปรแกรมระหว่างการประมวลผล นอกจากนี้ยังมีหน่วยเก็บข้อมูลแบบ microSD card ซึ่งใช้ติดตั้งระบบปฏิบัติการ Raspberry Pi OS และจัดเก็บโปรแกรมประยุกต์ ผู้ใช้งานสามารถเชื่อมต่ออุปกรณ์ภายนอกผ่านพอร์ตต่าง ๆ เช่น USB, HDMI, Ethernet และ GPIO ทำให้ Raspberry Pi สามารถรองรับการเชื่อมต่อเซ็นเซอร์ กล้อง โมดูลสื่อสาร และอุปกรณ์ควบคุมต่าง ๆ ได้อย่างยืดหยุ่น (Halvorsen, 2026; Mathe et al., 2024) องค์ประกอบสำคัญของ Raspberry Pi มีดังรูปที่ 7.26



รูปที่ 7.26 องค์ประกอบหลักของ Raspberry Pi และพอร์ตเชื่อมต่ออุปกรณ์ภายนอก

1) หน่วยประมวลผลกลาง (Central Processing Unit: CPU)

CPU เป็นหน่วยประมวลผลหลักของ Raspberry Pi ทำหน้าที่ประมวลผลคำสั่งของระบบปฏิบัติการและโปรแกรมประยุกต์ รวมถึงควบคุมการทำงานของอุปกรณ์ต่อพ่วงทั้งหมด ปัจจุบัน Raspberry Pi ใช้หน่วยประมวลผลสถาปัตยกรรม ARM แบบหลายแกน (multi-core ARM processor) ซึ่งมีประสิทธิภาพเพียงพอสำหรับงานประมวลผลภาพ การประมวลผลข้อมูลจากเซ็นเซอร์ และการประมวลผลปัญญาประดิษฐ์ระดับ Edge AI (Mathe et al., 2024)

2) หน่วยความจำหลัก (Random Access Memory: RAM)

RAM ใช้สำหรับเก็บข้อมูลและโปรแกรมที่กำลังประมวลผล โดยข้อมูลใน RAM จะถูกลบเมื่อปิดเครื่อง ขนาดของ RAM มีผลโดยตรงต่อประสิทธิภาพของระบบ โดยเฉพาะการประมวลผลภาพ การประมวลผลแบบหลายภารกิจ (multitasking) และการทำงานของอัลกอริทึมด้าน machine learning (Mathe et al., 2024)

3) หน่วยจัดเก็บข้อมูล (Storage)

Raspberry Pi ใช้ microSD card เป็นอุปกรณ์จัดเก็บข้อมูลหลักสำหรับติดตั้งระบบปฏิบัติการ โปรแกรม และข้อมูลผู้ใช้งาน นอกจากนี้ Raspberry Pi รุ่นใหม่ยังรองรับการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอกผ่าน USB หรือ PCI express (PCIe) เพื่อเพิ่มความเร็วในการอ่านและเขียนข้อมูล (Halvorsen, 2026; Joshi & Gawande, 2025)

4) ขาอินพุต/เอาต์พุตอเนกประสงค์ (General Purpose Input/Output: GPIO)

GPIO เป็นชุดขาดิจิทัลที่ใช้เชื่อมต่อ Raspberry Pi กับอุปกรณ์อิเล็กทรอนิกส์ภายนอก เช่น เซ็นเซอร์ รีเลย์ มอเตอร์ และโมดูลสื่อสาร โดย Raspberry Pi มีหัวต่อ GPIO จำนวน 40 ขา รองรับการสื่อสารผ่านโปรโตคอลต่าง ๆ ได้แก่ GPIO, I²C, SPI, UART และ PWM ทำให้สามารถพัฒนาระบบควบคุมและระบบ IoT ได้อย่างหลากหลาย (Mathe et al., 2024; Halvorsen, 2026)

5) พอร์ต USB (Universal Serial Bus)

พอร์ต USB ใช้เชื่อมต่ออุปกรณ์ต่อพ่วง เช่น เมาส์ แป้นพิมพ์ กล้อง USB หน่วยความจำภายนอก และอุปกรณ์สื่อสารต่าง ๆ โดย Raspberry Pi รุ่นใหม่รองรับทั้ง USB 2.0 และ USB 3.0 ซึ่งมีอัตราการรับส่งข้อมูลสูงกว่า เหมาะสำหรับงานที่ต้องรับส่งข้อมูลภาพหรือวิดีโอความละเอียดสูง (Mathe et al., 2024)

6) พอร์ตแสดงผล HDMI (High-Definition Multimedia Interface)

Raspberry Pi รองรับการเชื่อมต่อจอภาพผ่านพอร์ต HDMI หรือ Micro-HDMI เพื่อแสดงผลภาพและเสียงความละเอียดสูง โดยรุ่นใหม่สามารถรองรับการแสดงผลระดับ 4k และเชื่อมต่อจอภาพได้มากกว่าหนึ่งจอ (Halvorsen, 2026)

7) ระบบเครือข่าย (Network Interface)

Raspberry Pi รองรับการเชื่อมต่อเครือข่ายทั้งแบบใช้สายผ่าน Gigabit Ethernet และแบบไร้สายผ่าน Wi-Fi รวมถึงรองรับ Bluetooth สำหรับเชื่อมต่อกับอุปกรณ์ไร้สายต่าง ๆ เช่น สมาร์ตโฟน เซ็นเซอร์ และอุปกรณ์ IoT ทำให้สามารถสื่อสารข้อมูลกับระบบคลาวด์หรืออุปกรณ์อื่นผ่านเครือข่ายอินเทอร์เน็ตได้ (Mathe et al., 2024)

8) พอร์ตเชื่อมต่อกล้อง (Camera Serial Interface: CSI)

Raspberry Pi มีพอร์ต CSI สำหรับเชื่อมต่อกับ Raspberry Pi camera module โดยตรง ซึ่งรองรับการรับภาพความละเอียดสูงและการประมวลผลภาพแบบเรียลไทม์ เหมาะสำหรับงานด้าน computer vision การตรวจจับใบหน้า (face detection) การรู้จำใบหน้า (face recognition) และระบบเฝ้าระวังอัจฉริยะ (smart surveillance) (Mathe et al., 2024)

9) พอร์ตเชื่อมต่อจอแสดงผล (Display Serial Interface: DSI)

พอร์ต DSI ใช้เชื่อมต่อกับจอสัมผัส (touchscreen display) ของ Raspberry Pi โดยตรง ช่วยให้สามารถพัฒนาระบบควบคุมหรือระบบแสดงผลแบบฝังตัว (embedded display system) ได้สะดวกยิ่งขึ้น (Mathe et al., 2024)

10) แหล่งจ่ายไฟ (Power Supply)

Raspberry Pi รับพลังงานผ่านพอร์ต USB-C หรือ micro-USB (ขึ้นอยู่กับรุ่น) โดยใช้แรงดันไฟฟ้า 5 V และต้องเลือกแหล่งจ่ายไฟที่สามารถจ่ายกระแสได้เพียงพอ เพื่อให้ระบบทำงานได้อย่างมีเสถียรภาพ โดยเฉพาะเมื่อเชื่อมต่อกับกล้อง เซ็นเซอร์ หรืออุปกรณ์ USB หลายชนิดพร้อมกัน (Halvorsen, 2026)

จากองค์ประกอบดังกล่าว Raspberry Pi จึงสามารถทำหน้าที่เป็นศูนย์กลางของระบบ IoT ได้อย่างมีประสิทธิภาพ โดยรองรับการรับข้อมูลจากเซ็นเซอร์ การประมวลผลข้อมูล การประมวลผลภาพจากกล้อง การเชื่อมต่อเครือข่าย และการส่งข้อมูลไปยังบริการคลาวด์หรือฐานข้อมูลออนไลน์ เช่น Google Sheets รวมถึงการแจ้งเตือนผ่าน LINE Messaging API ได้ภายในอุปกรณ์เดียว จึงเหมาะสำหรับการพัฒนาระบบเข้าเรียนด้วยการสแกนใบหน้าร่วมกับการวัดอุณหภูมิและการบันทึกข้อมูลแบบอัตโนมัติ (Mathe et al., 2024)

7.4.3 คุณสมบัติของ Raspberry Pi

คุณสมบัติที่สำคัญของ Raspberry Pi มีดังนี้

1) มีประสิทธิภาพในการประมวลผลสูง

Raspberry Pi ใช้หน่วยประมวลผลสถาปัตยกรรม ARM แบบหลายแกน (multi-core ARM processor) ซึ่งสามารถประมวลผลข้อมูลได้อย่างรวดเร็ว รองรับการทำงานหลายภารกิจ (multitasking) และสามารถประมวลผลข้อมูลจากเซ็นเซอร์ ภาพ และวิดีโอได้พร้อมกัน นอกจากนี้ Raspberry Pi รุ่นใหม่ยังมีหน่วยความจำ RAM หลายขนาดให้เลือกใช้งาน ตั้งแต่ 2 GB ถึง 8 GB ทำ

ให้รองรับงานด้าน computer vision, machine learning และ Edge AI ได้อย่างมีประสิทธิภาพ (Joshi & Gawande, 2025; Mathe et al., 2024)

2) รองรับระบบปฏิบัติการหลายประเภท

Raspberry Pi สามารถติดตั้งระบบปฏิบัติการได้หลายชนิด เช่น Raspberry Pi OS, Ubuntu, Debian, Kali Linux และ LibreELEC โดยระบบปฏิบัติการหลักคือ Raspberry Pi OS ซึ่งได้รับการพัฒนาให้เหมาะสมกับฮาร์ดแวร์ของ Raspberry Pi และรองรับทั้งการใช้งานแบบกราฟิก (Graphical User Interface: GUI) และการใช้งานผ่านบรรทัดคำสั่ง (Command Line Interface: CLI) (Halvorsen, 2026)

3) รองรับภาษาโปรแกรมและเครื่องมือพัฒนาที่หลากหลาย

Raspberry Pi รองรับการพัฒนาโปรแกรมด้วยหลายภาษา เช่น Python, C/C++, Java และ JavaScript โดยภาษา Python ได้รับความนิยมมากที่สุด เนื่องจากมีโครงสร้างภาษาเข้าใจง่าย และมีไลบรารีจำนวนมากสำหรับการพัฒนาระบบ IoT การประมวลผลภาพ และปัญญาประดิษฐ์ เช่น OpenCV, NumPy, TensorFlow Lite, Flask และ MQTT client ส่งผลให้ Raspberry Pi สามารถนำไปพัฒนาระบบอัจฉริยะได้อย่างรวดเร็ว (Halvorsen, 2026)

4) รองรับการเชื่อมต่อเครือข่าย

Raspberry Pi รองรับการเชื่อมต่อเครือข่ายทั้งแบบใช้สายผ่าน Gigabit Ethernet และแบบไร้สายผ่าน Wi-Fi รวมถึง Bluetooth ทำให้สามารถรับ–ส่งข้อมูลกับอุปกรณ์ IoT เซิร์ฟเวอร์ และบริการคลาวด์ได้อย่างสะดวก นอกจากนี้ยังรองรับโปรโตคอลเครือข่ายที่สำคัญ เช่น TCP/IP, HTTP, HTTPS, MQTT, SSH และ VNC ซึ่งช่วยให้สามารถพัฒนาระบบควบคุมและระบบตรวจสอบระยะไกลได้ (Mathe et al., 2024)

5) รองรับการเชื่อมต่ออุปกรณ์อิเล็กทรอนิกส์ภายนอก

Raspberry Pi มีหัวต่อ GPIO จำนวน 40 ขา สำหรับเชื่อมต่อกับเซ็นเซอร์ แอ็กชูเอเตอร์ และโมดูลอิเล็กทรอนิกส์ต่าง ๆ โดยรองรับการสื่อสารผ่านโปรโตคอล GPIO, I^2C, SPI, UART และ PWM ทำให้สามารถเชื่อมต่อกับเซ็นเซอร์ตรวจจับการเคลื่อนไหว เซ็นเซอร์อุณหภูมิ รีเลย์ จอแสดงผล และอุปกรณ์ควบคุมอื่น ๆ ได้โดยตรง (Mathe et al., 2024; Halvorsen, 2026)

6) รองรับการประมวลผลภาพและปัญญาประดิษฐ์

Raspberry Pi รองรับการเชื่อมต่อกล้องผ่านพอร์ต Camera Serial Interface (CSI) และกล้อง USB ทำให้สามารถนำไปใช้ในงานด้านการประมวลผลภาพ (computer vision) เช่น การตรวจจับวัตถุ (object detection) การตรวจจับใบหน้า (face detection) การรู้จำใบหน้า (face recognition) และการวิเคราะห์ภาพด้วยอัลกอริทึมปัญญาประดิษฐ์ โดยสามารถใช้งานร่วมกับไลบรารี OpenCV, TensorFlow Lite และ MediaPipe ได้อย่างมีประสิทธิภาพ (Joshi & Gawande, 2025)

7) รองรับการเชื่อมต่อกับบริการคลาวด์

Raspberry Pi สามารถเชื่อมต่อกับบริการคลาวด์และฐานข้อมูลออนไลน์ผ่านเครือข่ายอินเทอร์เน็ต เช่น Google Sheets, Firebase, ThingSpeak บริการ Web API ต่าง ๆ รวมถึงสามารถเชื่อมต่อกับ LINE Messaging API เพื่อส่งข้อความแจ้งเตือน และใช้ REST API หรือ MQTT ในการแลกเปลี่ยนข้อมูลกับระบบอื่นได้ จึงเหมาะสำหรับการพัฒนาระบบ IoT ที่ต้องการจัดเก็บและวิเคราะห์ข้อมูลแบบเรียลไทม์ (Halvorsen, 2026)

8) ใช้พลังงานต่ำและมีต้นทุนไม่สูง

Raspberry Pi ได้รับการออกแบบให้ใช้พลังงานไฟฟ้าต่ำเมื่อเปรียบเทียบกับคอมพิวเตอร์ตั้งโต๊ะหรือโน้ตบุ๊ก โดยใช้แรงดันไฟฟ้า 5 V และมีอัตราการใช้พลังงานเพียงไม่กี่วัตต์ ทำให้เหมาะสำหรับการใช้งานต่อเนื่องเป็นเวลานาน นอกจากนี้ยังมีราคาที่เหมาะสม ส่งผลให้ได้รับความนิยมในงานวิจัย การศึกษา และการพัฒนาระบบต้นแบบ (prototype development) (Mathe et al., 2024)

9) เหมาะสำหรับการพัฒนาระบบ IoT และระบบรักษาความปลอดภัยอัจฉริยะ

ด้วยคุณสมบัติด้านการประมวลผล การเชื่อมต่อเครือข่าย การรองรับเซ็นเซอร์ กล้อง และบริการคลาวด์ Raspberry Pi จึงสามารถทำหน้าที่เป็นหน่วยประมวลผลกลางของระบบ IoT ได้อย่างมีประสิทธิภาพ ตัวอย่างการประยุกต์ใช้งาน ได้แก่ ระบบบ้านอัจฉริยะ ระบบเกษตรอัจฉริยะ ระบบเฝ้าระวัง ระบบควบคุมการเข้าออกอาคาร และระบบเข้าเรียนด้วยการสแกนใบหน้าร่วมกับการวัดอุณหภูมิ โดยสามารถประมวลผลภาพจากกล้อง บันทึกข้อมูลลง Google Sheets และส่งข้อความแจ้งเตือนผ่าน LINE Messaging API ได้แบบเรียลไทม์ (Joshi & Gawande, 2025; Mathe et al., 2024)

7.4.4 GPIO ของ Raspberry Pi

GPIO เป็นชุดขาอินพุตและเอาต์พุตอเนกประสงค์ที่ติดตั้งอยู่บนบอร์ด Raspberry Pi เพื่อใช้สำหรับเชื่อมต่อกับอุปกรณ์อิเล็กทรอนิกส์ภายนอก เช่น เซ็นเซอร์ แอ็กชูเอเตอร์ โมดูลสื่อสาร และอุปกรณ์ควบคุมต่าง ๆ โดยผู้พัฒนาสามารถกำหนดหน้าที่ของขา GPIO ผ่านซอฟต์แวร์ให้ทำงานเป็นอินพุต หรือเอาต์พุต ได้ตามความต้องการ นอกจากนี้ GPIO ยังรองรับโปรโตคอลการสื่อสารมาตรฐาน เช่น I²C, SPI, UART, และ PWMทำให้ Raspberry Pi สามารถเชื่อมต่อกับอุปกรณ์อิเล็กทรอนิกส์ได้อย่างยืดหยุ่น และเหมาะสำหรับการพัฒนาระบบ IoT และระบบสมองกลฝังตัว (Halvorsen, 2026; Mathe et al., 2024) Raspberry Pi รุ่นปัจจุบันใช้หัวต่อ GPIO แบบ 40 ขา (40-pin header) ซึ่งเป็นมาตรฐานเดียวกันตั้งแต่ Raspberry Pi Model B+ เป็นต้นมา ภายในหัวต่อประกอบด้วยขาสำหรับจ่ายไฟ ขากราวด์ ขาอินพุต/เอาต์พุตดิจิทัล และขาสำหรับการสื่อสารแบบอนุกรม โดยใช้ระดับแรงดันไฟฟ้า 3.3 V สำหรับการรับ–ส่งสัญญาณ ดังนั้นการเชื่อมต่ออุปกรณ์ที่ใช้แรงดัน 5 V ต้องใช้อุปกรณ์แปลงระดับแรงดัน (logic level converter) เพื่อป้องกันความเสียหายต่อหน่วยประมวลผลของ Raspberry Pi (Halvorsen, 2026).

1) โครงสร้างของหัวต่อ GPIO

หัวต่อ GPIO ของ Raspberry Pi ประกอบด้วยขาสำคัญ 4 กลุ่ม ได้แก่

1.1) ขาจ่ายไฟ (power pins) ใช้สำหรับจ่ายแรงดันไฟฟ้าให้กับเซ็นเซอร์และอุปกรณ์ภายนอก ประกอบด้วยขา 3.3 V, ขา 5 V, ขา GND โดยผู้พัฒนาควรเลือกแรงดันไฟฟ้าให้เหมาะสมกับอุปกรณ์ที่เชื่อมต่อ โดยอุปกรณ์ที่รองรับแรงดัน 3.3V สามารถต่อเข้ากับ Raspberry Pi ได้โดยตรง ส่วนอุปกรณ์ที่ใช้แรงดัน 5 V ควรใช้วงจรแปลงระดับแรงดันหรือวงจรขับ (driver circuit) เพื่อความปลอดภัยของระบบ

1.2) ขาอินพุตและเอาต์พุตดิจิทัล (Digital GPIO)

ขา GPIO สามารถกำหนดให้เป็นอินพุตหรือเอาต์พุตผ่านโปรแกรมได้

1.2.1) Input ใช้รับสัญญาณจากเซ็นเซอร์ เช่น เซ็นเซอร์ตรวจจับการเคลื่อนไหว (PIR sensor) สวิตช์ หรือปุ่มกด

1.2.2) Output ใช้ส่งสัญญาณเพื่อควบคุมอุปกรณ์ เช่น LED รีเลย์ บัซเซอร์ และมอเตอร์

1.3) การสื่อสารแบบ I²C

I²C เป็นโปรโตคอลการสื่อสารแบบอนุกรมที่ใช้สายสัญญาณเพียง 2 เส้น ได้แก่ (1) SDA (serial data) และ (2) SCL (serial clock) I²C เหมาะสำหรับการเชื่อมต่ออุปกรณ์ที่มีหลายตัวบนบัสเดียวกัน เช่นเซ็นเซอร์อุณหภูมิ MLX90614, RTC module, OLED display, EEPROM, หรือเซ็นเซอร์วัดความชื้นและความดัน อุปกรณ์แต่ละตัวจะมี address เฉพาะ ทำให้สามารถเชื่อมต่อหลายอุปกรณ์บนสายเดียวกันได้

1.4) การสื่อสารแบบ SPI

SPI เป็นโปรโตคอลการสื่อสารที่มีความเร็วสูงกว่าระบบ I²C โดยใช้สายสัญญาณหลัก 4 เส้น ได้แก่ (1) MOSI (Master Out Slave In), (2) MISO (Master In Slave Out) (3) SCLK (Serial Clock) และ (4) CE หรือ CS (Chip Enable/Chip Select) โดย SPI เหมาะสำหรับอุปกรณ์ที่ต้องการรับ–ส่งข้อมูลด้วยความเร็วสูง เช่น RFID Reader, SD Card Module, TFT LCD, และ Analog-to-Digital Converter (ADC)

1.5) การสื่อสารแบบ UART

UART เป็นการสื่อสารข้อมูลแบบอนุกรมที่ใช้สายสัญญาณหลัก 2 เส้น ได้แก่ (1) TX (transmit) และ (2) RX (receive) โดย UART นิยมใช้เชื่อมต่อกับอุปกรณ์ เช่น GPS module, GSM/4G module, fingerprint scanner, ESP8266, ESP32, หรือ Arduino โดยไม่จำเป็นต้องใช้สัญญาณนาฬิกา

1.6) การสร้างสัญญาณ PWM

PWM เป็นเทคนิคการสร้างสัญญาณดิจิทัลที่สามารถปรับค่า duty cycle ได้ เพื่อควบคุมกำลังไฟฟ้าเฉลี่ยที่ส่งไปยังอุปกรณ์ PWM นิยมใช้สำหรับควบคุมความเร็วของมอเตอร์กระแสตรง ปรับความสว่างของหลอด LED ควบคุมเซอร์โวมอเตอร์ ควบคุมอุปกรณ์กำลังไฟฟ้า แม้ว่า Raspberry Pi จะมีขา PWM แบบฮาร์ดแวร์เพียงบางขา แต่สามารถสร้าง PWM ผ่านซอฟต์แวร์ได้สำหรับงานทั่วไป

1.7) การกำหนดหมายเลขขา GPIO

Raspberry Pi มีการกำหนดหมายเลขขา 2 รูปแบบ ได้แก่ (1) physical pin number เป็นหมายเลขตำแหน่งของขาบนหัวต่อ GPIO และ (2) BCM GPIO number เป็นหมายเลข GPIO ของชิป Broadcom ซึ่งนิยมใช้ในการเขียนโปรแกรมด้วยภาษา Python ผู้พัฒนาควรเลือกใช้รูปแบบการกำหนดหมายเลขให้สอดคล้องกับไลบรารีที่ใช้งาน และหลีกเลี่ยงการใช้ทั้งสองระบบร่วมกันภายในโปรแกรมเดียวเพื่อป้องกันความสับสน

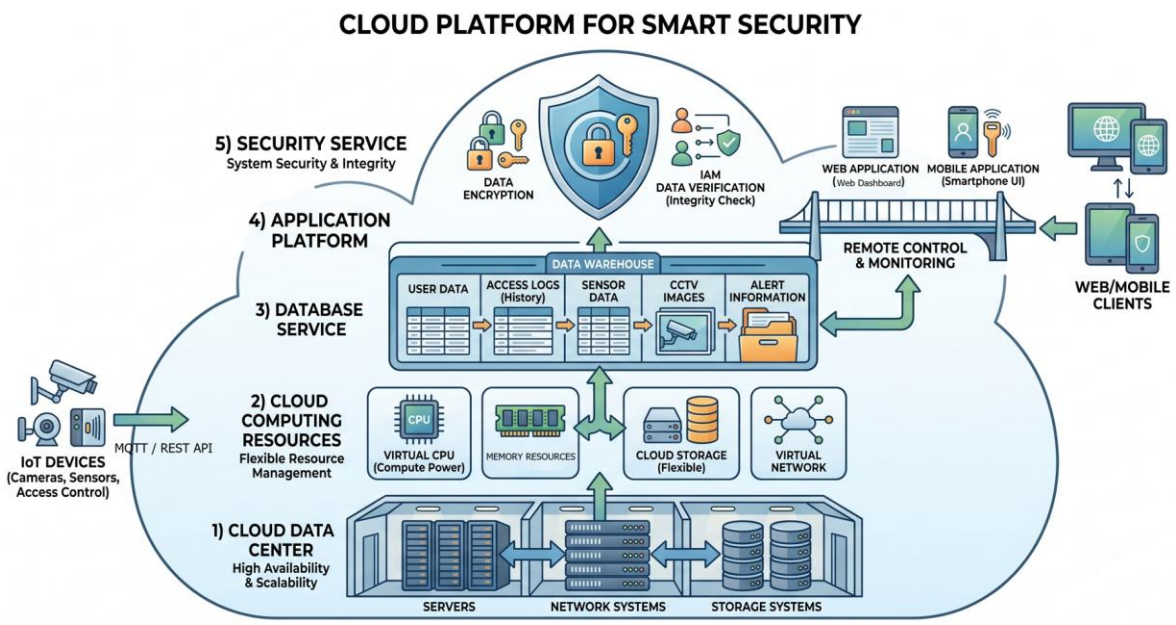
7.5 แพลตฟอร์มคลาวด์เพื่อใช้ในระบบความปลอดภัยอัจฉริยะ

7.5.1 ความหมายของ Cloud Platform

แพลตฟอร์มคลาวด์ (cloud platform) หมายถึง แพลตฟอร์มที่ให้บริการทรัพยากรด้านเทคโนโลยีสารสนเทศผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ใช้สามารถเข้าถึงทรัพยากรต่าง ๆ เช่น หน่วยประมวลผล (computing resources) พื้นที่จัดเก็บข้อมูล (storage) ฐานข้อมูล (database) ระบบเครือข่าย (networking) และบริการซอฟต์แวร์ (software services) ได้ทุกที่ทุกเวลา โดยไม่จำเป็นต้องติดตั้งหรือดูแลโครงสร้างพื้นฐานด้วยตนเอง ผู้ให้บริการคลาวด์จะเป็นผู้บริหารจัดการศูนย์ข้อมูล (data center) การสำรองข้อมูล การขยายทรัพยากร และการบำรุงรักษาระบบทั้งหมด ทำให้ผู้ใช้สามารถมุ่งเน้นการพัฒนาแอปพลิเคชันและบริการได้อย่างเต็มที่ (Huawei Technologies Co., Ltd., 2023) สำหรับระบบความปลอดภัยอัจฉริยะ cloud platform ทำหน้าที่เป็นศูนย์กลางในการรวบรวม ประมวลผล จัดเก็บ และบริหารจัดการข้อมูลที่ส่งมาจากอุปกรณ์ IoT เช่น กล้อง IP Camera เซ็นเซอร์ตรวจจับความเคลื่อนไหว เซ็นเซอร์ควัน เครื่องอ่าน RFID ระบบตรวจจับใบหน้า และอุปกรณ์ควบคุมการเข้าออก ทำให้ผู้ดูแลระบบสามารถติดตามสถานะของอุปกรณ์และตรวจสอบเหตุการณ์ต่าง ๆ ผ่านอินเทอร์เน็ตได้แบบเรียลไทม์

7.5.2 องค์ประกอบของ Cloud Platform

Cloud platform ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะประกอบด้วยองค์ประกอบสำคัญดังนี้



รูปที่ 7.27 องค์ประกอบของ cloud platform

1) Cloud Data Center

เป็นศูนย์ข้อมูลที่ประกอบด้วยเซิร์ฟเวอร์ ระบบเครือข่าย และระบบจัดเก็บข้อมูลจำนวนมาก ทำหน้าที่รองรับการประมวลผลและจัดเก็บข้อมูลจากอุปกรณ์ IoT โดยออกแบบให้มีความ

พร้อมใช้งานสูง (high availability) และสามารถขยายระบบได้ตามความต้องการ (Huawei Technologies Co., Ltd., 2023)

2) Cloud Computing Resources

เป็นหน่วยประมวลผลเสมือน (virtual CPU) หน่วยความจำ (memory) พื้นที่จัดเก็บข้อมูล (cloud storage) และระบบเครือข่ายเสมือน (virtual network) ซึ่งสามารถเพิ่มหรือลดทรัพยากรได้อย่างยืดหยุ่น

3) Database Service

ทำหน้าที่จัดเก็บข้อมูลผู้ใช้งาน ประวัติการเข้าออก ข้อมูลเซ็นเซอร์ ภาพจากกล้องวงจรปิด และข้อมูลการแจ้งเตือน

4) Application Platform

เป็นส่วนที่ให้บริการ Web application และ mobile application สำหรับการควบคุมและติดตามระบบจากระยะไกล

5) Security Service

ประกอบด้วยระบบเข้ารหัสข้อมูล (encryption) การจัดการสิทธิ์ผู้ใช้งาน (Identity and Access Management: IAM) และการตรวจสอบความถูกต้องของข้อมูล เพื่อรักษาความมั่นคงปลอดภัยของระบบคลาวด์ (Huawei Technologies Co., Ltd., 2023)

7.5.3 รูปแบบการให้บริการของ Cloud Platform

การให้บริการของแพลตฟอร์มคลาวด์สามารถจำแนกตามระดับของทรัพยากรที่ผู้ให้บริการจัดเตรียมและระดับความรับผิดชอบที่ผู้ใช้งานต้องบริหารจัดการออกเป็น 3 รูปแบบหลัก ได้แก่ (1) โครงสร้างพื้นฐานในรูปแบบบริการ (Infrastructure as a Service: IaaS) (2) แพลตฟอร์มในรูปแบบบริการ (Platform as a Service: PaaS) และ (3) ซอฟต์แวร์ในรูปแบบบริการ (Software as a Service: SaaS) แต่ละรูปแบบมีความแตกต่างกันในด้านประเภทของทรัพยากร กลุ่มผู้ใช้งาน ระดับการควบคุมระบบ และภาระในการดูแลรักษา โดยบริการระดับบนสามารถพัฒนาต่อยอดจากบริการระดับล่างได้ เช่น PaaS อาจสร้างขึ้นบนโครงสร้างพื้นฐานแบบ IaaS และ SaaS อาจพัฒนาขึ้นโดยใช้บริการของ PaaS หรือ IaaS เป็นพื้นฐาน (Huawei Technologies Co., Ltd., 2023) สำหรับระบบความปลอดภัยอัจฉริยะ การเลือกรูปแบบบริการควรพิจารณาจากความต้องการควบคุมระบบ ความสามารถของทีมพัฒนา ความอ่อนไหวของข้อมูล ปริมาณข้อมูลจากอุปกรณ์ และค่าใช้จ่ายในการดำเนินงาน เนื่องจากข้อมูลของระบบดังกล่าวอาจประกอบด้วยภาพจากกล้องวงจรปิด ข้อมูลการเข้า–ออก ข้อมูลระบุตัวบุคคล สถานะของเซ็นเซอร์ และประวัติการแจ้งเตือน ซึ่งต้องได้รับการจัดเก็บ ประมวลผล และควบคุมการเข้าถึงอย่างเหมาะสม

1) Infrastructure as a Service (IaaS)

IaaS เป็นรูปแบบบริการที่ผู้ให้บริการคลาวด์จัดเตรียมทรัพยากรโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้แก่ผู้ใช้ผ่านเครือข่าย ทรัพยากรดังกล่าวประกอบด้วยหน่วยประมวลผล หน่วยความจำ เครื่องแม่ข่ายเสมือน ระบบจัดเก็บข้อมูล และระบบเครือข่ายเสมือน ผู้ใช้สามารถเลือกขนาดและคุณลักษณะของทรัพยากรให้เหมาะสมกับภาระงาน และสามารถเพิ่ม ลด หรือยกเลิกทรัพยากรได้ตามความต้องการ โดยทั่วไปค่าใช้บริการจะสัมพันธ์กับปริมาณทรัพยากรหรือระยะเวลาที่ใช้งาน หน่วยบริการพื้นฐานของ IaaS มักอยู่ในรูปของ เครื่องแม่ข่ายเสมือน (virtual

server หรือ Virtual Machine: VM) ซึ่งประกอบด้วยหน่วยประมวลผลเสมือน หน่วยความจำ ระบบปฏิบัติการ และพื้นที่จัดเก็บข้อมูล เมื่อได้รับทรัพยากรแล้ว ผู้ใช้มีหน้าที่ติดตั้งและกำหนดค่าระบบปฏิบัติการ มิดเดิลแวร์ ฐานข้อมูล และโปรแกรมประยุกต์ด้วยตนเอง ขณะที่ผู้ให้บริการคลาวด์รับผิดชอบโครงสร้างพื้นฐานทางกายภาพ ได้แก่ ศูนย์ข้อมูล เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล เครือข่าย และชั้นการจำลองเสมือน (Huawei Technologies Co., Ltd., 2023)

ในระบบความปลอดภัยอัจฉริยะ IaaS เหมาะสำหรับองค์กรที่ต้องการควบคุมสภาพแวดล้อมของระบบอย่างละเอียด เช่น การติดตั้งเครื่องแม่ข่ายสำหรับระบบบริหารจัดการวิดีโอ ระบบฐานข้อมูลประวัติการเข้า–ออก ระบบตรวจสอบเหตุการณ์ หรือโปรแกรมวิเคราะห์ภาพด้วยปัญญาประดิษฐ์ องค์กรสามารถกำหนดระบบปฏิบัติการ โครงสร้างฐานข้อมูล กฎของไฟร์วอลล์ และนโยบายการสำรองข้อมูลให้สอดคล้องกับข้อกำหนดของตนเองได้ ตัวอย่างการประยุกต์ใช้ IaaS ได้แก่ การสร้างเครื่องแม่ข่ายเสมือนเพื่อรับข้อมูลจากกล้องและเซ็นเซอร์ การจัดเก็บบันทึกเหตุการณ์จากระบบควบคุมการเข้า–ออก การติดตั้ง MQTT Broker หรือ Web Server และการติดตั้งโปรแกรมวิเคราะห์ใบหน้าหรือวัตถุต้องสงสัย อย่างไรก็ตาม ความยืดหยุ่นและการควบคุมระดับสูงของ IaaS ทำให้ผู้ใช้ต้องรับผิดชอบด้านการติดตั้งแพตช์ การกำหนดค่าความปลอดภัย การสำรองข้อมูล การเฝ้าติดตามระบบ และการบำรุงรักษาซอฟต์แวร์มากกว่ารูปแบบอื่น

ดังนั้น IaaS จึงเหมาะกับองค์กรที่มีบุคลากรด้านเทคโนโลยีสารสนเทศหรือวิศวกรระบบ และต้องการพัฒนาระบบความปลอดภัยที่มีข้อกำหนดเฉพาะ เช่น ต้องเชื่อมต่อกับระบบเดิม ต้องติดตั้งซอฟต์แวร์เฉพาะทาง หรือต้องกำหนดมาตรการควบคุมข้อมูลด้วยตนเอง

2) Platform as a Service (PaaS)

PaaS เป็นรูปแบบบริการที่ผู้ให้บริการจัดเตรียมสภาพแวดล้อมสำหรับพัฒนา ทดสอบ ติดตั้ง และดำเนินงานแอปพลิเคชันผ่านเครือข่าย โดยครอบคลุมองค์ประกอบที่จำเป็นต่อวงจรชีวิตของซอฟต์แวร์ เช่น ระบบปฏิบัติการ สภาพแวดล้อมสำหรับรันโปรแกรม ฐานข้อมูล ระบบไฟล์ เครื่องมือพัฒนา และส่วนต่อประสานโปรแกรมประยุกต์ หรือ API ด้วยเหตุนี้ PaaS จึงมักเปรียบเสมือน “ระบบปฏิบัติการของคลาวด์” และมีกลุ่มผู้ใช้หลักเป็นนักพัฒนาซอฟต์แวร์ ในรูปแบบ PaaS ผู้ให้บริการรับผิดชอบตั้งแต่โครงสร้างพื้นฐานทางกายภาพ ชั้นการจำลองเสมือน ระบบปฏิบัติการ และสภาพแวดล้อมสำหรับการทำงานของโปรแกรม ผู้พัฒนาจึงไม่จำเป็นต้องติดตั้งและดูแลเครื่องแม่ข่ายหรือระบบปฏิบัติการโดยตรง แต่สามารถมุ่งเน้นการเขียนโปรแกรม การกำหนดตรรกะของระบบ และการจัดการข้อมูลของแอปพลิเคชันได้ การพัฒนาอาจดำเนินการผ่านเว็บเบราว์เซอร์ คอนโซลระยะไกล หรือเครื่องมือพัฒนาบนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับสภาพแวดล้อมคลาวด์

เมื่อนำ PaaS มาใช้กับระบบความปลอดภัยอัจฉริยะ นักพัฒนาสามารถสร้างระบบรับข้อมูลจากอุปกรณ์ IoT ได้โดยไม่ต้องจัดตั้งเครื่องแม่ข่ายทั้งหมดด้วยตนเอง ตัวอย่างเช่น อุปกรณ์ Raspberry Pi หรือไมโครคอนโทรลเลอร์ส่งข้อมูลสถานะเซ็นเซอร์ ข้อมูลอุณหภูมิ หรือเหตุการณ์การเข้า–ออกผ่าน REST API หรือ MQTT ไปยังบริการบนคลาวด์ จากนั้นแอปพลิเคชันบน PaaS จะตรวจสอบความถูกต้อง ประมวลผล และบันทึกข้อมูลลงในฐานข้อมูล รวมถึงส่งผลไปยังเว็บแดชบอร์ดหรือแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ PaaS ยังเหมาะกับงานที่ต้องรองรับจำนวนอุปกรณ์หรือปริมาณคำขอที่เปลี่ยนแปลง เพราะแพลตฟอร์มสามารถจัดสรรทรัพยากรให้เหมาะสมกับภาระงานได้ ตัวอย่างเช่น เมื่อกล้องหรือเซ็นเซอร์จำนวนมากส่งเหตุการณ์พร้อมกัน ระบบสามารถขยาย

ทรัพยากรเพื่อรองรับการประมวลผล และลดทรัพยากรลงเมื่อปริมาณงานลดลง คุณลักษณะดังกล่าวช่วยลดภาระในการดูแลโครงสร้างพื้นฐานและทำให้การพัฒนาระบบเป็นไปอย่างรวดเร็ว อย่างไรก็ตาม ผู้พัฒนาอาจไม่สามารถควบคุมระบบปฏิบัติการหรือโครงสร้างพื้นฐานได้อย่างสมบูรณ์ และอาจต้องพัฒนาโปรแกรมตามภาษา เครื่องมือ หรือข้อจำกัดที่ผู้ให้บริการกำหนด นอกจากนี้ การย้ายแอปพลิเคชันจากผู้ให้บริการรายหนึ่งไปยังอีกรายหนึ่งอาจมีความซับซ้อน หากระบบใช้บริการเฉพาะของแพลตฟอร์มนั้นเป็นจำนวนมาก (Huawei Technologies Co., Ltd., 2023)

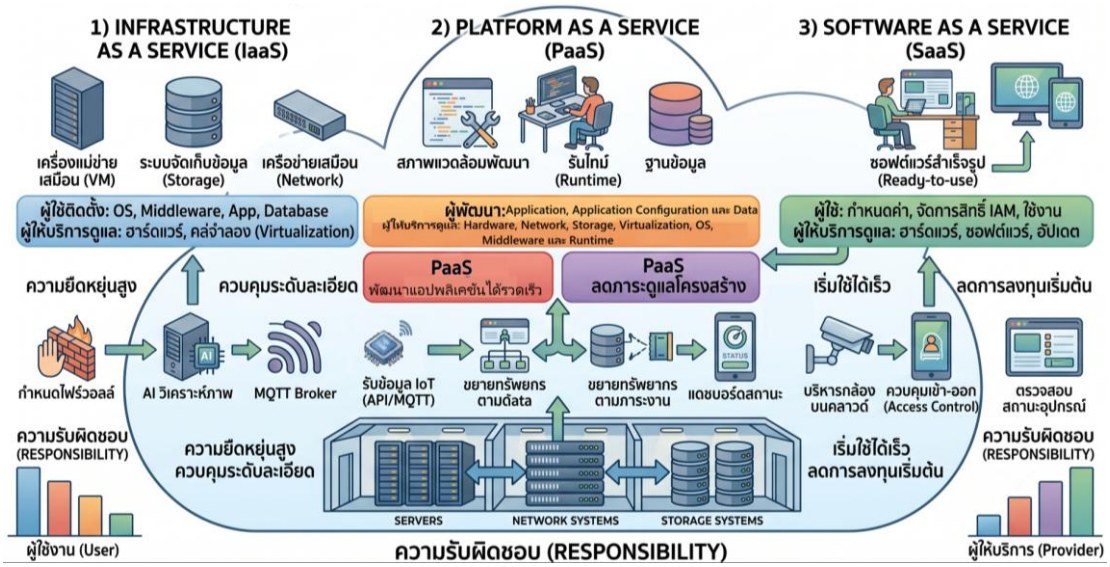
ดังนั้น PaaS จึงเหมาะสำหรับการพัฒนาระบบความปลอดภัยอัจฉริยะที่ต้องการความรวดเร็ว เช่น ระบบบันทึกข้อมูลจากเซ็นเซอร์ ระบบแจ้งเตือน ระบบแดชบอร์ดตรวจสอบสถานะอุปกรณ์ และระบบประมวลผลเหตุการณ์ โดยทีมพัฒนาต้องการมุ่งเน้นที่โปรแกรมประยุกต์มากกว่าการดูแลเครื่องแม่ข่าย

3) Software as a Service (SaaS)

SaaS เป็นรูปแบบบริการที่ผู้ให้บริการจัดเตรียมซอฟต์แวร์สำเร็จรูปให้ผู้ใช้งานผ่านอินเทอร์เน็ต ผู้ใช้สามารถเข้าถึงระบบผ่านเว็บเบราว์เซอร์ แอปพลิเคชันบนโทรศัพท์เคลื่อนที่ หรือโปรแกรมลูกข่าย โดยไม่ต้องติดตั้งและบำรุงรักษาโครงสร้างพื้นฐาน ระบบปฏิบัติการ หรือโปรแกรมหลักด้วยตนเอง ผู้ให้บริการเป็นผู้รับผิดชอบทั้งฮาร์ดแวร์ ซอฟต์แวร์ การอัปเดตระบบ และการบำรุงรักษาบริการ ส่วนผู้ใช้รับผิดชอบการกำหนดค่าการใช้งาน การจัดการบัญชีผู้ใช้ สิทธิ์การเข้าถึง และข้อมูลที่นำเข้าสู่ระบบ SaaS เป็นบริการคลาวด์ที่อยู่ในระดับบนสุดและใกล้ชิดกับผู้ใช้งานมากที่สุด เนื่องจากผู้ใช้สามารถนำซอฟต์แวร์ไปใช้งานได้โดยไม่ต้องพัฒนาระบบทั้งหมดขึ้นใหม่ รูปแบบการคิดค่าบริการอาจเป็นการสมัครสมาชิก การคิดตามจำนวนผู้ใช้ จำนวนอุปกรณ์ ระยะเวลาการใช้งาน ความจุในการจัดเก็บ หรือปริมาณข้อมูลที่ประมวลผล การใช้ SaaS จึงช่วยลดระยะเวลาในการติดตั้ง ลดภาระในการบำรุงรักษาซอฟต์แวร์ และลดความต้องการบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน (Huawei Technologies Co., Ltd., 2023)

ในระบบความปลอดภัยอัจฉริยะ ตัวอย่างของ SaaS ได้แก่ ระบบบริหารจัดการกล้องวงจรปิดบนคลาวด์ ระบบบริหารจัดการวิดีโอที่ให้บริการผ่านคลาวด์ ระบบควบคุมการเข้า–ออกบนคลาวด์ ระบบบริหารผู้มาติดต่อ ระบบตรวจสอบสถานะอุปกรณ์ และระบบแจ้งเตือนเหตุการณ์ผ่านเว็บหรือแอปพลิเคชัน ผู้ดูแลระบบสามารถเพิ่มกล้อง กำหนดสิทธิ์ผู้ใช้งาน ตรวจสอบภาพย้อนหลัง ดูประวัติการเข้า–ออก และรับการแจ้งเตือนจากระยะไกลได้โดยไม่ต้องติดตั้งเครื่องแม่ข่ายและซอฟต์แวร์บริหารจัดการภายในสถานที่ อย่างไรก็ตาม Video Management System (VMS) ไม่ได้หมายความว่าเป็น SaaS เสมอไป ระบบ VMS จะจัดเป็น SaaS เมื่อซอฟต์แวร์และองค์ประกอบหลักถูกให้บริการจากคลาวด์ และผู้ให้บริการเป็นผู้ดูแลระบบให้แก่ผู้ใช้ หากองค์กรติดตั้ง VMS บนเครื่องแม่ข่ายภายในองค์กร ระบบดังกล่าวจะเป็นซอฟต์แวร์แบบติดตั้งภายใน ไม่ใช่ SaaS ข้อดีของ SaaS คือสามารถเริ่มใช้งานได้รวดเร็ว ลดการลงทุนเริ่มต้น และเข้าถึงระบบจากหลายสถานที่ผ่านอุปกรณ์ที่หลากหลาย แต่ผู้ใช้มีอำนาจควบคุมโครงสร้างพื้นฐานและการปรับแต่งระบบน้อยกว่า IaaS และ PaaS อีกทั้งยังต้องพิจารณานโยบายการจัดเก็บข้อมูล ที่ตั้งของศูนย์ข้อมูล ความเป็นส่วนตัว ระยะเวลาการเก็บรักษาภาพและบันทึกเหตุการณ์ การส่งออกข้อมูล และข้อตกลงระดับการให้บริการ เนื่องจากข้อมูลในระบบรักษาความปลอดภัยอาจมีความอ่อนไหวและส่งผลต่อสิทธิส่วนบุคคล

ดังนั้น SaaS จึงเหมาะกับองค์กรที่ต้องการนำระบบความปลอดภัยมาใช้งานอย่างรวดเร็ว ไม่มีทีมงานสำหรับดูแลโครงสร้างพื้นฐานโดยตรง หรือต้องการใช้บริการในรูปแบบการสมัครสมาชิก แต่ควรตรวจสอบคุณสมบัติด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลของผู้ให้บริการก่อนเลือกใช้งาน



รูปที่ 7.28 สรุปภาพรวมของรูปแบบการให้บริการของ cloud platform

ตารางที่ 7.6 ความแตกต่างของรูปแบบบริการของ Cloud Platform

ประเด็น	IaaS	PaaS	SaaS
ทรัพยากรที่ได้รับ	เครื่องแม่ข่ายเสมือน ระบบจัดเก็บข้อมูล และเครือข่าย	สภาพแวดล้อมสำหรับพัฒนาและรันแอปพลิเคชัน	ซอฟต์แวร์สำเร็จรูปพร้อมใช้งาน
ผู้ใช้หลัก	ผู้ดูแลระบบและวิศวกรโครงสร้างพื้นฐาน	นักพัฒนาโปรแกรม	ผู้ใช้งานและผู้ดูแลระบบความปลอดภัย
การควบคุมของผู้ใช้	สูง	ปานกลาง	ต่ำ
ภาระการดูแลระบบ	สูง	ปานกลาง	ต่ำ
สิ่งที่ผู้ใช้ดูแล	ระบบปฏิบัติการ โปรแกรม ฐานข้อมูลและข้อมูล	โปรแกรม การกำหนดค่า และข้อมูล	บัญชีผู้ใช้ การตั้งค่า และข้อมูล
การประยุกต์ใน smart security	เครื่องแม่ข่าย VMS ฐานข้อมูล และระบบวิเคราะห์ภาพ	ระบบรับข้อมูล IoT, API, ฐานข้อมูล และแดชบอร์ด	Cloud CCTV และระบบควบคุมการเข้า–ออกบนคลาวด์
ความเหมาะสม	ระบบเฉพาะที่ต้องการควบคุมสูง	ระบบที่ต้องการพัฒนาและขยายได้รวดเร็ว	ระบบสำเร็จรูปที่ต้องการเริ่มใช้งานทันที

7.5.4 บทบาทของ Cloud Platform ในระบบความปลอดภัยอัจฉริยะ

Cloud platform มีบทบาทเป็นศูนย์กลางในการรับส่ง จัดเก็บ ประมวลผล และบริหารจัดการข้อมูลจากอุปกรณ์ในระบบความปลอดภัยอัจฉริยะ เช่น กล้องวงจรปิด เซ็นเซอร์ตรวจจับความเคลื่อนไหว เซ็นเซอร์ควัน เครื่องอ่าน RFID อุปกรณ์ควบคุมการเข้า–ออก และอุปกรณ์ตรวจจับทางชีวมิติ โดยอาศัยทรัพยากรด้านการประมวลผล ระบบจัดเก็บข้อมูล ฐานข้อมูล ระบบเครือข่าย และบริการซอฟต์แวร์ที่ให้ใช้งานผ่านอินเทอร์เน็ต Cloud Platform จึงช่วยให้ระบบรักษาความปลอดภัยสามารถทำงานร่วมกันได้จากหลายสถานที่ และรองรับการตรวจสอบจากระยะไกลได้อย่างมีประสิทธิภาพ (Huawei Technologies Co., Ltd., 2023) บทบาทสำคัญของ cloud platform ในระบบความปลอดภัยอัจฉริยะมีดังต่อไปนี้

1) การรับข้อมูลจากอุปกรณ์ IoT ผ่านเครือข่าย

Cloud platform ทำหน้าที่รับข้อมูลจากอุปกรณ์ IoT และอุปกรณ์รักษาความปลอดภัยที่ติดตั้งอยู่ในพื้นที่ต่าง ๆ ข้อมูลที่ส่งเข้าสู่ระบบอาจประกอบด้วยค่าจากเซ็นเซอร์ ภาพนิ่ง วิดีโอ สถานะของอุปกรณ์ บันทึกการเข้า–ออก และเหตุการณ์แจ้งเตือน การรับส่งข้อมูลมักดำเนินการผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายส่วนตัว โดยใช้โปรโตคอลที่เหมาะสม เช่น HTTPS, REST API หรือ MQTT ตัวอย่างเช่น เมื่อเซ็นเซอร์ตรวจจับความเคลื่อนไหวพบกิจกรรมในพื้นที่ควบคุม อุปกรณ์จะส่งข้อมูลเวลา ตำแหน่ง และสถานะการตรวจจับไปยัง cloud platform เพื่อบันทึกและประมวลผลต่อไป คุณลักษณะการเข้าถึงผ่านเครือข่ายทำให้อุปกรณ์หลายชนิดจากหลายพื้นที่สามารถเชื่อมต่อเข้าสู่ระบบส่วนกลางได้ (Huawei Technologies Co., Ltd., 2023)

2) การจัดเก็บข้อมูลบน Cloud Storage และฐานข้อมูล

Cloud platform สามารถจัดเก็บข้อมูลหลายรูปแบบ เช่น ภาพจากกล้องวงจรปิด ไฟล์วิดีโอ ข้อมูลเซ็นเซอร์ ประวัติการเข้า–ออก ข้อมูลผู้ใช้งาน และบันทึกเหตุการณ์ โดยข้อมูลที่มีโครงสร้าง เช่น รหัสผู้ใช้ วัน เวลา และสถานะอุปกรณ์ มักจัดเก็บในฐานข้อมูล ส่วนภาพและวิดีโอซึ่งมีขนาดใหญ่จะจัดเก็บใน cloud storage โดยการจัดเก็บข้อมูลไว้บนคลาวด์ช่วยให้ผู้ดูแลสามารถค้นหา เรียกดู และตรวจสอบข้อมูลย้อนหลังได้จากหลายสถานที่ นอกจากนี้ ทรัพยากรจัดเก็บข้อมูลยังสามารถเพิ่มหรือลดได้ตามปริมาณข้อมูลที่เกิดขึ้น จึงเหมาะกับระบบรักษาความปลอดภัยที่มีข้อมูลสะสมต่อเนื่อง โดยเฉพาะระบบกล้องวงจรปิดและระบบบันทึกเหตุการณ์จำนวนมาก แนวคิดดังกล่าวสอดคล้องกับคุณลักษณะการรวมทรัพยากรและการจัดสรรพื้นที่จัดเก็บตามความต้องการของระบบคลาวด์ (Huawei Technologies Co., Ltd., 2023)

3) การประมวลผลและวิเคราะห์ข้อมูลด้วย AI

Cloud platform สามารถรองรับการประมวลผลข้อมูลด้วยเทคโนโลยีปัญญาประดิษฐ์ เช่น การรู้จำใบหน้า การตรวจจับบุคคลหรือวัตถุ การวิเคราะห์ความเคลื่อนไหว การจำแนกเหตุการณ์ และการตรวจจับพฤติกรรมที่อาจผิดปกติ การประมวลผลบนคลาวด์เหมาะกับงานที่ต้องใช้กำลังประมวลผลสูงหรือมีข้อมูลจากอุปกรณ์จำนวนมาก เนื่องจากสามารถจัดสรรหน่วยประมวลผลและหน่วยความจำเพิ่มเติมได้ตามภาระงาน ตัวอย่างเช่น ระบบสามารถวิเคราะห์ภาพจากกล้องเพื่อเปรียบเทียบใบหน้ากับฐานข้อมูลผู้มีสิทธิ์เข้าใช้งาน หากพบใบหน้าที่ไม่ตรงกับข้อมูลที่ลงทะเบียนไว้ ระบบอาจจัดประเภทเหตุการณ์ว่าเป็นการเข้าถึงที่ไม่ได้รับอนุญาตและส่งข้อมูลไปยังส่วนแจ้งเตือน ทั้งนี้ หนังสือของ Huawei ระบุว่าบริการคลาวด์สามารถรองรับบริการ AI เช่น การ

รู้จำใบหน้า การรู้จำภาพ และการรู้จำเสียงได้ (Huawei Technologies Co., Ltd., 2023) อย่างไรก็ตาม ในการใช้งานจริง อาจแบ่งการประมวลผลระหว่างอุปกรณ์ปลายทางหรือ Edge computing กับคลาวด์ เพื่อให้ตอบสนองได้รวดเร็วและลดปริมาณข้อมูลที่ต้องส่งผ่านเครือข่าย

4) การเฝ้าติดตามและควบคุมระบบจากระยะไกล

Cloud platform ช่วยให้ผู้ดูแลสามารถตรวจสอบสถานะของอุปกรณ์และเหตุการณ์ด้านความปลอดภัยผ่าน Web dashboard หรือ mobile application ได้จากระยะไกล ข้อมูลที่แสดงอาจประกอบด้วยสถานะการเชื่อมต่อของอุปกรณ์ ภาพจากกล้องแบบเวลาจริง ประวัติการแจ้งเตือน สถานะประตู และค่าที่ตรวจวัดจากเซ็นเซอร์ โดยในบางระบบ ผู้มีสิทธิ์อาจส่งคำสั่งควบคุมกลับไปยังอุปกรณ์ เช่น สั่งล็อกหรือปลดล็อกประตู เปิดหรือปิดสัญญาณเตือน หรือปรับการตั้งค่าของอุปกรณ์ การควบคุมดังกล่าวต้องใช้กลไกยืนยันตัวตน กำหนดสิทธิ์ และบันทึกการใช้งาน เพื่อป้องกันการสั่งงานจากบุคคลที่ไม่ได้รับอนุญาต

5) การแจ้งเตือนเหตุการณ์แบบใกล้เคียงเวลาจริง

เมื่อ cloud platform ตรวจพบเหตุการณ์ที่ตรงกับเงื่อนไขที่กำหนด ระบบสามารถส่งการแจ้งเตือนไปยังผู้ดูแลผ่านแอปพลิเคชันบนสมาร์ตโฟน อีเมล บริการส่งข้อความ ตัวอย่างเหตุการณ์ที่อาจทำให้เกิดการแจ้งเตือน ได้แก่ การตรวจพบการเคลื่อนไหวในพื้นที่หวงห้าม การเปิดประตูนอกเวลาที่กำหนด การพยายามเข้าสู่ระบบหลายครั้งโดยไม่สำเร็จ การตรวจพบควัน เปลวไฟ หรืออุณหภูมิผิดปกติ หรือกล้องหรือเซ็นเซอร์หยุดเชื่อมต่อกับระบบ คำว่า “แบบเรียลไทม์” ในทางปฏิบัติควรพิจารณาความหน่วงของเครือข่าย การประมวลผล และบริการแจ้งเตือนร่วมด้วย จึงอาจเรียกว่า การแจ้งเตือนแบบใกล้เคียงเวลาจริง (near real-time notification) เมื่อไม่สามารถรับประกันการตอบสนองได้ทันทีทุกกรณี

6) การสำรองและกู้คืนข้อมูล

Cloud platform สามารถกำหนดให้สำรองข้อมูลโดยอัตโนมัติตามช่วงเวลาหรือนโยบายที่องค์กรกำหนด เช่น การสำรองฐานข้อมูลรายวัน การทำสำเนาบันทึกเหตุการณ์ หรือการเก็บสำเนาวิดีโอไว้ในระบบจัดเก็บข้อมูลอีกชุดหนึ่ง การสำรองข้อมูลช่วยลดความเสี่ยงจากความเสียหายของอุปกรณ์ การลบข้อมูลโดยไม่ตั้งใจ หรือความขัดข้องของระบบ นอกจากนี้ การออกแบบคลาวด์อาจใช้ระบบจัดเก็บข้อมูลแบบซ้ำซ้อนและการจำลองทรัพยากร เพื่อเพิ่มความพร้อมใช้งานและสนับสนุนการกู้คืนระบบเมื่อเกิดความล้มเหลว อย่างไรก็ตาม การสำรองข้อมูลที่ดีต้องกำหนดระยะเวลาเก็บรักษา รอบการสำรอง ตำแหน่งจัดเก็บ และวิธีทดสอบการกู้คืนอย่างชัดเจน ไม่ควรพิจารณาเฉพาะการมีไฟล์สำรองเท่านั้น (Huawei Technologies Co., Ltd., 2023)

7) การขยายระบบตามปริมาณงาน

ระบบความปลอดภัยอัจฉริยะอาจมีจำนวนอุปกรณ์และข้อมูลเพิ่มขึ้นตามการขยายพื้นที่ เช่น การเพิ่มกล้อง เซ็นเซอร์ หรือจุดควบคุมการเข้า–ออก cloud platform สามารถเพิ่มทรัพยากรประมวลผล หน่วยความจำ พื้นที่จัดเก็บ และความสามารถของเครือข่ายตามความต้องการได้ โดยไม่จำเป็นต้องเปลี่ยนโครงสร้างพื้นฐานทั้งหมด การขยายระบบอาจแบ่งเป็นการเพิ่มทรัพยากรให้เครื่องเดิม หรือการเพิ่มจำนวนเครื่องและบริการเพื่อกระจายภาระงาน ในทางกลับกันเมื่อปริมาณงานลดลง ระบบสามารถลดทรัพยากรเพื่อประหยัดค่าใช้จ่ายได้ คุณลักษณะนี้เรียกว่าความยืดหยุ่นและการปรับขนาดอย่างรวดเร็ว (rapid elasticity and scalability) ซึ่งเป็นลักษณะสำคัญของ cloud computing (Huawei Technologies Co., Ltd., 2023)

8) การเชื่อมต่อกับบริการและระบบภายนอก

Cloud platform สามารถเชื่อมโยงกับบริการภายนอกผ่าน API หรือโปรโตคอล การสื่อสารต่าง ๆ เพื่อแลกเปลี่ยนข้อมูลหรือขยายความสามารถของระบบ ตัวอย่างเช่น (1) การบันทึกผลการเข้า–ออกหรือข้อมูลการเข้าเรียนลงใน Google Sheets (2) เชื่อมต่อกับ Firebase เพื่อจัดเก็บหรือซิงโครไนซ์ข้อมูล (3) ใช้ MQTT broker เป็นตัวกลางรับส่งข้อความระหว่างอุปกรณ์ IoT กับระบบคลาวด์ (4) ส่งการแจ้งเตือนผ่านอีเมล แอปพลิเคชันส่งข้อความ หรือระบบ push notification และ (5) เชื่อมโยงกับระบบบริหารผู้ใช้ ระบบบุคลากร หรือฐานข้อมูลขององค์กร อย่างไรก็ตาม Google Sheets, Firebase และ MQTT broker ไม่ได้มีบทบาทเหมือนกันทั้งหมด โดย Google Sheets เป็นบริการซอฟต์แวร์และตารางข้อมูลออนไลน์ Firebase เป็นชุดบริการสำหรับพัฒนาแอปพลิเคชันบนคลาวด์ ส่วน MQTT broker เป็นตัวกลางรับส่งข้อความตามโปรโตคอล MQTT ดังนั้น ควรเลือกใช้แต่ละบริการให้เหมาะกับหน้าที่และข้อกำหนดของระบบ

9) การบริหารจัดการความมั่นคงปลอดภัยของข้อมูล

Cloud platform ยังมีบทบาทในการคุ้มครองข้อมูลและควบคุมการเข้าถึงระบบ โดยใช้กลไก เช่น การเข้ารหัสข้อมูล การยืนยันตัวตน การกำหนดสิทธิ์ตามบทบาท การตรวจสอบความถูกต้องของข้อมูล และการบันทึกกิจกรรมของผู้ใช้งาน Huawei ระบุกลไกด้านความมั่นคงปลอดภัยของคลาวด์ไว้หลายด้าน เช่น encryption, hashing, digital signature, public key infrastructure และ identity and access management (Huawei Technologies Co., Ltd., 2023) สำหรับระบบความปลอดภัยอัจฉริยะ กลไกเหล่านี้มีความสำคัญอย่างยิ่ง เนื่องจากข้อมูลภาพ ใบหน้า ประวัติการเข้า–ออก และข้อมูลระบุตัวบุคคลเป็นข้อมูลที่มีความอ่อนไหว จึงควรกำหนดสิทธิ์การเข้าถึง ระยะเวลาการจัดเก็บ และวิธีการส่งข้อมูลอย่างเหมาะสม

กล่าวโดยสรุป cloud platform ทำหน้าที่เป็นศูนย์กลางของระบบความปลอดภัยอัจฉริยะ ตั้งแต่การเชื่อมต่ออุปกรณ์ การจัดเก็บและวิเคราะห์ข้อมูล การแจ้งเตือน การควบคุมจากระยะไกล การสำรองข้อมูล ไปจนถึงการขยายระบบและการรักษาความมั่นคงปลอดภัย การนำ cloud platform มาใช้จึงช่วยให้ระบบมีความยืดหยุ่น รองรับอุปกรณ์จำนวนมาก และบริหารจัดการจากส่วนกลางได้สะดวกยิ่งขึ้น แต่จำเป็นต้องออกแบบด้านเครือข่าย สิทธิ์การเข้าถึง ความเป็นส่วนตัว และแผนกู้คืนข้อมูลควบคู่กันไป

7.6 REST API

REST API ย่อมาจาก Representational State Transfer Application Programming Interface เป็นรูปแบบการออกแบบช่องทางสื่อสารระหว่างโปรแกรมหรืออุปกรณ์ผ่านเครือข่าย โดยมักใช้โปรโตคอล HTTP เช่นเดียวกับการเปิดเว็บไซต์ ในระบบ IoT อุปกรณ์อย่าง ESP8266 สามารถใช้ REST API เพื่อส่งข้อมูลเซ็นเซอร์ไปยังเซิร์ฟเวอร์ หรือรับคำสั่งควบคุมอุปกรณ์จากแอปพลิเคชันได้

7.6.1 หลักการทำงานของ REST API

REST API มองข้อมูลหรืออุปกรณ์แต่ละรายการเป็น ทรัพยากร และระบุทรัพยากรนั้นด้วย URL หรือ Endpoint เช่น http://192.168.1.100/api/led จากนั้นใช้คำสั่ง HTTP เพื่อดำเนินการกับทรัพยากร ดังตารางที่ 7.7

ตารางที่ 7.7 การใช้คำสั่ง HTTP เพื่อดำเนินการกับทรัพยากร

คำสั่ง HTTP	หน้าที่	ตัวอย่าง
GET	อ่านข้อมูลหรือสถานะ	อ่านสถานะ LED
POST	สร้างข้อมูลหรือส่งคำสั่งใหม่	ส่งข้อมูลเซ็นเซอร์
PUT	ปรับปรุงหรือแทนที่ข้อมูล	เปลี่ยนสถานะ LED
PATCH	แก้ไขข้อมูลบางส่วน	เปลี่ยนเฉพาะค่าความสว่าง
DELETE	ลบข้อมูลหรือทรัพยากร	ลบรายการอุปกรณ์

ตัวอย่างการควบคุม ESP8266 ยกตัวอย่างเช่นใช้งาน ESP8266 ควบคุมหลอดไฟผ่าน GPIO5 อาจออกแบบ Endpoint ดังนี้

- `GET /api/led`; ใช้ตรวจสอบสถานะของหลอดไฟ
- `PUT /api/led`; ใช้เปลี่ยนสถานะของหลอดไฟ โดยส่งข้อมูลแบบ JSON เช่น

```
{
  "state": "on"
}
```

เซิร์ฟเวอร์อาจตอบกลับว่า

```
{
  "gpio": 5,
  "state": "on",
  "success": true
}
```

ความแตกต่างจากตัวอย่าง Web Server เดิม โปรแกรม ESP8266 ก่อนหน้านี้ใช้ URL เช่น

- `/5/on`
- `/5/off`

วิธีนี้สามารถใช้งานได้ แต่ยังเป็นการควบคุมผ่าน URL แบบง่าย ไม่ได้ออกแบบเป็น REST API อย่างชัดเจน รูปแบบ REST API ที่เป็นระบบมากกว่าจะใช้ทรัพยากรเดียว เช่น

- `/api/outputs/5`

แล้วเลือกการทำงานด้วย HTTP Method เช่น

- `GET /api/outputs/5`
- `PUT /api/outputs/5`

พร้อมส่งข้อมูล JSON เพื่อระบุสถานะที่ต้องการ

คุณลักษณะสำคัญของ REST API มักมีลักษณะสำคัญดังนี้

1) Client-server จะแยกส่วนผู้ร้องขอ เช่น แอปพลิเคชันหรือเว็บเบราว์เซอร์ ออกจากส่วนเซิร์ฟเวอร์ เช่น ESP8266 หรือ cloud server

2) Stateless โดยคำขอแต่ละครั้งต้องมีข้อมูลเพียงพอให้เซิร์ฟเวอร์ประมวลผลได้ โดยไม่ควรพึ่งพาสถานะจากคำขอก่อนหน้า

3) Resource-oriented จะใช้ URL แทนทรัพยากร เช่น เซ็นเซอร์ หลอดไฟ ประตู หรือผู้ใช้งาน

4) ใช้รูปแบบข้อมูลมาตรฐาน นิยมรับส่งข้อมูลด้วย JSON เพราะมีโครงสร้างอ่านง่าย และใช้ได้กับหลายภาษาโปรแกรม

5) ใช้รหัสสถานะ HTTP ตัวอย่างเช่น

➲200 OK หมายถึงดำเนินการสำเร็จ

➲400 Bad Request หมายถึงคำขอไม่ถูกต้อง

➲404 Not Found หมายถึงไม่พบทรัพยากร

➲500 Internal Server Error หมายถึงเซิร์ฟเวอร์เกิดข้อผิดพลาด

7.6.2 LINE Messaging API

LINE Messaging API เป็นส่วนต่อประสานโปรแกรมประยุกต์ที่ช่วยเชื่อมต่อระบบของผู้พัฒนากับ LINE Official Account โดยการเรียกใช้บริการส่วนใหญ่มีลักษณะเป็น REST API ผ่านโปรโตคอล HTTPS และรับส่งข้อมูลในรูปแบบ JSON ระบบของผู้พัฒนาสามารถเรียก Endpoint ของ LINE เพื่อส่งข้อความ ดึงข้อมูลผู้ใช้ หรือจัดการองค์ประกอบต่าง ๆ ของบัญชี ขณะเดียวกัน LINE platform ใช้กลไก Webhook เพื่อส่งเหตุการณ์จากผู้ใช้มายังเซิร์ฟเวอร์ เช่น การส่งข้อความหรือการเพิ่มบัญชีเป็นเพื่อน ดังนั้น LINE Messaging API จึงทำงานร่วมกันระหว่าง REST API และ Webhook เพื่อให้เกิดการสื่อสารแบบสองทิศทาง

1) หน้าที่ของ LINE Messaging API

LINE Messaging API เป็นบริการสำหรับพัฒนาแชตบอตหรือระบบแจ้งเตือนผ่านบัญชีทางการ LINE Official Account โดยระบบสามารถส่งและรับข้อมูลระหว่างเซิร์ฟเวอร์หรืออุปกรณ์ IoT กับแพลตฟอร์ม LINE ผ่าน HTTPS ในรูปแบบ JSON ได้ ในการประยุกต์ใช้งานกับระบบ RFID door lock นั้น เมื่อมีการอ่านบัตร RFID หรือมีการกดสวิตช์เปิดประตู ESP8266 จะประมวลผลสถานะของระบบ เช่น บัตรถูกต้อง บัตรไม่ถูกต้อง หรือมีการเปิดประตูจากภายใน จากนั้นจึงส่งข้อมูลไปยัง LINE Messaging API เพื่อแจ้งเตือนไปยังผู้ใช้งานผ่าน LINE Official Account ตัวอย่างข้อความแจ้งเตือน เช่น มีการเปิดประตูสำเร็จ มีการใช้บัตร RFID ที่ไม่ได้รับอนุญาต หรือ มีการกดสวิตช์เปิดประตูจากด้านใน

2) รูปแบบการสื่อสารของ LINE Messaging API

ระบบประกอบด้วยการสื่อสารหลัก 2 ทิศทาง ได้แก่

2.1) ระบบของผู้พัฒนาเรียก LINE Messaging API

เมื่อเซิร์ฟเวอร์หรืออุปกรณ์ของผู้พัฒนาต้องการส่งข้อความไปยังผู้ใช้ จะส่ง HTTPS Request ไปยัง Endpoint ของ LINE platform ลักษณะเป็น REST API เช่น การส่งข้อความตอบกลับ

➲POST https://api.line.me/v2/bot/message/reply

พร้อมส่งข้อมูล JSON เช่น

```
{
  "replyToken": "REPLY_TOKEN",
  "messages": [
    {
      "type": "text",
      "text": "ตรวจพบการเปิดประตู"
    }
  ]
}
```

ในส่วนหัวของคำขอต้องมี channel access token เพื่อยืนยันสิทธิ์ เช่น

➲Authorization: Bearer CHANNEL_ACCESS_TOKEN
➲Content-Type: application/json

นอกจากการส่งข้อความแล้ว LINE Messaging API ยังมี Endpoint สำหรับส่งข้อความแบบ Push ดึงข้อมูลโปรไฟล์ผู้ใช้ จัดการ Rich Menu และดำเนินการอื่น ๆ ผ่าน HTTP Request

2.2) LINE platform ส่ง Webhook มายังเซิร์ฟเวอร์

เมื่อผู้ใช้ส่งข้อความ เพิ่ม LINE Official Account เป็นเพื่อน หรือเกิดเหตุการณ์อื่น LINE platform จะส่ง HTTPS POST Request ไปยัง Webhook URL ที่ผู้พัฒนาลงทะเบียนไว้ โดยข้อมูลเหตุการณ์จะอยู่ในรูปแบบ JSON

ตัวอย่าง Webhook Event:

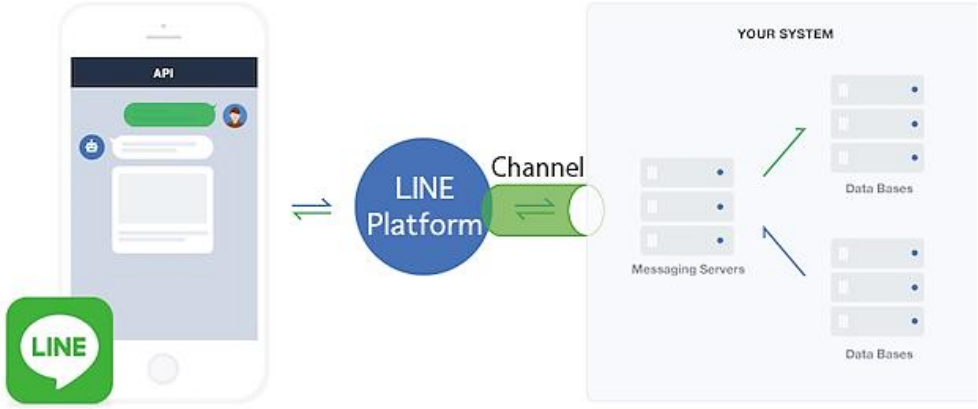
```
{
  "destination": "xxxxxxxxxx",
  "events": [
    {
      "type": "message",
      "replyToken": "xxxxxxxxxx",
      "source": {
        "type": "user",
        "userId": "Uxxxxxxxxxx"
      },
      "message": {
        "type": "text",
        "text": "สถานะประตู"
      }
    }
  ]
}
```

ดังนั้น Webhook ไม่ใช่การที่ระบบของเราเรียก LINE API แต่เป็นการที่ LINE ส่งเหตุการณ์เข้ามายังเซิร์ฟเวอร์ของเรา

3) ขั้นตอนการสร้าง LINE Messaging API

ในการใช้งาน Messaging API ผู้ใช้งานจำเป็นต้องมี channel ก่อน โดยการสร้าง channel สามารถทำได้โดยสร้างบัญชี LINE Official Account และเปิดใช้งาน Messaging API สำหรับบัญชีดังกล่าว ในหัวข้อนี้จะอธิบายขั้นตอนการสร้าง Messaging API Channel ซึ่งประกอบด้วย 2 ขั้นตอนหลัก ได้แก่ (1) การสร้าง LINE Official Account และ (2) การเปิดใช้งาน Messaging API สำหรับ LINE Official Account หากมีบัญชี LINE Official Account อยู่แล้ว ให้เริ่มต้นที่ขั้นตอนที่ 2 (LINE Developers, 2024)

Channel คือ ช่องทางการสื่อสารที่ผู้พัฒนาสามารถใช้บริการต่าง ๆ ของ LINE platform เช่น Messaging API และ LINE Login เพื่อนำไปประยุกต์ใช้งานในระบบหรือแอปพลิเคชันของตนเอง ในการใช้งานบริการของ LINE platform จำเป็นต้องมี channel ก่อน จากนั้นจึงสามารถใช้งานฟังก์ชันต่าง ๆ ของ Messaging API ได้ เช่น การส่งข้อความแจ้งเตือน การสร้างแชตบอต หรือการเชื่อมต่อระบบ IoT โดยใช้ข้อมูลของ channel เช่น access token

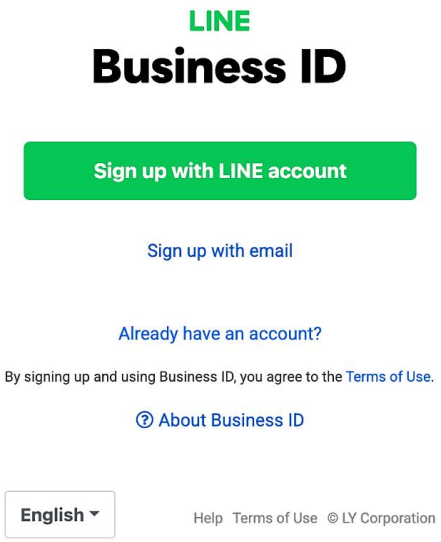


รูปที่ 7.29 ช่องทางการสื่อสารที่ผู้พัฒนาสามารถใช้บริการต่าง ๆ ของ LINE platform (LINE Developers, 2024)

3.1) ขั้นตอนที่ 1 การสร้าง LINE Official Account

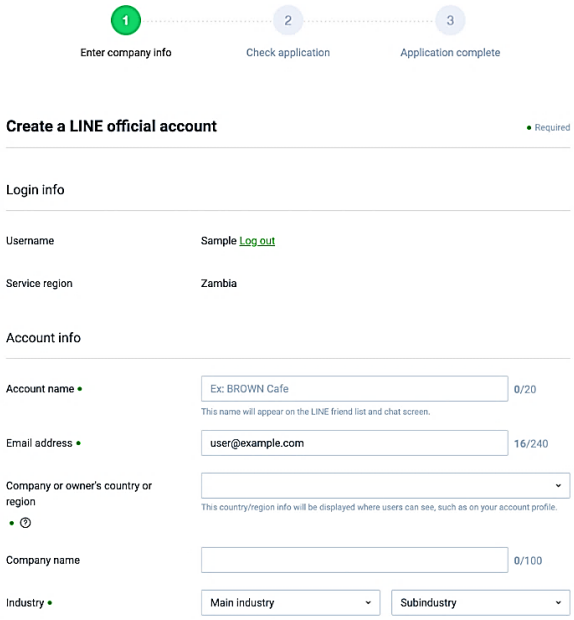
ในการใช้งาน Messaging API ผู้ใช้งานจำเป็นต้องสร้าง LINE Official Account ก่อน โดยสามารถดำเนินการได้ตามขั้นตอนดังต่อไปนี้ (1) ลงทะเบียน Business ID (2) กรอกแบบฟอร์มสมัครใช้งาน และ (3) ตรวจสอบ LINE Official Account ดังนี้

3.1.1) ขั้นตอนที่ 1-1 ลงทะเบียน Business ID เป็นการสร้าง LINE Official Account จำเป็นต้องลงทะเบียน Business ID ก่อน โดยสามารถลงทะเบียนได้ผ่านบัญชี LINE หรือใช้อีเมลในการสมัครก็ได้



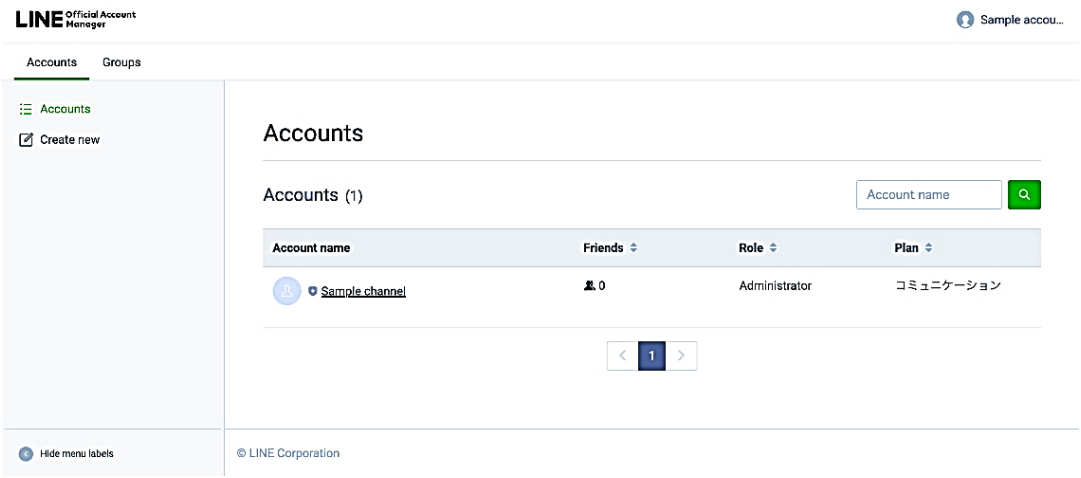
รูปที่ 7.30 การลงทะเบียน Business ID (LINE Developers, 2024)

3.1.2) ขั้นตอนที่ 1-2 กรอกแบบฟอร์มสมัครใช้งาน หลังจากลงทะเบียน Business ID เรียบร้อยแล้ว ระบบจะแสดงแบบฟอร์มสำหรับสร้าง LINE Official Account ให้กรอกข้อมูลที่จำเป็น เช่น (1) ชื่อบัญชี (2) ประเภทธุรกิจ (3) อีเมล และ (4) ประเทศหรือภูมิภาค เมื่อกรอกข้อมูลครบถ้วน ระบบจะทำการสร้าง LINE Official Account ให้โดยอัตโนมัติ



รูปที่ 7.31 การกรอกแบบฟอร์มสมัครใช้งาน (LINE Developers, 2024)

3.1.3) ขั้นตอนที่ 1-3 ตรวจสอบ LINE Official Account เมื่อดำเนินการครบทุกขั้นตอนแล้ว LINE Official Account จะถูกสร้างขึ้น และสามารถตรวจสอบบัญชีที่สร้างได้ผ่าน LINE Official Account Manager เมื่อยืนยันว่าบัญชีถูกสร้างเรียบร้อยแล้ว ให้ดำเนินการต่อในขั้นตอนที่ 2.2



รูปที่ 7.32 การตรวจสอบ LINE Official Account (LINE Developers, 2024)

3.2) ขั้นตอนที่ 2 เปิดใช้งาน Messaging API สำหรับ LINE Official Account

เมื่อเปิดใช้งาน Messaging API สำหรับ LINE Official Account ที่สร้างไว้ ระบบจะสร้าง Messaging API Channel ขึ้นโดยอัตโนมัติ โดยมีขั้นตอนดังนี้ (1) ขั้นตอนที่ 2-1 เปิดใช้งาน Messaging API (2) ขั้นตอนที่ 2-2 เข้าสู่ระบบ LINE Developers Console และ 3.2.3) ขั้นตอนที่ 2-3 ตรวจสอบ Channel

3.2.1) ขั้นตอนที่ 2-1 เปิดใช้งาน Messaging API

เมื่อเปิดใช้งาน Messaging API ผ่าน LINE Official Account Manager ระบบจะสร้าง Messaging API Channel สำหรับใช้งานร่วมกับ LINE platform หากบัญชีที่ใช้เข้าสู่ระบบ LINE Official Account Manager ยังไม่เคยใช้งาน LINE Developers Console มาก่อน ระบบจะให้ลงทะเบียนข้อมูลนักพัฒนา (developer information) เช่น ชื่อผู้พัฒนา อีเมล เพื่อสร้างบัญชีนักพัฒนา

จากนั้นให้เลือก provider สำหรับใช้จัดการ LINE Official Account โดยหากต้องการเชื่อมต่อกับบริการอื่น เช่น LINE Login ควรเลือก provider เดียวกันกับบริการที่ต้องการเชื่อมต่อ ข้อควรระวังในการเลือก provider เมื่อกำหนด provider แล้ว จะไม่สามารถเปลี่ยนหรือยกเลิก provider ภายหลังได้ จึงควรพิจารณาเลือก provider ให้เหมาะสมก่อนดำเนินการ กรณีที่ควรระมัดระวังเป็นพิเศษ ได้แก่

การจัดการ Channel และ provider โดยบุคคลหรือบริษัทหลายแห่ง

การสร้าง Channel ของบริการที่ไม่เกี่ยวข้องกันภายใต้ provider เดียวกัน

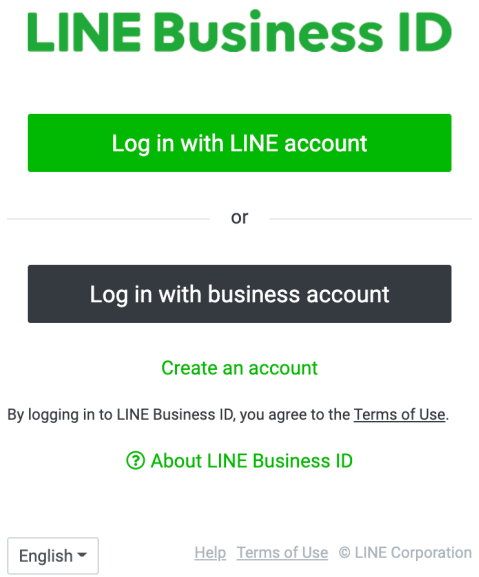
การสร้าง Channel ภายใต้ provider ของบริษัทที่ให้บริการระบบจัดการ Channel

รูปที่ 7.33 การพิจารณาเลือก Provider (LINE Developers, 2024)

กรณีดังกล่าว อาจเกิดปัญหาในอนาคต เช่น ไม่สามารถย้าย Channel ไปยัง provider อื่นได้ หรือผู้ใช้งานได้รับ User ID แตกต่างกันในแต่ละ provider ดังนั้นควรพิจารณาความเหมาะสมก่อนเลือกใช้งาน

3.2.2) ขั้นตอนที่ 2-2 เข้าสู่ระบบ LINE Developers Console

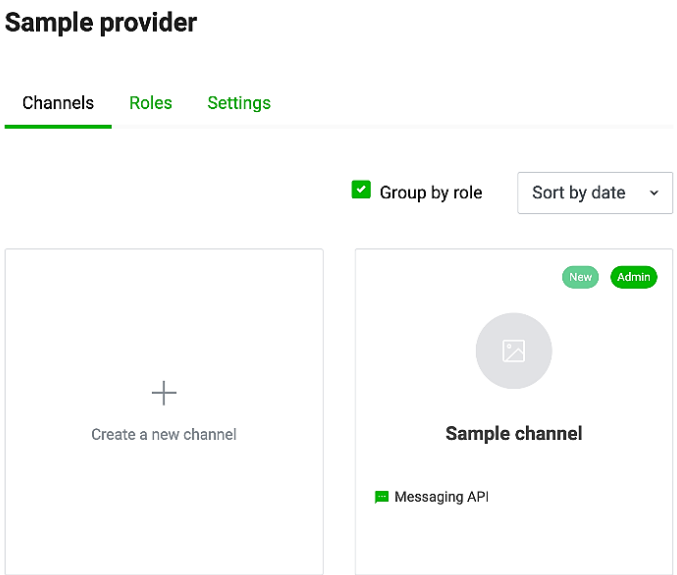
Messaging API Channel ที่สร้างขึ้นสามารถกำหนดค่าและจัดการได้ผ่าน LINE Developers Console โดยให้เข้าสู่ระบบด้วยบัญชีเดียวกับที่ใช้ใน LINE Official Account Manager



รูปที่ 7.34 การเปิดใช้งาน Messaging API (LINE Developers, 2024)

3.2.3) ขั้นตอนที่ 2-3 ตรวจสอบ Channel

เลือก provider ที่กำหนดไว้ในขั้นตอนก่อนหน้า จากนั้นตรวจสอบว่ามี Messaging API Channel ถูกสร้างขึ้นภายใต้ Provider ดังกล่าวเรียบร้อยแล้ว เมื่อสร้าง channel เรียบร้อยแล้ว ระบบก็พร้อมสำหรับการใช้งาน Messaging API



รูปที่ 7.35 การตรวจสอบ Channel (LINE Developers, 2024)

ขั้นตอนต่อไปคือการกำหนดค่า Channel เพื่อใช้พัฒนา Chatbot หรือระบบแจ้งเตือนต่าง ๆ เช่น ระบบแจ้งเตือนผ่าน LINE สำหรับงาน IoT ระบบ RFID หรือระบบควบคุมอุปกรณ์อัจฉริยะ เป็นต้น

หมายเหตุเกี่ยวกับการสร้าง Channel ปัจจุบัน LINE ได้ยกเลิกการสร้าง Messaging API Channel โดยตรงผ่าน LINE Developers Console แล้ว ตั้งแต่วันที่ 4 กันยายน 2024 เป็นต้นไป ผู้ใช้งานจะต้องสร้าง LINE Official Account ก่อน แล้วจึงเปิดใช้งาน Messaging API ผ่าน LINE Official Account Manager เท่านั้น

4) การติดตั้งไลบรารีสำหรับ LINE Messaging API ลงใน Arduino IDE

ในการใช้งาน LINE Messaging API ร่วมกับ ESP8266 จำเป็นต้องติดตั้งไลบรารีสำหรับเชื่อมต่อ HTTPS และส่งข้อความผ่าน LINE โดยสามารถใช้ไลบรารี เช่น WiFiClientSecure และ HTTPClient ซึ่งมีอยู่ใน Arduino ESP8266 core อยู่แล้ว ก่อนเริ่มใช้งาน ให้ติดตั้งบอร์ด ESP8266 ลงใน Arduino IDE โดยไปที่

4.1) File > Preferences

4.2) แล้วเพิ่ม URL สำหรับ ESP8266 Board Manager จากนั้นติดตั้งผ่าน Tools > Board > Boards Manager

4.3) ค้นหาคำว่า ESP8266 แล้วกด Install

4.4) หลังจากติดตั้งเสร็จ ให้เลือกบอร์ด NodeMCU หรือ ESP8266 ที่ใช้งาน

4.5) โปรแกรมนี้ทำหน้าที่เชื่อมต่อ ESP8266 เข้ากับเครือข่าย Wi-Fi จากนั้นใช้ LINE Messaging API ส่งข้อความแจ้งเตือนไปยังผู้ใช้งานผ่าน LINE Official Account ในการกำหนดค่า ต่าง ๆ ดังนี้

4.5.1) ssid และ password ใช้กำหนดชื่อและรหัสผ่านของเครือข่าย Wi-Fi

4.5.2) accessToken คือ Channel Access Token ที่ได้จาก LINE Developers Console

4.5.3) userId คือ User ID หรือ Group ID ของผู้รับข้อความ

4.5.4) ฟังก์ชัน sendLineMessage() ใช้ส่งข้อความไปยัง LINE Messaging API ผ่าน HTTPS

4.5.5) เมื่อเชื่อมต่อ Wi-Fi สำเร็จ โปรแกรมจะส่งข้อความ "ESP8266 Connected to LINE Messaging API" ไปยัง LINE โดยอัตโนมัติ

7.6.3 การเชื่อมต่อ Google Cloud และ Google Sheets

ระบบบันทึกการเข้าเรียนสามารถส่งข้อมูลจาก Raspberry Pi ไปจัดเก็บใน Google Sheets โดยใช้ Google Sheets API และบัญชีบริการ หรือ Service Account สำหรับยืนยันตัวตนของโปรแกรม บัญชีบริการเป็นบัญชีที่ใช้แทนแอปพลิเคชัน ไม่ใช่บัญชีผู้ใช้ทั่วไป การกำหนดสิทธิ์จึงควรยึดหลักสิทธิ์เท่าที่จำเป็น หรือ principle of least privilege โดยอนุญาตให้บัญชีบริการเข้าถึงเฉพาะไฟล์ที่ระบบต้องใช้งานเท่านั้น (Google for Developers, 2026)

1) การสร้างโปรเจกต์ใน Google Cloud

1.1) เข้าสู่ระบบ https://console.cloud.google.com/welcome/new?pli=1 ด้วยบัญชี Google ที่ต้องการใช้จัดการระบบ

1.2) เลือกตัวเลือกโปรเจกต์บริเวณส่วนบนของหน้าจอ แล้วเลือก **New Project** หรือไปที่ **IAM & Admin** > **Manage Resources**

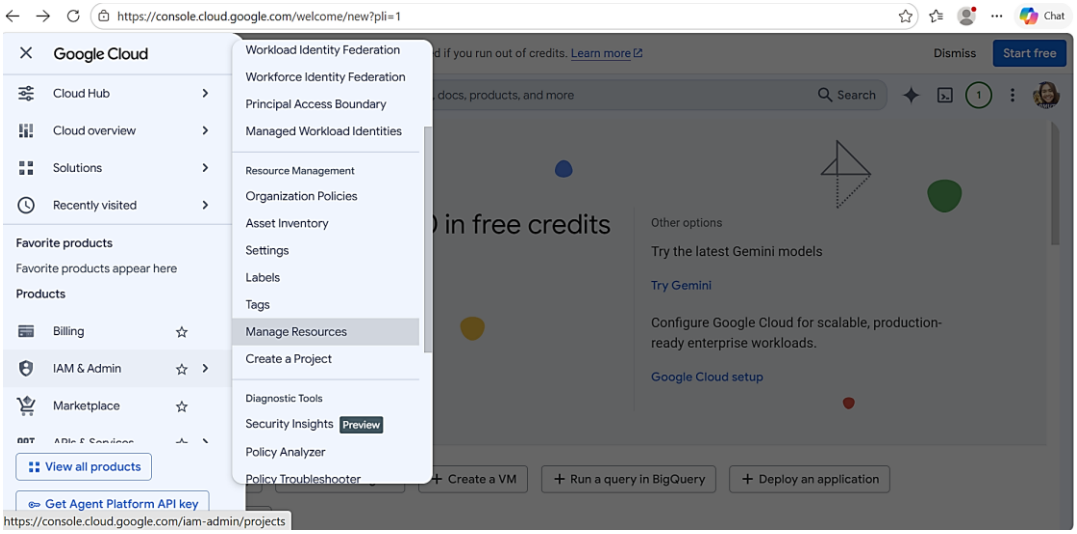
1.3) เลือก **Create Project**

1.4) กำหนดชื่อโปรเจกต์ เช่น face-attendance-system

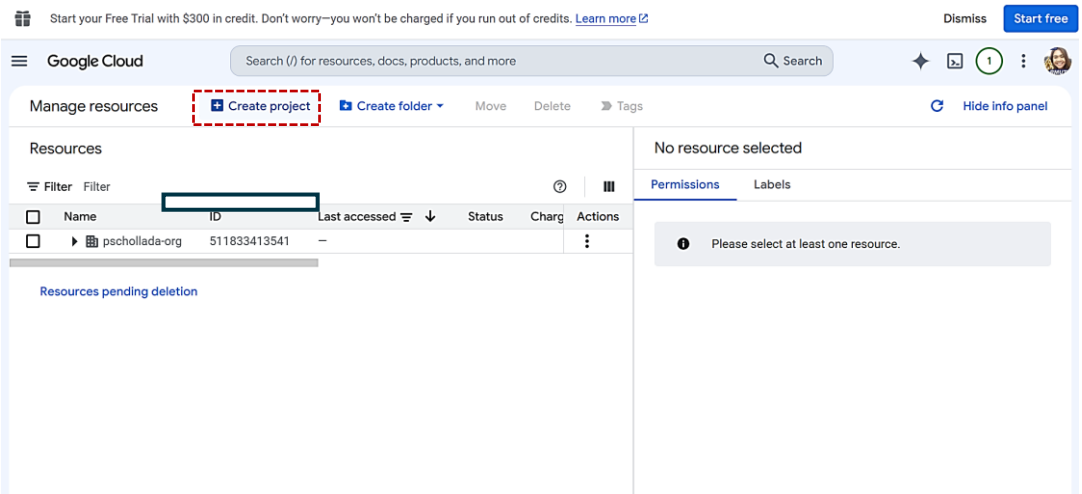
1.5) ตรวจสอบ Organization และ Location หากบัญชีดังกล่าวอยู่ภายใต้หน่วยงาน

1.6) คลิก **Create** และรอจนกระทั่งระบบสร้างโปรเจกต์เสร็จสมบูรณ์

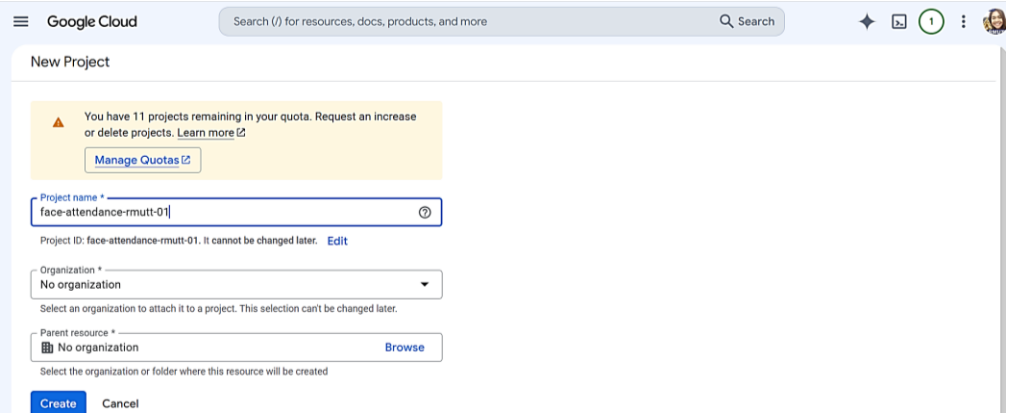
1.7) เลือกโปรเจกต์ที่สร้างขึ้นให้เป็นโปรเจกต์ปัจจุบันก่อนดำเนินการขั้นตอนต่อไป



รูปที่ 7.36 การเข้าสู่หน้าจัดการทรัพยากรเพื่อสร้างโปรเจกต์ใน Google Cloud



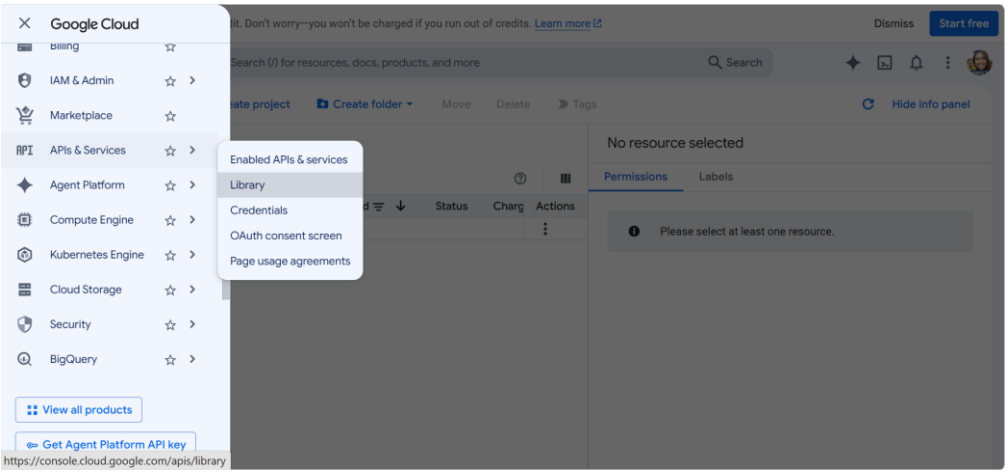
รูปที่ 7.37 การสร้างโปรเจกต์สำหรับระบบบันทึกข้อมูลลง Google Sheets



รูปที่ 7.38 การกำหนดชื่อและรายละเอียดของโปรเจกต์

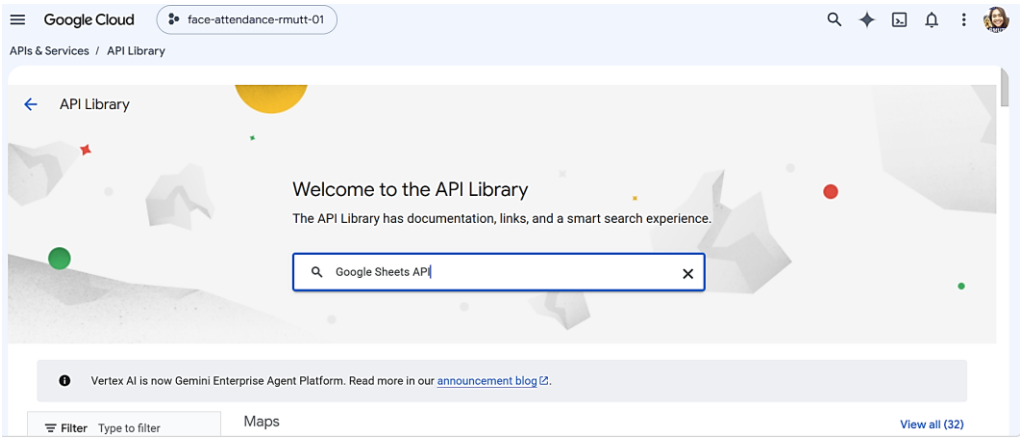
2) การเปิดใช้งาน Google Sheets API

2.1) ไปที่เมนู **APIs & Services** > **Library**



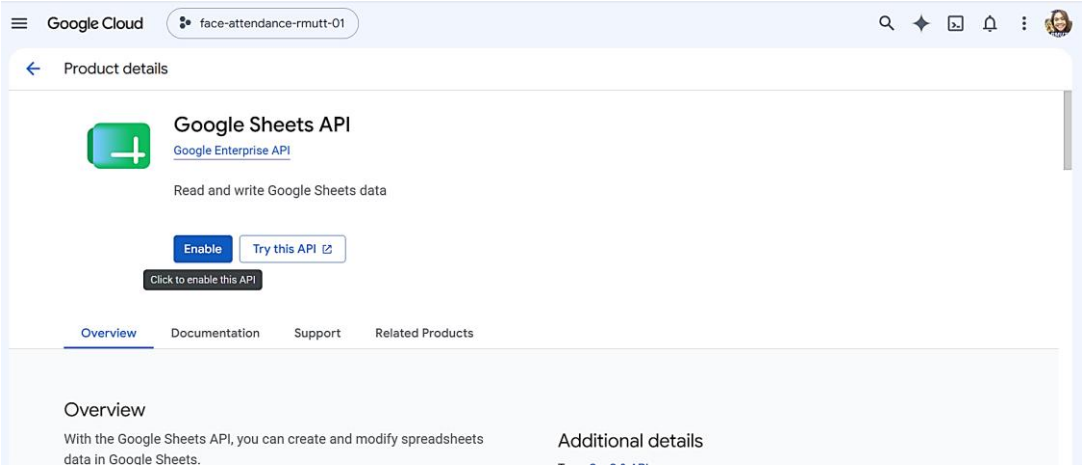
รูปที่ 7.39 หน้าแดชบอร์ดสำหรับตรวจสอบ API ของโปรเจกต์

2.2) ค้นหา **Google Sheets API**



รูปที่ 7.40 การค้นหาและเลือก Google Sheets API

2.3) เลือก **Google Sheets API** แล้วคลิก **Enable**

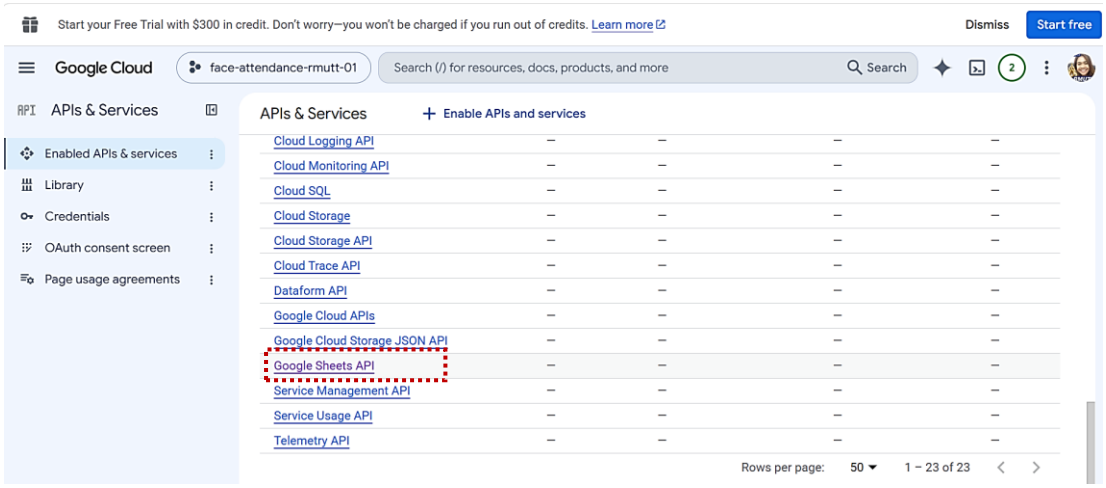


รูปที่ 7.41 การเปิดใช้งาน Google Sheets API

2.4) กลับไปที่หน้า **APIs & Services** > **Enabled APIs & services** เพื่อตรวจสอบว่า API อยู่ในสถานะเปิดใช้งานแล้ว

Google Sheets API เป็น API หลักที่จำเป็นสำหรับการอ่านและเขียนข้อมูลในเซลล์ ส่วน Google Drive API ไม่จำเป็นสำหรับการเขียนข้อมูลลงในสเปรดชีตที่ทราบรหัสไฟล์และแชร์สิทธิ์ให้บัญชีบริการแล้ว อย่างไรก็ตาม ควรเปิด Google Drive API เพิ่มเติมเมื่อโปรแกรมต้องค้นหา สร้าง คัดลอก ย้าย หรือจัดการสิทธิ์ของไฟล์ใน Google Drive หรือเมื่อไลบรารีที่เลือกใช้เรียกใช้ความสามารถดังกล่าว (Google for Developers, 2026)

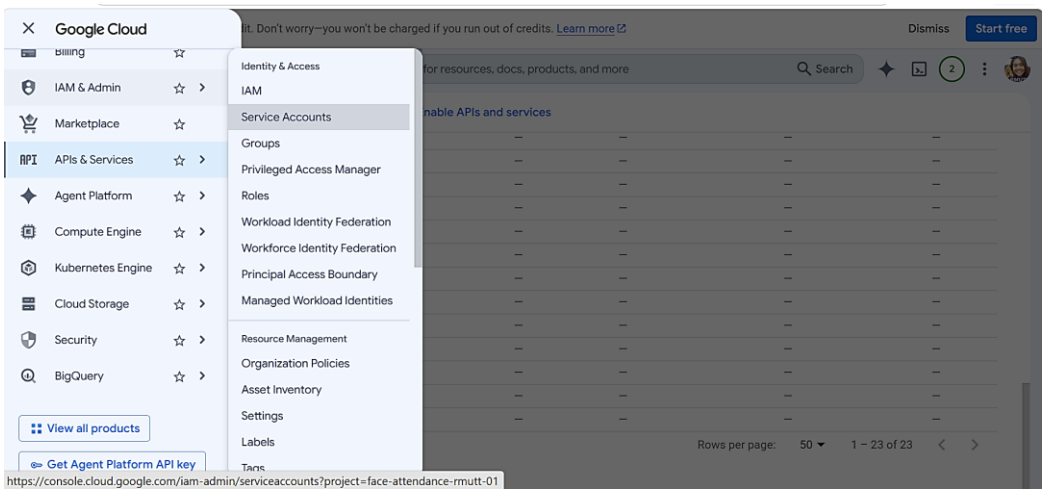
2.5) หากโปรแกรมจำเป็นต้องดำเนินการกับไฟล์ใน Google Drive ให้ค้นหา **Google Drive API** และคลิก **Enable**



รูปที่ 7.42 การตรวจสอบสถานะของ API ที่เปิดใช้งานแล้ว

3) การสร้างบัญชีบริการ

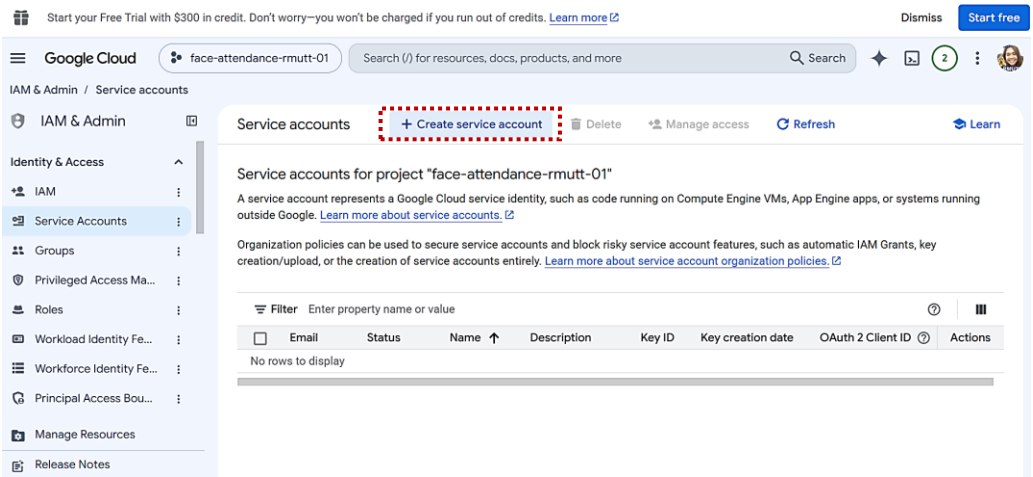
3.1) ไปที่เมนู **IAM & Admin** > **Service Accounts**



รูปที่ 7.43 การสร้างบัญชีบริการสำหรับแอปพลิเคชัน

3.2) เลือกโปรเจกต์ที่สร้างไว้

3.3) คลิก **Create Service Account**

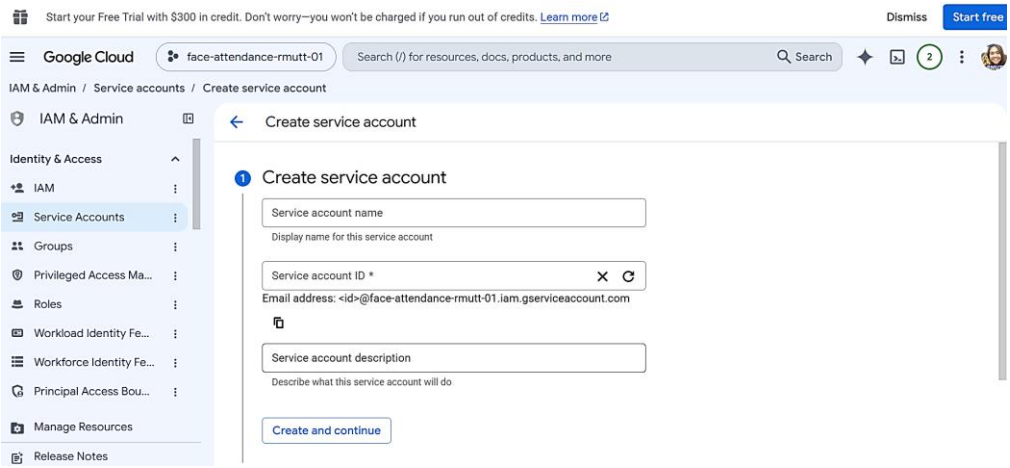


รูปที่ 7.44 ขั้นการ Create Service Account

3.4) กำหนดชื่อบัญชีบริการ เช่น face-attendance-service

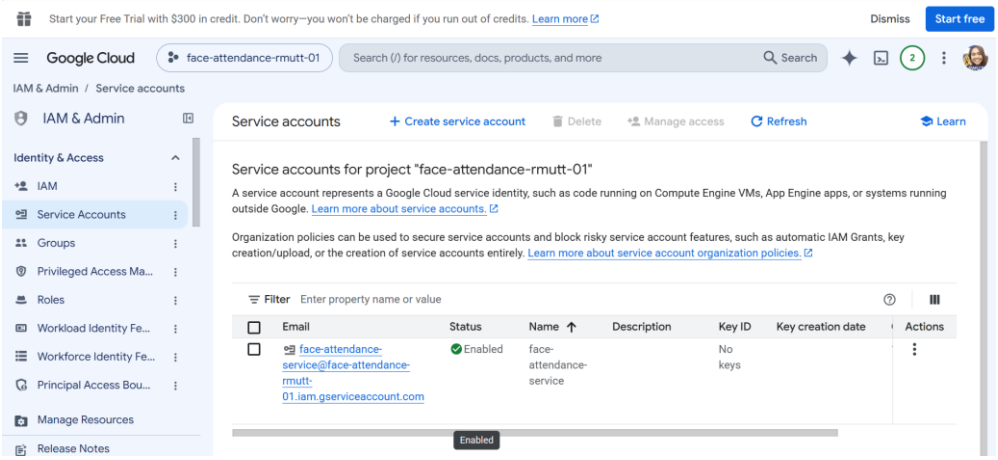
3.5) ตรวจสอบ Service Account ID ซึ่งระบบสร้างให้อัตโนมัติ

3.6) คลิก **Create and Continue**



รูปที่ 7.45 การกำหนดชื่อและรหัสของบัญชีบริการ

3.7) สำหรับระบบที่ต้องการอ่านและเขียนเฉพาะ Google Sheets ที่แชร์ให้โดยตรง ไม่จำเป็นต้องกำหนดบทบาท Editor ให้บัญชีบริการในระดับโปรเจกต์ จึงสามารถข้ามการกำหนดบทบาทและเลือก **Done** ได้



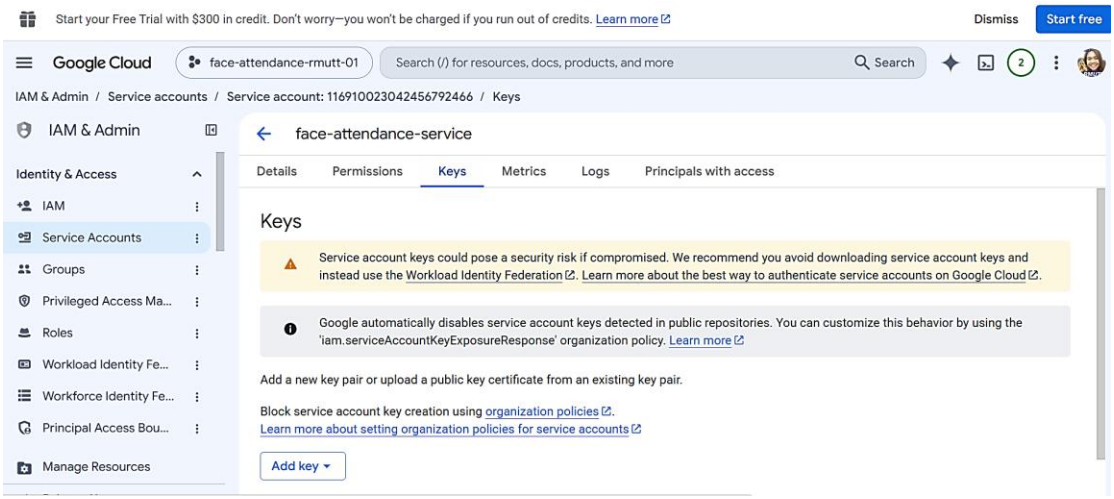
รูปที่ 7.46 เสร็จสิ้นการสร้างบัญชีบริการ

บทบาท IAM ของ Google Cloud ใช้ควบคุมทรัพยากรภายในโปรเจกต์ แต่ไม่ได้ให้สิทธิ์เข้าถึงไฟล์ Google Sheets โดยอัตโนมัติ การเข้าถึงสเปรดชีตต้องกำหนดผ่านเมนู Share ของไฟล์นั้นแยกต่างหาก (Google for Developers, 2026)

4) การสร้างไฟล์กุญแจของบัญชีบริการ

4.1) เปิดบัญชีบริการที่สร้างไว้

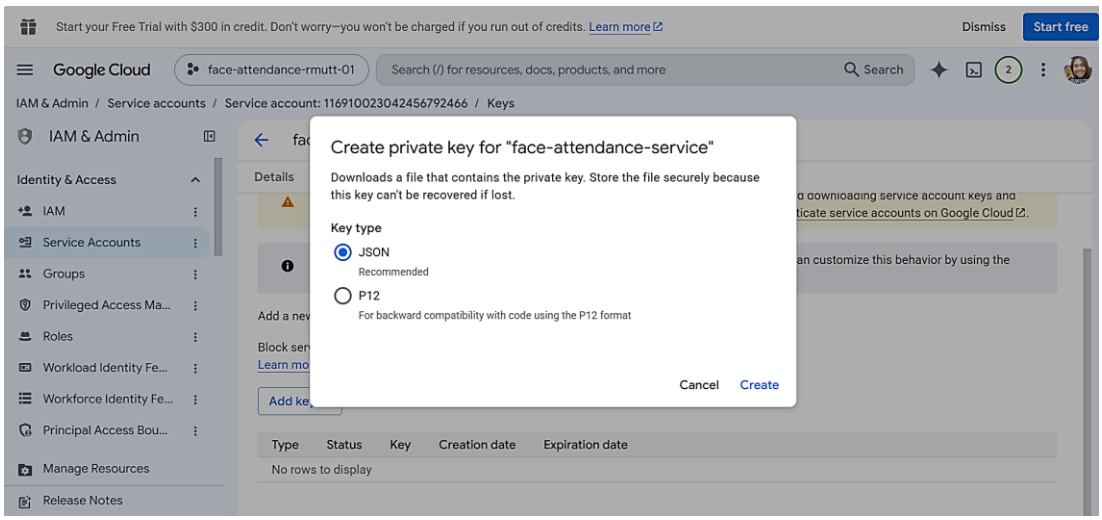
4.2) เลือกแท็บ **Keys**



รูปที่ 7.47 การเข้าสู่แท็บ Keys ของบัญชีบริการ

4.3) เลือก **Add Key** > **Create New Key**

4.4) เลือกประเภทกุญแจเป็น **JSON**



รูปที่ 7.48 การสร้างกุญแจของบัญชีบริการในรูปแบบ JSON

4.5) คลิก **Create** ระบบจะดาวน์โหลดไฟล์กุญแจลงในคอมพิวเตอร์โดยอัตโนมัติ

4.6) ย้ายไฟล์ดังกล่าวไปยัง Raspberry Pi ด้วยวิธีที่ปลอดภัย

อาจเปลี่ยนชื่อไฟล์เป็น credentials.json หรือ creds.json เพื่อให้เรียกใช้ในโปรแกรมได้สะดวก แต่การเปลี่ยนชื่อไม่ใช่ข้อกำหนดของ Google ไฟล์ JSON ดังกล่าวมี private key ซึ่งใช้ยืนยันตัวตนของแอปพลิเคชัน จึงห้ามเผยแพร่ผ่าน GitHub แนบไว้ในรายงาน ใส่ในภาพหน้าจอ หรือส่งผ่านช่องทางสาธารณะ หากกุญแจรั่วไหลต้องยกเลิกหรือลบกุญแจเดิมและสร้างกุญแจใหม่ทันที (Google Cloud, 2026)

5) การกำหนดสิทธิ์เข้าถึง Google Sheets

5.1) เปิดไฟล์ JSON ด้วยโปรแกรมแก้ไขข้อความ

5.2) คัดลอกค่าในรายการ client_email ตัวอย่างเช่น

face-attendance-service@project-id.iam.gserviceaccount.com

5.3) สร้างหรือเปิด Google Sheets ที่ต้องการใช้จัดเก็บข้อมูล

5.4) คลิก **Share**

5.5) วางอีเมลของบัญชีบริการลงในช่องเพิ่มผู้ใช้งาน

5.6) กำหนดสิทธิ์เป็น **Editor** หากโปรแกรมต้องเขียนข้อมูล หรือกำหนดเป็น **Viewer** หากต้องการอ่านข้อมูลเพียงอย่างเดียว

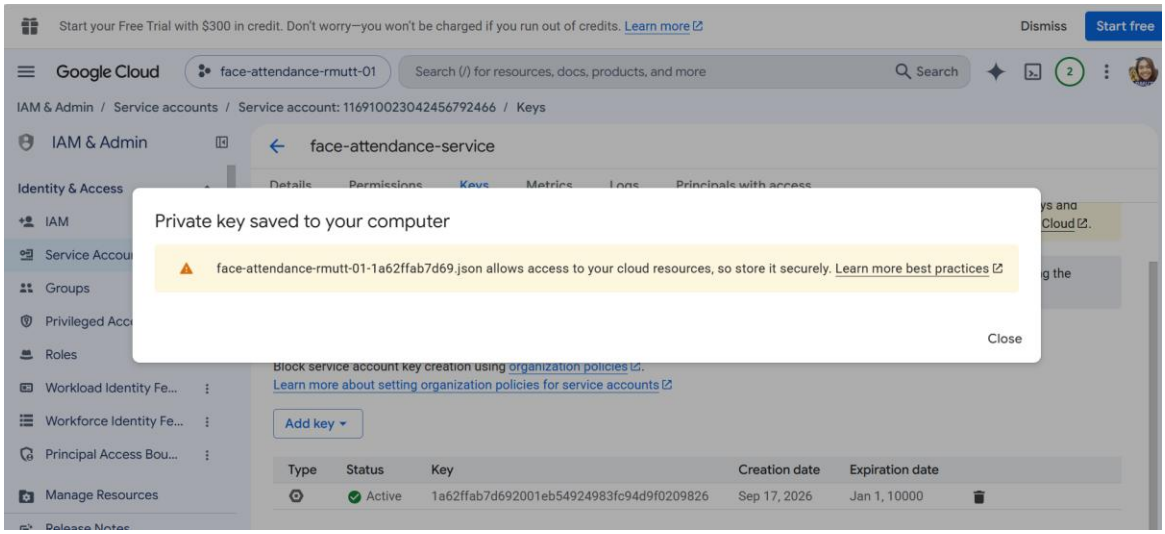
5.7) ปิดตัวเลือก **Notify people** เนื่องจากบัญชีบริการไม่มีกล่องรับอีเมล

5.8) คลิก **Share** เพื่อบันทึกการกำหนดสิทธิ์

5.9) คัดลอก Spreadsheet ID จาก URL ของ Google Sheets ตัวอย่างเช่น

https://docs.google.com/spreadsheets/d/SPREADSHEET_ID/edit

การแชร์ไฟล์โดยตรงให้อีเมลของบัญชีบริการเป็นวิธีที่เหมาะสมสำหรับระบบที่เข้าถึงเฉพาะสเปรดชีตที่กำหนด และไม่จำเป็นต้องเปิดใช้ Domain-wide Delegation (Google for Developers, 2026)



รูปที่ 7.49 การยืนยันการดาวน์โหลดกุญแจส่วนตัวของบัญชีบริการในรูปแบบ JSON

บรรณานุกรมบทที่ 7

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095Atzori et al., 2010;

Ayeni, J. (2020). Internet of Things (IoT): The technology, architecture and applications – prospects in Nigeria. *Internet of Things and Cloud Computing*, *8*(4), 41-45. https://doi.org/10.11648/j.iotcc.20200804.11.

Ayeni, P. O., & Adesoba, O. C. (2025). IoT-based home control system using NodeMCU and Firebase. *Journal of Edge Computing, 4*(1), 17–34. https://doi.org/10.55056/jec.814.

Ghael, H. D., Solanki, L., & Sahu, G. (2021). A Review paper on Raspberry Pi and its applications. *International Journal of Advances in Engineering and Management, 2*(12), 225–227. https://doi.org/10.35629/5252-0212225227.

Google Cloud. (2026). *Create and delete service account keys*. https://docs.cloud.google.com/iam/docs/keys-create-delete

Google Cloud. (2026). *Set up Application Default Credentials*. https://docs.cloud.google.com/docs/authentication/provide-credentials-adc

Google for Developers. (2026). *Create access credentials*. https://developers.google.com/workspace/guides/create-credentials

Google for Developers. (2026). *Enable Google Workspace APIs*. https://developers.google.com/workspace/guides/enable-apis

Gubsky, S. (2023). Development of low-cost Arduino-based equipment for analytical and educational applications. *Engineering Proceedings*, *48*(1), 8. https://doi.org/10.3390/CSAC2023-14893.

Huawei Technologies Co., Ltd. (2023). *Cloud computing technology*. Springer. https://doi.org/10.1007/978-981-19-3026-3.

Halvorsen, H.-P. (2026). *Raspberry Pi and Python*. https://www.halvorsen.blog/documents/programming/python/resources/Python%20Programming.pdf.

Joshi, A., & Gawande, P. G. (2025). Raspberry Pi 5 unleashed: Powering the next generation of IoT and Edge AI. *International Journal of Novel Research and Development, 10*(10).

Kim, Wan-Soo & Lee, W. S. & Kim, Yong-Joo. (2020). A Review of the applications of the Internet of Things (IoT) for agricultural automation. *Journal of Biosystems Engineering. 45*, 385-400. https://doi.org/10.1007/s42853-020-00078-3.

LINE Developers. (2024). *Get started with the Messaging API*. LINE Developers Documentation. https://developers.line.biz/en/docs/messaging-api/getting-started/.

Mathe, S. E., Kondaveeti, H. K., Vappangi, S., Vanambathina, S. D., & Kumaravelu, N. K. (2024). A comprehensive review on applications of Raspberry Pi. *Computer Science Review, 52*, 100636.

Prabhu, S. (2026). *What is RFID? How it works? Interface RC522 RFID module with Arduino*. Last Minute Engineers. https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/.

Raja, P., Kumar, S., Yadav, D. S., & Singh, T. (2023). The Internet of Things (IoT): A review of concepts, technologies, and applications. *International Journal of Information Technology & Computer Engineering, 3*(2), 21–32. https://doi.org/10.55529/ijitc.32.21.32.

Santos, R., & Santos, S. (2016). *ESP8266 web server with Arduino IDE: Step-by-step project guide*. Random Nerd Tutorials.

The MagPi Magazine. (2019). *The official Raspberry Pi projects book: Volume 5*. Raspberry Pi Press. https://magazines-static.raspberrypi.org/books/full_pdfs/000/000/029/original/Pi-Projects5.pdf.

The MagPi. (2019). *The MagPi* (Issue 83). Raspberry Pi Foundation. https://www.raspberrypi.org/magpi/issues/83/.

สรุปสาระสำคัญของบทที่ 7
อินเทอร์เน็ตของสรรพสิ่งสำหรับระบบรักษาความปลอดภัย

พื้นฐานของ Internet of Things (IoT)

IoT เป็นแนวคิดในการเชื่อมโยงอุปกรณ์ วัตถุ เครื่องจักร และระบบต่าง ๆ เข้ากับเครือข่ายอินเทอร์เน็ต เพื่อให้อุปกรณ์สามารถตรวจวัดสภาพแวดล้อม แลกเปลี่ยนข้อมูล วิเคราะห์ข้อมูล และสั่งงานอุปกรณ์ได้โดยอัตโนมัติหรือกึ่งอัตโนมัติ เทคโนโลยี IoT เกิดจากการทำงานร่วมกันของเซ็นเซอร์ ระบบสมองกลฝังตัว ระบบสื่อสารไร้สาย cloud computing และปัญญาประดิษฐ์ ทำให้อุปกรณ์ทางกายภาพพัฒนาเป็นอุปกรณ์อัจฉริยะที่สามารถรับรู้ ประมวลผล และตอบสนองต่อเหตุการณ์ได้ โดยมีเป้าหมายเพื่อเพิ่มประสิทธิภาพ ลดการใช้ทรัพยากร และสนับสนุนการตัดสินใจบนพื้นฐานของข้อมูล

องค์ประกอบพื้นฐานของระบบ IoT ประกอบด้วยเซ็นเซอร์สำหรับตรวจวัดข้อมูลจากสภาพแวดล้อม แอคชูเอเตอร์สำหรับเปลี่ยนคำสั่งจากระบบประมวลผลให้เป็นการกระทำทางกายภาพ หน่วยประมวลผล เช่น Arduino, ESP8266, ESP32 หรือ Raspberry Pi ระบบสื่อสารสำหรับส่งข้อมูลผ่าน Ethernet, Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN หรือเครือข่ายโทรศัพท์เคลื่อนที่ ตลอดจน gateway สำหรับรวบรวม กรอง และแปลงโปรโตคอลก่อนส่งข้อมูลไปยัง cloud นอกจากนี้ cloud computing ยังทำหน้าที่จัดเก็บ ประมวลผล วิเคราะห์ และแสดงผลข้อมูล ส่วน application layer เป็นส่วนที่ผู้ใช้ติดต่อกับระบบผ่านแอปพลิเคชันหรือแดชบอร์ด

หลักการทำงานของระบบ IoT เริ่มจากเซ็นเซอร์ตรวจวัดข้อมูล หน่วยประมวลผลรวบรวมและประมวลผลข้อมูลเบื้องต้น จากนั้นส่งข้อมูลผ่านเครือข่ายไปยัง gateway หรือ cloud เพื่อจัดเก็บและวิเคราะห์ เมื่อระบบประเมินข้อมูลแล้วจะสร้างคำสั่งหรือการแจ้งเตือนและส่งกลับมายังอุปกรณ์ปลายทาง เพื่อให้แอคชูเอเตอร์ดำเนินการตามเงื่อนไขที่กำหนด กระบวนการนี้ทำให้ระบบสามารถทำงานอัตโนมัติ ติดตามสถานะ และควบคุมอุปกรณ์จากระยะไกลได้ คุณลักษณะที่สำคัญของ IoT ได้แก่ การเชื่อมต่อ การรับรู้สภาพแวดล้อม ระบบอัตโนมัติ การประมวลผลอัจฉริยะ ความสามารถในการขยายระบบ และการทำงานร่วมกันระหว่างอุปกรณ์ต่างชนิด

IoT มีความสำคัญต่อระบบรักษาความปลอดภัยอัจฉริยะ เพราะช่วยเชื่อมโยงกล้อง IP Camera เซ็นเซอร์ตรวจจับควันและก๊าซ เซ็นเซอร์ตรวจจับความเคลื่อนไหว ระบบควบคุมประตู และระบบแจ้งเตือนให้สามารถแลกเปลี่ยนข้อมูลและทำงานร่วมกันได้ ผู้ดูแลจึงสามารถติดตามสถานะ รับแจ้งเหตุผิดปกติ และควบคุมอุปกรณ์จากสมาร์ตโฟนหรือศูนย์ควบคุมได้ เมื่อประยุกต์ร่วมกับ cloud computing, Edge computing และ AI ระบบยังสามารถวิเคราะห์เหตุการณ์ คาดการณ์ความเสี่ยง และตอบสนองต่อภัยคุกคามได้รวดเร็วขึ้น

ไมโครคอนโทรลเลอร์ Arduino

Arduino เป็นแพลตฟอร์มพัฒนาต้นแบบอิเล็กทรอนิกส์แบบเปิด ซึ่งประกอบด้วยบอร์ดไมโครคอนโทรลเลอร์และซอฟต์แวร์สำหรับเขียนโปรแกรม จุดเด่นคือใช้งานไม่ซับซ้อน มีความ

ยืดหยุ่น และรองรับการเชื่อมต่อกับเซ็นเซอร์ จอแสดงผล โมดูลสื่อสาร และแอคชูเอเตอร์หลายชนิด Arduino สามารถรับข้อมูลทั้งแบบดิจิทัลและแอนะล็อก ประมวลผลข้อมูลตามโปรแกรม และส่งสัญญาณไปควบคุม LED รีเลย์ มอเตอร์ หรือจอแสดงผล จึงเหมาะสำหรับการศึกษา การสร้างต้นแบบ ระบบอัตโนมัติ หุ่นยนต์ และระบบ IoT

แพลตฟอร์ม Arduino แบ่งออกเป็นฮาร์ดแวร์และซอฟต์แวร์ โดยบอร์ดแต่ละรุ่นแตกต่างกันในด้านชนิดของไมโครคอนโทรลเลอร์ จำนวนขาอินพุตและเอาต์พุต หน่วยความจำ แรงดันใช้งาน ความเร็วสัญญาณนาฬิกา และอินเทอร์เฟซการสื่อสาร ตัวอย่างบอร์ดในไฟล์ ได้แก่ Arduino Uno R3, Uno R4 WiFi, Nano, Mega 2560, Leonardo, Due, Zero, Nano 33 IoT, GIGA R1 WiFi และ Portenta ซึ่งควรเลือกใช้ตามจำนวนอุปกรณ์ที่ต้องเชื่อมต่อ สมรรถนะ และลักษณะของงาน

Arduino Uno R3 ใช้ไมโครคอนโทรลเลอร์ ATmega328P เป็นหน่วยประมวลผลหลัก มีองค์ประกอบภายใน ได้แก่ Flash Program Memory, SRAM, EEPROM, ชุดรีจิสเตอร์ทั่วไป หน่วยคำนวณและตรรกะหรือ ALU รีจิสเตอร์สถานะ บัสข้อมูลแบบ 8 bit หน่วยขัดจังหวะ SPI, Watchdog Timer, Analog Comparator และโมดูล I/O ต่าง ๆ Flash ใช้เก็บโปรแกรม SRAM ใช้เก็บตัวแปรระหว่างการทำงาน ส่วน EEPROM ใช้เก็บข้อมูลที่ต้องคงอยู่แม้หยุดจ่ายไฟ เช่น รหัสผ่านหรือค่าปรับเทียบเซ็นเซอร์ Watchdog Timer มีความสำคัญต่อระบบรักษาความปลอดภัย เพราะช่วยรีเซตระบบโดยอัตโนมัติเมื่อโปรแกรมค้าง

ซอฟต์แวร์ Arduino IDE ใช้สำหรับเขียน ตรวจสอบ คอมไพล์ และอัปโหลดโปรแกรมลงบอร์ด โปรแกรม Arduino เรียกว่า Sketch และใช้ภาษา C/C++ เป็นพื้นฐาน โดยมีโครงสร้างสำคัญคือ ฟังก์ชัน setup() ซึ่งทำงานหนึ่งครั้งเมื่อเริ่มต้นระบบ และฟังก์ชัน loop() ซึ่งทำงานวนซ้ำอย่างต่อเนื่อง เนื้อหาในไฟล์ยังอธิบายตัวดำเนินการทางคณิตศาสตร์ ตัวเพิ่มและลดค่า ตัวกำหนดค่าแบบประกอบ ตัวดำเนินการระดับbit และตัวอย่างการเขียนโปรแกรมให้ LED กระพริบเพื่อทดสอบการทำงานของบอร์ดและกระบวนการอัปโหลดโปรแกรม

การประยุกต์ใช้ Arduino ในบทนี้เน้นการเชื่อมต่อกับโมดูล RFID RC522 ผ่านการสื่อสารแบบ SPI โดยโมดูลทำงานที่แรงดัน 3.3 V ขาสื่อสารหลักประกอบด้วย SDA/SS, SCK, MOSI, MISO และ RST การใช้งานต้องติดตั้งไลบรารี MFRC522 และทดสอบการอ่านแท็กด้วยโปรแกรม DumpInfo ผ่าน Serial Monitor ข้อมูลที่อ่านได้ประกอบด้วย UID ขนาดหน่วยความจำ และโครงสร้างของบล็อกข้อมูล ในบัตร MIFARE แต่ละ Sector มีบล็อกสำหรับเก็บข้อมูลผู้ใช้และ Sector Trailer สำหรับเก็บ Access Bits ที่ใช้ควบคุมสิทธิ์การอ่านและเขียน

เมื่ออ่านค่า UID ได้แล้ว สามารถนำ UID มาใช้เป็นเงื่อนไขควบคุม LED หรืออุปกรณ์ภายนอก หาก UID ตรงกับค่าที่กำหนด Arduino จะสั่งให้อุปกรณ์ทำงาน หากไม่ตรงจะไม่อนุญาตให้ทำงาน เนื้อหาในไฟล์ยังพัฒนาต่อยอดเป็นระบบควบคุมการเข้า–ออกประตูด้วย RFID ร่วมกับ Keypad 4×4, LCD, servo motor, LED และ buzzer โดยผู้ใช้ต้องแตะบัตรและป้อนรหัสผ่านให้ถูกต้อง ระบบจึงจะหมุนเซอร์โวมอเตอร์เพื่อจำลองการปลดล็อกประตู หากข้อมูลไม่ถูกต้อง ระบบจะแสดงข้อความปฏิเสธ เปิด LED สีแดง และส่งเสียงแจ้งเตือน

ESP8266

ESP8266 เป็นระบบบนชิปที่รวมหน่วยประมวลผลแบบ 32-bit วงจร Wi-Fi และชุดโปรโตคอล TCP/IP ไว้ในอุปกรณ์เดียว จึงสามารถทำหน้าที่เป็นทั้งตัวควบคุมระบบสมองกลฝังตัวและอุปกรณ์เชื่อมต่อเครือข่าย เหมาะสำหรับระบบ IoT ระบบบ้านอัจฉริยะ ระบบตรวจวัดจากระยะไกล และระบบรักษาความปลอดภัยที่ต้องรับข้อมูลจากเซ็นเซอร์ ประมวลผล และส่งข้อมูลผ่านเครือข่าย Wi-Fi นอกจากนี้ยังสามารถสร้างเว็บเซิร์ฟเวอร์ขนาดเล็กสำหรับควบคุม GPIO ผ่านคอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ตได้

ESP8266 มีทั้งแบบโมดูลและบอร์ดพัฒนา โมดูลที่กล่าวถึงในไฟล์ ได้แก่ ESP-01 ซึ่งมีขนาดเล็กและมี GPIO จำกัด ESP-07 ซึ่งรองรับเสาอากาศภายนอก และ ESP-12E/ESP-12F ซึ่งมีขาใช้งานและหน่วยความจำมากกว่า ส่วนบอร์ดพัฒนาที่นิยม ได้แก่ NodeMCU V2, NodeMCU V3 และ WeMos D1 Mini ซึ่งมีวงจรควบคุมแรงดัน USB-to-UART และปุ่มรีเซตติดตั้งมาให้ ทำให้สามารถอัปโหลดโปรแกรมผ่านพอร์ต USB ได้สะดวก

โครงสร้างของ NodeMCU ESP8266 ประกอบด้วยขาจ่ายไฟ VIN, 3.3V และ GND ขาสื่อสารแบบ I²C, GPIO, ADC, UART, SPI, SDIO, PWM และขาควบคุม EN, RST และ WAKE ขาเหล่านี้รองรับการเชื่อมต่อกับเซ็นเซอร์ RFID จอแสดงผล GPS และอุปกรณ์ภายนอกหลายประเภท ผู้พัฒนาต้องคำนึงถึงระดับแรงดัน 3.3 Vและข้อจำกัดของขาแต่ละขา โดยเฉพาะขาที่เกี่ยวข้องกับการบูตระบบและการสื่อสาร

การพัฒนาโปรแกรมสำหรับ ESP8266 สามารถทำผ่าน Arduino IDE โดยติดตั้งแพ็กเกจ ESP8266 Community และเลือกบอร์ด NodeMCU 1.0 หรือรุ่นที่ใช้งานจริง สำหรับ NodeMCU สามารถเชื่อมต่อและอัปโหลดโปรแกรมผ่าน USB ได้โดยตรง ส่วน ESP-01 ต้องใช้อุปกรณ์ USB-to-UART และกำหนด GPIO0 ลงกราวด์ในระหว่างเข้าสู่โหมดดาวน์โหลดโปรแกรม เนื้อหาในไฟล์ยังอธิบายการสร้างเว็บเซิร์ฟเวอร์ด้วย ESP8266 เพื่อควบคุม LED หรือรีเลย์ผ่านเว็บเบราว์เซอร์ภายในเครือข่ายเดียวกัน

การเชื่อมต่อ RFID RC522 กับ ESP8266 ใช้การสื่อสารแบบ SPI โดย NodeMCU ทำหน้าที่ประมวลผล UID ของบัตรและสามารถส่งข้อมูลผ่าน Wi-Fi ไปยังระบบออนไลน์ได้ บทนี้ยังนำ MCP23017 มาใช้เป็น I/O Expander เพื่อเพิ่มจำนวนขาอินพุตและเอาต์พุต ทำให้สามารถเชื่อมต่อ LED หลายดวง จอ LCD รีเลย์ และอุปกรณ์อื่นร่วมกันได้ การประยุกต์ใช้งานที่สำคัญคือระบบควบคุมกลอนประตูโซลินอยด์ โดยใช้รีเลย์เป็นตัวสวิตช์แหล่งจ่ายไฟให้กลอน เพราะขา GPIO ของ ESP8266 ไม่สามารถจ่ายกระแสให้กลอนได้โดยตรง ระบบจะปลดล็อกประตูเมื่อ UID ถูกต้อง แสดงผลผ่าน LCD และ LED และกลับสู่สถานะล็อกเมื่อครบเวลาที่กำหนด

อีกส่วนหนึ่งของหัวข้อ ESP8266 กล่าวถึงการแจ้งเตือนผ่าน LINE Messaging API โดยต้องสร้าง LINE Official Account เปิดใช้งาน Messaging API รับ Channel Access Token และกำหนด User ID หรือ Group ID ในโปรแกรม ESP8266 จะเชื่อมต่อ Wi-Fi และส่งข้อความผ่าน HTTPS ฟังก์ชันดังกล่าวสามารถนำไปใช้แจ้งเตือนเมื่ออ่านบัตร RFID สำเร็จ เมื่อมีการเปิดประตู หรือเมื่อมีผู้พยายามเข้าใช้งานโดยไม่ได้รับอนุญาต

Cloud Platform

Cloud platform เป็นแพลตฟอร์มที่ให้บริการทรัพยากรเทคโนโลยีสารสนเทศผ่านเครือข่าย เช่น หน่วยประมวลผล พื้นที่จัดเก็บข้อมูล ฐานข้อมูล ระบบเครือข่าย และบริการซอฟต์แวร์ โดยผู้ใช้ไม่จำเป็นต้องสร้างและดูแลโครงสร้างพื้นฐานทั้งหมดด้วยตนเอง สำหรับระบบความปลอดภัย อัจฉริยะ Cloud Platform ทำหน้าที่เป็นศูนย์กลางในการรวบรวม ประมวลผล จัดเก็บ และบริหารข้อมูลจากกล้อง IP Camera เซ็นเซอร์ตรวจจับความเคลื่อนไหว เซ็นเซอร์ควัน เครื่องอ่าน RFID ระบบตรวจจับใบหน้า และระบบควบคุมการเข้า–ออก ทำให้สามารถติดตามอุปกรณ์และเหตุการณ์จากระยะไกลผ่านอินเทอร์เน็ตได้

องค์ประกอบของ Cloud Platform ในไฟล์ประกอบด้วย cloud data center ซึ่งรวมเครื่องแม่ข่าย ระบบเครือข่าย และระบบจัดเก็บข้อมูล cloud computing resources ซึ่งจัดเตรียม CPU หน่วยความจำ พื้นที่จัดเก็บ และเครือข่ายเสมือน database service สำหรับเก็บข้อมูลผู้ใช้ ประวัติการเข้า–ออก ข้อมูลเซ็นเซอร์ ภาพจากกล้อง และข้อมูลแจ้งเตือน application platform สำหรับให้บริการเว็บและแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ และ security service ซึ่งใช้การเข้ารหัส การจัดการตัวตนและสิทธิ์เข้าถึง และการตรวจสอบความถูกต้องของข้อมูล

รูปแบบการให้บริการ cloud platform แบ่งเป็น 3 ระดับ ได้แก่ IaaS, PaaS และ SaaS โดย IaaS ให้บริการโครงสร้างพื้นฐาน เช่น เครื่องเสมือน พื้นที่จัดเก็บ และเครือข่าย ผู้ใช้รับผิดชอบระบบปฏิบัติการ มิดเดิลแวร์ ฐานข้อมูล และแอปพลิเคชัน PaaS จัดเตรียมระบบปฏิบัติการ Runtime มิดเดิลแวร์และเครื่องมือพัฒนาให้ นักพัฒนาจึงมุ่งเน้นการสร้างแอปพลิเคชันและจัดการข้อมูล ส่วน SaaS เป็นซอฟต์แวร์พร้อมใช้งานผ่านเว็บหรือแอปพลิเคชัน โดยผู้ให้บริการดูแลระบบเกือบทั้งหมด ความแตกต่างสำคัญจึงอยู่ที่ระดับการควบคุมและขอบเขตความรับผิดชอบระหว่างผู้ใช้กับผู้ให้บริการ

Cloud platform มีบทบาทในการรับข้อมูลจากอุปกรณ์ IoT ผ่านเครือข่าย จัดเก็บภาพ วิดีโอ ประวัติการเข้า–ออก และข้อมูลเซ็นเซอร์ วิเคราะห์ข้อมูลด้วย AI เฝ้าติดตามและควบคุมระบบจากระยะไกล ส่งการแจ้งเตือน สำรองและกู้คืนข้อมูล ตลอดจนเพิ่มหรือลดทรัพยากรตามปริมาณงาน นอกจากนี้ยังช่วยเชื่อมต่อบริการภายนอกและควบคุมการเข้าถึงข้อมูลผ่านกลไกความมั่นคงปลอดภัย ทำให้ระบบรักษาความปลอดภัยจากหลายพื้นที่สามารถบริหารจัดการร่วมกันจากส่วนกลางได้

แบบฝึกหัดท้ายบทที่ 7
อินเทอร์เน็ตของสรรพสิ่งสำหรับระบบรักษาความปลอดภัย

ตอนที่ 1 คำถามปรนัย

จงเลือกคำตอบที่ถูกต้องที่สุดเพียงคำตอบเดียว

1. ข้อใดอธิบายความหมายของ Internet of Things ได้ถูกต้องที่สุด
   ก. ระบบที่ใช้คอมพิวเตอร์เพียงเครื่องเดียวควบคุมอุปกรณ์ทั้งหมด
   ข. การเชื่อมโยงอุปกรณ์ วัตถุ และระบบต่าง ๆ ผ่านเครือข่ายเพื่อรับส่งและประมวลผลข้อมูล
   ค. ระบบสำหรับจัดเก็บข้อมูลบนฮาร์ดดิสก์ภายในเครื่อง
   ง. การเขียนโปรแกรมเพื่อควบคุมมอเตอร์โดยไม่ใช้เครือข่าย
2. อุปกรณ์ใดทำหน้าที่ตรวจวัดข้อมูลจากสภาพแวดล้อม
   ก. Actuator ข. Gateway
   ค. Sensor ง. Relay
3. ข้อใดเป็นหน้าที่หลักของ Actuator
   ก. ตรวจวัดอุณหภูมิ ข. เปลี่ยนคำสั่งควบคุมให้เป็นการกระทำทางกายภาพ
   ค. จัดเก็บข้อมูลบน Cloud ง. แปลงหมายเลข IP เป็นชื่อโดเมน
4. อุปกรณ์ใดทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์ IoT กับเครือข่ายอินเทอร์เน็ต
   ก. Gateway ข. LED
   ค. Buzzer ง. Keypad
5. ข้อใดไม่ใช่คุณลักษณะสำคัญของระบบ IoT
   ก. Connectivity ข. Automation
   ค. Scalability ง. Standalone operation เท่านั้น
6. Arduino Uno R3 ใช้ไมโครคอนโทรลเลอร์รุ่นใดเป็นหน่วยประมวลผลหลัก
   ก. ESP8266EX ข. ATmega328P
   ค. STM32F4 ง. RP2040
7. หน่วยความจำใดใช้เก็บโปรแกรมหลักของ Arduino
   ก. SRAM ข. EEPROM
   ค. Flash Program Memory ง. Cache Memory
8. หน่วยความจำใดใช้เก็บค่าที่ต้องคงอยู่แม้ปิดแหล่งจ่ายไฟ
   ก. SRAM ข. EEPROM
   ค. Register ง. Stack
9. ฟังก์ชันใดของ Arduino ทำงานเพียงครั้งเดียวเมื่อเริ่มต้นระบบ
   ก. loop() ข. setup()
   ค. digitalRead() ง. delay()

10. ฟังก์ชันใดของ Arduino ทำงานวนซ้ำอย่างต่อเนื่อง

ก. setup() ข. pinMode()

ค. loop() ง. analogRead()

11. โมดูล RFID RC522 สื่อสารกับ Arduino ผ่านโปรโตคอลใดเป็นหลัก

ก. I²C ข. SPI

ค. UART ง. HTTP

12. แรงดันไฟฟ้าที่เหมาะสมสำหรับจ่ายให้โมดูล RFID RC522 คือข้อใด

ก. 1.5 V ข. 3.3 V

ค. 9 V ง. 12 V

13. ค่าใดใช้ระบุตัวตนของแท็ก RFID

ก. SSID ข. UID

ค. IP Address ง. Baud Rate

14. ส่วนใดของหน่วยความจำ MIFARE ใช้เก็บ Access Bits

ก. Manufacturer Block ข. Sector Trailer

ค. SRAM ง. Data Bus

15. ข้อใดเป็นจุดเด่นสำคัญของ ESP8266

ก. มีเพียง ADC และไม่มีระบบสื่อสาร ข. รวมหน่วยประมวลผล Wi-Fi และ TCP/IP ในชิปเดียว

ค. ใช้งานได้เฉพาะระบบแบบใช้สาย ง. ไม่สามารถเขียนโปรแกรมผ่าน Arduino IDE ได้

16. บอร์ดพัฒนาใดใช้โมดูล ESP-12E หรือ ESP-12F เป็นพื้นฐาน

ก. Arduino Mega ข. NodeMCU

ค. Arduino Leonardo ง. Raspberry Pi Pico

17. ข้อใดเป็นขาสำหรับรับแรงดันไฟฟ้าภายนอกของ NodeMCU

ก. VIN ข. GND

ค. SDA ง. MISO

18. โมดูลใดใช้เพิ่มจำนวนขาอินพุตและเอาต์พุตให้ NodeMCU

ก. RC522 ข. MCP23017

ค. FTDI ง. ESP-01

19. เหตุใดจึงไม่ควรต่อกลอนประตูโซลินอยด์เข้ากับขา GPIO ของ ESP8266 โดยตรง

ก. เพราะใช้แรงดันและกระแสสูงกว่าที่ GPIO สามารถจ่ายได้

ข. เพราะโซลินอยด์ใช้สัญญาณ I²C

ค. เพราะ ESP8266 ไม่มีขาเอาต์พุต

ง. เพราะ GPIO ใช้ได้เฉพาะกับ LED

20. อุปกรณ์ใดใช้เป็นตัวกลางในการควบคุมแหล่งจ่ายไฟให้กลอนประตูโซลินอยด์

ก. Sensor ข. Relay

ค. EEPROM ง. Gateway

21. รูปแบบการให้บริการคลาวด์ใดให้ผู้ใช้ควบคุมระบบปฏิบัติการและแอปพลิเคชันได้มากที่สุด

ก. SaaS ข. PaaS

ค. IaaS ง. Web Service

22. รูปแบบบริการใดเหมาะสำหรับนักพัฒนาที่ต้องการสร้างแอปพลิเคชันโดยไม่ดูแลระบบปฏิบัติการเอง

ก. IaaS ข. PaaS

ค. SaaS ง. LAN

23. ระบบบริหารกล้องวงจรปิดบนคลาวด์แบบพร้อมใช้งานจัดอยู่ในบริการประเภทใด

ก. IaaS ข. PaaS

ค. SaaS ง. VLAN

24. ข้อใดเป็นบทบาทของ Cloud Platform ในระบบความปลอดภัยอัจฉริยะ

ก. รับและจัดเก็บข้อมูลจากอุปกรณ์ IoT ข. วิเคราะห์ข้อมูลและส่งการแจ้งเตือน

ค. สนับสนุนการควบคุมจากระยะไกล ง. ถูกทุกข้อ

25. กล้อง IP Camera แตกต่างจากกล้องวงจรปิดแบบแอนะล็อกในประเด็นสำคัญใด

ก. ไม่สามารถส่งภาพผ่านเครือข่ายได้ ข. สามารถเชื่อมต่อเครือข่ายและเข้าถึงจากระยะไกลได้

ค. ไม่สามารถบันทึกภาพได้ ง. ไม่มีระบบตรวจจับความเคลื่อนไหว

ตอนที่ 2 คำถามถูก–ผิด

ให้เขียนคำว่า “ถูก” หรือ “ผิด” พร้อมแก้ไขข้อความที่ผิดให้ถูกต้อง

----- 1. เซ็นเซอร์ทำหน้าที่รับคำสั่งจากระบบประมวลผลและเปลี่ยนเป็นการกระทำทางกายภาพ

----- 2. Gateway สามารถทำหน้าที่รวบรวมข้อมูลและแปลงโปรโตคอลได้

----- 3. Arduino Uno R3 สามารถเชื่อมต่อ Wi-Fi ได้โดยไม่ต้องใช้อุปกรณ์เพิ่มเติม

----- 4. ฟังก์ชัน setup() ทำงานวนซ้ำตลอดเวลาที่บอร์ดได้รับไฟเลี้ยง

----- 5. โมดูล RC522 ควรได้รับแรงดันไฟฟ้า 3.3 V

----- 6. ขา MISO ใช้ส่งข้อมูลจากไมโครคอนโทรลเลอร์ไปยังโมดูล RFID

----- 7. UID สามารถนำมาใช้ตรวจสอบสิทธิ์ในการเข้า–ออกได้

----- 8. ESP8266 มีวงจร Wi-Fi อยู่ภายในชิป

----- 9. NodeMCU สามารถอัปโหลดโปรแกรมผ่าน USB ได้โดยตรง

----- 10. ESP-01 มีวงจร USB-to-UART ติดตั้งอยู่ภายในบอร์ด

----- 11. MCP23017 สื่อสารกับ NodeMCU ผ่าน I^2C

----- 12. รีเลย์ช่วยให้ไมโครคอนโทรลเลอร์ควบคุมโหลดที่ใช้แรงดันหรือกระแสสูงได้

----- 13. IaaS เป็นซอฟต์แวร์สำเร็จรูปที่ผู้ใช้เปิดใช้งานผ่านเว็บเบราว์เซอร์ทันที

----- 14. SaaS ทำให้ผู้ใช้ไม่ต้องดูแลโครงสร้างพื้นฐานและระบบปฏิบัติการด้วยตนเอง

----- 15. Cloud Platform สามารถรองรับการสำรองข้อมูลและการขยายทรัพยากรได้

ตอนที่ 3 คำถามอัตนัย

สถานการณ์ที่ 1 ระบบควบคุมการเข้า–ออกห้องปฏิบัติการ

ห้องปฏิบัติการแห่งหนึ่งต้องการใช้บัตร RFID ร่วมกับรหัสผ่านเพื่อควบคุมประตู เมื่อข้อมูลถูกต้อง ระบบต้องปลดล็อกประตูเป็นเวลา 5 วินาที แสดงข้อความบน LCD เปิดไฟสีเขียว และบันทึกเหตุการณ์ หากข้อมูลไม่ถูกต้อง ระบบต้องเปิดไฟสีแดงและส่งเสียงเตือน จงตอบคำถามต่อไปนี้

1. ระบุอุปกรณ์ที่จำเป็นสำหรับระบบนี้
2. อธิบายลำดับการทำงานตั้งแต่ผู้ใช้แตะบัตรจนถึงการปลดล็อกประตู
3. อธิบายหน้าที่ของ RFID RC522, Keypad, LCD, Relay และ Solenoid Door Lock
4. เสนอวิธีเพิ่มความปลอดภัยของระบบอย่างน้อย 3 วิธี
5. หากระบบอ่านบัตรได้แต่ไม่สามารถปลดล็อกประตูได้ ควรตรวจสอบส่วนใดบ้าง

สถานการณ์ที่ 2 ระบบแจ้งเตือนผู้บุกรุกผ่านอินเทอร์เน็ต

บ้านพักอาศัยติดตั้งเซ็นเซอร์ตรวจจับความเคลื่อนไหวและ IP Camera เมื่อเซ็นเซอร์ตรวจพบการเคลื่อนไหวในช่วงเวลากลางคืน ระบบต้องบันทึกเหตุการณ์ ส่งข้อความแจ้งเตือนไปยังผู้ดูแล และเปิดไฟบริเวณทางเข้า จงตอบคำถามต่อไปนี้

1. ระบุ Sensor, Actuator, Processing Unit และ Application ที่ใช้ในระบบ
2. อธิบายเส้นทางของข้อมูลตั้งแต่เซ็นเซอร์จนถึงผู้ดูแล
3. อธิบายบทบาทของ Cloud Platform ในระบบนี้
4. วิเคราะห์ผลกระทบหากอินเทอร์เน็ตขัดข้อง
5. เสนอแนวทางให้ระบบยังทำงานได้แม้อินเทอร์เน็ตขัดข้อง

สถานการณ์ที่ 3 ระบบ RFID เชื่อมต่อ Cloud

องค์กรต้องการให้ NodeMCU อ่าน UID จากบัตร RFID แล้วส่งข้อมูลไปยัง Cloud Platform เพื่อบันทึกวัน เวลา และผลการอนุญาตเข้าใช้งาน จงตอบคำถามต่อไปนี้

1. อธิบายข้อมูลที่ควรส่งไปยัง Cloud
2. เสนอรูปแบบฐานข้อมูลที่เหมาะสม
3. อธิบายเหตุผลที่ต้องใช้ HTTPS หรือกลไกการเข้ารหัส
4. อธิบายวิธีป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล
5. วิเคราะห์ข้อดีและข้อจำกัดของการจัดเก็บข้อมูลบน Cloud

สถานการณ์ที่ 4 การเลือกบริการ Cloud

หน่วยงานหนึ่งต้องการพัฒนาระบบรักษาความปลอดภัย โดยมีทีมโปรแกรมเมอร์แต่ไม่มีเจ้าหน้าที่ดูแลเครื่องแม่ข่าย ขณะที่อีกหน่วยงานต้องการติดตั้งระบบสำเร็จรูปและเริ่มใช้งานทันที จงตอบคำถามต่อไปนี้

1. หน่วยงานแรกควรเลือก IaaS, PaaS หรือ SaaS เพราะเหตุใด
2. หน่วยงานที่สองควรเลือกบริการประเภทใด
3. เปรียบเทียบระดับการควบคุมและภาระในการดูแลของทั้งสองกรณี
4. ระบุประเด็นด้านความมั่นคงปลอดภัยที่ควรพิจารณาก่อนเลือกผู้ให้บริการ

---

8 ปัญญาประดิษฐ์สำหรับระบบรักษาความปลอดภัย

81

ความรู้พื้นฐานของปัญญาประดิษฐ์

8.1.1 ความหมายของปัญญาประดิษฐ์ในระบบรักษาความปลอดภัยอัจฉริยะ
8.1.2 บทบาทของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ
8.1.3 เทคโนโลยี AI ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ
8.1.4 การทำงานของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ
8.1.5 ข้อดีของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ
8.1.6 ข้อจำกัดและประเด็นด้านจริยธรรมของ AI

82

การเรียนรู้ของเครื่อง

8.2.1 ความหมายของการเรียนรู้ของเครื่อง
8.2.2 หลักการทำงานของ Machine Learning
8.2.3 ประเภทของ Machine Learning
8.2.4 การประยุกต์ใช้ Machine Learning ในระบบรักษาความปลอดภัยอัจฉริยะ
8.2.5 กระบวนการพัฒนา Machine Learning
8.2.6 การประเมินแบบจำลอง
8.2.7 การกำหนดเกณฑ์การตัดสินใจและการแจ้งเตือน
8.2.8 การรักษาความปลอดภัยของกระบวนการ Machine Learning
8.2.9 การติดตามแบบจำลองหลังนำไปใช้งาน

83

การตรวจจับใบหน้าจากกล้องด้วยแบบจำลองตระกูล YOLO

8.3.1 กระบวนการตรวจจับใบหน้าด้วย YOLO
8.3.2 การเตรียมสภาพแวดล้อม
8.3.3 การเตรียมชุดข้อมูลใบหน้า
8.3.4 รูปแบบการจัดชุดข้อมูล YOLO
8.3.5 การแบ่งชุดข้อมูล
8.3.6 การเลือกแบบจำลอง YOLO
8.3.7 การฝึกแบบจำลอง
8.3.8 การตรวจสอบผลการฝึก
8.3.9 การตรวจสอบการทำงานของกล้องก่อนนำไปใช้กับ YOLO

8.3.10 การทำงานภายในโปรแกรม

8.3.11 การวาดกรอบด้วยตนเอง

8.3.12 การบันทึกภาพเมื่อพบใบหน้า

8.3.13 การเพิ่มการแจ้งเตือนของระบบตรวจจับใบหน้าด้วย YOLO

8.3.14 การปรับค่า Confidence และ IoU

8.3.15 การเพิ่มความเร็วของการประมวลผลข้อมูล

8.3.16 ข้อควรระวังด้านความเป็นส่วนตัว

บทที่ 8 ปัญญาประดิษฐ์สำหรับระบบรักษาความปลอดภัย

Artificial Intelligence for Smart Security

8.1 ความรู้พื้นฐานของปัญญาประดิษฐ์

8.1.1 ความหมายของปัญญาประดิษฐ์ในระบบรักษาความปลอดภัยอัจฉริยะ

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) หมายถึง เทคโนโลยีที่ทำให้ระบบคอมพิวเตอร์สามารถเรียนรู้ (learning) วิเคราะห์ (analysis) ให้เหตุผล (reasoning) ตัดสินใจ (decision making) และตอบสนองต่อเหตุการณ์ต่าง ๆ ได้ในลักษณะที่คล้ายกับกระบวนการคิดของมนุษย์ โดยอาศัยข้อมูลที่ได้รับจากเซ็นเซอร์ กล้องวงจรปิด และอุปกรณ์ในระบบอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) เพื่อนำมาประมวลผลด้วยเทคนิคด้าน machine learning, deep learning และ computer vision ส่งผลให้ระบบสามารถตรวจจับ วิเคราะห์ และคาดการณ์เหตุการณ์ได้อย่างอัตโนมัติ (Muhammad et al., 2025; Sabit, 2025)

ในระบบรักษาความปลอดภัยแบบดั้งเดิม (traditional security system) กล้องวงจรปิดและเซ็นเซอร์มีหน้าที่หลักในการบันทึกภาพหรือแจ้งเตือนเมื่อเกิดการเคลื่อนไหวเท่านั้น โดยยังต้องอาศัยมนุษย์ในการเฝ้าติดตาม วิเคราะห์ และตัดสินใจเมื่อเกิดเหตุการณ์ผิดปกติ อย่างไรก็ตาม การประยุกต์ใช้ปัญญาประดิษฐ์ในระบบรักษาความปลอดภัยอัจฉริยะ (smart security system) ได้เปลี่ยนรูปแบบการทำงานจากการบันทึกข้อมูลเพียงอย่างเดียวไปสู่การวิเคราะห์ข้อมูลแบบเรียลไทม์ (real-time analytics) ซึ่งสามารถจำแนกบุคคล ตรวจจับวัตถุ วิเคราะห์พฤติกรรม ตรวจจับความผิดปกติ และตอบสนองต่อเหตุการณ์ได้โดยอัตโนมัติ ส่งผลให้ระบบมีความแม่นยำสูงขึ้น ลดการแจ้งเตือนที่ผิดพลาด (false alarm) และสามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ (Al Sharah et al., 2025; Sabit, 2025) การพัฒนาระบบรักษาความปลอดภัยอัจฉริยะในปัจจุบันอาศัยการทำงานร่วมกันของเทคโนโลยี AI, IoT, Edge computing และ cloud computing โดยข้อมูลจากกล้องและเซ็นเซอร์จะถูกประมวลผลด้วยแบบจำลองปัญญาประดิษฐ์เพื่อดำเนินการ เช่น การรู้จำใบหน้า (face recognition) การตรวจจับการบุกรุก (intrusion detection) การวิเคราะห์พฤติกรรม (behavior analysis) และการตรวจจับเหตุการณ์ผิดปกติ (anomaly detection) ก่อนส่งผลลัพธ์ไปยังผู้ใช้งานผ่านระบบแจ้งเตือนแบบเรียลไทม์หรือแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ซึ่งช่วยลดระยะเวลาในการตอบสนองและเพิ่มประสิทธิภาพของระบบรักษาความปลอดภัยโดยรวม (Ali et al., 2026; Morales Cauti et al., 2023)

ดังนั้น ปัญญาประดิษฐ์จึงมีบทบาทสำคัญในการเปลี่ยนระบบรักษาความปลอดภัยจากระบบเฝ้าระวังแบบรับเหตุการณ์ (passive security) ซึ่งทำหน้าที่เพียงบันทึกและแจ้งเตือน ไปสู่ระบบรักษาความปลอดภัยเชิงรุก (proactive security) ที่สามารถเรียนรู้รูปแบบการใช้งาน วิเคราะห์สถานการณ์ คาดการณ์ความเสี่ยง และแจ้งเตือนล่วงหน้าก่อนที่เหตุการณ์ผิดปกติจะส่งผลกระทบต่อความปลอดภัยของบุคคลหรือทรัพย์สินได้อย่างมีประสิทธิภาพ (Al Sharah et al., 2025; Radovanovic et al., 2026)

8.1.2 บทบาทของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ

AI มีบทบาทสำคัญในการยกระดับประสิทธิภาพของระบบรักษาความปลอดภัยอัจฉริยะ โดยทำหน้าที่ประมวลผลข้อมูลจำนวนมากที่ได้รับจากอุปกรณ์ IoT เช่น กล้องวงจรปิด เซ็นเซอร์ตรวจจับการเคลื่อนไหว เซ็นเซอร์ตรวจจับควัน เซ็นเซอร์ตรวจจับแก๊ส และอุปกรณ์ควบคุมต่าง ๆ เพื่อให้ระบบสามารถรับรู้ (perception) วิเคราะห์ (analysis) ตัดสินใจ (decision making) และตอบสนองต่อเหตุการณ์ (response) ได้โดยอัตโนมัติ (Sabit, 2025; Muhammad et al., 2025) บทบาทสำคัญของ AI ในระบบ smart security ประกอบด้วย

1) การวิเคราะห์ข้อมูลภาพ วิดีโอแบบเรียลไทม์ (seal-time video analytics)
2) การตรวจจับการบุกรุก (intrusion detection)
3) การรู้จำใบหน้า (face recognition)
4) การวิเคราะห์พฤติกรรมของบุคคล (human activity recognition)
5) การตรวจจับเหตุการณ์ผิดปกติ (anomaly detection)
6) การประเมินระดับความเสี่ยงของเหตุการณ์ (risk assessment)
7) การแจ้งเตือนผู้ใช้งานผ่านระบบ cloud และ mobile application
8) การเรียนรู้รูปแบบพฤติกรรมของผู้ใช้งาน (behavior learning) เพื่อเพิ่มความแม่นยำของระบบ

ระบบ AI สามารถเรียนรู้รูปแบบการใช้งานของสมาชิกภายในบ้านหรือผู้ใช้งานในพื้นที่ เช่น เวลาที่กลับบ้าน พื้นที่ที่มีการเคลื่อนไหวเป็นประจำ หรือเส้นทางการเดิน เมื่อเกิดเหตุการณ์ที่แตกต่างจากรูปแบบปกติ ระบบจะประเมินว่าเป็นเหตุการณ์ผิดปกติและแจ้งเตือนผู้ใช้งานทันที ส่งผลให้สามารถลดการแจ้งเตือนที่ไม่จำเป็น (false alarm) และเพิ่มประสิทธิภาพในการเฝ้าระวังได้อย่างมีนัยสำคัญ (Ali et al., 2026; Al Sharah et al., 2025)

8.1.3 เทคโนโลยี AI ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ

ระบบรักษาความปลอดภัยอัจฉริยะในปัจจุบันอาศัยการทำงานร่วมกันของเทคโนโลยีปัญญาประดิษฐ์หลายแขนง เพื่อให้สามารถวิเคราะห์ข้อมูลจากภาพ เสียง และเซ็นเซอร์ได้อย่างมีประสิทธิภาพ โดยเทคโนโลยีหลักที่นำมาใชแต่ละเทคโนโลยีมีบทบาทแตกต่างกัน ดังนี้

1) Machine Learning

Machine Learning (ML) เป็นสาขาหนึ่งของปัญญาประดิษฐ์ที่ทำให้คอมพิวเตอร์สามารถเรียนรู้จากข้อมูลที่ผ่านมา เพื่อสร้างแบบจำลอง (model) สำหรับการจำแนกข้อมูลหรือการพยากรณ์ ไม่จำเป็นต้องกำหนดกฎการทำงานทุกขั้นตอนอย่างชัดเจน เทคโนโลยีนี้เหมาะสำหรับการวิเคราะห์รูปแบบการใช้งาน จำแนกบุคคล ประเมินความเสี่ยง และตรวจจับเหตุการณ์ผิดปกติในระบบรักษาความปลอดภัย (Muhammad et al., 2025; Morales Cauti et al., 2023)

2) Deep Learning

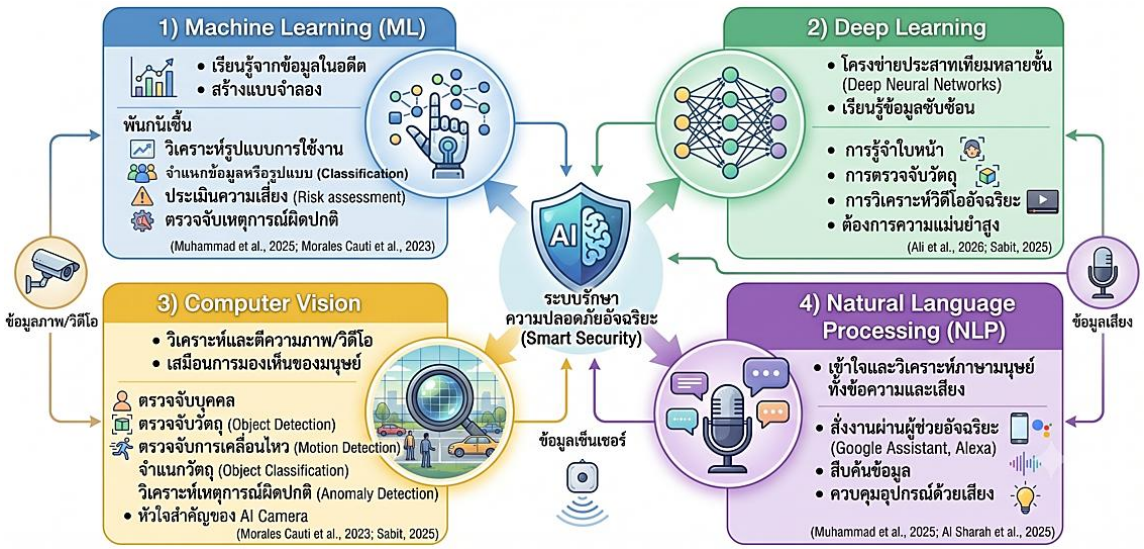
Deep learning เป็นแขนงหนึ่งของ ML ที่ใช้โครงข่ายประสาทเทียมหลายชั้น (deep neural networks) ในการเรียนรู้ข้อมูลที่มีความซับซ้อน เช่น ภาพ เสียง และวิดีโอ เหมาะสำหรับงานรู้จำใบหน้า (face recognition) ตรวจจับวัตถุ (object detection) และวิเคราะห์วิดีโออัจฉริยะ (intelligent video analytics) ซึ่งต้องการความแม่นยำสูง (Ali et al., 2026; Sabit, 2025)

3) Computer Vision

Computer vision เป็นเทคโนโลยีที่ทำให้คอมพิวเตอร์สามารถวิเคราะห์และตีความข้อมูลจากภาพและวิดีโอได้เสมือนการมองเห็นของมนุษย์ โดยสามารถประยุกต์ใช้สำหรับ การตรวจจับบุคคล (person detection) การตรวจจับวัตถุ (object detection) การตรวจจับการเคลื่อนไหว (motion detection) การจำแนกประเภทของวัตถุ (object classification) การวิเคราะห์เหตุการณ์ผิดปกติ (anomaly detection) เทคโนโลยีนี้ถือเป็นหัวใจสำคัญของกล้อง AI camera ที่ใช้ในระบบ smart security ในปัจจุบัน (Morales Cauti et al., 2023; Sabit, 2025)

4) Natural Language Processing (NLP)

NLP เป็นเทคโนโลยีที่ช่วยให้ระบบสามารถเข้าใจ วิเคราะห์ และตอบสนองต่อภาษามนุษย์ ทั้งในรูปแบบข้อความและเสียง ทำให้ผู้ใช้งานสามารถสั่งงานระบบรักษาความปลอดภัยผ่านผู้ช่วยอัจฉริยะ เช่น Google Assistant หรือ Amazon Alexa รวมถึงรองรับการสืบค้นข้อมูลและควบคุมอุปกรณ์ภายในบ้านด้วยคำสั่งเสียงได้อย่างสะดวก (Muhammad et al., 2025; Al Sharah et al., 2025)



รูปที่ 8.1 เทคโนโลยี AI ที่ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ

8.1.4 การทำงานของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ

การทำงานของ AI ในระบบรักษาความปลอดภัยอัจฉริยะสามารถอธิบายเป็นลำดับขั้นตอนดังนี้

1) เซ็นเซอร์และกล้องรวบรวมข้อมูลจากสภาพแวดล้อม
2) ข้อมูลถูกส่งผ่านเครือข่าย IoT ไปยังอุปกรณ์ประมวลผล
3) Edge device หรือ cloud ประมวลผลข้อมูลด้วยแบบจำลอง AI
4) AI วิเคราะห์ภาพ เสียง หรือข้อมูลจากเซ็นเซอร์
5) ระบบจำแนกบุคคล วัตถุ หรือเหตุการณ์ที่ตรวจพบ
6) ประเมินระดับความเสี่ยงของเหตุการณ์

7) แจ้งเตือนผู้ใช้งานผ่าน mobile application หรือระบบ cloud

8) บันทึกข้อมูลลงฐานข้อมูลบน cloud เพื่อใช้ในการเรียนรู้และปรับปรุงแบบจำลองในอนาคต

ในระบบ smart security รุ่นใหม่ นิยมใช้ Edge computing ร่วมกับ cloud computing โดยให้อุปกรณ์ปลายทาง เช่น Raspberry Pi หรือ Edge AI ประมวลผลข้อมูลเบื้องต้นเพื่อลดเวลาในการตอบสนอง (latency) และลดปริมาณข้อมูลที่ต้องส่งผ่านเครือข่าย ขณะที่ cloud ทำหน้าที่จัดเก็บข้อมูล ฝึกแบบจำลอง AI และบริหารจัดการระบบในระยะยาว แนวทางดังกล่าวช่วยเพิ่มความรวดเร็วของระบบ ลดภาระด้านเครือข่าย และช่วยรักษาความเป็นส่วนตัวของข้อมูลชีวมิติของผู้ใช้งานได้ดียิ่งขึ้น (Ali et al., 2026; Sabit, 2025)

8.1.5 ข้อดีของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ

การประยุกต์ใช้ AI ในระบบรักษาความปลอดภัยอัจฉริยะก่อให้เกิดประโยชน์หลายอย่าง เช่น

1) วิเคราะห์ข้อมูลภาพและวิดีโอแบบเรียลไทม์
2) ลดการแจ้งเตือนที่ผิดพลาด (false alarm)
3) เพิ่มความแม่นยำในการตรวจจับบุคคลและวัตถุ
4) ตรวจจับพฤติกรรมผิดปกติได้โดยอัตโนมัติ
5) ลดภาระของเจ้าหน้าที่รักษาความปลอดภัย
6) รองรับการเฝ้าระวังตลอด 24 ชั่วโมง
7) เชื่อมต่อกับอุปกรณ์ IoT และ cloud ได้อย่างมีประสิทธิภาพ
8) เรียนรู้และปรับปรุงความแม่นยำของระบบอย่างต่อเนื่อง

ด้วยความสามารถดังกล่าว AI จึงช่วยให้ระบบรักษาความปลอดภัยสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว มีความแม่นยำสูง และลดต้นทุนในการดำเนินงานเมื่อเทียบกับระบบที่ต้องอาศัยการเฝ้าระวังโดยมนุษย์เพียงอย่างเดียว (Muhammad et al., 2025; Sabit, 2025; Morales Cauti et al., 2023)

8.1.6 ข้อจำกัดและประเด็นด้านจริยธรรมของ AI

แม้ว่าปัญญาประดิษฐ์จะช่วยเพิ่มประสิทธิภาพของระบบรักษาความปลอดภัยอย่างมาก แต่ยังมีข้อจำกัดและประเด็นด้านจริยธรรมที่ต้องพิจารณา ได้แก่

1) ความเป็นส่วนตัวของข้อมูล (privacy)
2) ความปลอดภัยของข้อมูลชีวมิติ (biometric data security)
3) ความถูกต้องของการรู้จำใบหน้าในสภาพแวดล้อมที่ซับซ้อน
4) อคติของแบบจำลอง AI (algorithmic bias)
5) ความโปร่งใสในการตัดสินใจของระบบ (explainability)
6) ความเสี่ยงจากการโจมตีทางไซเบอร์ (cybersecurity threats)
7) ต้นทุนในการพัฒนาและบำรุงรักษาระบบ

งานวิจัยในปัจจุบันเสนอว่าการพัฒนาระบบ AI สำหรับ smart security ควรดำเนินควบคู่กับมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล การเข้ารหัสข้อมูล (encryption) การยืนยันตัวตนที่

ปลอดภัย (secure authentication) และการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยและความเป็นส่วนตัว เพื่อให้ระบบมีทั้งประสิทธิภาพ ความน่าเชื่อถือ และสอดคล้องกับหลักจริยธรรมในการใช้ปัญญาประดิษฐ์ (Al Sharah et al., 2025; Radovanovic et al., 2026; Sabit, 2025)

8.2 การเรียนรู้ของเครื่อง (Machine Learning)

8.2.1 ความหมายของการเรียนรู้ของเครื่อง

การเรียนรู้ของเครื่อง (ML) เป็นแขนงหนึ่งของปัญญาประดิษฐ์ ที่มุ่งเน้นการพัฒนาแบบจำลองทางคณิตศาสตร์และอัลกอริทึมที่สามารถเรียนรู้จากข้อมูล (data) เพื่อค้นหารูปแบบ ความสัมพันธ์หรือแนวโน้มของข้อมูล และนำความรู้ที่ได้ไปใช้ในการทำนาย (prediction) การจำแนกประเภท (classification) หรือการตัดสินใจ (decision making) โดยไม่จำเป็นต้องกำหนดกฎการทำงานของระบบไว้อย่างละเอียดในทุกขั้นตอน (Muhammad et al., 2025; Sabit, 2025) หลักการสำคัญของ ML คือการให้ระบบคอมพิวเตอร์เรียนรู้จากข้อมูลตัวอย่าง (training data) แล้วสร้างแบบจำลอง (model) ที่สามารถนำไปใช้กับข้อมูลใหม่ที่ไม่เคยพบมาก่อน (unseen data) ได้อย่างถูกต้อง กระบวนการเรียนรู้ดังกล่าวช่วยให้ระบบสามารถปรับปรุงประสิทธิภาพของตนเองเมื่อได้รับข้อมูลเพิ่มเติม ส่งผลให้มีความแม่นยำในการตัดสินใจเพิ่มขึ้นตามปริมาณและคุณภาพของข้อมูลที่ใช้ฝึกแบบจำลอง (Morales Cauti et al., 2023)

ในระบบรักษาความปลอดภัยอัจฉริยะ ML ถูกนำมาใช้เพื่อวิเคราะห์ข้อมูลจากกล้องวงจรปิด เซ็นเซอร์ และอุปกรณ์ IoT เช่น การตรวจจับการบุกรุก การจำแนกบุคคล การประเมินระดับความเสี่ยง และการตรวจจับเหตุการณ์ผิดปกติ ซึ่งช่วยลดภาระของผู้ปฏิบัติงาน เพิ่มความรวดเร็วในการตอบสนอง และลดความผิดพลาดจากการวิเคราะห์ด้วยมนุษย์ (Sabit, 2025; Muhammad et al., 2025)

8.2.2 หลักการทำงานของ Machine Learning

การทำงานของ ML ประกอบด้วยกระบวนการหลัก 5 ขั้นตอน รายละเอียด ดังนี้

1) การรวบรวมข้อมูล (Data Collection)

ระบบรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น กล้องวงจรปิด เซ็นเซอร์ตรวจจับการเคลื่อนไหว เซ็นเซอร์ตรวจจับควัน เซ็นเซอร์ตรวจจับแก๊ส หรือฐานข้อมูลภายในระบบ

2) การเตรียมข้อมูล (Data Preprocessing)

ข้อมูลที่รวบรวมได้จะถูกตรวจสอบ แก้ไขข้อมูลที่ผิดพลาด กำจัดข้อมูลซ้ำ และแปลงข้อมูลให้อยู่ในรูปแบบที่เหมาะสมสำหรับการเรียนรู้ของแบบจำลอง

3) การฝึกแบบจำลอง (Model Training)

อัลกอริทึม ML วิเคราะห์ข้อมูลตัวอย่างเพื่อเรียนรู้ความสัมพันธ์ของข้อมูล และสร้างแบบจำลองที่สามารถใช้ทำนายหรือจำแนกข้อมูลใหม่ได้

4) การประเมินผลแบบจำลอง (Model Evaluation)

ประสิทธิภาพของแบบจำลองจะถูกประเมินด้วยชุดข้อมูลทดสอบ (testing data) เพื่อวัดความถูกต้อง ความแม่นยำ และความสามารถในการนำไปใช้งานจริง

5) การนำแบบจำลองไปใช้งาน (Model Deployment)

เมื่อแบบจำลองมีประสิทธิภาพเพียงพอ จะถูกนำไปประยุกต์ใช้ในระบบ Smart Security สำหรับการวิเคราะห์ข้อมูลแบบเรียลไทม์และสนับสนุนการตัดสินใจอัตโนมัติ (Ali et al., 2026; Sabit, 2025)

8.2.3 ประเภทของ Machine Learning

ML สามารถแบ่งออกเป็น 3 ประเภทหลัก รายละเอียดดังนี้

1) การเรียนรู้แบบมีผู้สอน (Supervised Learning)

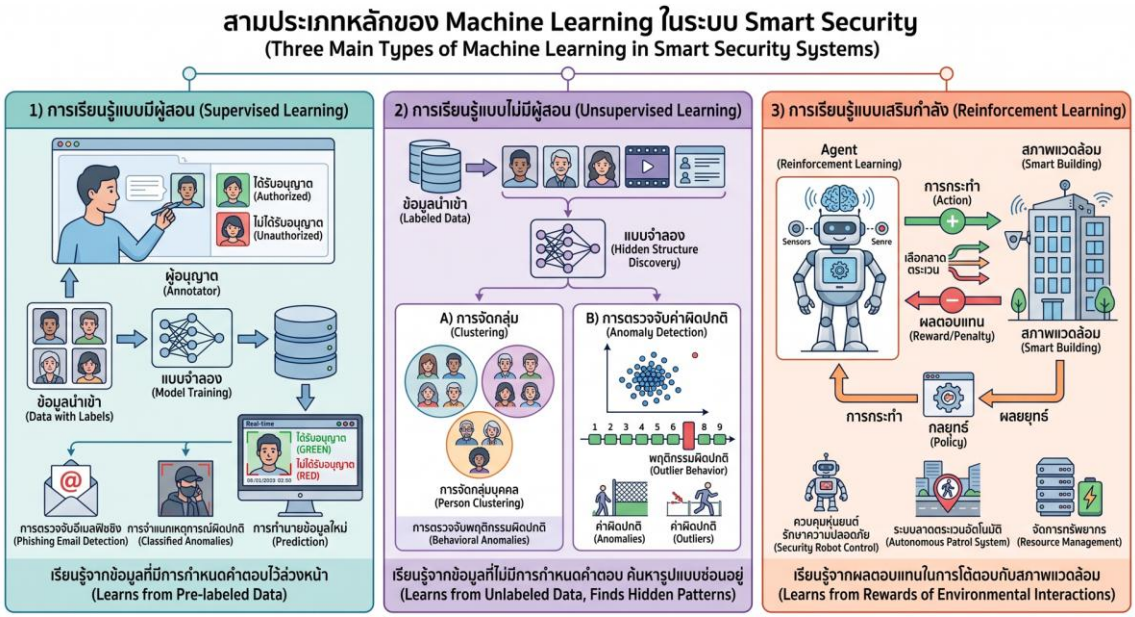
เป็นการเรียนรู้จากข้อมูลที่มีการกำหนดคำตอบ (label) ไว้ล่วงหน้า โดยแบบจำลองจะเรียนรู้ความสัมพันธ์ระหว่างข้อมูลนำเข้า (input) และผลลัพธ์ (output) เพื่อนำไปใช้ทำนายข้อมูลใหม่ ตัวอย่างการประยุกต์ใช้ในระบบ smart security ได้แก่ การจำแนกบุคคลที่ได้รับอนุญาตและไม่ได้รับอนุญาต การตรวจจับอีเมลฟิชชิง และการจำแนกเหตุการณ์ผิดปกติจากข้อมูลที่มีการระบุประเภทไว้แล้ว (Muhammad et al., 2025)

2) การเรียนรู้แบบไม่มีผู้สอน (Unsupervised Learning)

เป็นการเรียนรู้จากข้อมูลที่ไม่มีการกำหนดคำตอบไว้ล่วงหน้า โดยแบบจำลองจะค้นหารูปแบบหรือโครงสร้างที่ซ่อนอยู่ภายในข้อมูล เช่น การจัดกลุ่ม (clustering) หรือการตรวจจับค่าผิดปกติ (outlier detection) ซึ่งสามารถนำไปใช้ในการตรวจจับพฤติกรรมที่ผิดปกติของบุคคลหรือเหตุการณ์ภายในระบบรักษาความปลอดภัย (Morales Cauti et al., 2023)

3) การเรียนรู้แบบเสริมกำลัง (Reinforcement Learning)

เป็นการเรียนรู้ที่ตัวแทน (agent) โต้ตอบกับสภาพแวดล้อมและเรียนรู้จากผลตอบแทน (reward) หรือบทลงโทษ (penalty) เพื่อเลือกการกระทำที่เหมาะสมที่สุด แม้ว่าปัจจุบัน Reinforcement Learning จะยังไม่ถูกนำมาใช้อย่างแพร่หลายในระบบ smart security แต่มีศักยภาพสำหรับการควบคุมหุ่นยนต์รักษาความปลอดภัย ระบบลาดตระเวนอัตโนมัติ และการจัดการทรัพยากรของระบบในอนาคต



รูปที่ 8.2 ประเภทของ Machine Learning

8.2.4 การประยุกต์ใช้ Machine Learning ในระบบรักษาความปลอดภัยอัจฉริยะ

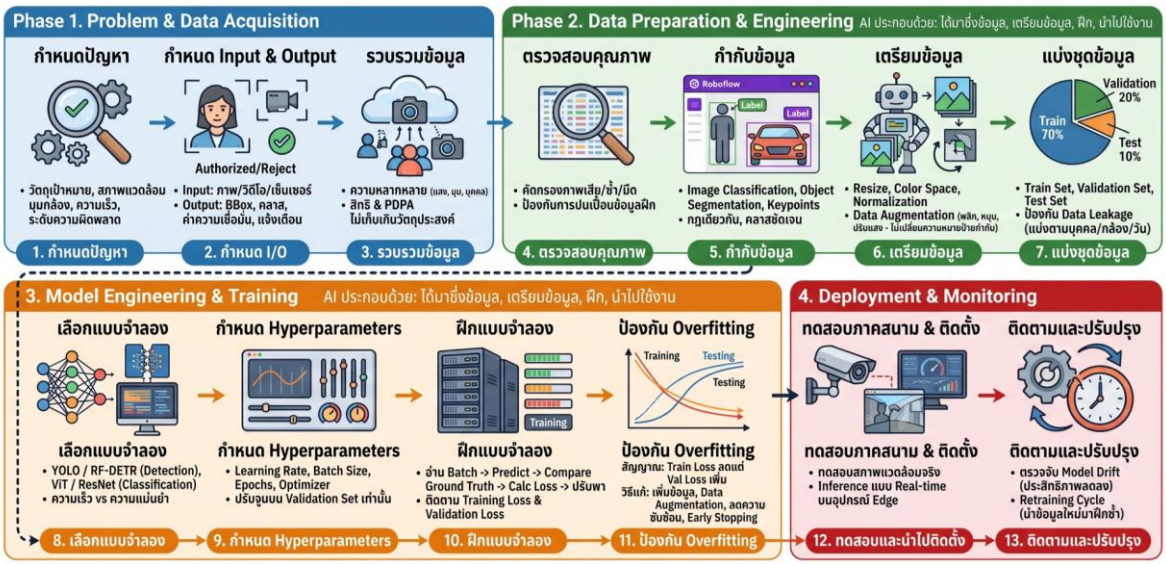
ML ถูกนำมาประยุกต์ใช้ในระบบรักษาความปลอดภัยอัจฉริยะอย่างกว้างขวาง เนื่องจากสามารถวิเคราะห์ข้อมูลจำนวนมากได้อย่างรวดเร็วและแม่นยำ ตัวอย่างการประยุกต์ใช้ ได้แก่

1) การตรวจจับการบุกรุก (intrusion detection)
2) การจำแนกบุคคลที่ได้รับอนุญาตและไม่ได้รับอนุญาต
3) การวิเคราะห์รูปแบบการใช้งานของผู้ใช้งาน (behavior analysis)
4) การประเมินระดับความเสี่ยงของเหตุการณ์ (risk assessment)
5) การตรวจจับเหตุการณ์ผิดปกติ (anomaly detection)
6) การวิเคราะห์ข้อมูลจากกล้องวงจรปิดแบบเรียลไทม์
7) การสนับสนุนการตัดสินใจของระบบแจ้งเตือนอัจฉริยะ (smart alert system)

จากการศึกษาพบว่า การประยุกต์ใช้ ML ช่วยเพิ่มความแม่นยำของระบบ ลดการแจ้งเตือนที่ผิดพลาด (false alarm) และเพิ่มประสิทธิภาพในการเฝ้าระวังเมื่อเปรียบเทียบกับระบบรักษาความปลอดภัยแบบดั้งเดิมที่อาศัยการตรวจสอบโดยมนุษย์เพียงอย่างเดียว (Sabit, 2025; Ali et al., 2026)

8.2.5 กระบวนการพัฒนา Machine Learning

กระบวนการพัฒนา ML ไม่ใช่เพียงการนำรูปภาพเข้าสู่โปรแกรมแล้วสั่ง train แต่เป็นวงจรที่ประกอบด้วยการกำหนดปัญหา การจัดการข้อมูล การฝึก การประเมิน การนำไปติดตั้ง และการติดตามผล กระบวนการหลักสามารถสรุปได้ดังนี้ (1) กำหนดปัญหา (2) รวบรวมข้อมูล (3) ตรวจสอบข้อมูล (4) กำกับข้อมูล (5) เตรียมข้อมูล (6) แบ่งชุดข้อมูล (7) เลือกแบบจำลอง (8) ฝึกแบบจำลอง (9) ประเมินผล (10) ทดสอบภาคสนาม (11) นำไปใช้งาน และ (12) ติดตามและปรับปรุง ดังรูปที่ 8.3



รูปที่ 8.3 กระบวนการพัฒนา Machine Learning

โดย AI ประกอบด้วยการได้มาซึ่งข้อมูล การเตรียมข้อมูล การฝึก และการนำแบบจำลองไปใช้งาน แต่ละระยะมีทั้งงานทางวิศวกรรมและความเสี่ยงด้านความปลอดภัยที่ต้องควบคุม (Lendák & Kiss, 2026) ซึ่งอธิบายรายละเอียด ดังนี้

1) ขั้นตอนที่ 1 การกำหนดปัญหา

ผู้พัฒนาต้องเริ่มจากการระบุว่า ระบบต้องแก้ปัญหาอะไร ไม่ควรเริ่มจากการเลือกอัลกอริทึมก่อนกำหนดวัตถุประสงค์ ตัวอย่างโจทย์ที่ชัดเจน ได้แก่ ตรวจจับบุคคลที่เข้ามาในพื้นที่หวงห้าม ตรวจจับรถที่ไม่อยู่ในฐานข้อมูล รู้จำใบหน้าของผู้ได้รับอนุญาต ตรวจจับการล้มของผู้สูงอายุ ตรวจจับบุคคลที่เดินย้อนทาง ตรวจจับสิ่งของที่ถูกทิ้งไว้โดยไม่มีผู้ดูแล การกำหนดปัญหาควรระบุอย่างน้อย 6 ประเด็น ได้แก่

1.1) วัตถุหรือเหตุการณ์เป้าหมาย

1.2) ตำแหน่งและสภาพแวดล้อมที่ติดตั้ง

1.3) ระยะและมุมที่ต้องตรวจจับ

1.4) ความเร็วในการตอบสนอง

1.5) ระดับความผิดพลาดที่ยอมรับได้

1.6) การตอบสนองหลังตรวจพบเหตุการณ์

ตัวอย่างการกำหนดปัญหาที่ไม่ชัดเจน “สร้าง AI รักษาความปลอดภัย” ส่วนตัวอย่างที่ชัดเจนกว่าคือ “สร้างระบบตรวจจับบุคคลที่เข้าสู่พื้นที่หวงห้ามหลังเวลา 20.00 น. และส่งภาพแจ้งเตือนภายใน 5 วินาที”

2) ขั้นตอนที่ 2 การกำหนดข้อมูลนำเข้าและผลลัพธ์ ข้อมูลนำเข้าอาจเป็นข้อมูลประกอบด้วย ภาพนิ่ง วิดีโอ เสียง ข้อมูลการเคลื่อนไหว เวลาและตำแหน่ง ข้อมูลจากเซ็นเซอร์บันทึกการเข้า–ออก หรือ ข้อมูลจาก RFID หรือระบบควบคุมประตู ส่วนผลลัพธ์ต้องกำหนดให้วัดได้ เช่น ชื่อประเภทวัตถุ ตำแหน่ง bounding box รหัสบุคคล ค่าความเชื่อมั่น ระดับความเสี่ยง สถานะอนุญาตหรือปฏิเสธ หรือข้อความแจ้งเตือน

ในระบบรู้จำใบหน้า ขั้นตอนการทำงานอาจเริ่มจากรับวิดีโอ ลดสัญญาณรบกวน ปรับคุณลักษณะและทำ normalization จากนั้นตรวจจับใบหน้า สกัดคุณลักษณะ และเปรียบเทียบกับฐานข้อมูลบุคคลที่ได้รับอนุญาต หากตรงกันจึงอนุญาตให้ผ่าน แต่ถ้าไม่ตรง ระบบจะแจ้งเตือนว่าเป็นบุคคลไม่รู้จัก (Ali et al., 2026)

3) ขั้นตอนที่ 3 การรวบรวมข้อมูล

ข้อมูลต้องสะท้อนสภาพการใช้งานจริง ไม่ควรรวบรวมเฉพาะภาพที่สวย ชัด และถ่ายจากมุมเดียว เนื่องจากแบบจำลองจะเรียนรู้ได้เฉพาะรูปแบบที่ปรากฏในชุดข้อมูลสำหรับระบบรักษาความปลอดภัยอัจฉริยะ ควรรวบรวมข้อมูลภายใต้ความหลากหลาย เช่นกลางวันและกลางคืน แสงสว่างมากและน้อย แสงย้อน หลายมุมกล้อง หลายระยะ ฉากหลังแตกต่างกัน บุคคลหลายลักษณะ เสื้อผ้าและอุปกรณ์ประกอบแตกต่างกัน วัตถุถูกบังบางส่วน ภาพจากกล้องจริงที่ใช้ติดตั้ง หรือ เหตุการณ์ปกติและเหตุการณ์ผิดปกติ ข้อมูลที่ได้จากอินเทอร์เน็ตอาจไม่สอดคล้องกับภาพจากกล้องจริง เช่น กล้องจริงอาจมีความละเอียดต่ำ แสงไม่คงที่ และฉากหลังเปลี่ยนแปลง งานของ Ali et al. (2026) จึงใช้ข้อมูลที่เก็บจากกล้องบนอุปกรณ์ Raspberry Pi ภายใต้สภาพใช้งานจริง เพื่อ

ประเมินการทำงานระดับระบบ แม้ว่าผู้วิจัยระบุว่าชุดข้อมูลดังกล่าวมีขนาดเล็กและไม่สามารถยืนยันความสามารถในการใช้ได้ทั่วไปกับประชากรทั้งหมด หลักการสำคัญในการรวบรวมข้อมูล

3.1) ต้องมีสิทธิ์ใช้ข้อมูลอย่างถูกต้อง

3.2) ต้องได้รับความยินยอมเมื่อเก็บข้อมูลใบหน้าหรือชีวมิติ

3.3) ต้องไม่รวบรวมข้อมูลเกินวัตถุประสงค์

3.4) ต้องกำหนดระยะเวลาจัดเก็บ

3.5) ต้องบันทึกแหล่งที่มาและเงื่อนไขการเก็บข้อมูล

3.6) ต้องป้องกันข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต

3.7) ต้องหลีกเลี่ยงข้อมูลซ้ำจำนวนมากจากเหตุการณ์เดียวกัน

4) ขั้นตอนที่ 4 การตรวจสอบคุณภาพข้อมูล

ก่อนกำกับข้อมูล ต้องตรวจสอบและคัดกรองข้อมูลที่ไม่เหมาะสม เช่น ภาพเสียหรือเปิดไม่ได้ ภาพมืดเกินไปจนไม่เห็นเป้าหมาย ภาพซ้ำ ภาพที่วัตถุเป้าหมายอยู่นอกเฟรม ภาพที่ไม่สอดคล้องกับคลาส ภาพที่มีข้อมูลส่วนบุคคลซึ่งไม่จำเป็น ภาพที่เกิดจากการบันทึกผิดเงื่อนไข การตรวจสอบข้อมูลเป็นขั้นตอนด้านความถูกต้องและด้านความปลอดภัย เพราะการปนเปื้อนข้อมูลฝึกอาจทำให้แบบจำลองตัดสินใจผิดอย่างเป็นระบบ

5) ขั้นตอนที่ 5 การกำกับข้อมูล

การกำกับข้อมูล (data annotation) คือการกำหนดคำตอบที่ถูกต้องให้ข้อมูลตัวอย่าง รูปแบบการกำกับขึ้นอยู่กับชนิดงาน ได้แก่

5.1) Image classification คือ การกำหนดป้ายกำกับให้ทั้งภาพ เช่น authorized_person, unknown_person, fire, normal

5.2) Object detection คือ การตรวจจับตำแหน่งของวัตถุด้วยการสร้างกรอบล้อมรอบวัตถุ (bounding box) พร้อมกำหนดป้ายกำกับคลาส (class label) เช่น person, car, helmet และ bag

5.3) Segmentation คือ การหนดขอบเขตของวัตถุในระดับพิกเซล เหมาะกับงานที่ต้องการรูปร่างหรือพื้นที่ของวัตถุอย่างละเอียด

5.4) Keypoint detection เป็นการ กำหนดตำแหน่งจุดสำคัญ เช่น จุดข้อต่อของร่างกาย เพื่อนำไปวิเคราะห์ท่าทางหรือการล้ม สามารถใช้ Roboflow เพื่อจัดการชุดข้อมูล โดยรองรับการวาด bounding box การกำหนด label และการเตรียมข้อมูลสำหรับ image classification, object detection และ segmentation หลักการกำกับข้อมูลที่ถูกต้อง

5.4.1) ทุกคลาสต้องมีนิยามชัดเจน

5.4.2) ผู้กำกับหลายคนต้องใช้กฎเดียวกัน

5.4.3) กรอบควรครอบวัตถุเป้าหมายพอดี

5.4.4) ไม่ควรวาดกรอบครอบหลายวัตถุที่เป็นคนละ instance

5.4.5) ต้องกำหนดวิธีจัดการวัตถุที่ถูกบัง

5.4.6) ต้องทบทวนตัวอย่างที่ไม่แน่ใจ

5.4.7) ควรสุ่มตรวจคุณภาพ annotation

5.4.8) ไม่ควรให้ชื่อคลาสเดียวกันมีการสะกดหลายแบบ

6) ขั้นตอนที่ 6 การเตรียมข้อมูล

การเตรียมข้อมูล (data preprocessing) มีวัตถุประสงค์เพื่อทำให้ข้อมูลมีรูปแบบสอดคล้องกับสิ่งที่แบบจำลองต้องการ เช่น ปรับขนาดภาพ เปลี่ยนระบบสี ปรับค่าพิกเซลให้อยู่ในช่วงที่เหมาะสม ลดสัญญาณรบกวน ปรับความคมชัดหรือความสว่าง ตัดพื้นที่ที่ไม่เกี่ยวข้อง ตรวจสอบสัดส่วนภาพ หรือ แปลงไฟล์ให้อยู่ในรูปแบบมาตรฐาน ต้องใช้กระบวนการเตรียมข้อมูลที่สอดคล้องกันทั้งช่วงฝึกและช่วงใช้งานจริง หากฝึกด้วยภาพขนาดหนึ่งแต่ใช้งานจริงด้วยกระบวนการแปลงภาพอีกแบบ ประสิทธิภาพอาจลดลง การเพิ่มความหลากหลายของข้อมูล data augmentation เป็นการสร้างรูปแบบเพิ่มเติมจากข้อมูลเดิม เช่นหมุนภาพเล็กน้อย พลิกภาพตามความเหมาะสม ปรับความสว่าง ปรับ contrast ย่อหรือขยาย ครอบตัดบางส่วน หรือการเพิ่มสัญญาณรบกวนในระดับที่สมจริง โดยการทำ augmentation ต้องไม่เปลี่ยนความหมายของป้ายกำกับ เช่น การหมุนป้ายทะเบียนกลับหัวหรือการพลิกข้อความอาจทำให้ข้อมูลไม่สอดคล้องกับสภาพใช้งานจริง

7) ขั้นตอนที่ 7 การแบ่งชุดข้อมูล

ชุดข้อมูลต้องแบ่งอย่างน้อยเป็น 3 ส่วน

7.1) ชุดฝึก (training set) ใช้ปรับค่าพารามิเตอร์ของแบบจำลอง แบบจำลองเห็นข้อมูลส่วนนี้หลายรอบระหว่างการฝึก

7.2) ชุดตรวจสอบ (validation set) ใช้ประเมินแบบจำลองระหว่างการพัฒนา เลือก Hyperparameters เลือก epoch หรือเลือกเวอร์ชันของแบบจำลอง แต่ไม่ควรนำข้อมูลส่วนนี้ไปปรับน้ำหนักโดยตรง

7.3) ชุดทดสอบ (test set) ใช้ประเมินแบบจำลองฉบับสุดท้าย และควรใช้เมื่อการเลือกแบบจำลองเสร็จสิ้นแล้ว หากนำ test set มาตรวจซ้ำและปรับแบบจำลองหลายรอบ test set จะสูญเสียความเป็นข้อมูลที่ไม่เคยเห็น

ขั้นตอนการแบ่งข้อมูลภาพออกเป็นชุดฝึก (training set), ชุดตรวจสอบความถูกต้อง (validation set), และชุดทดสอบ (test set) ควรดำเนินการก่อนการฝึกแบบกำหนดเอง (custom training) และประเมินประสิทธิภาพของแบบจำลองด้วย F1-score และ confusion matrix ทั้งนี้ต้องป้องกันการรั่วไหลของข้อมูลระหว่างชุด (data leakage) ข้อผิดพลาดที่สำคัญ เช่น การนำเฟรมที่อยู่ติดกันจากวิดีโอเดียวกันไปไว้ทั้งใน training set และ test set เนื่องจากภาพเหล่านั้นมีความคล้ายคลึงกันสูง ซึ่งอาจทำให้ผลการทดสอบดูดีกว่าประสิทธิภาพจริง แนวทางที่เหมาะสมคือควรแบ่งข้อมูลตามแหล่งที่มา เช่น วิดีโอ กล้อง สถานที่ หรือช่วงเวลา ก่อนแยกเฟรม เพื่อไม่ให้ข้อมูลจากแหล่งเดียวกันปรากฏอยู่ในข้อมูลมากกว่าหนึ่งชุด คือ

7.3.1) แบ่งตามบุคคล หากต้องการทดสอบกับบุคคลที่ไม่เคยเห็น

7.3.2) แบ่งตามกล้อง หากต้องการทดสอบความสามารถข้ามกล้อง

7.3.3) แบ่งตามวันหรือเหตุการณ์

7.3.4) เก็บวิดีโอเดียวกันไว้ในชุดเดียว

7.3.5) ทำ augmentation หลังแบ่งชุดข้อมูลแล้ว

7.3.6) ไม่สร้างภาพดัดแปลงจากภาพเดียวกันข้ามชุด

8) ขั้นตอนที่ 8 การเลือกแบบจำลอง

การเลือกแบบจำลองต้องสัมพันธ์กับลักษณะงานและอุปกรณ์ที่จะนำไปติดตั้ง

ตารางที่ 8.1 ลักษณะงานและผลลัพธ์ที่ต้องการในการเลือกแบบจำลอง

ลักษณะงาน	ผลลัพธ์ที่ต้องการ
Image Classification	ชื่อประเภทของภาพ
Object Detection	ชื่อและตำแหน่งของวัตถุ
Instance Segmentation	พื้นที่วัตถุระดับพิกเซล
Keypoint Detection	ตำแหน่งจุดสำคัญ
Face Recognition	อัตลักษณ์หรือค่าความคล้าย
Anomaly Detection	คะแนนความผิดปกติ

สถาปัตยกรรมที่ใช้ เช่น RF-DETR และโมเดลตระกูล YOLO สำหรับการตรวจจับวัตถุ (object detection), ViT และ ResNet สำหรับการจำแนกประเภท (classification) รวมถึงแบบจำลองที่รองรับการแบ่งส่วนภาพ (segmentation) หรือการตรวจจับจุดสำคัญ (keypoint detection) เกณฑ์การเลือกแบบจำลองประกอบด้วยความแม่นยำ ความเร็วในการประมวลผล ขนาดของแบบจำลอง ปริมาณหน่วยความจำที่ใช้ กำลังประมวลผลของอุปกรณ์ ความสามารถในการทำงานแบบเวลาจริง ความสะดวกในการนำไปติดตั้งใช้งาน ความทนทานต่อสภาพแสงและมุมกล้อง ตลอดจนความปลอดภัยและความน่าเชื่อถือของแหล่งที่มาของแบบจำลอง (Ultralytics, 2023)

9) ขั้นตอนที่ 9 การกำหนด Hyperparameters

Hyperparameters เป็นค่าที่ผู้พัฒนากำหนดก่อนหรือระหว่างการฝึกแบบจำลอง เช่น learning rate, batch size, จำนวน epochs, ขนาดภาพนำเข้า, optimizer, weight decay, confidence threshold, Intersection over Union (IoU) threshold และอัตราการทำ data augmentation การปรับ hyperparameters ประเมินผลโดยใช้ชุดตรวจสอบความถูกต้อง (validation set) และไม่ควรเลือกค่าจากผลการประเมินบนชุดทดสอบ (test set)

10) ขั้นตอนที่ 10 การฝึกแบบจำลอง

การฝึกแบบจำลองประกอบด้วยกระบวนการหลักดังนี้

10.1) อ่านข้อมูลหนึ่ง batch

10.2) ส่งข้อมูลเข้าสู่แบบจำลอง

10.3) แบบจำลองคำนวณผลทำนาย

10.4) เปรียบเทียบผลทำนายกับ ground truth

10.5) คำนวณ loss

10.6) คำนวณ gradient

10.7) ปรับค่าพารามิเตอร์

10.8) ทำซ้ำจนครบข้อมูลหนึ่ง epoch

10.9) ประเมินผลบน validation set

10.10) บันทึกแบบจำลองที่ให้ผลเหมาะสมที่สุด

ระหว่างการฝึกควรติดตาม training loss, validation loss, precision, recall, F1-score, learning rate, ระยะเวลาต่อ epoch ตลอดจนการใช้งาน CPU, GPU และหน่วยความจำ สำหรับระบบรักษาความปลอดภัยที่ใช้ AI ควรติดตาม learning rate และการลู่เข้า (convergence)

ความแม่นยำของชุดฝึกและชุดตรวจสอบความถูกต้อง (validation set) อิทธิพลของแต่ละ batch และผลของ regularization เพื่อใช้ตรวจสอบความผิดปกติและประกอบการตัดสินใจว่าควรฝึกแบบจำลองใหม่หรือไม่ (Ultralytics, 2023; Lendák & Kiss, 2026)

11) ขั้นตอนที่ 11 การป้องกัน overfitting

Overfitting เกิดขึ้นเมื่อแบบจำลองจดจำรายละเอียดของ training set มากเกินไป จนให้ผลดีมากกับข้อมูลฝึก แต่ทำงานไม่ดีเมื่อพบข้อมูลใหม่ สัญญาณที่อาจบ่งชี้ overfitting ได้แก่

11.1) Training loss ลดลงต่อเนื่อง แต่ validation loss เพิ่มขึ้น

11.2) คะแนน training สูงมาก แต่ validation ต่ำ

11.3) ทำงานดีเฉพาะฉากหลังหรือกล้องที่ใช้ฝึก

11.4) จดจำเสื้อผ้าหรือพื้นหลังแทนบุคคล

11.5) ประสิทธิภาพลดลงมากเมื่อเปลี่ยนแสงหรือมุมกล้อง

วิธีลด overfitting ได้แก่ การเพิ่มข้อมูลที่หลากหลาย การใช้ data augmentation การลดความซับซ้อนของแบบจำลอง การใช้ early stopping, weight regularization, dropout และ cross-validation เมื่อเหมาะสม รวมถึงการตรวจสอบความซ้ำซ้อนของข้อมูล การทำ regularization มีเป้าหมายเพื่อลด overfitting และช่วยให้แบบจำลองสามารถสรุปไปใช้กับข้อมูลที่ไม่เคยพบมาก่อนได้ดีขึ้น แม้ว่าคะแนนบน training set อาจลดลง แต่ประสิทธิภาพของแบบจำลองเมื่อใช้กับข้อมูลใหม่จะมีความสม่ำเสมอและน่าเชื่อถือมากขึ้น (Ultralytics, 2023; Lendák & Kiss, 2026)

8.2.6 การประเมินแบบจำลอง

การประเมินต้องใช้ตัวชี้วัดที่สัมพันธ์กับลักษณะความเสี่ยง ไม่ควรพิจารณา accuracy เพียงค่าเดียว

1) Confusion matrix

สำหรับการจำแนกสองคลาส มีค่าพื้นฐานดังนี้

1.1)True Positive (TP) ระบบตรวจพบเหตุการณ์และเหตุการณ์นั้นเกิดขึ้นจริง

1.2)False Positive (FP) ระบบแจ้งเตือน แต่เหตุการณ์นั้นไม่ได้เกิดขึ้นจริง

1.3)True Negative (TN) ระบบระบุว่าไม่มีเหตุการณ์และไม่มีเหตุการณ์จริง

1.4)False Negative (FN) ระบบไม่แจ้งเตือน ทั้งที่เหตุการณ์เกิดขึ้นจริง

ในระบบรักษาความปลอดภัย FN มักมีความรุนแรงสูง เพราะหมายถึงระบบพลาดภัยคุกคาม ส่วน FP ที่มากเกินไปทำให้ผู้ใช้เกิดความเหนื่อยล้าจากการแจ้งเตือนและอาจละเลยสัญญาณเตือนจริง

2) Precision

Precision ตอบคำถามว่า ในเหตุการณ์ทั้งหมดที่ระบบแจ้งเตือน มีสัดส่วนเท่าใดที่เป็นเหตุการณ์จริง โดยค่า precision สูงหมายถึงระบบมีการแจ้งเตือนผิดค่อนข้างน้อย

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{8.1}$$

3) Recall

Recall ตอบคำถามว่า ในเหตุการณ์จริงทั้งหมด ระบบสามารถตรวจพบได้มากเพียงใด สำหรับงานตรวจจับการบุกรุกหรืออัคคีภัย recall มักมีความสำคัญสูง เพราะการตรวจไม่พบเหตุการณ์อาจก่อให้เกิดความเสียหาย

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{8.2}$$

4) F1-score

F1-score เป็นค่าเฉลี่ยฮาร์มอนิกของ precision และ recall เหมาะกับปัญหาที่ข้อมูลแต่ละคลาสมีจำนวนไม่สมดุล และต้องการพิจารณาทั้งการแจ้งเตือนผิดและการพลาดเหตุการณ์จริง

$$\text{F1} = 2\left(\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}\right) \tag{8.3}$$

การตีความที่ถูกต้อง ซึ่งค่า F1-score ร้อยละ 71 หมายความว่า ผลรวมเชิงสมดุลของ precision และ recall ภายใต้ชุดข้อมูลและเกณฑ์ที่ใช้ทดสอบอยู่ที่ 0.71ไม่ได้หมายความว่าแบบจำลองมี accuracy ร้อยละ 71 และไม่ได้หมายความว่าระบบถูกต้องร้อยละ 71 ในทุกสถานการณ์

5) Intersection over Union (IoU)

สำหรับ object detection ต้องประเมินว่ากรอบที่แบบจำลองทำนายซ้อนทับกับกรอบ ground truth มากเพียงใด

$$\text{IoU} = \frac{\text{พื้นที่ซ้อนทับระหว่างกรอบทำนายกับกรอบจริง}}{\text{พื้นที่รวมของกรอบทั้งสอง}} \tag{8.4}$$

โดยใช้ค่า IoU โดย ค่า IoU ใกล้ 1 หมายถึงกรอบทำนายใกล้เคียง ground truth ส่วนค่าใกล้ 0 หมายถึงกรอบแทบไม่ซ้อนทับกัน อย่างไรก็ตาม การประเมิน object detection ไม่ควรใช้ IoU เพียงค่าเดียว แต่ต้องพิจารณา precision, recall และค่า average precision ของแต่ละคลาสร่วมด้วย

6) Mean Average Precision

Mean average precision (mAP) เป็นตัวชี้วัดประสิทธิภาพที่นิยมใช้สำหรับประเมินแบบจำลองตรวจจับวัตถุ (object detection) เช่น YOLO โดยพิจารณาทั้งความถูกต้องในการจำแนกวัตถุและความถูกต้องของตำแหน่งกรอบล้อมรอบวัตถุ (bounding box) ที่แบบจำลองตรวจจับได้ ดังนั้น mAP จึงเหมาะสำหรับประเมินระบบตรวจจับใบหน้ามากกว่าการพิจารณาค่า accuracy เพียงอย่างเดียว การคำนวณ mAP มีความสัมพันธ์กับค่า IoU, precision, recall, precision–recall curve และ average precision (AP) โดยสามารถอธิบายตามลำดับได้ดังนี้

6.1) ขั้นที่ 1 กำหนดว่า bounding box ที่ตรวจพบถูกต้องหรือไม่ด้วย IoU

เมื่อ YOLO ตรวจพบใบหน้า ระบบจะได้กรอบที่แบบจำลองทำนาย (predicted bounding box) จากนั้นนำกรอบดังกล่าวไปเปรียบเทียบกับกรอบคำตอบจริง (ground-truth bounding box) โดยใช้ค่า IoU ตามสามการที่ 8.4

ค่า IoU มีค่าระหว่าง 0 ถึง 1 หากกรอบที่ทำนายตรงกับกรอบจริงมาก ค่า IoU จะสูงขึ้น ตัวอย่างเช่น หากกำหนดเกณฑ์ IoU เท่ากับ 0.50 และกรอบที่ YOLO ตรวจพบมี IoU = 0.78 กับ ground truth การตรวจจับนั้นสามารถถือเป็น TP ได้ ภายใต้เงื่อนไขว่าคลาสถูกต้องและ ground truth นั้นยังไม่ได้ถูกจับคู่กับ prediction อื่นมาก่อน ในทางกลับกัน หาก IoU ต่ำกว่าเกณฑ์ที่กำหนด การตรวจจับนั้นจะไม่ถือว่าเป็นการตรวจจับที่ถูกต้องตามเกณฑ์ดังกล่าว

6.2) ขั้นที่ 2 คำนวณ precision และ recall

เมื่อจำแนกผลการตรวจจับเป็น TP, FP, และ FN แล้ว สามารถคำนวณ precision และ recall ได้จากสมการที่ 8.1 และ 8.2 ตามลำดับ ค่า precision แสดงว่าจากวัตถุทั้งหมดที่ระบบระบุว่าเป็นใบหน้า มีสัดส่วนเท่าใดที่ตรวจจับได้ถูกต้อง ส่วน recall แสดงว่าจากใบหน้าที่มีอยู่จริงทั้งหมด ระบบสามารถตรวจพบได้เป็นสัดส่วนเท่าใด

สำหรับระบบรักษาความปลอดภัย recall มีความสำคัญมาก เพราะค่า recall ต่ำหมายความว่าระบบมี FN สูง หรือมีใบหน้าจริงที่กล้องมองเห็นแต่แบบจำลองตรวจไม่พบ ซึ่งอาจทำให้ระบบพลาดเหตุการณ์ที่ต้องเฝ้าระวัง

6.3) ขั้นที่ 3 สร้าง precision–recall curve

แบบจำลอง YOLO จะให้ค่าความเชื่อมั่น (confidence score) แก่การตรวจจับแต่ละรายการ เช่น

- Face A Confidence = 0.96
- Face B Confidence = 0.87
- Face C Confidence = 0.74
- Face D Confidence = 0.41

เมื่อเปลี่ยน confidence Threshold จำนวน TP, FP และ FN ก็จะเปลี่ยนตาม ส่งผลให้ precision และ recall เปลี่ยนแปลงด้วย

ตัวอย่างเช่น หากกำหนด confidence threshold ไว้สูงมาก ระบบอาจยอมรับเฉพาะใบหน้า A (face A) และใบหน้า B (face B) ทำให้ผลการตรวจจับมีความน่าเชื่อถือสูง แต่แบบจำลองอาจพลาดการตรวจจับใบหน้าบางส่วน ส่งผลให้ค่า recall ลดลง ในทางกลับกัน หากลดค่า threshold ระบบจะตรวจพบใบหน้ามากขึ้น แต่อาจตรวจจับวัตถุอื่นผิดว่าเป็นใบหน้า ส่งผลให้จำนวนผลบวกลวง (FP) เพิ่มขึ้น และค่า precision ลดลง เมื่อนำค่า precision และ recall ที่ได้จากระดับ confidence threshold ต่าง ๆ มาพล็อตเป็นกราฟ จะได้ เส้นโค้ง precision–recall (precision–recall curve: PR curve)

6.4) ขั้นที่ 4 คำนวณ Average Precision (AP)

AP เป็นค่าที่สรุปประสิทธิภาพของคลาสหนึ่งจาก PR curve โดยพิจารณาพื้นที่ภายใต้เส้นโค้ง precision–recall ตามวิธีการประเมินที่กำหนด กล่าวอย่างง่ายคือ “AP แสดงความสามารถของแบบจำลองในการรักษาสมดุลระหว่างการตรวจพบวัตถุจริงให้ครบ (recall) และการลดการตรวจผิด (precision) สำหรับคลาสหนึ่ง” หากระบบมีเพียงคลาสเดียวคือ face ค่า AP จึงเป็นการประเมินประสิทธิภาพของการตรวจจับใบหน้าโดยตรง

6.5) ขั้นที่ 5 คำนวณ Mean Average Precision (mAP)

ในกรณีที่แบบจำลองตรวจจับหลายคลาส จะคำนวณ AP แยกสำหรับแต่ละคลาส แล้วหาค่าเฉลี่ยเพื่อให้ได้ mAP จากสมการที่ 8.5

$$mAP = \frac{1}{N} \sum_{i=1}^{N} APi \quad (8.5)$$

เมื่อ N คือ จำนวนคลาส และ Api คือ AP ของคลาส ตัวอย่างเช่น ระบบ smart security ตรวจจับ 3 คลาส ดังตารางที่ 8.2

ตารางที่ 8.2 ตัวอย่างของแบบจำลองตรวจจับหลายคลาส

คลาส	AP
Face	0.92
Person	0.88
Car	0.84

ดังนั้น

$$mAP = \frac{0.92 + 0.88 + 0.84}{3}$$
$$= 0.88$$

จึงกล่าวได้ว่า mAP ของแบบจำลองเท่ากับ 0.88 หรือ 88% ภายใต้เกณฑ์ IoU และวิธีคำนวณ AP ที่กำหนด อย่างไรก็ตามสำหรับโมเดลตรวจจับใบหน้าที่มีเพียงคลาส face เพียงคลาสเดียว ค่าเฉลี่ยข้ามคลาสจะมีเพียงหนึ่งค่า ดังนั้น mAP ในเชิงการเฉลี่ยข้ามคลาสจึงมีค่าเท่ากับ AP ของคลาส face ภายใต้เกณฑ์ IoU เดียวกัน

7) การประเมินระดับระบบ

คะแนนแบบจำลองและประสิทธิภาพของอุปกรณ์เป็นคนละระดับกัน

7.1) การประเมินแบบจำลอง

การวัดว่าแบบจำลองสามารถทำนายข้อมูลได้ดีเพียงใด ใช้ตัวชี้วัด precision, recall, F1-score, IoU, AP, mAP, False Acceptance Rate (FAR) และ False Rejection Rate (FRR)

7.2) การประเมินระบบจริง

เป็นวัดการทำงานของระบบทั้งหมด เช่น ระยะเวลาในการตรวจจับ ระยะเวลาในการส่งแจ้งเตือน จำนวนเฟรมต่อวินาที ความเสถียรของการเชื่อมต่อ การทำงานในสภาพแสงต่าง ๆ ประสิทธิภาพในแต่ละระยะและมุม ความถูกต้องของข้อความแจ้งเตือน การใช้พลังงาน หรือความสามารถเมื่ออินเทอร์เน็ตขัดข้อง

8.2.7 การกำหนดเกณฑ์การตัดสินใจและการแจ้งเตือน

หลังจากแบบจำลองส่งผลลัพธ์ ระบบต้องมีกฎการตัดสินใจระดับแอปพลิเคชัน เช่น

- หากตรวจพบ person
- และค่า confidence ≥ เกณฑ์ที่กำหนด
- และตำแหน่งอยู่ในเขตหวงห้าม
- และเวลาอยู่ในช่วงเฝ้าระวัง
- ให้บันทึกภาพและส่งแจ้งเตือน

ไม่ควรแจ้งเตือนจากผลเพียงเฟรมเดียวเสมอไป เพราะอาจเกิดการตรวจจับผิดชั่วคราว แนวทางลด False Alarm ได้แก่ ต้องตรวจพบต่อเนื่องหลายเฟรม การใช้ object tracking ยืนยันว่าเป็นวัตถุเดียวกัน การรวมข้อมูลจากกล้องและเซ็นเซอร์ การกำหนดเขตสนใจ การกำหนดเวลาเฝ้าระวัง การใช้ระดับความรุนแรงหลายระดับ หรือการให้มนุษย์ยืนยันก่อนสั่งการที่มีผลกระทบสูง

8.2.8 การรักษาความปลอดภัยของกระบวนการ Machine Learning

ระบบที่ใช้ AI เพื่อรักษาความปลอดภัยต้องป้องกันตัว AI ด้วย เพราะผู้โจมตีอาจมุ่งโจมตีข้อมูล แบบจำลอง หรือผลลัพธ์

1) การปนเปื้อนข้อมูลฝึก (Data Poisoning)

Data poisoning คือการแก้ไข เพิ่ม หรือติดป้ายข้อมูลฝึกผิด เพื่อให้แบบจำลองตัดสินใจตามที่ผู้โจมตีต้องการ เช่น ทำให้ใบหน้าของบุคคลหนึ่งถูกระบุผิดเป็นบุคคลที่ได้รับอนุญาต การโจมตีอาจมุ่งเป้าหมายเฉพาะหรือทำให้ประสิทธิภาพโดยรวมลดลง (Lendák & Kiss, 2026) แนวทางป้องกัน ได้แก่ ตรวจสอบแหล่งข้อมูล จำกัดสิทธิ์แก้ไขชุดข้อมูล เก็บประวัติ version ตรวจสอบ label ตรวจจับ outlier ตรวจสอบการกระจายของข้อมูล ใช้การอนุมัติข้อมูลก่อนนำเข้าชุดฝึก หรือเปรียบเทียบผลหลายแบบจำลอง

2) การดัดแปลงข้อมูลนำเข้า (Adversarial Input)

Adversarial input คือข้อมูลที่ถูกปรับเปลี่ยนอย่างจงใจเพื่อหลอกแบบจำลอง แม้การเปลี่ยนแปลงอาจมองเห็นได้ยากสำหรับมนุษย์ แต่ทำให้แบบจำลองตัดสินใจผิด แนวทางป้องกันประกอบด้วยการตรวจสอบข้อมูลนำเข้า การกรองความผิดปกติ การฝึกด้วยตัวอย่างโจมตี และการติดตามประสิทธิภาพของแบบจำลอง

3) การขโมยหรือย้อนกลับแบบจำลอง

ผู้โจมตีอาจส่งคำถามจำนวนมากไปยัง API และวิเคราะห์ผลลัพธ์ เพื่อเลียนแบบแบบจำลองหรืออนุมานข้อมูลฝึกที่มีความอ่อนไหว โดยเฉพาะภาพใบหน้าและข้อมูลชีวมิติ (Lendák & Kiss, 2026) มาตรการที่เหมาะสม ได้แก่

3.1) การยืนยันตัวตนก่อนใช้ API

3.2) Rate limiting

3.3) ลดรายละเอียดผลลัพธ์ที่ไม่จำเป็น

3.4) เข้ารหัสไฟล์แบบจำลอง

3.5) จำกัดสิทธิ์เข้าถึง

3.6) บันทึกและตรวจสอบ query

3.7) ใช้ model watermarking

3.8) ไม่เปิดเผย confidence score เกินความจำเป็น

4) การป้องกัน overfitting และเพิ่ม robustness

แบบจำลองที่ overfit อาจมีความเสี่ยงต่อการรั่วไหลของข้อมูลและการตัดสินใจผิดกับข้อมูลใหม่ วิธีเพิ่มความทนทาน ได้แก่

4.1) Regularization

4.2) Data augmentation

4.3) Early stopping

4.4) Adversarial training

4.5) Ensemble learning

4.6) Robustness testing

4.7) การตรวจสอบ Distribution Shift

Adversarial training เป็นการนำข้อมูลที่ถูกสร้างหรือดัดแปลงเพื่อหลอกแบบจำลองเข้าสู่กระบวนการฝึก เพื่อเพิ่มความทนทานต่อการโจมตี แต่ไม่ได้ป้องกันการโจมตีทุกชนิดอย่างสมบูรณ์ (Lendák & Kiss, 2026)

8.2.9 การติดตามแบบจำลองหลังนำไปใช้งาน

ประสิทธิภาพของแบบจำลองอาจลดลงเมื่อสภาพแวดล้อมเปลี่ยน เช่น เปลี่ยนกล้อง แสง ฉากหลัง รูปแบบเสื้อผ้า หรือพฤติกรรมผู้ใช้ จึงต้องติดตามอย่างต่อเนื่อง ตัวชี้วัดที่ควรติดตาม ได้แก่ accuracy หรือ error rate, precision, recall และ F1-score, confidence distribution, latency, throughput, การใช้ CPU, GPU และหน่วยความจำ, จำนวนการแจ้งเตือนต่อวัน, false alarm, เหตุการณ์ที่ผู้ใช้แก้ไขผลลัพธ์, คะแนน anomaly, การเปลี่ยนแปลงการกระจายของข้อมูล, และความแตกต่างระหว่างกลุ่มผู้ใช้ โดย Lendák และ Kiss (2026) เสนอให้ติดตามทั้งข้อมูลนำเข้า ผลลัพธ์ สมรรถนะ สถานะภายใน และพฤติกรรมผู้ใช้ รวมถึงกำหนด cut-off threshold ด้านความแม่นยำ เวลาแฝง การใช้ทรัพยากร คะแนนความเชื่อมั่น ความผิดปกติ และความเป็นธรรม เมื่อพบว่าแบบจำลองเสื่อมประสิทธิภาพ ควรดำเนินการตามลำดับดังนี้

1) ตรวจสอบคุณภาพกล้องและเซ็นเซอร์

2) ตรวจสอบ preprocessing

3) ตรวจสอบการเปลี่ยนแปลงของข้อมูล

4) ตรวจสอบ threshold

5) เก็บตัวอย่างที่ระบบทำนายผิด

6) กำกับข้อมูลใหม่

7) ฝึกหรือ fine-tune แบบจำลอง

8) ทดสอบกับชุดข้อมูลอิสระ

9) ทดลองแบบจำกัดก่อนแทนที่รุ่นเดิม

10) เก็บรุ่นเดิมไว้สำหรับ rollback

การรายงานผลถูกต้องควรระบุ (1) จำนวนเหตุการณ์ที่ใช้ (2) จำนวนคลาส (3) วิธีแบ่ง train, validation, test (4) แหล่งที่มาของข้อมูล (5) วิธี annotation (6) สถาปัตยกรรม/ขนาดแบบจำลอง (7) ขนาดภาพนำเข้า (8) จำนวน epoch (9) hyperparameters ที่สำคัญ (10) confidence และ IoU threshold (11) hardware ที่ใช้ฝึกและทดสอบ (12) precision, recall และ F1-score รายคลาส (13) confusion matrix (14) ความเร็วและ latency (15) ข้อจำกัดของชุดข้อมูล และ (16) เงื่อนไขการทดสอบจริง ไม่ควรใช้ถ้อยคำว่า “ระบบมีความแม่นยำร้อยละ 100” โดยไม่มีรายละเอียด ควรเขียนว่า “ภายใต้กลุ่มตัวอย่างและเงื่อนไขการทดสอบที่กำหนด ระบบตรวจพบเหตุการณ์ถูกต้องทุกครั้งจากที่ทดลองที่ดำเนินการ อย่างไรก็ตาม ผลดังกล่าวยังไม่เพียงพอสำหรับสรุปประสิทธิภาพกับประชากรหรือสภาพแวดล้อมอื่น”

กล่าวโดยสรุป ML ในระบบรักษาความปลอดภัยอัจฉริยะ เริ่มจากการกำหนดปัญหาและผลลัพธ์ที่ต้องการ รวบรวมและตรวจสอบข้อมูล กำกับข้อมูล เตรียมและแบ่งชุดข้อมูล เลือกแบบจำลอง ฝึก และประเมินผล ก่อนนำไปใช้งานบน Edge, cloud หรือแบบผสม จากนั้นติดตามประสิทธิภาพ ความผิดปกติ ความปลอดภัย การเปลี่ยนแปลงของข้อมูลอย่างต่อเนื่อง คุณภาพของระบบไม่ได้ขึ้นอยู่กับอัลกอริทึมอย่างเดียว แต่ขึ้นอยู่กับคุณภาพข้อมูล ความถูกต้องของ annotation วิธีแบ่งชุดข้อมูล การเลือกตัวชี้วัด การออกแบบเกณฑ์แจ้งเตือน และการทดสอบภายใต้สภาพแวดล้อมจริง นอกจากนี้ต้องป้องกันการปนเปื้อนข้อมูล การดัดแปลงข้อมูลนำเข้า การขโมยแบบจำลอง และการรั่วไหลของข้อมูลส่วนบุคคลตลอดวงจรของ ML

8.3 การตรวจจับใบหน้าจากกล้องด้วยแบบจำลองตระกูล YOLO

การตรวจจับใบหน้า (face detection) คือกระบวนการค้นหาว่าในภาพหรือเฟรมวิดีโอมีใบหน้าปรากฏอยู่หรือไม่ และระบุตำแหน่งของใบหน้าด้วยกรอบสี่เหลี่ยมล้อมรอบวัตถุ (bounding box) พร้อมค่าความเชื่อมั่นของการตรวจจับ การตรวจจับใบหน้าแตกต่างจากการรู้จำใบหน้า (face recognition) เพราะ face detection ตอบเพียงว่า “ใบหน้าอยู่ที่ใด” ขณะที่ face recognition ต้องเปรียบเทียบคุณลักษณะของใบหน้ากับฐานข้อมูลเพื่อระบุบุคคล

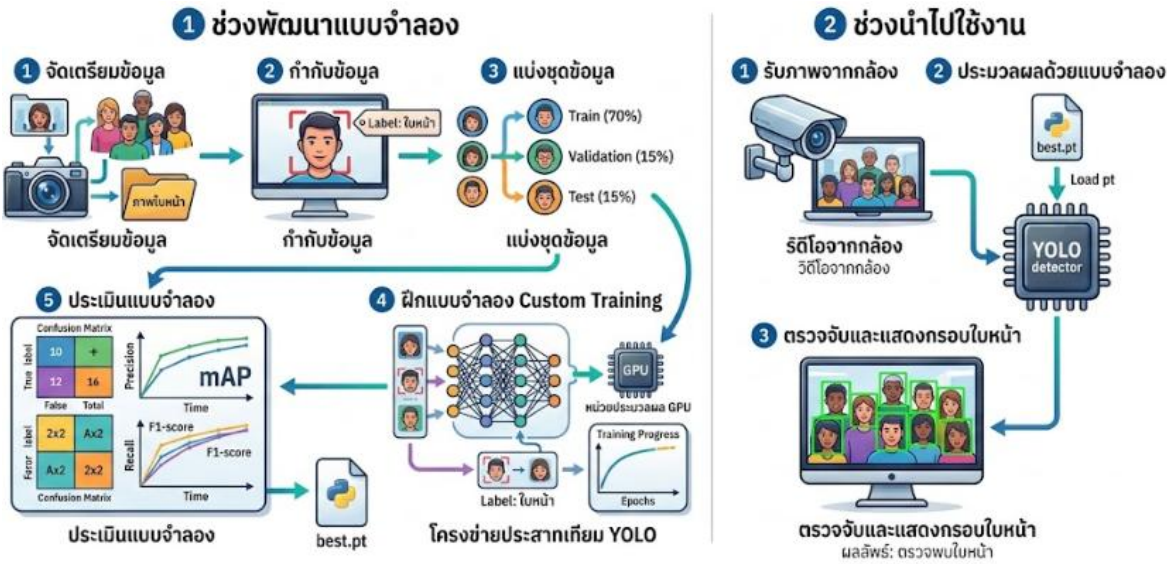
8.3.1 กระบวนการตรวจจับใบหน้าด้วย YOLO

YOLO หรือ You Only Look Once เป็นสถาปัตยกรรมการตรวจจับวัตถุแบบขั้นตอนเดียว (One-stage object detector) ซึ่งประมวลผลภาพทั้งภาพด้วยโครงข่ายเดียวเพื่อทำนายตำแหน่งกรอบวัตถุและความน่าจะเป็นของคลาส จึงเหมาะกับงานที่ต้องการประมวลผลวิดีโอแบบเวลาจริง (Redmon et al., 2016) อย่างไรก็ตาม แบบจำลอง YOLO ที่ฝึกด้วยชุดข้อมูลทั่วไป เช่น COCO มักมีคลาส person แต่ไม่มีคลาส face โดยตรง ดังนั้น การตรวจจับ “ใบหน้า” อย่างถูกต้องต้องใช้แบบจำลองที่ฝึกกับชุดข้อมูลใบหน้า หรือฝึกแบบจำลองใหม่ด้วยชุดข้อมูลที่กำหนดคลาส face ส่วนการใช้แบบจำลองมาตรฐานตรวจจับ person จะให้กรอบรอบตัวบุคคล ไม่ใช่กรอบรอบใบหน้าโดยเฉพาะ กระบวนการตรวจจับใบหน้าจากกล้องด้วย YOLO แบ่งเป็นสองช่วง (Redmon et al., 2016; Qi et al., 2022; Ultralytics, 2023; Yu et al., 2024; Ali et al., 2026 ; Jocher et al, 2026)

1) ช่วงพัฒนาแบบจำลอง เป็นการจัดเตรียมข้อมูล กำกับข้อมูล ฝึก และประเมินแบบจำลอง

2) ช่วงนำไปใช้งาน โดยการรับภาพจากกล้อง ประมวลผลด้วยแบบจำลอง และแสดงกรอบใบหน้า

ขั้นตอนการพัฒนา ประกอบด้วยการกำกับข้อมูล การแบ่งชุด train, validation และ test การฝึกแบบ custom Training และการประเมินด้วย confusion matrix, precision, recall และ F1-score



รูปที่ 8.4 กระบวนการตรวจจับใบหน้าด้วยสถาปัตยกรรม YOLO

8.3.2 การเตรียมสภาพแวดล้อม

1) ฮาร์ดแวร์

อุปกรณ์ขั้นต่ำประกอบด้วย (1) คอมพิวเตอร์ที่ติดตั้ง Python (2) กล้องเว็บแคม หรือกล้อง USB (3) หน่วยความจำเพียงพอสำหรับประมวลผลภาพ และ (4) GPU เป็นทางเลือกสำหรับการฝึกแบบจำลอง สำหรับการทดลองพื้นฐานสามารถใช้ CPU ได้ แต่การฝึกแบบจำลองด้วยภาพจำนวนมากจะใช้เวลานานกว่า GPU ส่วนการนำแบบจำลองขนาดเล็กไปตรวจจับแบบเวลาจริงสามารถทำงานบนคอมพิวเตอร์ทั่วไปหรืออุปกรณ์ Edge เช่น Raspberry Pi ได้ แต่ต้องเลือกขนาดแบบจำลองและขนาดภาพให้เหมาะสม

2) ติดตั้ง Python และไลบรารี

แนะนำให้สร้าง virtual environment แยกจากระบบหลัก

2.1) Windows

```
python -m venv face_yolo_env
face_yolo_env\Scripts\activate
```

2.2) macOS หรือ Linux

```
python3 -m venv face_yolo_env
source face_yolo_env/bin/activate
```

2.3) ติดตั้งไลบรารี

```
python -m pip install --upgrade pip
pip install ultralytics opencv-python
```

2.4) ตรวจสอบการติดตั้ง

```
python -c "from ultralytics import YOLO; import cv2;
print('Installation complete')"
```

Ultralytics แบ่งการทำงานออกเป็นโหมดสำคัญ ได้แก่ train, validation, predict, export และ track โดย train ใช้ฝึกแบบจำลองจากชุดข้อมูลเฉพาะ ส่วน predict ใช้ประมวลผลภาพหรือวิดีโอจริง

8.3.3 การเตรียมชุดข้อมูลใบหน้า

1) ขั้นตอนที่ 1 กำหนดคลาส

หากต้องการเพียงตรวจจับว่ามีใบหน้าหรือไม่ ให้กำหนดหนึ่งคลาส ได้แก่ “face” โดยไม่ควรกำหนดชื่อบุคคลแต่ละคนเป็นคลาสสำหรับงาน face detection เพราะการระบุชื่อบุคคลเป็นงาน face recognition ซึ่งต้องใช้ขั้นตอนสกัด face embedding และเปรียบเทียบอัตลักษณ์เพิ่มเติม

2) ขั้นตอนที่ 2 รวบรวมภาพ

ภาพควรครอบคลุมสถานการณ์ใช้งานจริง เช่น ใบหน้าตรง หันซ้ายและขวา ก้มและเงย ระยะใกล้และไกล หลายขนาดใบหน้า แสงสว่างมากและน้อย แสงย้อน สวมแว่นตา สวมหมวก ใบหน้าถูกบังบางส่วน มีหลายใบหน้าในภาพ ฉากหลังหลายรูปแบบ ภาพจากกล้องรุ่นเดียวกับที่จะนำไปใช้งาน และไม่ควรใช้เฉพาะภาพใบหน้าตรงที่มีแสงสมบูรณ์ เพราะแบบจำลองอาจทำงานได้ดีเฉพาะในสภาพคล้ายชุดฝึก

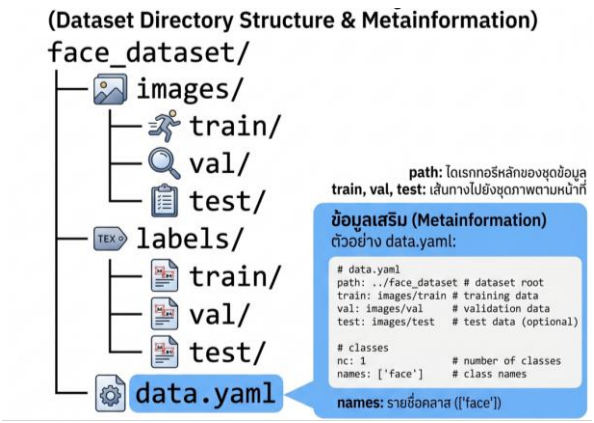
การตรวจจับใบหน้าเป็นงานที่มีความท้าทาย จากใบหน้าขนาดเล็ก การบดบัง มุมการหัน แบบจำลอง YOLO-FaceV2 จึงเพิ่มกลไกสำหรับจัดการใบหน้าขนาดเล็กและใบหน้าที่ถูกบดบังที่มีความหลากหลายของข้อมูลฝึก ซึ่งเป็นองค์ประกอบสำคัญในการตรวจจับ (Yu et al., 2024)

3) ขั้นตอนที่ 3 กำกับข้อมูล

ในแต่ละภาพ ให้วาด bounding box ครอบใบหน้าแต่ละใบและกำหนดคลาสเป็น “face” หลักการวาดกรอบที่เหมาะสมดังนี้ (1) กรอบควรครอบส่วนใบหน้าที่มองเห็นได้ (2) ไม่ควรรวมลำตัวหรือพื้นหลังมากเกินไป (3) ใบหน้าทุกใบที่มองเห็นชัดควรถูกกำกับ (4) หากมีหลายใบหน้า ต้องสร้างหนึ่งกรอบต่อหนึ่งใบหน้า (5) ต้องใช้แนวทางเดียวกันตลอดชุดข้อมูล และ (6) ควรตรวจสอบภาพที่กำกับแล้วอีกครั้ง

8.3.4 รูปแบบการจัดชุดข้อมูล YOLO

โครงสร้างโฟลเดอร์ที่สร้างสำหรับเก็บชุดข้อมูล แนะนำ ดังนี้



รูปที่ 8.5 โครงสร้างโฟลเดอร์สำหรับเก็บข้อมูล

ไฟล์ภาพและไฟล์ Label ต้องใช้ชื่อเดียวกัน เช่น

```
images/train/image001.jpg
labels/train/image001.txt
```

รูปแบบไฟล์ Label สำหรับ YOLO ใช้หนึ่งบรรทัดต่อหนึ่งวัตถุ ดังนี้

```
class_id x_center y_center width height
```

ค่าพิกัดถูก normalize ให้อยู่ระหว่าง 0 ถึง 1 ตัวอย่าง เช่น และมีความหมาย ดังนี้

```
0 0.5125 0.4300 0.2750 0.3600
```

- 0 คือรหัสคลาส face
- 0.5125 คือตำแหน่งกึ่งกลางกรอบในแนวแกน x
- 0.4300 คือตำแหน่งกึ่งกลางกรอบในแนวแกน y
- 0.2750 คือความกว้างของกรอบ
- 0.3600 คือความสูงของกรอบ

โค้ดในไฟล์ data.yaml (ไฟล์คอนฟิกสำหรับการฝึกโมเดล YOLO) ซึ่งทำหน้าที่เป็น “แผนที่ระบุที่อยู่ของข้อมูลและกำหนดชื่อคลาส” เพื่อบอกให้โมเดลรู้ว่าจะไปดึงรูปภาพจากโฟลเดอร์ไหน และสิ่งที่จะให้ตรวจจับคืออะไร เช่น

```
path: face_dataset
train: images/train
val: images/val
test: images/test

names:
  0: face
```

โดยมีความหมายในแต่ละบรรทัดดังนี

- path: face_dataset
  คือ โฟลเดอร์หลัก (root directory) ที่เก็บชุดข้อมูลทั้งหมดไว้
- train: images/train
  คือ ที่อยู่ของโฟลเดอร์รูปภาพที่ใช้สำหรับ การฝึกโมเดล (training set)
- val: images/val
  คือ ที่อยู่ของโฟลเดอร์รูปภาพที่ใช้สำหรับ การตรวจสอบระหว่างฝึก (validation set)
- test: images/test
  คือ ที่อยู่ของโฟลเดอร์รูปภาพที่ใช้สำหรับ การทดสอบโมเดลฉบับสมบูรณ์ (test set)
- names:
  คือ ส่วนกำหนดชื่อคลาส (class names) ของวัตถุที่ต้องการให้โมเดลตรวจจับ
  0: face หมายถึง คลาสลำดับที่ 0 (ID 0) มีชื่อป้ายกำกับว่า face (ใบหน้า) ซึ่งในงานนี้มีเพียง 1 คลาสเท่านั้น

8.3.5 การแบ่งชุดข้อมูล

การแบ่งชุดข้อมูล ควรแบ่งข้อมูลเป็นสามส่วน ได้แก่

1) Training Set ใช้ปรับค่าพารามิเตอร์ของแบบจำลอง

2) Validation Set ใช้เลือกแบบจำลองและปรับ Hyperparameters

3) Test Set ใช้ประเมินผลครั้งสุดท้ายกับข้อมูลที่แบบจำลองไม่เคยเห็น

ตัวอย่างสัดส่วนที่ใช้ได้คือ

```
Training    70%
Validation  20%
Test        10%
```

หรือ

```
Training    80%
Validation  10%
Test        10%
```

หลักสำคัญกว่าสัดส่วนคือการป้องกัน data leakage เช่น ไม่ควรนำเฟรมที่อยู่ติดกันจากวิดีโอเดียวกันไปกระจายไว้ทั้ง train และ test เพราะภาพมีความคล้ายกันสูงและอาจทำให้ผลประเมินสูงเกินจริง ควรแบ่งตามวิดีโอ วัน สถานที่ หรือบุคคล ตัวอย่างเช่น ภาพจากวิดีโอชุดที่ 1–8 ใช้สำหรับ train วิดีโอชุดที่ 9 ใช้สำหรับ validation และวิดีโอชุดที่ 10 ใช้สำหรับ test

8.3.6 การเลือกแบบจำลอง YOLO

สำหรับการเริ่มต้น ควรใช้แบบจำลองขนาดเล็ก เช่นรุ่น n หรือ Nano เพราะประมวลผลได้เร็วและเหมาะกับกล้องแบบเวลาจริง จากนั้นจึงทดลองแบบจำลองขนาดใหญ่ขึ้นเมื่อความแม่นยำยังไม่เพียงพอ ตัวอย่างนี้ใช้แบบจำลองพื้นฐานของ Ultralytics แล้ว fine-tune ให้ตรวจจับคลาส face

```
from ultralytics import YOLO
model = YOLO("yolo26n.pt")
```

คำว่า n หมายถึงแบบจำลองขนาด Nano ซึ่งเน้นความเร็ว หากระบบมี GPU และต้องตรวจจับใบหน้าขนาดเล็กจำนวนมาก อาจพิจารณารุ่น s, m หรือรุ่นที่ใหญ่กว่า แต่ต้องประเมินความเร็วบนอุปกรณ์จริง แบบจำลอง YOLO สำหรับใบหน้าบางโครงการปรับโครงสร้างเพิ่มเติมเพื่อรองรับ Landmark และใบหน้าขนาดเล็ก ตัวอย่างเช่น YOLO5Face เพิ่มหัวทำนายจุดสำคัญบนใบหน้าและสร้างหลายขนาดโมเดลสำหรับงานแบบเวลาจริงบนอุปกรณ์พกพา (Qi et al., 2022; Yu et al., 2024)

8.3.7 การฝึกแบบจำลอง (Model Training)

กระบวนการฝึกแบบจำลองเป็นการนำชุดข้อมูลใบหน้าที่ผ่านการกำกับและจัดเตรียมเรียบร้อยแล้ว เข้าสู่กระบวนการเรียนรู้ผ่านเทคนิค transfer learning เพื่อให้แบบจำลองสามารถระบุตำแหน่งของใบหน้าได้อย่างแม่นยำ

1) โค้ดโปรแกรมสำหรับการฝึกแบบจำลอง (train_face.py)

```
from pathlib import Path

from ultralytics import YOLO

def main() -> None:
    """Train a single-class YOLO face detector."""

    data_file = Path("face_dataset/data.yaml")

    if not data_file.exists():
        raise FileNotFoundError(
            f"Dataset configuration not found: {data_file.resolve()}"
        )

    # Load a pretrained detector for transfer learning.
    model = YOLO("yolo26n.pt")

    results = model.train(
        data=str(data_file),
        epochs=100,
        imgsz=640,
        batch=16,
        patience=20,
        device="cpu",       # Change to 0 when using the first CUDA GPU.
        workers=4,
        project="runs_face",
        name="yolo_face",
        pretrained=True,
        seed=42,
        deterministic=True,
        plots=True,
    )

    print("Training complete.")
    print(results)


if __name__ == "__main__":
    main()
```

2) คำสั่งเรียกใช้งาน (Execution)

รันคำสั่งผ่าน command line/terminal ในโฟลเดอร์โปรเจกต์:

```
python train_face.py
```

3) คำอธิบายพารามิเตอร์และกระบวนการทำงาน (hyperparameters explanation) สามารถอิบายได้ดังตารางที่

ตารางที่ 8.3 คำอธิบายพารามิเตอร์ในการเขียนโค้ดโปรแกรมสำหรับการฝึกแบบจำลอง

พารามิเตอร์	ค่าที่กำหนด	คำอธิบายเชิงวิชาการ/เทคนิค
data	face_dataset/ data.yaml	ระบุตำแหน่งไฟล์คอนฟิกชุดข้อมูล (Dataset Configuration File) ที่ระบุ Path รูปภาพและคลาส
epochs	100	จำนวนรอบสูงสุดที่แบบจำลองจะเรียนรู้ผ่านชุดข้อมูลฝึก (Training Set) ทั้งหมด
imgsz	640	ขนาดภาพนำเข้า (640×640 พิกเซล) ซึ่งเป็นขนาดมาตรฐานที่ให้สมดุลระหว่างความเร็วและความแม่นยำ
batch	16	จำนวนรูปภาพที่ส่งเข้าไปประมวลผลและคำนวณ Gradient พร้อมกันในหนึ่งรอบย่อย
patience	20	กลไก Early Stopping หากค่าความแม่นยำบน Validation Set ไม่พัฒนาต่อเนื่อง 20 Epochs ระบบจะหยุดฝึกทันทีเพื่อป้องกัน Overfitting
device	"cpu" หรือ 0	ฮาร์ดแวร์ที่ใช้ประมวลผล (ใช้ "cpu" สำหรับเครื่องทั่วไป หรือระบุ 0 เมื่อใช้งานการ์ดจอ GPU เพื่อความเร็วที่สูงขึ้น)
workers	4	จำนวน Sub-processes (เธรด) ในการช่วยโหลดและเตรียมข้อมูลภาพเข้าสู่หน่วยความจำ
project & name	runs_face/yolo_face	ไดเรกทอรีสำหรับบันทึกผลลัพธ์ กราฟสถิติ และไฟล์น้ำหนักโมเดล
pretrained	True	นำค่าน้ำหนักที่ผ่านการฝึกจากฐานข้อมูลขนาดใหญ่มาเป็นจุดเริ่มต้น (Transfer Learning) ช่วยลดเวลาและเพิ่มความแม่นยำ
seed & deterministic	42 / True	กำหนดค่าสุ่มตั้งต้น เพื่อให้ผลการฝึกสามารถทดลองซ้ำแล้วได้ผลลัพธ์ตรงกัน (Reproducibility)
plots	True	สร้าง บันทึกภาพกราฟแสดงประสิทธิภาพ เช่น Loss Curves, Confusion Matrix, Precision-Recall Curve อัตโนมัติ

4) ผลลัพธ์หลังเสร็จสิ้นกระบวนการ (Expected Artifacts)

เมื่อฝึกแบบจำลองจนเสร็จสิ้น ระบบจะสร้างโฟลเดอร์ runs_face/yolo_face/ ซึ่งบรรจุไฟล์สำคัญ ดังนี้:

- weights/best.pt: ไฟล์น้ำหนักแบบจำลองที่ให้ค่าความแม่นยำบน validation set ดีที่สุด (นำไฟล์นี้ไปใช้ในช่วงการ Deployment)
- weights/last.pt: ไฟล์น้ำหนักแบบจำลองที่ epoch สุดท้ายของการฝึก
- results.png & confusion_matrix.png: กราฟสรุปค่า loss, precision, recall, F1-score และ confusion matrix เพื่อนำไปใช้รายงานผลทางวิชาการ

5) กำหนดอุปกรณ์ประมวลผล

```
device="cpu"
```

หรือ GPU หมายเลข 0

```
device=0
```

8.3.8 การตรวจสอบผลการฝึก

หลังฝึกเสร็จ ไฟล์สำคัญมักอยู่ในโฟลเดอร์

```
runs_face/yolo_face/
```

และค่าน้ำหนักอยู่ที่

```
runs_face/yolo_face/weights/best.pt
runs_face/yolo_figure/weights/last.pt
```

ควรใช้ best.pt สำหรับการทดสอบ เพราะเป็นแบบจำลองที่ให้ผล validation เหมาะสมที่สุด ไม่จำเป็นต้องเป็น epoch สุดท้าย

1) การประเมินด้วย validation set

สร้างไฟล์ validate_face.py

```
from pathlib import Path

from ultralytics import YOLO

def main() -> None:
    weights = Path("runs_face/yolo_face/weights/best.pt")
    data_file = Path("face_dataset/data.yaml")

    if not weights.exists():
        raise FileNotFoundError(f"Model not found:
{weights.resolve()}")

    model = YOLO(str(weights))

    metrics = model.val(
        data=str(data_file),
        split="test",
        imgsz=640,
        conf=0.25,
        iou=0.50,
        plots=True,
    )

    print(f"mAP50: {metrics.box.map50:.4f}")
    print(f"mAP50-95: {metrics.box.map:.4f}")
    print(f"Precision: {metrics.box.mp:.4f}")
    print(f"Recall: {metrics.box.mr:.4f}")

if __name__ == "__main__":
    main()
```

2) ตัวชี้วัดที่ควรพิจารณา

2.1) Precision

Precision สูงหมายถึง เมื่อระบบแจ้งว่าพบใบหน้า ส่วนใหญ่เป็นใบหน้าจริง และมี FP ต่ำ

2.2) Recall

Recall สูงหมายถึง ระบบตรวจพบใบหน้าจริงได้เป็นสัดส่วนมาก และพลาดใบหน้าน้อย

2.3) IoU

IoU ใช้วัดความใกล้เคียงระหว่าง bounding box ที่ระบบทำนายกับกรอบ ground truth

2.4) mAP

mAP สรุปคุณภาพของการตรวจจับจาก precision–recall ภายใต้เกณฑ์ IoU หนึ่งค่าหรือหลายค่า เช่น mAP50 และ mAP50–95

8.3.9 การตรวจสอบการทำงานของกล้องก่อนนำไปใช้กับ YOLO

ก่อนเข้าสู่ขั้นตอนการตรวจจับวัตถุหรือใบหน้าแบบเรียลไทม์ (real-time inference) จำเป็นต้องทดสอบการเชื่อมต่อและดึงสัญญาณภาพจากกล้อง (video stream) ด้วยโมดูล OpenCV (cv2) เพื่อยืนยันความพร้อมของฮาร์ดแวร์และสิทธิ์การเข้าถึงอุปกรณ์

1) โค้ดโปรแกรมทดสอบกล้อง (test_camera.py)

```
import cv2

def main() -> None:
    camera = cv2.VideoCapture(0)

    if not camera.isOpened():
        raise RuntimeError(
            "Cannot open camera. Check camera index, cable, and
permission."
        )

    try:
        while True:
            ok, frame = camera.read()

            if not ok:
                print("Unable to read a frame.")
                break

            cv2.imshow("Camera Test", frame)

            # Press q to exit.
            if cv2.waitKey(1) & 0xFF == ord("q"):
                break

    finally:
        camera.release()
        cv2.destroyAllWindows()

if __name__ == "__main__":
    main()
```

2) คำสั่งเรียกใช้งาน (execution)

รันคำสั่งผ่าน command line/terminal

```
python detect_face_camera.py
```

จากนั้นกด q เพื่อปิดโปรแกรม

หากกล้องไม่เปิด ให้ทดลองเปลี่ยน

`cv2.VideoCapture(0)` **เป็น** `cv2.VideoCapture(1)` **(กรณีที่มีหลายกล้อง)**

3) คำอธิบายการทำงานและฟังก์ชันสำคัญ

- cv2.VideoCapture(index): ใช้สร้างออบเจกต์เพื่อเชื่อมต่อกับกล้อง
  0 หมายถึง กล้องตัวแรก (default camera) เช่น เว็บแคมในตัวโน้ตบุ๊ก
  1, 2 หมายถึง กล้องภายนอก (external USB camera) หรือกล้องตัวถัดไป
- camera.isOpened(): ตรวจสอบว่าระบบปฏิบัติการอนุญาตและสามารถเปิดกล้องได้หรือไม่ หากเปิดไม่ได้จะส่งข้อความแจ้งเตือน RuntimeError
- camera.read(): คืนค่า 2 ตัวแปร
  ok (Boolean): สถานะการอ่านเฟรม (true = สำเร็จ, false = ขัดข้อง)
  frame (NumPy Array): ข้อมูลภาพในรูปแมทริกซ์สี BGR
- cv2.waitKey(1) & 0xFF == ord("q"): ดักจับอีเวนต์การกดแป้นพิมพ์ หากกดแป้นพิมพ์ "q" จะหลุดจากลูปทันที
- บล็อก finally: เป็นการเขียนโค้ดตามแนวทาง clean code เพื่อรับประกันว่าแม้โปรแกรมจะเกิดข้อผิดพลาด ระบบจะทำคำสั่ง
  camera.release() เพื่อคืนสิทธิ์การใช้งานกล้องให้ระบบปฏิบัติการเสมอ
  cv2.destroyAllWindows() เพื่อปิดหน้าต่าง GUI ทั้งหมด

4) แนวทางการแก้ไขปัญหาเมื่อกล้องไม่ทำงาน (troubleshooting)

เมื่อกล้องไม่ทำงาน หลัก ๆ ปัญหาที่พบและแนวทางแก้ไข แสดงดังตารางที่ 8.4

ตารางที่ 8.4 ปัญหาที่พบและแนวทางแก้ไขเมื่อไม่สามารถเปิดกล้องกล้องไม่ทำงาน

ปัญหาที่พบ	สาเหตุที่เป็นไปได้	แนวทางแก้ไข
เปิดกล้องไม่สำเร็จ (Cannot open camera)	ดัชนีกล้อง (Index) ไม่ตรงกับพอร์ตที่เสียบ	เปลี่ยน cv2.VideoCapture(0) เป็น 1 หรือ 2
หน้าต่างไม่แสดงภาพ / จอดำ	อุปกรณ์อื่นกำลังใช้งานกล้องอยู่	ปิดโปรแกรมอื่นที่ใช้กล้อง (เช่น Zoom, Teams หรือหน้าต่าง Python อื่น)
Permission Denied	ระบบปฏิบัติการไม่อนุญาตให้แอปเข้าถึงกล้อง	ตรวจสอบการตั้งค่าความเป็นส่วนตัว (Privacy Settings) ของWindows/macOS/ Linux เพื่ออนุญาตสิทธิ์การเข้าถึงกล้อง
ภาพหน่วงหรือเปิดช้า	แบนด์วิดท์ของพอร์ต USB หรือการตั้งค่า Driver	เปลี่ยนช่องเสียบ USB (แนะนำพอร์ต USB 3.0) หรือกำหนด Backend เช่น cv2.VideoCapture(0, cv2.CAP_DSHOW) บนระบบ Windows

8.3.10 การทำงานภายในโปรแกรม

1) เปิดกล้อง ใช้คำสั่ง

```
camera = cv2.VideoCapture(0)
```

ในที่นี้ระบบเชื่อมต่อกล้องหมายเลข 0 ซึ่งโดยทั่วไปคือกล้องหลัก

2) อ่านภาพ

```
ok, frame = camera.read()
```

กล้องส่งภาพออกมาเป็นเฟรมต่อเนื่อง “ok” ระบุว่าสามารถอ่านภาพได้หรือไม่

3) ส่งเฟรมเข้าสู่ YOLO

```
results = model.predict(
    source=frame,
    imgsz=640,
    conf=0.40,
    iou=0.50,
    verbose=False,
)
```

YOLO จะดำเนินการหลัก ได้แก่

3.1) ปรับขนาดและเตรียมภาพ

3.2) ส่งภาพผ่านโครงข่ายประสาท

3.3) ทำนายกรอบและค่าความเชื่อมั่น

3.4) กรองกรอบที่มีค่าต่ำกว่า confidence threshold

3.5) ใช้ non-maximum suppression เพื่อลบกรอบซ้ำ

4) อ่านผลลัพธ์

ผลลัพธ์ของแต่ละกรอบประกอบด้วย

```
result.boxes.xyxy
result.boxes.conf
result.boxes.cls
```

- xyxy คือ พิกัดซ้ายบนและขวาล่าง
- conf คือ ค่าความเชื่อมั่น
- cls คือ หมายเลขคลาส

5) วาดกรอบ

```
annotated_frame = result.plot()
```

คำสั่งนี้สร้างภาพที่มี bounding box, label และ confidence score

6) แสดงผล

```
cv2.imshow("YOLO Face Detection", annotated_frame)
```

ภาพถูกแสดงอย่างต่อเนื่องจนผู้ใช้กด q

8.3.11 การวาดกรอบด้วยตนเอง

หากต้องการควบคุมข้อความ สี หรือรูปแบบกรอบ สามารถอ่านค่าจาก result.boxes ได้โดยตรง

```
from pathlib import Path

import cv2
from ultralytics import YOLO

MODEL_PATH = Path("runs_face/yolo_face/weights/best.pt")

def main() -> None:
    model = YOLO(str(MODEL_PATH))
    camera = cv2.VideoCapture(0)

    if not camera.isOpened():
        raise RuntimeError("Camera cannot be opened.")

    try:
        while True:
            ok, frame = camera.read()

            if not ok:
                break

            result = model.predict(
                frame,
                conf=0.40,
                iou=0.50,
                imgsz=640,
                verbose=False,
            )[0]

            if result.boxes is not None:
                for box in result.boxes:
                    x1, y1, x2, y2 = map(
                        int,
                        box.xyxy[0].tolist(),
                    )

                    confidence = float(box.conf[0])

                    cv2.rectangle(
                        frame,
                        (x1, y1),
                        (x2, y2),
                        (0, 255, 0),
                        2,
                    )

                    label = f"Face {confidence:.2f}"

                    cv2.putText(
                        frame,
                        label,
                        (x1, max(y1 - 10, 20)),
                        cv2.FONT_HERSHEY_SIMPLEX,
                        0.7,
                        (0, 255, 0),
                        2,
```

```
                    cv2.LINE_AA,
                )

            cv2.imshow("Face Detection", frame)

            if cv2.waitKey(1) & 0xFF == ord("q"):
                break
    finally:
        camera.release()
        cv2.destroyAllWindows()

if __name__ == "__main__":
    main()
```

8.3.12 การบันทึกภาพเมื่อพบใบหน้า

สามารถเพิ่มการบันทึกหลักฐานเมื่อระบบตรวจพบใบหน้า

```
from datetime import datetime
from pathlib import Path

import cv2
from ultralytics import YOLO

MODEL_PATH = Path("runs_face/yolo_face/weights/best.pt")
OUTPUT_DIRECTORY = Path("detected_faces")

def main() -> None:
    OUTPUT_DIRECTORY.mkdir(parents=True, exist_ok=True)

    model = YOLO(str(MODEL_PATH))
    camera = cv2.VideoCapture(0)

    if not camera.isOpened():
        raise RuntimeError("Camera cannot be opened.")

    last_saved_time = 0.0
    minimum_save_interval = 5.0

    try:
        while True:
            ok, frame = camera.read()

            if not ok:
                break

            result = model.predict(
                frame,
                conf=0.50,
                imgsz=640,
                verbose=False,
            )[0]

            annotated = result.plot()
            face_count = len(result.boxes) if result.boxes is not None
else 0

            current_time = datetime.now().timestamp()

            if (
                face_count > 0
```

```
                and current_time - last_saved_time >=
minimum_save_interval
            ):
                timestamp = datetime.now().strftime("%Y%m%d_%H%M%S")
                output_file = OUTPUT_DIRECTORY /
f"face_{timestamp}.jpg"

                if not cv2.imwrite(str(output_file), annotated):
                    print(f"Unable to save: {output_file}")
                else:
                    print(f"Saved: {output_file}")

                last_saved_time = current_time

            cv2.imshow("Face Detection and Capture", annotated)

            if cv2.waitKey(1) & 0xFF == ord("q"):
                break

    finally:
        camera.release()
        cv2.destroyAllWindows()

if __name__ == "__main__":
    main()
```

การกำหนดช่วงเวลาอย่างน้อย 5 s ช่วยไม่ให้ระบบบันทึกภาพทุกเฟรมจนมีไฟล์จำนวนมากเกินไป

8.3.13 การเพิ่มการแจ้งเตือนของระบบตรวจจับใบหน้าด้วย YOLO

หลักการทำงานของระบบตรวจจับใบหน้าด้วย YOLO และการแจ้งเตือน แสดงดังรูปที่ 8.6 กระบวนการทำงานหลังจากนำแบบจำลองตระกูล YOLO ที่ผ่านการฝึกสำหรับคลาสใบหน้า (face) มาใช้งานกับภาพจากกล้องแบบเวลาจริง โดยมีวัตถุประสงค์เพื่อไม่ให้ระบบรักษาความปลอดภัยส่งสัญญาณเตือนทันทีที่ตรวจพบใบหน้าเพียงครั้งเดียว แต่เพิ่มเงื่อนไขสำหรับตรวจสอบความน่าเชื่อถือของเหตุการณ์ก่อนดำเนินการแจ้งเตือน ซึ่งช่วยลดการแจ้งเตือนผิดพลาด (false alarm) กระบวนการทำงานประกอบด้วยขั้นตอนสำคัญดังนี้

1) รับภาพจากกล้องแบบเวลาจริง (Real-time Camera Input)

ระบบเริ่มจากรับข้อมูลวิดีโอจากกล้อง โดยวิดีโอจะถูกอ่านเป็นภาพแต่ละเฟรม (frame) อย่างต่อเนื่อง จากนั้นเฟรมจะถูกเตรียมให้อยู่ในรูปแบบที่เหมาะสมกับแบบจำลอง เช่น การปรับขนาดภาพและการแปลงข้อมูลก่อนส่งเข้าสู่แบบจำลอง YOLO

2) ตรวจจับใบหน้าด้วย YOLO (Face Detection)

แต่ละเฟรมถูกส่งเข้าสู่แบบจำลอง YOLO ที่ฝึกให้ตรวจจับคลาส face แบบจำลองจะทำนายตำแหน่งของใบหน้าที่พบในภาพในรูปของ bounding box พร้อมคลาสและconfidence score ซึ่งแสดงระดับความเชื่อมั่นของแบบจำลองต่อการตรวจจับนั้น โดยจุดนี้ต้องแยกให้ชัดเจนว่า face detection เป็นการค้นหาตำแหน่งของใบหน้า ไม่ใช่ face recognition ดังนั้นผลจากขั้นตอนนี้ยังไม่สามารถระบุได้ว่าบุคคลในภาพคือใคร

3) ตรวจสอบค่า Confidence

ผลการตรวจจับจะถูกเปรียบเทียบกับค่าเกณฑ์ความเชื่อมั่นที่กำหนดไว้ หรือ confidence threshold โดยสามารถเขียนเงื่อนไขได้เป็น

$$C \geq T_C \tag{8.6}$$

เมื่อ C คือ confidence score ของการตรวจจับ และ T_C คือ confidence threshold

หาก confidence ต่ำกว่าเกณฑ์ ระบบจะไม่นำผลดังกล่าวไปดำเนินการต่อ เนื่องจากมีความน่าเชื่อถือไม่เพียงพอ แต่หากผ่านเกณฑ์จึงเข้าสู่ขั้นตอนตรวจสอบต่อไป ส่วนค่า threshold ไม่ควรกำหนดโดยไม่มีการทดลอง แต่ควรเลือกจากผลการประเมินบน validation set โดยพิจารณาความสัมพันธ์ระหว่าง precision, recall, FP และ FN ให้เหมาะกับวัตถุประสงค์ของระบบรักษาความปลอดภัย

4) ตรวจสอบการปรากฏต่อเนื่องหลายเฟรม (multi-frame verification)

แม้การตรวจจับในเฟรมหนึ่งจะมี confidence สูง ก็ยังไม่ควรสรุปทันทีว่าเป็นเหตุการณ์ที่ต้องแจ้งเตือน เนื่องจากอาจเป็นการตรวจจับผิดชั่วขณะ ระบบจึงตรวจสอบว่าใบหน้าถูกตรวจพบอย่างต่อเนื่องในหลายเฟรมหรือไม่ ตัวอย่างเช่น อาจกำหนดให้ตรวจพบใบหน้าอย่างน้อย 3 เฟรมจาก 5 เฟรมล่าสุด ก่อนยืนยันเหตุการณ์ ซึ่งแนวคิดนี้มีประโยชน์ต่อระบบ smart security เพราะช่วยลดผลกระทบจากการตรวจจับผิดเพียงเฟรมเดียว แต่จำนวนเฟรมที่เหมาะสมต้องทดลองกับระบบจริง เนื่องจากการกำหนดจำนวนมากเกินไปจะเพิ่มเวลาแฝง (latency) และอาจทำให้ระบบพลาดบุคคลที่เคลื่อนผ่านกล้องอย่างรวดเร็ว

5) ตรวจสอบพื้นที่และช่วงเวลา (ROI and Time Window)

เมื่อยืนยันการตรวจจับแล้ว ระบบตรวจสอบบริบทของเหตุการณ์เพิ่มเติม ได้แก่ Region of Interest (ROI) และ time window โดย ROI หมายถึงพื้นที่ในภาพที่กำหนดให้เป็นบริเวณเฝ้าระวัง เช่น ทางเข้า ประตู เขตหวงห้าม บริเวณหน้าอาคาร ส่วน time window หมายถึงช่วงเวลาที่กำหนดให้ระบบเฝ้าระวังเป็นพิเศษ เช่น หลังเวลาปิดอาคาร ดังนั้นการพบใบหน้าไม่ได้หมายความว่าจะต้องแจ้งเตือนทุกกรณี เช่น บุคคลเดินอยู่ในพื้นที่สาธารณะช่วงเวลาทำการอาจเป็นเหตุการณ์ปกติ แต่บุคคลเข้าสู่เขตหวงห้ามในเวลากลางคืนอาจเข้าเงื่อนไขที่ต้องแจ้งเตือน

6) บันทึกเหตุการณ์ (Event Logging)

หากตรวจพบใบหน้าอย่างน่าเชื่อถือ แต่เหตุการณ์ ไม่เข้าเงื่อนไข ROI และ/หรือ time window ที่กำหนด ตามตรรกะของภาพ ระบบจะไม่ส่งสัญญาณเตือน แต่บันทึก log เพื่อใช้ตรวจสอบย้อนหลัง เช่น วันและเวลา ตำแหน่งกล้อง confidence score และประเภทเหตุการณ์ การแยก event logging ออกจาก alert มีความสำคัญ เพราะไม่ใช่ทุกเหตุการณ์ที่ระบบตรวจพบจะต้องถือเป็นภัยคุกคาม

7) บันทึกภาพหลักฐาน (Save Snapshot)

หากการตรวจจับผ่าน confidence threshold ผ่านการตรวจสอบหลายเฟรม และอยู่ภายในพื้นที่กับช่วงเวลาที่กำหนด ระบบจะบันทึกภาพเหตุการณ์ไว้เป็นหลักฐาน ซึ่งในระบบจริง

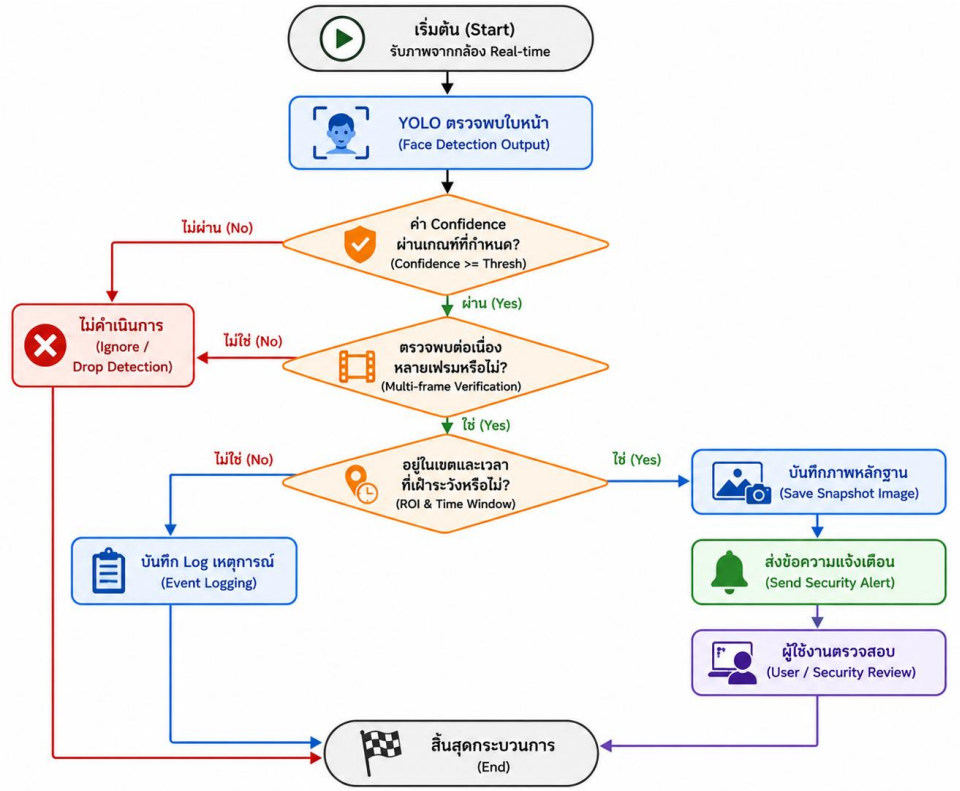
ควรบันทึกข้อมูลประกอบ เช่น timestamp, camera ID, bounding box และ confidence score เพื่อสนับสนุนการตรวจสอบย้อนหลัง ทั้งนี้ การจัดเก็บภาพใบหน้าต้องคำนึงถึงข้อกำหนดด้านข้อมูลส่วนบุคคลและกำหนดระยะเวลาการเก็บรักษาอย่างเหมาะสม

8) ส่งการแจ้งเตือน (Security Alert)

หลังยืนยันเหตุการณ์ ระบบจึงส่งการแจ้งเตือนไปยังผู้ใช้งานหรือเจ้าหน้าที่รักษาความปลอดภัย เช่น mobile application, dashboard, email หรือระบบ notification ที่กำหนดไว้ ซึ่งการออกแบบให้มีการตรวจสอบหลายเงื่อนไขก่อนแจ้งเตือนช่วยลดจำนวน false alarm เมื่อเทียบกับการกำหนดว่า “YOLO พบใบหน้า จะแจ้งเตือนทันที”

9) ผู้ใช้งานหรือเจ้าหน้าที่ตรวจสอบ (Human/Security Review)

ขั้นตอนสุดท้ายควรให้มนุษย์ตรวจสอบเหตุการณ์ก่อนดำเนินการที่มีผลกระทบสูง เนื่องจากผลจาก AI เป็นการทำนายและยังสามารถเกิด FP หรือ FN ได้ โดยหลักการนี้เรียกว่า human-in-the-loop กล่าวคือ AI ทำหน้าที่ตรวจจับ คัดกรอง และจัดลำดับเหตุการณ์ ขณะที่มนุษย์ยังคงมีบทบาทในการพิจารณาเหตุการณ์สำคัญและตัดสินใจขั้นสุดท้าย



รูปที่ 8.6 หลักการทำงานของระบบตรวจจับใบหน้าด้วย YOLO และการแจ้งเตือน

ดังนั้นจากรูปที่ 8.6 ไม่ได้แสดงเฉพาะขั้นตอน YOLO face detection แต่แสดง decision pipeline ของระบบ smart security หลังการตรวจจับ ซึ่งสามารถสรุปได้ว่ากระบวนการเริ่มจาก samera > YOLO face detection > confidence filtering > multi-frame verification > context verification (ROI & time) > evidence recording > alert > human review ซึ่งแนวคิดสำคัญคือ

“detection ≠ security event” กล่าวคือ การที่ YOLO ตรวจพบใบหน้าไม่ได้หมายความว่าเกิดภัยคุกคามทันที ระบบต้องนำผลการตรวจจับมาประเมินร่วมกับ ความเชื่อมั่น ความต่อเนื่องของการตรวจพบ พื้นที่ เวลา และกฎของระบบรักษาความปลอดภัย ก่อนสร้าง Alert วิธีนี้เหมาะสมกว่าการใช้ผลจาก AI เพียงเฟรมเดียวเป็นตัวตัดสินเหตุการณ์

8.3.14 การปรับค่า Confidence และ IoU

1) Confidence Threshold ค่าต่ำ เช่น

```
conf=0.20
```

อาจตรวจพบใบหน้าได้มากขึ้น แต่มี False Positive มากขึ้น ปรับเป็นค่าสูง เช่น

```
conf=0.70
```

ช่วยลดการตรวจผิด แต่เสี่ยงพลาดใบหน้าที่มืด เล็ก หรือถูกบัง และควรเลือกค่าจากผล validation และความเสี่ยงของระบบ ไม่ควรเลือกจากความรู้สึกเพียงอย่างเดียว

2) IoU Threshold สำหรับ NMS

หากตรวจพบกรอบซ้อนหลายกรอบรอบใบหน้าเดียวกัน ค่า IoU threshold มีผลต่อการตัดกรอบซ้ำ

```
iou=0.50
```

เป็นจุดเริ่มต้นที่เหมาะสม แต่ต้องทดสอบกับภาพที่มีใบหน้าอยู่ใกล้กัน เพราะค่าไม่เหมาะสมอาจลบกรอบของใบหน้าคนละคน

8.3.15 การเพิ่มความเร็วของการประมวลผลข้อมูล

แนวทางเพิ่มความเร็ว ได้แก่

1) ใช้แบบจำลองขนาด Nano
2) ลด imgsz จาก 640 เป็น 512 หรือ 416
3) ลดความละเอียดกล้อง
4) ประมวลผลทุกสองหรือสามเฟรม
5) ใช้ GPU
6) Export เป็น ONNX หรือ TensorRT
7) ใช้ tracking เพื่อไม่ต้องตรวจจับเต็มรูปแบบทุกเฟรม
8) ประมวลผลเฉพาะ RoI

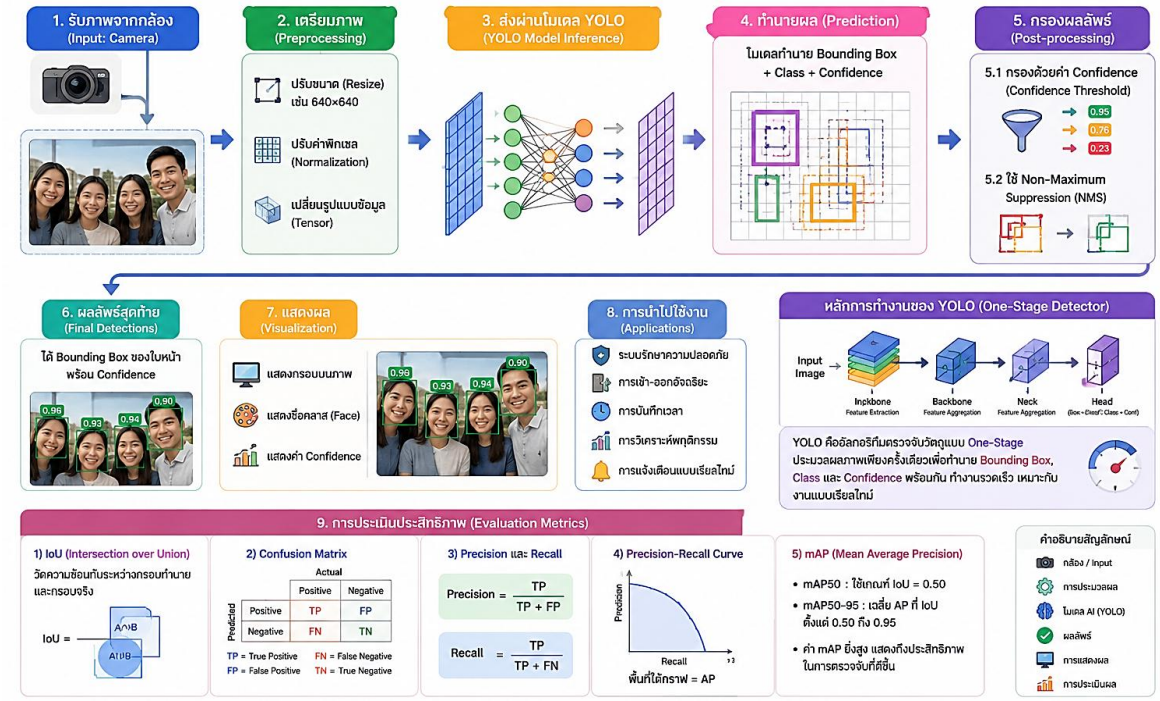
ตัวอย่างประมวลผลทุกสองเฟรม

```
frame_index = 0
last_result = None
while True:
    ok, frame = camera.read()

    if not ok:
        break

    frame_index += 1
```

```
if frame_index % 2 == 0:
    last_result = model.predict(
        frame,
        conf=0.40,
        imgsz=640,
        verbose=False,
    )[0]

if last_result is not None:
    displayed_frame = last_result.plot()
else:
    displayed_frame = frame

cv2.imshow("Face Detection", displayed_frame)
```

8.3.16 ข้อควรระวังด้านความเป็นส่วนตัว

ใบหน้าเป็นข้อมูลชีวมิติที่มีความอ่อนไหว การพัฒนาระบบควรดำเนินการดังนี้ (1) แจ้งวัตถุประสงค์ในการติดตั้งกล้อง (2) ขอความยินยอมตามความเหมาะสม (3) เก็บข้อมูลเท่าที่จำเป็น (4) จำกัดสิทธิ์เข้าถึง (5) เข้ารหัสข้อมูล (6) กำหนดระยะเวลาลบภาพ (7) ไม่เผยแพร่ข้อมูลใบหน้าโดยไม่ได้รับอนุญาต (8) บันทึกการเข้าถึงและการแก้ไขข้อมูล และ (9) หลีกเลี่ยงการนำภาพไปใช้ต่างจากวัตถุประสงค์เดิม โดยหากระบบทำเพียง face detection และไม่มีความจำเป็นต้องเก็บภาพ ควรประมวลผลบนอุปกรณ์ Edge แล้วเก็บเฉพาะจำนวนหรือเหตุการณ์ แทนการส่งวิดีโอทั้งหมดขึ้น cloud สถาปัตยกรรม Edge–cloud สามารถช่วยลด latency และลดการส่งข้อมูลชีวมิติออกจากอุปกรณ์ได้ (Ali et al., 2026)



รูปที่ 8.7 การตรวจจับใบหน้าด้วยสถาปัตยกรรม YOLO และการประเมินประสิทธิภาพ

บรรณานุกรมบทที่ 8

Ali, F. A., Mali, S., Mahakud, R., & Yadav, G. (2026). AI-enabled smart surveillance system for secure monitoring and authentication. *Scientific Reports, 16*, 21686. https://doi.org/10.1038/s41598-026-52387-w.

Al Sharah, A., Alawneh, T. A., Abu Owida, H., Alkasassbeh, J. S., & Iqbal, Z. (2025). Artificial intelligence in smart home security: Balancing innovation with ethics. *Bulletin of Electrical Engineering and Informatics, 14*(6), 4601–4613. https://doi.org/10.11591/eei.v14i6.9674.

Jocher, G., Qiu, J., Liu, M., Lyu, S., Akyon, F. C., & Kalfaoglu, M. E. (2026). *Ultralytics YOLO26: Unified real-time end-to-end vision models*. arXiv. https://doi.org/10.48550/arXiv.2606.03748.

Lendák, I., & Kiss, P. (2026). *Introduction to artificial intelligence security*. Faculty of Informatics, Eötvös Loránd University.

Morales Cauti, G. P., Ypanaque-Pereira, I. L., Vargas-Murillo, A. R., & Guevara-Soto, F. de J. (2023). Intelligent video surveillance: Artificial intelligence and its applications on security systems. In *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 986–991). IEEE. https://doi.org/10.1109/ICOSEC58147.2023.10275947.

Muhammad, R., Sagara, M. S. A., Teluma, Y. M., & Wicaksana, F. A. (2025). AI as modern technology for home security systems: A systematic literature review. *Engineering Proceedings, 107*, Article 35. https://doi.org/10.3390/engproc2025107035.

Qi, D., Tan, W., Yao, Q., & Liu, J. (2021). *YOLO5Face: Why reinventing a face detector?* arXiv. https://doi.org/10.48550/arXiv.2105.12931.

Radovanovic, D., Savanovic, N., Janackovic, J., & Kresoja, P. (2026). A systematic review of smart home IoT security: Applications, threat taxonomy, privacy risks, and emerging defensive solutions. *Big Data and Cognitive Computing, 10*(8), Article 252. https://doi.org/10.3390/bdcc10080252.

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 779–788). IEEE. https://doi.org/10.1109/CVPR.2016.91.

Sabit, H. (2025). Artifical intelligence-based smart security system using Internet of Things for smart home applications. *Electronics, 14*(3), 608. https://doi.org/10.3390/electronics14030608.

Ultralytics. (2023). *Ultralytics YOLO documentation*. https://docs.ultralytics.com/.

Yu, S., Wang, Y., Huang, H., & Deng, W. (2024). YOLO-FaceV2: A scale and occlusion aware face detector. *Pattern Recognition, 155*, 110714. https://doi.org/10.1016/j.patcog.2024.110714.

สรุปสาระสำคัญของบทที่ 8
ปัญญาประดิษฐ์สำหรับระบบรักษาความปลอดภัย

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) สำหรับระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security)

โดย AI ช่วยให้ระบบคอมพิวเตอร์สามารถเรียนรู้ วิเคราะห์ ให้เหตุผล ตัดสินใจ และตอบสนองต่อเหตุการณ์ต่าง ๆ จากข้อมูลที่ได้รับจากกล้องวงจรปิด เซ็นเซอร์ และอุปกรณ์ Internet of Things (IoT) ผ่านเทคโนโลยีสำคัญ ได้แก่ Machine Learning (ML), deep learning, computer vision และ Natural Language Processing (NLP) ทำให้ระบบรักษาความปลอดภัยเปลี่ยนจากการเฝ้าระวังแบบรับเหตุการณ์ที่อาศัยมนุษย์เป็นหลัก ไปสู่ระบบเชิงรุกที่สามารถวิเคราะห์ข้อมูลแบบเรียลไทม์ ตรวจจับบุคคลและวัตถุ วิเคราะห์พฤติกรรม ตรวจจับความผิดปกติ ประเมินความเสี่ยง และแจ้งเตือนได้โดยอัตโนมัติ ส่งผลให้ตอบสนองต่อภัยคุกคามได้รวดเร็วและลดการแจ้งเตือนที่ผิดพลาด

ส่วนสำคัญของบทคือ Machine Learning (ML)

ซึ่งเป็นกระบวนการที่ทำให้ระบบเรียนรู้รูปแบบจากข้อมูลและนำความรู้ไปใช้ในการทำนาย จำแนก และตัดสินใจ โดยสามารถประยุกต์ใช้กับการตรวจจับการบุกรุก การจำแนกบุคคล การวิเคราะห์พฤติกรรม การประเมินความเสี่ยง และการตรวจจับเหตุการณ์ผิดปกติ การพัฒนาแบบจำลองต้องดำเนินการอย่างเป็นระบบตั้งแต่การกำหนดปัญหา รวบรวมและตรวจสอบคุณภาพข้อมูล กำกับข้อมูล (annotation) เตรียมข้อมูล แบ่งข้อมูลเป็น training, validation และ test set เลือกและฝึกแบบจำลอง ปรับ hyperparameters ประเมินผล และนำแบบจำลองไปใช้งานจริง โดยต้องระวังปัญหา data leakage และ overfitting เพื่อให้ผลการประเมินสะท้อนความสามารถของแบบจำลองอย่างแท้จริง การประเมินประสิทธิภาพไม่ควรพิจารณาเพียง accuracy แต่ควรใช้ตัวชี้วัดที่เหมาะสม เช่น precision, recall, F1-score, Intersection over Union (IoU) และ Mean Average Precision (mAP) โดยเฉพาะงานตรวจจับวัตถุและใบหน้า ซึ่ง mAP สามารถสะท้อนทั้งความถูกต้องในการจำแนกและตำแหน่งของ bounding box ได้

การประยุกต์ใช้ YOLO (You Only Look Once)

สำหรับการตรวจจับใบหน้าจากกล้องแบบเรียลไทม์ โดยเน้นให้แยกความแตกต่างระหว่าง face detection ซึ่งเป็นการค้นหาและระบุตำแหน่งของใบหน้า กับ face recognition ซึ่งเป็นการระบุตัวบุคคล ระบบต้องเตรียมชุดข้อมูลใบหน้าที่หลากหลาย กำกับ bounding box แบ่งชุดข้อมูล ฝึกและประเมินแบบจำลอง ก่อนนำโมเดลที่เหมาะสมไปเชื่อมต่อกับกล้องเพื่อประมวลผลภาพจริง การนำผลตรวจจับไปใช้ในระบบรักษาความปลอดภัยไม่ควรแจ้งเตือนทันทีเมื่อ AI ตรวจพบวัตถุหรือใบหน้า แต่ควรตรวจสอบค่า confidence ความต่อเนื่องของการตรวจพบหลายเฟรม พื้นที่เฝ้าระวัง

และช่วงเวลา บันทึกหลักฐาน แล้วจึงส่งการแจ้งเตือน พร้อมให้มนุษย์ตรวจสอบเหตุการณ์สำคัญก่อนตัดสินใจขั้นสุดท้าย เพื่อช่วยลด false alarm และเพิ่มความน่าเชื่อถือของระบบ

อย่างไรก็ตาม การนำ AI มาใช้ด้านความปลอดภัยยังต้องคำนึงถึง ความเป็นส่วนตัว ความปลอดภัยของข้อมูลชีวมิติ ความแม่นยำของการรู้จำใบหน้า อคติของแบบจำลอง ความโปร่งใสในการตัดสินใจ ภัยคุกคามทางไซเบอร์ และต้นทุนในการพัฒนาและบำรุงรักษา จึงควรมีมาตรการคุ้มครองข้อมูล การเข้ารหัส การยืนยันตัวตนและการควบคุมสิทธิ์อย่างเหมาะสม นอกจากนี้ ตัวระบบ AI เองต้องได้รับการป้องกันจากภัยคุกคาม เช่น data poisoning, adversarial input และการขโมยแบบจำลอง และต้องติดตามประสิทธิภาพหลังนำไปใช้งานอย่างต่อเนื่อง เพราะสภาพแวดล้อมและข้อมูลจริงสามารถเปลี่ยนแปลงได้ สำหรับข้อมูลใบหน้าซึ่งเป็นข้อมูลชีวมิติที่มีความอ่อนไหว ควรเก็บเฉพาะข้อมูลที่จำเป็น จำกัดสิทธิ์การเข้าถึง เข้ารหัส กำหนดระยะเวลาการเก็บรักษา และพิจารณาประมวลผลบน Edge เพื่อลดการส่งข้อมูลชีวมิติขึ้น cloud

โดยสรุป AI ทำให้ระบบรักษาความปลอดภัยมีความอัจฉริยะ รวดเร็ว และเป็นระบบมากขึ้น แต่ประสิทธิภาพของระบบไม่ได้ขึ้นอยู่กับแบบจำลอง AI เพียงอย่างเดียว หากขึ้นอยู่กับคุณภาพของข้อมูล การฝึกและประเมินแบบจำลอง การออกแบบเงื่อนไขการแจ้งเตือน ความปลอดภัยของระบบ การคุ้มครองข้อมูลส่วนบุคคล และการมีมนุษย์ร่วมตรวจสอบและตัดสินใจ เพื่อให้สามารถนำ AI ไปใช้ในระบบรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ น่าเชื่อถือ และเหมาะสมในทางจริยธรรม

แบบฝึกหัดท้ายบทที่ 8
ปัญญาประดิษฐ์สำหรับระบบรักษาความปลอดภัย

ตอนที่ 1 คำถามปรนัย

คำชี้แจง: จงเลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียว

1. ข้อใดอธิบายความหมายของปัญญาประดิษฐ์ในระบบรักษาความปลอดภัยอัจฉริยะได้ถูกต้องที่สุด
   ก. เทคโนโลยีที่ใช้สำหรับบันทึกภาพจากกล้องเท่านั้น
   ข. เทคโนโลยีที่ทำให้ระบบสามารถเรียนรู้ วิเคราะห์ ตัดสินใจ และตอบสนองต่อเหตุการณ์ได้
   ค. เทคโนโลยีที่ใช้สำหรับเพิ่มความเร็วของอินเทอร์เน็ต
   ง. ระบบที่ทำงานได้เฉพาะเมื่อมีเจ้าหน้าที่ควบคุมตลอดเวลา
2. เทคโนโลยีใดมีบทบาทสำคัญในการวิเคราะห์และตีความข้อมูลภาพและวิดีโอ
   ก. Computer Vision
   ข. Database Management
   ค. Spreadsheet
   ง. Web Hosting
3. ข้อใดเป็นตัวอย่างการประยุกต์ใช้ Machine Learning ในระบบ Smart Security
   ก. การจัดรูปแบบเอกสาร
   ข. การตรวจจับการบุกรุกและเหตุการณ์ผิดปกติ
   ค. การเพิ่มความละเอียดของหน้าจอ
   ง. การสำรองไฟฟ้าให้กล้องวงจรปิด
4. ชุดข้อมูลใดใช้สำหรับปรับค่าพารามิเตอร์ของแบบจำลองระหว่างการฝึก
   ก. Test Set
   ข. Validation Set
   ค. Training Set
   ง. Deployment Set
5. Validation Set มีหน้าที่สำคัญอย่างไร
   ก. ใช้บันทึกข้อมูลจากกล้องหลังติดตั้งระบบ
   ข. ใช้เลือกแบบจำลองและปรับ Hyperparameters
   ค. ใช้แทนข้อมูลทั้งหมดในการฝึกแบบจำลอง
   ง. ใช้เก็บภาพหลักฐานเท่านั้น
6. ข้อใดหมายถึงกรณีที่ระบบแจ้งเตือนว่าเกิดเหตุการณ์ แต่ในความเป็นจริงไม่มีเหตุการณ์เกิดขึ้น
   ก. True Positive
   ข. True Negative
   ค. False Positive
   ง. False Negative

7. ตัวชี้วัดใดตอบคำถามว่า “จากเหตุการณ์จริงทั้งหมด ระบบสามารถตรวจพบได้มากเพียงใด”

ก. Precision

ข. Recall

ค. IoU

ง. Latency

8. ค่า Intersection over Union (IoU) ใช้ประเมินสิ่งใด

ก. ความเร็วของเครือข่าย

ข. ความใกล้เคียงระหว่าง Bounding Box ที่ทำนายกับ Ground Truth

ค. จำนวนภาพใน Training Set

ง. ความเร็วของ CPU

9. Face Detection แตกต่างจาก Face Recognition อย่างไร

ก. Face Detection ระบุว่าเป็นบุคคลใด ส่วน Face Recognition ระบุตำแหน่งใบหน้า

ข. Face Detection ระบุตำแหน่งใบหน้า ส่วน Face Recognition ใช้ระบุตัวบุคคล

ค. ทั้งสองมีความหมายเหมือนกัน

ง. Face Detection ใช้ได้เฉพาะภาพนิ่งเท่านั้น

10. เหตุใดระบบรักษาความปลอดภัยจึงไม่ควรส่งสัญญาณเตือนทันทีเมื่อ YOLO ตรวจพบใบหน้าเพียงหนึ่งเฟรม

ก. เพราะ YOLO ไม่สามารถประมวลผลภาพได้แบบเรียลไทม์

ข. เพราะการตรวจพบอาจเป็น False Positive และควรตรวจสอบเงื่อนไขอื่นร่วมด้วย

ค. เพราะต้องบันทึกวิดีโออย่างน้อยหนึ่งชั่วโมงก่อนเสมอ

ง. เพราะระบบต้องส่งข้อมูลทั้งหมดไปยัง Cloud ก่อนทุกครั้ง

ตอนที่ 2 ให้เขียนคำถามตอบสั้น

11. อธิบายบทบาทของ AI ในระบบรักษาความปลอดภัยอัจฉริยะ พร้อมยกตัวอย่างการใช้งานอย่างน้อย 3 ตัวอย่าง

---

12. อธิบายความแตกต่างระหว่าง Machine Learning, Deep Learning และ Computer Vision ในบริบทของระบบ Smart Security

---

---

13. อธิบายความหมายและหน้าที่ของ Training Set, Validation Set และ Test Set พร้อมอธิบายว่าเหตุใดจึงต้องป้องกัน Data Leakage

14. Precision, Recall และ F1-score มีความหมายแตกต่างกันอย่างไร และเพราะเหตุใดงานรักษาความปลอดภัยจึงไม่ควรพิจารณา Accuracy เพียงค่าเดียว

15. อธิบายความหมายของ Overfitting พร้อมยกตัวอย่างวิธีลด Overfitting อย่างน้อย 3 วิธี

ตอนที่ 3 คำถามวิเคราะห์และประยุกต์ใช้

16. สถานการณ์การตรวจจับผู้บุกรุก

โรงงานแห่งหนึ่งต้องการติดตั้งระบบ AI เพื่อตรวจจับบุคคลที่เข้าสู่พื้นที่หวงห้ามหลังเวลา 22.00 น. และส่งภาพแจ้งเตือนไปยังเจ้าหน้าที่ ให้นักศึกษาออกแบบลำดับการทำงานของระบบตั้งแต่ **กล้องรับภาพ** > **AI ตรวจจับ** > **ประเมินเหตุการณ์** > **แจ้งเตือน** > **เจ้าหน้าที่ตรวจสอบ** พร้อมระบุเงื่อนไขอย่างน้อย 3 ข้อที่ควรใช้ก่อนส่งการแจ้งเตือน

17. การลด False Alarm

ระบบตรวจจับใบหน้าหน้าอาคารแจ้งเตือนบ่อยครั้งจากเงาคน ภาพโปสเตอร์ และวัตถุที่มีลักษณะคล้ายใบหน้า นักศึกษาจะปรับปรุงระบบเพื่อลด False Positive อย่างไร ให้อธิบายโดยพิจารณาอย่างน้อย 4 ประเด็น เช่น

1) Confidence Threshold
2) การตรวจสอบหลายเฟรม
3) Region of Interest
4) คุณภาพและความหลากหลายของข้อมูลฝึก
5) การปรับปรุงแบบจำลอง

18. การประเมินประสิทธิภาพแบบจำลอง

แบบจำลองตรวจจับใบหน้าระบบหนึ่งมีผลการทดสอบดังนี้

1) Precision = 0.92
2) Recall = 0.68
3) F1-score = 0.78

ให้นักศึกษาวิเคราะห์ว่าแบบจำลองดังกล่าวมีจุดแข็งและจุดอ่อนอย่างไร และหากนำไปใช้กับระบบรักษาความปลอดภัยที่ไม่ต้องการพลาดผู้บุกรุก ควรปรับปรุงด้านใดเป็นสำคัญ

19. ความปลอดภัยของ Machine Learning

สมมติว่าผู้โจมตีสามารถแทรกภาพที่ติด Label ผิดเข้าไปในชุดข้อมูลฝึก ทำให้ระบบเรียนรู้ว่าบุคคลที่ไม่ได้รับอนุญาตเป็นบุคคลที่ได้รับอนุญาต

1) การโจมตีดังกล่าวเรียกว่าอะไร

2) ส่งผลกระทบต่อระบบอย่างไร

3) เสนอวิธีป้องกันอย่างน้อย 4 วิธี

ระบบ AI เองจำเป็นต้องได้รับการป้องกัน เนื่องจากผู้โจมตีอาจโจมตีข้อมูล แบบจำลอง หรือผลลัพธ์ เช่น การทำ Data Poisoning หรือการสร้าง Adversarial Input

20. จริยธรรมและความเป็นส่วนตัว

มหาวิทยาลัยต้องการติดตั้งระบบตรวจจับใบหน้าบริเวณทางเข้าอาคารเรียนและจัดเก็บภาพทั้งหมดไว้บน Cloud เป็นเวลา 5 ปี ให้นักศึกษาวิเคราะห์ความเสี่ยงด้านความเป็นส่วนตัวและข้อมูลชีวมิติ พร้อมเสนอแนวทางการออกแบบระบบที่เหมาะสมอย่างน้อย 5 ข้อ ในการจัดการข้อมูลใบหน้า ควรคำนึงถึงการแจ้งวัตถุประสงค์ การเก็บข้อมูลเท่าที่จำเป็น การจำกัดสิทธิ์ การเข้ารหัส การกำหนดระยะเวลาการเก็บข้อมูล และการพิจารณาประมวลผลบน Edge เพื่อลดการส่งข้อมูลชีวมิติขึ้น Cloud

9 โครงงานระบบรักษาความปลอดภัยอัจฉริยะ

91 **ระบบกล้องโทรทัศน์วงจรปิด**

9.1.1 งานออกแบบติดตั้งกล้องโทรทัศน์วงจรปิด
9.1.2 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก
9.1.3 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบ IP/Network
9.1.4 งานติดตั้งและใช้งานกล้อง IP Camera

92 **ระบบควบคุมประตูอัจฉริยะด้วยเทคโนโลยี RFID**

9.2.1 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino
9.2.2 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID โดยใช้ NodeMCU ESP8266
9.2.3 งานประยุกต์ใช้ RFID ร่วมกับ IP Camera และ LINE Messaging API

93 **ระบบประตูอัจฉริยะด้วยเทคโนโลยีตรวจสอบลายนิ้วมือ**

9.3.1 งานควบคุมการเปิด–ปิดอุปกรณ์ด้วยเซนเซอร์ตรวจสอบลายนิ้วมือ
9.3.2 งานควบคุมการเข้า–ออกประตูด้วยลายนิ้วมือร่วมกับ RFID
9.3.3 งานติดตั้งเครื่องสแกนลายนิ้วมือสำหรับระบบควบคุมการเข้า–ออกประตู

94 **ระบบประตูอัจฉริยะด้วยเทคโนโลยีจดจำใบหน้า**

9.4.1 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า
9.4.2 งานประยุกต์ใช้ Google Cloud และ Google Sheets

95 **การประยุกต์ใช้เซนเซอร์ตรวจจับก๊าซ MQ–2 ในระบบความปลอดภัย**

9.5.1 งานตรวจจับก๊าซและควบคุมวาล์วก๊าซอัตโนมัติด้วยเซนเซอร์ MQ–2 และ NodeMCU ESP8266

บทที่ 9 โครงงานระบบรักษาความปลอดภัยอัจฉริยะ

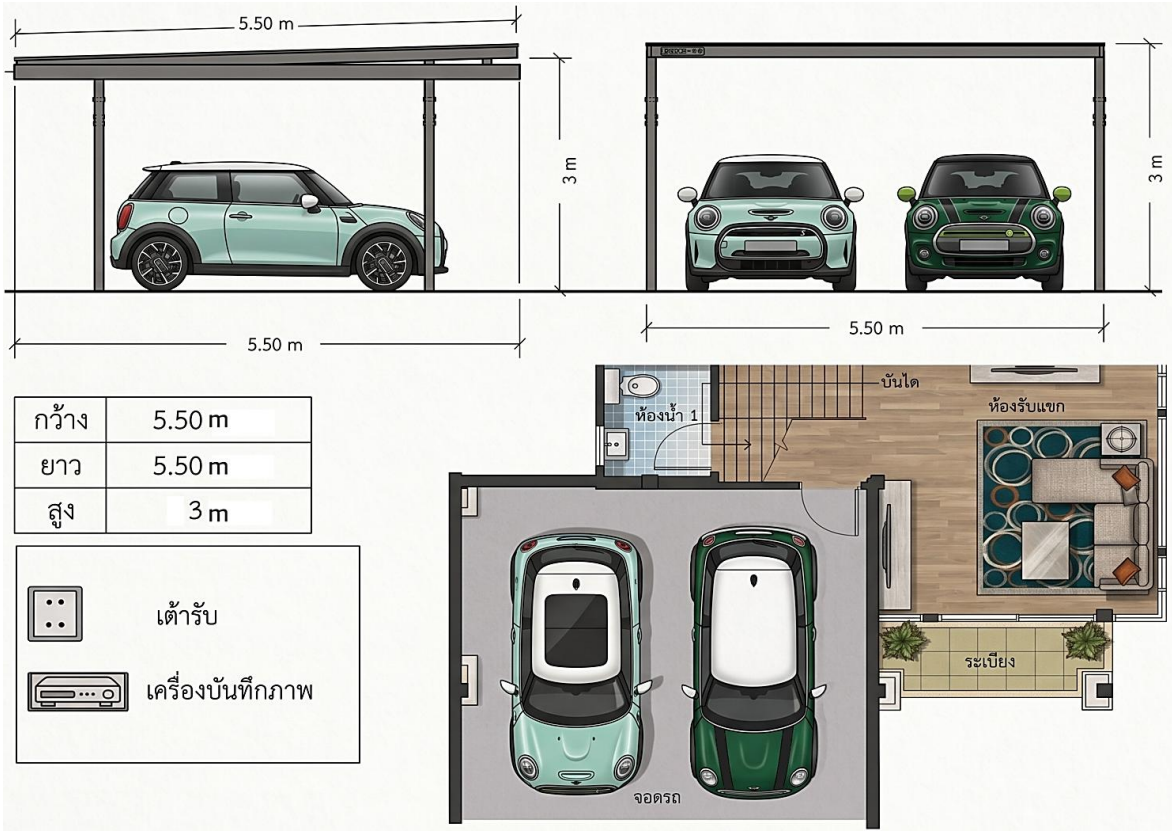
Smart Security System Projects

9.1 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิด

ระบบกล้องโทรทัศน์วงจรปิด เป็นระบบสำคัญสำหรับการเฝ้าระวังและบันทึกเหตุการณ์ในระบบรักษาความปลอดภัย การออกแบบระบบต้องพิจารณาลักษณะพื้นที่ วัตถุประสงค์ของการเฝ้าระวัง ตำแหน่งและมุมมองของกล้อง สภาพแสง ระยะการส่งสัญญาณ ตลอดจนรูปแบบการบันทึกและการเข้าถึงภาพ เพื่อให้ระบบสามารถครอบคลุมพื้นที่เป้าหมายและสนับสนุนการตรวจสอบเหตุการณ์ได้อย่างเหมาะสม

9.1.1 งานออกแบบติดตั้งกล้องโทรทัศน์วงจรปิด

งานนี้เป็นการประยุกต์หลักการออกแบบระบบกล้องโทรทัศน์วงจรปิดสำหรับเฝ้าระวังบริเวณโรงจอดรถ โดยกำหนดพื้นที่ตัวอย่างขนาด 5.50 × 5.50 × 3 m และใช้กล้องจำนวน 1 ตัว ดังรูปที่ 9.1 การออกแบบมีวัตถุประสงค์เพื่อให้กล้องสามารถตรวจสอบรถที่เข้า–ออกและเฝ้าระวังพื้นที่ภายในโรงจอดรถได้อย่างเหมาะสม รวมทั้งสามารถทำงานในสภาวะแสงน้อยและรองรับการดูภาพผ่านระบบเครือข่าย (ชลดา ปานสง และคณะ, 2561; ชลดา ปานสง และคณะ, 2566)



รูปที่ 9.1 แผนผังโรงจอดรถสำหรับออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด

การกำหนดตำแหน่งติดตั้งควรพิจารณาพื้นที่ครอบคลุม (coverage area) มุมมองของกล้อง (Field of View: FOV) ระดับความสูง ทิศทางการหันกล้อง สภาพแสง และบริเวณที่ต้องการเฝ้าระวังเป็นสำคัญ เพื่อให้สามารถบันทึกเหตุการณ์ที่เกี่ยวข้องได้อย่างชัดเจนและลดจุดอับของภาพ ทั้งนี้ การเลือกคุณลักษณะของกล้องควรสอดคล้องกับวัตถุประสงค์ของการเฝ้าระวังและสภาพแวดล้อมของพื้นที่ติดตั้ง

รายละเอียดการวิเคราะห์พื้นที่ การกำหนดตำแหน่งและมุมมองของกล้อง การเลือกอุปกรณ์และการออกแบบระบบ แสดงในภาคผนวก ก (ใบงานที่ 1)

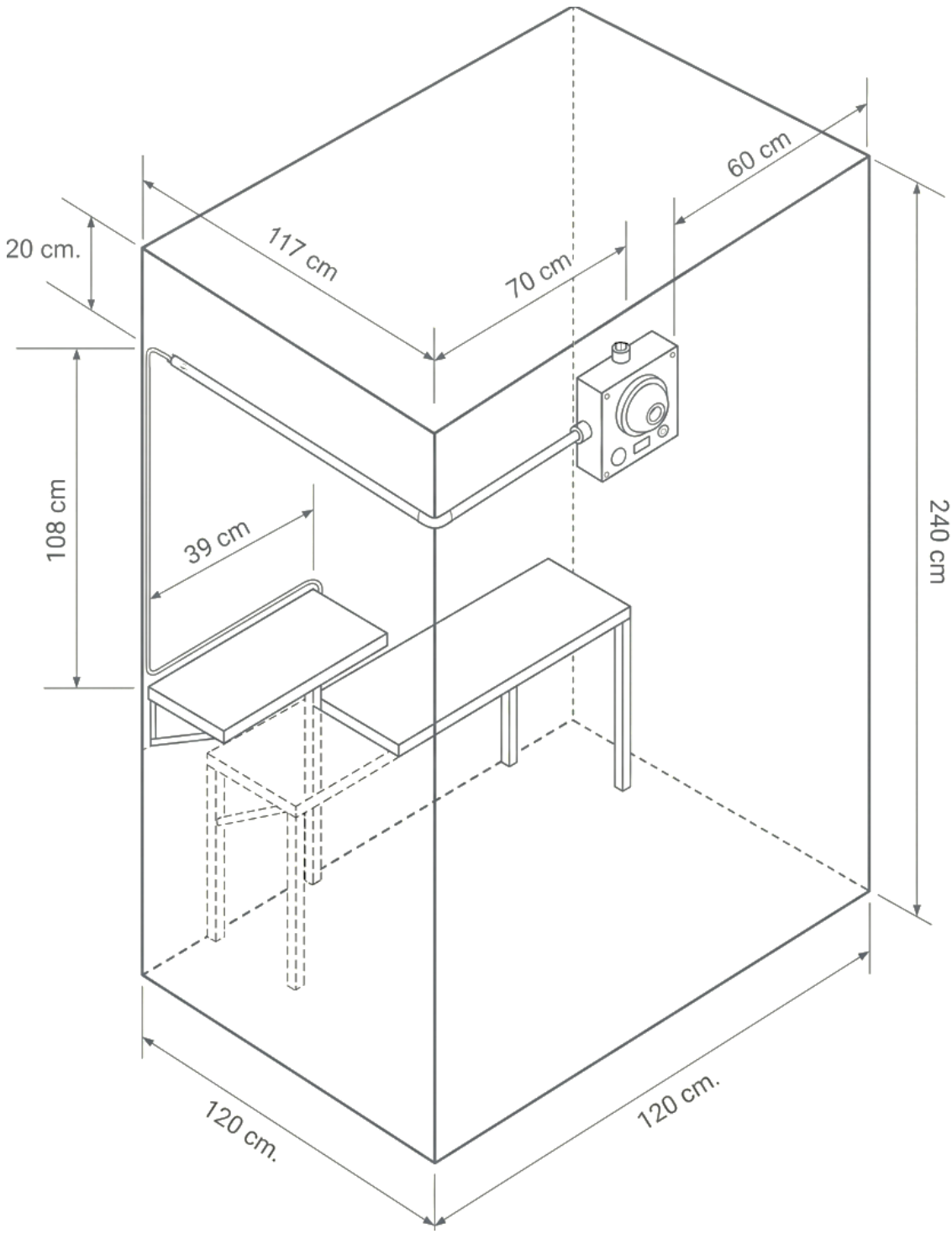
9.1.2 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก

ระบบกล้องโทรทัศน์วงจรปิดแบบแอนะล็อกเป็นระบบที่ส่งสัญญาณภาพจากกล้องไปยังเครื่องบันทึกภาพผ่านสายสัญญาณ โดยงานตัวอย่างนี้ใช้แบบจำลองการติดตั้งและเดินสายดังรูปที่ 9.2 เพื่อให้ผู้เรียนเข้าใจความสัมพันธ์ระหว่าง ตำแหน่งติดตั้งกล้อง แนวการเดินสาย และอุปกรณ์บันทึกภาพ ซึ่งเป็นพื้นฐานสำคัญของการติดตั้งระบบกล้องโทรทัศน์วงจรปิด

จากแบบจำลอง กำหนดให้ติดตั้งกล้องบริเวณมุมด้านบนของชุดฝึกปฏิบัติที่ระดับความสูงประมาณ 240 เซนติเมตร ห่างจากมุมด้านหน้าประมาณ 70 เซนติเมตร และห่างจากด้านข้างประมาณ 60 เซนติเมตร โดยปรับทิศทางของกล้องลงสู่พื้นที่ปฏิบัติงาน เพื่อให้ครอบคลุมพื้นที่ที่ต้องการเฝ้าระวังและลดจุดอับของภาพ (ชลดา ปานสง และคณะ, 2561; ชลดา ปานสง และคณะ, 2566)

ระบบตัวอย่างประกอบด้วยกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก รุ่น HA36513 พร้อมเลนส์ขนาด 4 mm เชื่อมต่อกับเครื่องบันทึกภาพดิจิทัล (DVR) รุ่น HA-5504 แบบ 4 ช่องสัญญาณ โดยใช้สายโคแอกเชียล RG59 สำหรับส่งสัญญาณภาพ และใช้แหล่งจ่ายไฟ 12 V สำหรับกล้อง ส่วนเครื่องบันทึกทำหน้าที่รับและบันทึกสัญญาณภาพเพื่อใช้สำหรับการแสดงผลและตรวจสอบเหตุการณ์ย้อนหลัง

หลักการทำงานโดยภาพรวมเริ่มจากกล้องรับภาพในพื้นที่เฝ้าระวังและแปลงเป็นสัญญาณที่เหมาะสมสำหรับส่งผ่านสายสัญญาณไปยัง DVR จากนั้น DVR ทำหน้าที่รับ ประมวลผล และบันทึกภาพลงในหน่วยจัดเก็บข้อมูล พร้อมส่งภาพไปยังจอแสดงผลหรือระบบที่เกี่ยวข้อง การติดตั้งจึงต้องพิจารณาทั้งตำแหน่งกล้อง คุณลักษณะของเลนส์ แนวการเดินสาย และการเชื่อมต่ออุปกรณ์ให้สัมพันธ์กัน



รูปที่ 9.2 แบบจำลองการติดตั้งและเดินสายระบบกล้องโทรทัศน์วงจรปิด
(ชลดา ปานสง และคณะ, 2561; ชลดา ปานสง และคณะ, 2566)

รายละเอียดเครื่องมือ การติดตั้ง การเดินสาย การเชื่อมต่ออุปกรณ์ และการทดสอบการทำงานของระบบ (ชลดา ปานสง และคณะ, 2561; ชลดา ปานสง และคณะ, 2565; ชลดา ปานสง และคณะ, 2566) แสดงในภาคผนวก ก (ใบงานที่ 2)

9.1.3 งานติดตั้งระบบกล้องโทรทัศน์วงจรปิดแบบ IP/Network

ระบบกล้องโทรทัศน์วงจรปิดแบบ IP/Network เป็นระบบที่กล้องทำหน้าที่รับและแปลงภาพเป็นข้อมูลดิจิทัล แล้วส่งข้อมูลผ่านเครือข่าย IP ไปยังอุปกรณ์หรือระบบที่เกี่ยวข้อง เช่น เครื่องบันทึกภาพเครือข่าย (Network Video Recorder: NVR) และอุปกรณ์สำหรับบริหารจัดการหรือแสดงผล ระบบลักษณะนี้ช่วยให้สามารถจัดการและเข้าถึงข้อมูลภาพผ่านโครงสร้างพื้นฐานเครือข่ายได้

งานตัวอย่างใช้แบบจำลองการติดตั้งตามรูปที่ 9.2 เช่นเดียวกับระบบแอนะล็อก โดยกำหนดตำแหน่งกล้องบริเวณมุมด้านบนของชุดฝึกปฏิบัติที่ระดับความสูงประมาณ 240 cm ห่างจากมุมด้านหน้าประมาณ 70 cm และห่างจากด้านข้างประมาณ 60 cm พร้อมปรับมุมกล้องให้ครอบคลุมพื้นที่ที่ต้องการเฝ้าระวัง การใช้ตำแหน่งติดตั้งเดียวกันยังช่วยให้สามารถเปรียบเทียบลักษณะของระบบแอนะล็อกกับระบบ IP/Network ได้อย่างชัดเจน

ระบบตัวอย่างประกอบด้วยกล้อง IP รุ่น HMP 88B10 พร้อมเลนส์ขนาด 3.6 mm และเครื่องบันทึกภาพเครือข่าย NVR รุ่น 8804A โดยใช้สาย UTP ประเภท Cat 5e สำหรับเชื่อมต่อเครือข่าย (Yu, 2016) และใช้แหล่งจ่ายไฟตามข้อกำหนดของอุปกรณ์ ทั้งนี้ หากกล้องและอุปกรณ์เครือข่ายรองรับ PoE สามารถส่งข้อมูลและจ่ายกำลังไฟฟ้าผ่านสาย Ethernet เดียวกันได้ ซึ่งช่วยลดจำนวนสายและเพิ่มความสะดวกในการติดตั้ง

หลักการทำงานเริ่มจากกล้อง IP รับและประมวลผลภาพ ก่อนส่งข้อมูลวิดีโอผ่านเครือข่ายไปยัง NVR เพื่อบันทึกและบริหารจัดการข้อมูล การสื่อสารอาศัยโครงสร้างเครือข่าย IP จึงต้องพิจารณาการเชื่อมต่อทางกายภาพและการกำหนดค่าทางเครือข่ายให้เหมาะสม เพื่อให้กล้อง NVR และอุปกรณ์ที่เกี่ยวข้องสามารถสื่อสารกันได้อย่างถูกต้อง

สำหรับการติดตั้งจริง การเลือกแนวเดินสายควรคำนึงถึงความปลอดภัย ความแข็งแรง ความเป็นระเบียบ และสภาพแวดล้อมของพื้นที่ติดตั้ง โดยอาจใช้ท่อร้อยสายหรืออุปกรณ์ยึดสายที่เหมาะสม ส่วนสาย UTP ต้องติดตั้งและเข้าหัวตามมาตรฐานการเดินสายแบบสมดุลที่เกี่ยวข้อง เพื่อรักษาคุณภาพของการรับส่งข้อมูล อย่างไรก็ตาม รายละเอียดดังกล่าวเป็นทักษะเชิงปฏิบัติ จึงแยกออกจากเนื้อหาหลักของบทนี้

รายละเอียดการเตรียมเครื่องมือ การติดตั้งกล้อง เดินสาย เข้าหัวสาย การเชื่อมต่ออุปกรณ์ การกำหนดค่าเครือข่าย และการทดสอบระบบ แสดงในภาคผนวก ก (ใบงานที่ 3)

9.1.4 งานติดตั้งและใช้งานกล้อง IP Camera

กล้อง IP camera เป็นกล้องวงจรปิดที่สามารถรับภาพ ประมวลผล และส่งข้อมูลภาพหรือวิดีโอผ่านเครือข่าย IP ทำให้ผู้ใช้งานสามารถตรวจสอบภาพจากระยะไกลผ่านเครือข่ายได้ กล้อง IP จึงเหมาะสำหรับประยุกต์ใช้ในระบบรักษาความปลอดภัยอัจฉริยะ โดยสามารถทำงานร่วมกับระบบเครือข่าย อุปกรณ์บันทึกภาพ และซอฟต์แวร์บริหารจัดการกล้องได้

1) ส่วนประกอบของกล้อง IP Camera รุ่น Vstarcam C7824WIP

ในงานตัวอย่างเลือกใช้กล้อง Vstarcam C7824WIP ซึ่งเป็นกล้อง IP แบบ Pan/Tilt ที่รองรับการเชื่อมต่อเครือข่ายแบบไร้สาย มีความละเอียดระดับ HD 720p รองรับการบีบอัดวิดีโอแบบ H.264 การมองเห็นในเวลากลางคืนด้วยอินฟราเรด การตรวจจับความเคลื่อนไหว การสื่อสารเสียงสองทาง และการบันทึกข้อมูลลงใน microSD Card นอกจากนี้ ยังสามารถใช้งาน

ผ่านแอปพลิเคชันที่รองรับและเชื่อมต่อกับระบบกล้องวงจรปิดที่รองรับมาตรฐาน ONVIF ตามคุณสมบัติของอุปกรณ์ (Global Column Limited, 2016)

3) หลักการเชื่อมต่อและติดตั้งกล้อง IP Camera

การติดตั้งกล้อง IP Camera ต้องเชื่อมต่อกล้องเข้ากับเครือข่าย IP ที่เหมาะสม เพื่อให้กล้องสามารถสื่อสารกับอุปกรณ์ของผู้ใช้งานหรือระบบบริหารจัดการกล้องได้ สำหรับระบบตัวอย่างสามารถตั้งค่าและตรวจสอบกล้องผ่านแอปพลิเคชัน Eye4 ตามวิธีการที่ผู้ผลิตกำหนด (Global Column Limited, 2016)

โดยทั่วไปกระบวนการติดตั้งประกอบด้วยการจ่ายไฟให้กล้อง การเชื่อมต่อกล้องกับเครือข่าย การเพิ่มอุปกรณ์เข้าสู่แอปพลิเคชัน การกำหนดค่าการเชื่อมต่อ และการตรวจสอบภาพหลังจากตั้งค่าเรียบร้อยแล้ว

เมื่อเชื่อมต่อกล้องเข้ากับเครือข่ายสำเร็จ ผู้ใช้งานสามารถตรวจสอบภาพ ปรับทิศทางกล้อง และใช้งานฟังก์ชันต่าง ๆ ตามที่กล้องและแอปพลิเคชันรองรับได้ ทั้งนี้ ควรกำหนดค่าด้านความมั่นคงปลอดภัยให้เหมาะสม โดยเฉพาะการ เปลี่ยนรหัสผ่านเริ่มต้นของอุปกรณ์เป็นรหัสผ่านที่คาดเดาได้ยาก และจำกัดการเข้าถึงกล้องจากเครือข่ายเฉพาะเท่าที่จำเป็น

4) แนวทางตรวจสอบปัญหาเบื้องต้น

หากกล้องไม่สามารถเชื่อมต่อหรือแสดงสถานะออนไลน์ได้ ควรตรวจสอบตั้งแต่แหล่งจ่ายไฟ สถานะของเครือข่าย Wi-Fi หรือ Ethernet การตั้งค่าเครือข่าย และสถานะของเราเตอร์ หากมีการเปลี่ยนแปลงเครือข่าย เช่น เปลี่ยนเราเตอร์หรือเปลี่ยน SSID/รหัสผ่าน Wi-Fi อาจจำเป็นต้องกำหนดค่าการเชื่อมต่อของกล้องใหม่ตามขั้นตอนของผู้ผลิต

หากการตั้งค่าผิดพลาดและไม่สามารถแก้ไขผ่านซอฟต์แวร์ได้ อาจใช้ฟังก์ชัน Factory Reset ตามคู่มือของอุปกรณ์ แล้วดำเนินการตั้งค่าใหม่ อย่างไรก็ตาม หลังการรีเซตควรกำหนดรหัสผ่านใหม่ทันที และไม่ควรคงรหัสผ่านเริ่มต้นจากโรงงานไว้สำหรับการใช้งานจริง เนื่องจากอาจเพิ่มความเสี่ยงต่อการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

โดยสรุป การติดตั้งกล้อง IP Camera สำหรับระบบรักษาความปลอดภัยอัจฉริยะไม่ควรพิจารณาเฉพาะการติดตั้งทางกายภาพเท่านั้น แต่ต้องคำนึงถึง ตำแหน่งและมุมมองของกล้อง คุณภาพของเครือข่าย การกำหนดค่า IP การจัดเก็บข้อมูล และความมั่นคงปลอดภัยของอุปกรณ์และบัญชีผู้ใช้งาน เพื่อให้ระบบสามารถเฝ้าระวังและบันทึกเหตุการณ์ได้อย่างมีประสิทธิภาพและปลอดภัย

รายละเอียดการติดตั้งแอปพลิเคชัน Eye4 การเพิ่มกล้องด้วย QR Code การกำหนดค่า Wi-Fi การตั้งค่ากล้อง การทดสอบการรับชมภาพ และการแก้ไขปัญหาเบื้องต้น แสดงในภาคผนวก ก (ใบงานที่ 4)

9.2 ระบบควบคุมประตูอัจฉริยะด้วยเทคโนโลยี RFID

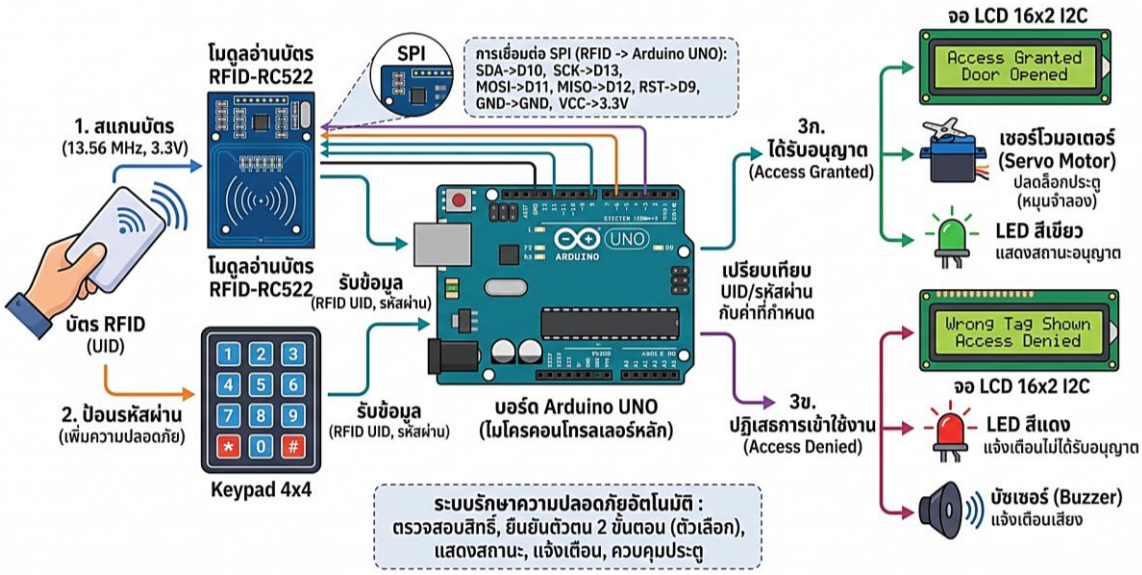
9.2.1 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino

ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยี RFID เป็นการประยุกต์ใช้การระบุเอกลักษณ์ด้วยคลื่นความถี่วิทยุร่วมกับไมโครคอนโทรลเลอร์ เพื่อใช้ตรวจสอบสิทธิ์ของผู้ใช้งานก่อนอนุญาตให้เข้าสู่พื้นที่ ระบบสามารถใช้บัตรหรือแท็ก RFID แทนกุญแจแบบดั้งเดิม และสามารถเพิ่มเติมการ

ตรวจสอบด้วยรหัสผ่านเพื่อเพิ่มระดับการควบคุมการเข้า–ออก เหมาะสำหรับประยุกต์ใช้กับห้องเรียน ห้องปฏิบัติการ สำนักงาน ห้องควบคุม หรือตู้จัดเก็บอุปกรณ์ที่ต้องการจำกัดสิทธิ์การเข้าถึง

1) การออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino

การออกแบบระบบตัวอย่างประกอบด้วย โมดูล RFID-RC522 บอร์ด Arduino UNO แป้นกด (keypad) จอแสดงผล LCD เซอร์โวมอเตอร์ (servo motor) หลอด LED และ buzzer ดังรูปที่ 9.3 โดย Arduino UNO ทำหน้าที่เป็นหน่วยควบคุมหลัก รับข้อมูลจากอุปกรณ์อินพุต ประมวลผลเงื่อนไขการอนุญาต และควบคุมอุปกรณ์เอาต์พุตของระบบ



รูปที่ 9.3 หลักการออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino

โมดูล RFID-RC522 ทำหน้าที่อ่านข้อมูลจากบัตรหรือแท็ก RFID ที่ย่านความถี่ 13.56 MHz และส่งข้อมูลไปยัง Arduino เพื่อใช้ตรวจสอบกับข้อมูลที่กำหนดไว้ในระบบ ในงานตัวอย่างสามารถใช้ keypad ร่วมกับ RFID เพื่อเพิ่มเงื่อนไขการตรวจสอบ โดยผู้ใช้ต้องแสดงบัตรที่ได้รับอนุญาตและป้อนรหัสผ่านที่ถูกต้องก่อนระบบจึงจะอนุญาตให้เปิดประตู

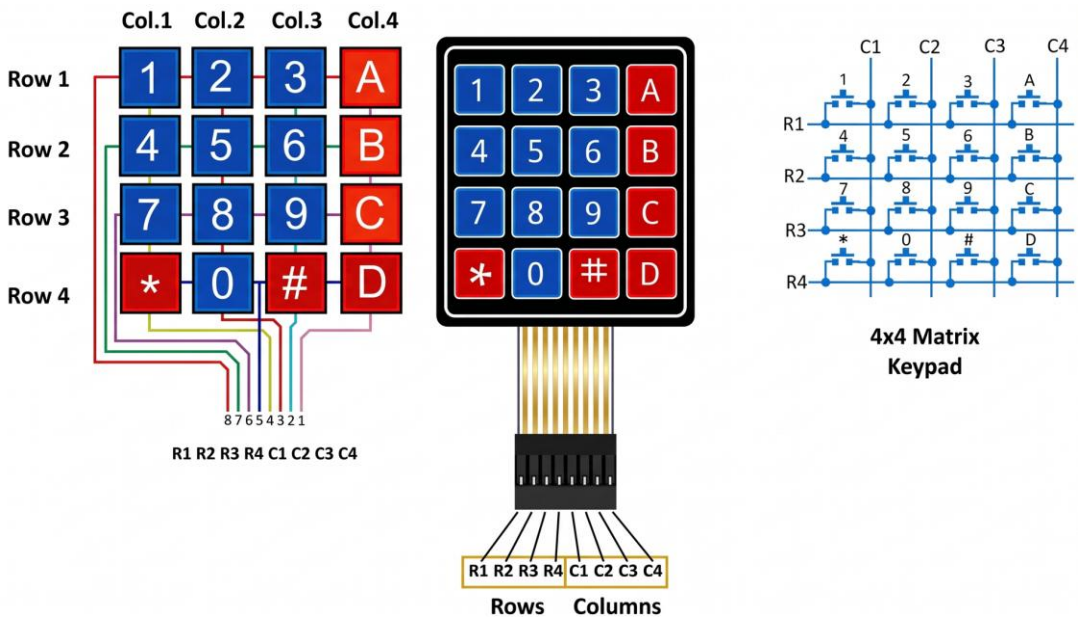
หลักการทำงานเริ่มจากผู้ใช้นำบัตรหรือแท็ก RFID เข้าใกล้เครื่องอ่าน ระบบจะอ่านข้อมูลประจำบัตรและส่งไปยัง Arduino เพื่อประมวลผล หากกำหนดให้มีการตรวจสอบด้วยรหัสผ่าน ผู้ใช้จะต้องป้อนรหัสผ่านผ่าน Keypad เพิ่มเติม เมื่อข้อมูลที่ใช้ตรวจสอบเป็นไปตามเงื่อนไขที่กำหนด Arduino จะสั่งให้เซอร์โวมอเตอร์ทำงานเพื่อจำลองการปลดล็อกประตู พร้อมแสดงสถานะอนุญาตผ่านจอ LCD และ LED

ในกรณีที่ข้อมูลบัตรหรือรหัสผ่านไม่ตรงตามเงื่อนไข ระบบจะปฏิเสธการเข้าใช้งาน โดยสามารถแสดงสถานะผ่านจอ LCD พร้อมใช้ LED และ Buzzer แจ้งเตือน การออกแบบในลักษณะนี้แสดงให้เห็นกระบวนการพื้นฐานของระบบควบคุมการเข้า–ออก ได้แก่ การรับข้อมูล (input) > การตรวจสอบและประมวลผล (processing and verification) > การตัดสินใจ (decision) > การควบคุมและแสดงผล (control and output) (Aqib, 2018)

2) แนวคิดการเชื่อมต่อและควบคุมระบบ

อุปกรณ์ต่าง ๆ ในระบบเชื่อมต่อกับ Arduino ผ่านรูปแบบการสื่อสารที่เหมาะสมกับอุปกรณ์แต่ละประเภท โดยโมดูล RFID-RC522 ใช้การสื่อสารแบบ SPI ขณะที่จอ LCD แบบ I²C ใช้การสื่อสารแบบ I²C ส่วน keypad เชื่อมต่อกับขาดิจิทัลของไมโครคอนโทรลเลอร์และตรวจจับการกดปุ่มด้วยหลักการสแกนเมทริกซ์ (matrix scanning)

keypad แบบ 4×4 ประกอบด้วย 4 แถว (Rows) และ 4 คอลัมน์ (Columns) ดังรูปที่ 9.4 เมื่อผู้ใช้กดปุ่ม จะเกิดการเชื่อมต่อระหว่างแถวและคอลัมน์ของปุ่มนั้น ทำให้ไมโครคอนโทรลเลอร์สามารถระบุตำแหน่งและค่าของปุ่มที่ถูกกดได้ หลักการดังกล่าวช่วยลดจำนวนขา I/O ที่ต้องใช้เมื่อเทียบกับการต่อสวิตช์แต่ละปุ่มแยกกัน และเหมาะสำหรับการนำมาใช้ป้อนรหัสผ่านในระบบควบคุมการเข้า–ออก



รูปที่ 9.4 โครงสร้างแถวและคอลัมน์ของแป้นกดแบบเมทริกซ์ 4×4

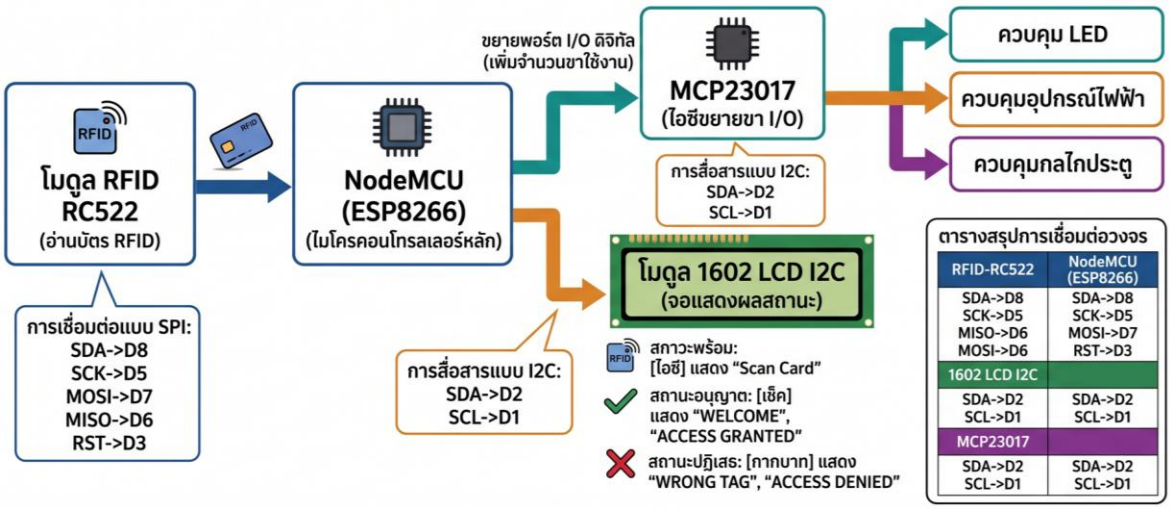
ข้อมูลจาก RFID และ keypad จะถูกประมวลผลตามเงื่อนไขที่กำหนดในโปรแกรม หากการตรวจสอบถูกต้อง ระบบจะควบคุมเซอร์โวมอเตอร์ให้จำลองการปลดล็อกประตู พร้อมแสดงผลการอนุญาตผ่าน LCD และ LED ในทางตรงกันข้าม หากการตรวจสอบไม่ผ่าน ระบบจะคงสถานะ ล็อกและแจ้งเตือนผ่านอุปกรณ์แสดงผลที่กำหนดไว้ แนวคิดดังกล่าวสามารถนำไปต่อยอดสู่ระบบล็อกประตูอัจฉริยะที่มีการบันทึกเหตุการณ์ การบริหารสิทธิ์ผู้ใช้งาน หรือการเชื่อมต่อกับระบบเครือข่ายได้ รายละเอียดแสดงในภาคผนวก ก (ใบงานที่ 5)

9.2.2 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID โดยใช้ NodeMCU ESP8266

การประยุกต์ใช้เทคโนโลยี RFID ร่วมกับ NodeMCU ESP8266 ช่วยให้ระบบควบคุมการเข้า–ออกประตูสามารถตรวจสอบสิทธิ์ผู้ใช้งาน ประมวลผลข้อมูล และแสดงสถานะการทำงานได้อย่างยืดหยุ่นมากขึ้น นอกจากนี้ ESP8266 ยังมีความสามารถด้านการเชื่อมต่อเครือข่ายไร้สาย จึงสามารถนำไปต่อยอดสู่ระบบ IoT ระบบบันทึกเหตุการณ์ หรือระบบแจ้งเตือนจากระยะไกลได้

1) ระบบควบคุมการเข้า–ออกประตูด้วย RFID และจอแสดงผล LCD

ระบบตัวอย่างประกอบด้วย NodeMCU ESP8266 ทำหน้าที่เป็นหน่วยควบคุมหลัก โมดูล RFID-RC522 ใช้สำหรับอ่านข้อมูลจากบัตรหรือแท็ก RFID และจอ LCD 1602 แบบ I²C ใช้สำหรับแสดงสถานะการทำงานของระบบ เช่น การรออ่านบัตร การอนุญาต หรือการปฏิเสธการเข้าใช้งาน ดังรูปที่ 9.5



รูปที่ 9.5 หลักการควบคุมการเข้า–ออกประตูด้วย RFID, NodeMCU ESP8266 และจอ LCD

หลักการทำงานเริ่มจากผู้ใช้นำบัตรหรือแท็ก RFID เข้าใกล้โมดูล RC522 ระบบจะอ่านข้อมูลประจำบัตรและส่งไปยัง NodeMCU ESP8266 เพื่อเปรียบเทียบกับข้อมูลที่กำหนดไว้ หากข้อมูลตรงกับสิทธิ์ที่อนุญาต ระบบจะแสดงผลการยืนยันผ่านจอ LCD และสามารถควบคุมอุปกรณ์แสดงสถานะ เช่น LED ได้ ในทางตรงกันข้าม หากข้อมูลไม่ถูกต้อง ระบบจะแสดงสถานะปฏิเสธและแจ้งเตือนผู้ใช้งาน

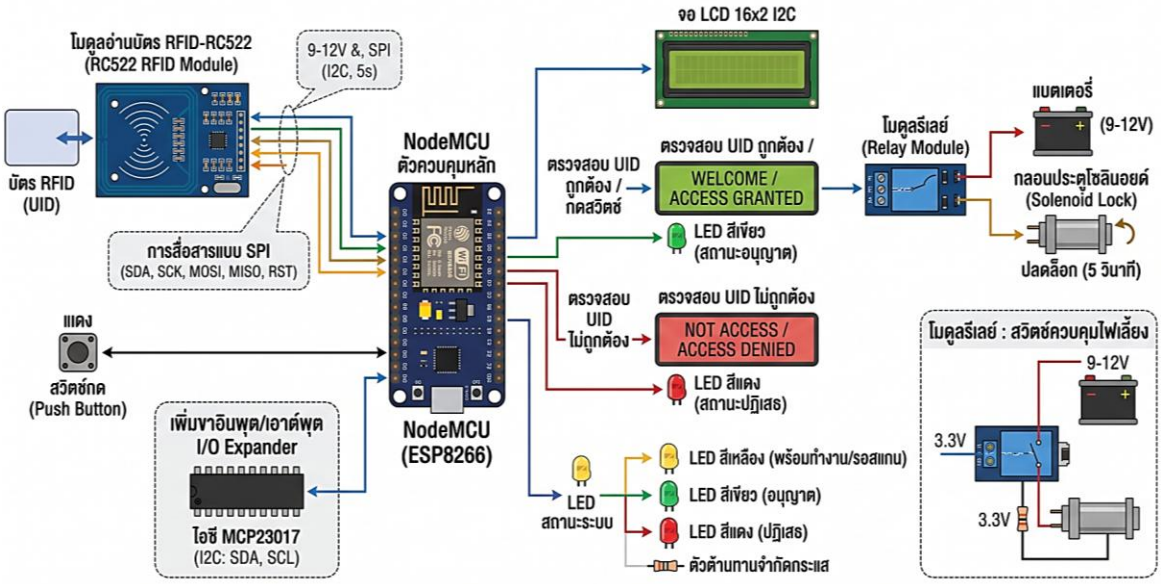
ในกรณีที่ระบบต้องใช้งานอุปกรณ์หลายชนิดร่วมกัน อาจใช้อุปกรณ์ขยายขาอินพุต/เอาต์พุต เช่น MCP23017 I/O expander เพื่อเพิ่มจำนวนขาที่สามารถควบคุมได้ โดยอุปกรณ์ดังกล่าวสื่อสารกับไมโครคอนโทรลเลอร์ผ่านบัส I²C ช่วยลดข้อจำกัดด้านจำนวนขาของ NodeMCU และทำให้สามารถเชื่อมต่ออุปกรณ์แสดงผลหรืออุปกรณ์ควบคุมเพิ่มเติมได้

ระบบลักษณะนี้เหมาะสำหรับนำไปประยุกต์ใช้กับ ระบบควบคุมการเข้า–ออก ระบบบันทึกเวลา ระบบตรวจสอบสิทธิ์ และระบบ IoT ที่ต้องการแสดงสถานะให้ผู้ใช้งานเข้าใจได้ชัดเจน

รายละเอียดการเชื่อมต่อวงจร การกำหนดขาอุปกรณ์ การอ่านค่า UID การเขียนโปรแกรม และการทดสอบการทำงาน แสดงในภาคผนวก ก (ใบงานที่ 6)

2) ระบบควบคุมกลอนประตูโซลินอยด์ด้วย RFID และ NodeMCU ESP8266

ระบบนี้เป็นการพัฒนาต่อยอดจากระบบตรวจสอบบัตร RFID โดยเพิ่ม กลอนประตูโซลินอยด์ (solenoid door lock) เพื่อให้สามารถควบคุมการล็อกและปลดล็อกประตูได้จริง องค์ประกอบสำคัญของระบบประกอบด้วย NodeMCU ESP8266, โมดูล RFID-RC522, จอ LCD, MCP23017, โมดูลรีเลย์, LED แสดงสถานะ, สวิตช์กด และกลอนประตูโซลินอยด์



รูปที่ 9.6 หลักการควบคุมกลอนประตูโซลินอยด์ด้วย RFID โดยใช้ NodeMCU ESP8266

หลักการทำงานเริ่มจากโมดูล RFID อ่านข้อมูลจากบัตรหรือแท็ก แล้วส่งข้อมูลไปยัง NodeMCU เพื่อประมวลผล หากข้อมูลตรงกับค่าที่ได้รับอนุญาต ระบบจะสั่งงาน Relay Module เพื่อควบคุมวงจรจ่ายกำลังให้กับกลอนประตูโซลินอยด์ ทำให้ประตูปลดล็อกชั่วคราว พร้อมแสดงสถานะอนุญาตผ่านจอ LCD และ LED เมื่อครบเวลาที่กำหนด ระบบจะยกเลิกคำสั่งควบคุมและนำกลอนกลับสู่สถานะล็อก

การใช้รีเลย์มีความสำคัญ เนื่องจากกลอนประตูโซลินอยด์ต้องการแรงดันและกระแสสูงกว่าที่ขาเอาต์พุตของ ESP8266 สามารถจ่ายได้โดยตรง ดังนั้น ไมโครคอนโทรลเลอร์จึงทำหน้าที่เพียงส่งสัญญาณควบคุมไปยังรีเลย์ ส่วนกำลังไฟฟ้าสำหรับกลอนประตูควรได้รับจากแหล่งจ่ายที่เหมาะสมกับคุณลักษณะของอุปกรณ์

ในกรณีที่ข้อมูล RFID ไม่ตรงกับสิทธิ์ที่กำหนด ระบบจะคงประตูไว้ในสถานะล็อก พร้อมแสดงสถานะปฏิเสธและแจ้งเตือนผู้ใช้งาน นอกจากนี้ ระบบสามารถเพิ่ม push button หรือ

exit switch เพื่อให้ผู้ใช้งานภายในสามารถสั่งปลดล็อกประตูได้โดยไม่ต้องใช้บัตร ซึ่งเป็นแนวทางที่พบได้ทั่วไปในระบบควบคุมการเข้า–ออก

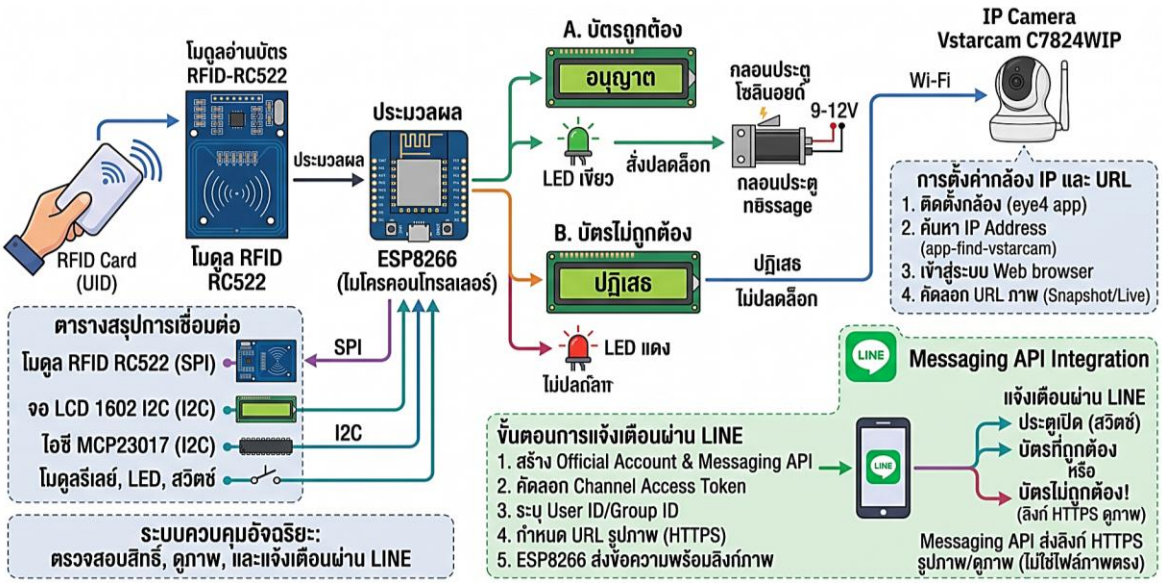
LED สามารถใช้แสดงสถานะของระบบ เช่น สถานะพร้อมทำงาน สถานะอนุญาต และสถานะปฏิเสธ เพื่อช่วยให้ผู้ใช้งานเข้าใจผลการตรวจสอบได้ทันที ขณะที่จอ LCD สามารถแสดงข้อความรายละเอียดเพิ่มเติมได้

โดยสรุป ระบบนี้แสดงแนวคิดพื้นฐานของ Input > Processing > Decision >Actuation กล่าวคือ RFID ทำหน้าที่รับข้อมูล, NodeMCU ประมวลผลและตัดสินใจ, relay ทำหน้าที่เป็นตัวกลางควบคุมกำลัง และ Solenoid Lock ทำหน้าที่เป็นอุปกรณ์กระทำ ระบบดังกล่าวสามารถต่อยอดไปสู่การบันทึกเหตุการณ์ การบริหารสิทธิ์ผู้ใช้งาน และการแจ้งเตือนผ่านเครือข่ายได้

รายละเอียดการเชื่อมต่อวงจร การเลือกแหล่งจ่ายไฟ การกำหนดขาอุปกรณ์ การเขียนโปรแกรม การตั้งเวลาปลดล็อก และการทดสอบการทำงาน (ภาคผนวก ก ใบงานที่ 7)

9.2.3 งานประยุกต์ใช้ RFID ร่วมกับ IP Camera และ LINE Messaging API

การประยุกต์ใช้ RFID ร่วมกับ IP camera และ LINE Messaging API เป็นการเพิ่มความสามารถให้ระบบควบคุมการเข้า–ออกสามารถตรวจสอบสิทธิ์ บันทึกภาพ และแจ้งเตือนผู้ดูแลระบบจากระยะไกลได้ ระบบตัวอย่างใช้ NodeMCU ESP8266 เป็นหน่วยควบคุมหลัก ทำงานร่วมกับโมดูล RFID-RC522 กลอนประตูโซลินอยด์ จอ LCD อุปกรณ์แสดงสถานะ และกล้อง IP



รูปที่ 9.7 การประยุกต์ใช้ RFID ร่วมกับ IP Camera และ LINE Messaging API

หลักการทำงานเริ่มจากผู้ใช้นำบัตรหรือแท็ก RFID เข้าใกล้เครื่องอ่าน ระบบจะอ่านค่า UID และส่งไปยัง ESP8266 เพื่อเปรียบเทียบกับข้อมูลที่ได้รับอนุญาต หากข้อมูลถูกต้อง ระบบจะสั่งปลดล็อกประตู แสดงสถานะผ่านจอ LCD และส่งข้อความแจ้งเตือนไปยังผู้ดูแลผ่าน LINE

Messaging API ในทางตรงกันข้าม หากข้อมูลไม่ถูกต้อง ระบบจะคงประตูไว้ในสถานะล็อก แสดงผลการปฏิเสธ และส่งข้อความแจ้งเตือนเหตุการณ์ที่ไม่ได้รับอนุญาต (LINE Developers, n.d.; LINE Developers, 2024)

IP camera สามารถใช้สำหรับดูภาพแบบเวลาจริงหรือบันทึกภาพประกอบเหตุการณ์ที่เกิดขึ้นในระบบ โดยข้อมูลภาพสามารถนำมาใช้ร่วมกับข้อความแจ้งเตือนเพื่อช่วยให้ผู้ดูแลตรวจสอบเหตุการณ์ได้สะดวกยิ่งขึ้น ทั้งนี้ การส่งภาพผ่าน LINE Messaging API โดยทั่วไปต้องอาศัย URL ของภาพที่ระบบ LINE สามารถเข้าถึงได้ผ่าน HTTPS หรือจัดเก็บภาพไว้บนเซิร์ฟเวอร์ก่อนแล้วจึงส่งลิงก์หรือข้อมูลอ้างอิงของภาพไปยังผู้ใช้

แนวทางดังกล่าวช่วยยกระดับระบบควบคุมการเข้า–ออกจากระบบเฉพาะที่ไปสู่ระบบรักษาความปลอดภัยแบบเชื่อมต่อเครือข่าย ซึ่งสามารถตรวจสอบสิทธิ์ ควบคุมประตู ตรวจสอบภาพ และแจ้งเตือนเหตุการณ์จากระยะไกลได้ รายละเอียดการเชื่อมต่อวงจร การตั้งค่า IP Camera การเขียนโปรแกรม การดึงภาพ Snapshot และการแจ้งเตือนผ่าน LINE Messaging API แสดงในภาคผนวก ก (ใบงานที่ 8)

9.3 ระบบประตูอัจฉริยะด้วยเทคโนโลยีตรวจสอบลายนิ้วมือ

ระบบตรวจสอบลายนิ้วมือเป็นการประยุกต์ใช้ข้อมูลชีวมิติ (biometric data) เพื่อยืนยันตัวตนของผู้ใช้งาน โดยอาศัยคุณลักษณะเฉพาะของลายนิ้วมือ เช่น จุดสิ้นสุดของเส้นลายและจุดแตกแขนงของเส้นลาย เพื่อนำมาใช้สร้างข้อมูลอ้างอิงและเปรียบเทียบกับลายนิ้วมือที่ตรวจจับได้ ระบบลักษณะนี้สามารถนำไปใช้ในการควบคุมการเข้า–ออก การบันทึกเวลา และการตรวจสอบสิทธิ์ในพื้นที่ที่ต้องการความปลอดภัยสูง

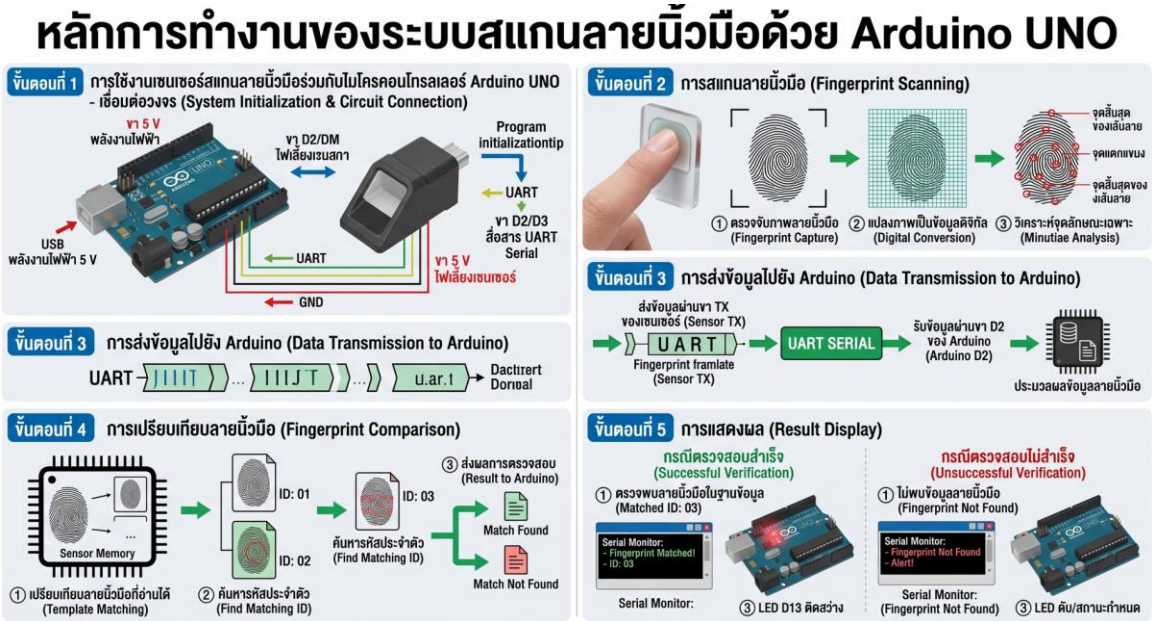
9.3.1 งานควบคุมการเปิด–ปิดอุปกรณ์ด้วยเซนเซอร์ตรวจสอบลายนิ้วมือ

ระบบตัวอย่างใช้ Arduino UNO เป็นหน่วยควบคุมหลัก ทำงานร่วมกับเซนเซอร์ตรวจสอบลายนิ้วมือและอุปกรณ์แสดงสถานะ เพื่อแสดงแนวคิดพื้นฐานของการรับข้อมูลชีวมิติ การตรวจสอบกับฐานข้อมูล และการควบคุมเอาต์พุตตามผลการยืนยันตัวตน

หลักการทำงานเริ่มจากผู้ใช้นำปลายนิ้วสัมผัสบริเวณเซนเซอร์ เซนเซอร์จะรับภาพลายนิ้วมือและแปลงข้อมูลเป็นรูปแบบที่เหมาะสมสำหรับการวิเคราะห์ จากนั้นระบบจะสกัดคุณลักษณะเฉพาะของลายนิ้วมือและนำไปเปรียบเทียบกับแม่แบบ (template) ที่ลงทะเบียนไว้ในหน่วยความจำของอุปกรณ์ หากพบข้อมูลที่ตรงกัน ระบบจะส่งผลการตรวจสอบและรหัสประจำตัวของผู้ใช้ไปยัง Arduino เพื่อสั่งงานอุปกรณ์เอาต์พุตตามเงื่อนไขที่กำหนด

ในกรณีที่ตรวจสอบสำเร็จ Arduino สามารถแสดงหมายเลขผู้ใช้หรือสถานะการยืนยันและควบคุม LED หรืออุปกรณ์อื่นให้ทำงาน ส่วนกรณีที่ไม่พบข้อมูลตรงกับฐานข้อมูล ระบบจะแสดงสถานะปฏิเสธหรือแจ้งเตือนตามการออกแบบ (Mohanan, 2021)

กระบวนการดังกล่าวแสดงลำดับพื้นฐานของระบบชีวมิติ ได้แก่ การรับข้อมูลลายนิ้วมือ > การสกัดคุณลักษณะ > การเปรียบเทียบกับฐานข้อมูล > การตัดสินใจ > การควบคุมเอาต์พุต รายละเอียดการเชื่อมต่อเซนเซอร์ การลงทะเบียนลายนิ้วมือ การเขียนโปรแกรม และการทดสอบการตรวจสอบตัวตน แสดงในภาคผนวก ก (ใบงานที่ 9)



รูปที่ 9.8 หลักการควบคุมอุปกรณ์ด้วยระบบตรวจสอบลายนิ้วมือ

9.3.2 งานควบคุมการเข้า–ออกประตูด้วยลายนิ้วมือร่วมกับ RFID

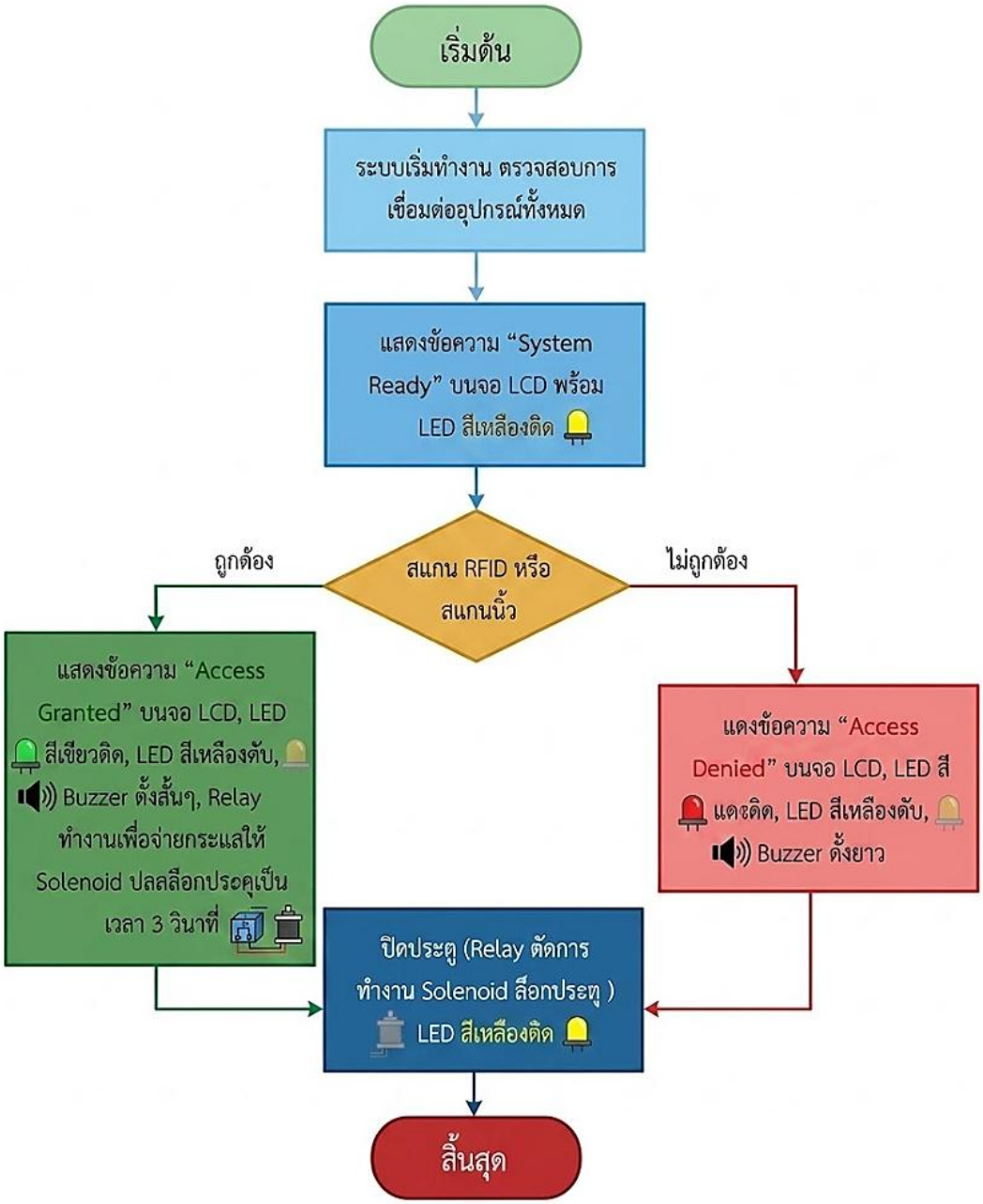
ระบบนี้เป็นการประยุกต์ใช้ RFID และการตรวจสอบลายนิ้วมือร่วมกัน เพื่อเพิ่มความยืดหยุ่นในการยืนยันตัวตนก่อนอนุญาตให้เข้าใช้งาน โดยระบบประกอบด้วย Arduino, โมดูล RFID, เซนเซอร์ลายนิ้วมือ, จอ LCD, relay, LED, buzzer, กลอนไฟฟ้า, และสวิตช์กดสำหรับควบคุมประตู

เมื่อเริ่มทำงาน ระบบจะตรวจสอบความพร้อมของอุปกรณ์และเข้าสู่สถานะรอการยืนยันตัวตน ผู้ใช้สามารถยืนยันสิทธิ์ด้วยบัตรหรือแท็ก RFID หรือด้วยลายนิ้วมือ ขึ้นอยู่กับเงื่อนไขที่กำหนดในระบบ หากข้อมูลที่ตรวจสอบตรงกับข้อมูลที่ลงทะเบียนไว้ ระบบจะอนุญาตการเข้าใช้งาน แสดงสถานะผ่านจอ LCD และอุปกรณ์แสดงผล พร้อมสั่ง Relay ให้ควบคุมกลอนไฟฟ้าเพื่อปลดล็อกประตูชั่วคราว ก่อนกลับเข้าสู่สถานะล็อกตามเวลาที่กำหนด

ในกรณีที่ข้อมูลไม่ถูกต้อง ระบบจะไม่อนุญาตให้เปิดประตู พร้อมแสดงสถานะปฏิเสธผ่านจอ LCD LED และ buzzer นอกจากนี้ ยังสามารถติดตั้ง push button หรือ exit switch สำหรับปลดล็อกประตูจากภายในตามเงื่อนไขการใช้งานของระบบ

การผสาน RFID และลายนิ้วมือช่วยให้ระบบสามารถรองรับวิธีการยืนยันตัวตนได้มากกว่าหนึ่งรูปแบบ และสามารถต่อยอดไปสู่ระบบที่มีการบันทึกเหตุการณ์ การกำหนดสิทธิ์ผู้ใช้ หรือการเชื่อมต่อเครือข่ายได้ อย่างไรก็ตาม หากต้องการใช้เป็นการยืนยันตัวตนหลายปัจจัยจริง ควรกำหนดให้ผู้ใช้ต้องผ่านมากกว่าหนึ่งวิธีตามลำดับ ไม่ใช่เพียงเลือกใช้วิธีใดวิธีหนึ่ง

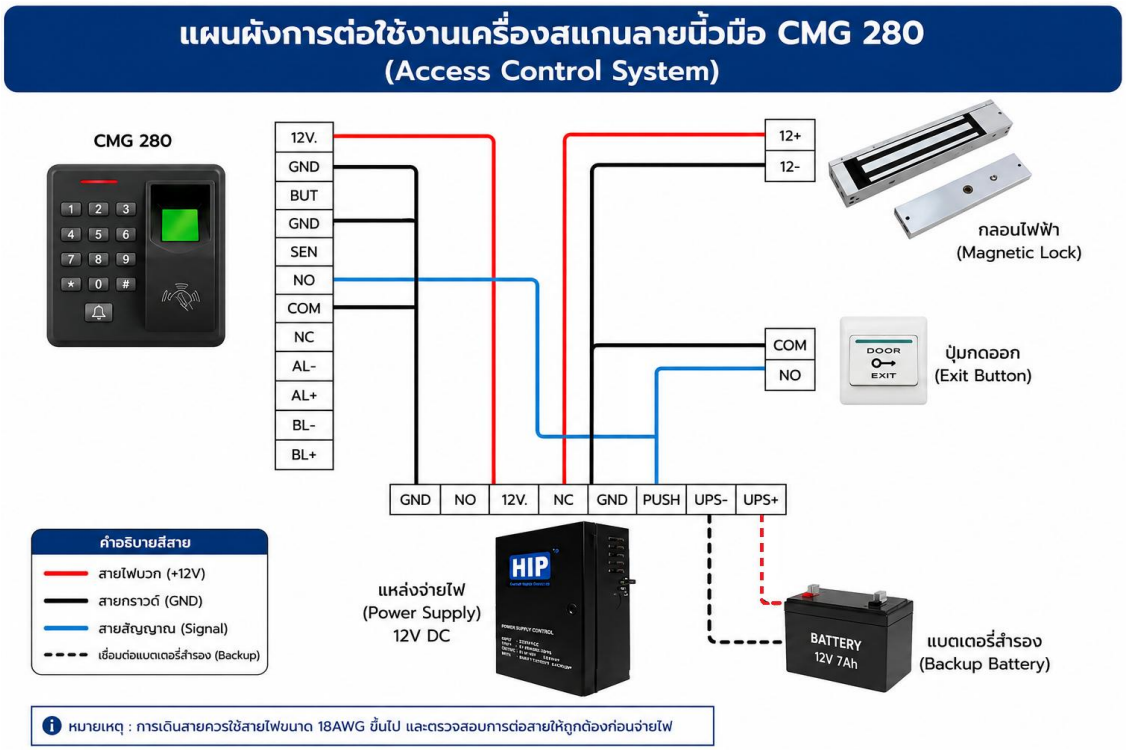
รายละเอียดการเชื่อมต่อวงจร การลงทะเบียนข้อมูล RFID และเก็บตัวอย่างลายนิ้วมือ การเขียนโปรแกรมควบคุมการทำงาน relay ในการเปิด–ปิด และการทดสอบระบบ แสดงในภาคผนวก ก (ใบงานที่ 9)



รูปที่ 9.9 แผนผังการทำงานของระบบควบคุมการเข้า–ออกประตูด้วยลายนิ้วมือร่วมกับ RFID

9.3.3 งานติดตั้งเครื่องสแกนลายนิ้วมือสำหรับระบบควบคุมการเข้า–ออกประตู

หัวข้อนี้เป็นการประยุกต์ใช้เครื่องสแกนลายนิ้วมือรุ่น CMG 280 สำหรับควบคุมการเข้า–ออกพื้นที่ โดยอุปกรณ์รองรับการยืนยันตัวตนด้วย ลายนิ้วมือ รหัสผ่าน และบัตรประจำตัว และสามารถเชื่อมต่อกับกลอนประตูไฟฟ้า รวมถึงอุปกรณ์เสริมที่ใช้ในระบบควบคุมการเข้า–ออก เช่น เซนเซอร์ตรวจสอบสถานะประตู ปุ่มกดออก และอุปกรณ์แจ้งเตือนภายนอก (เอชไอพี โกลบอล จำกัด, 2015; HIP, n.d.)



รูปที่ 9.10 ผังการเชื่อมต่อระบบควบคุมการเข้า–ออกด้วยเครื่องสแกนลายนิ้วมือรุ่น CMG 280

หลักการทำงานโดยทั่วไปเริ่มจากผู้ใช้งานยืนยันตัวตนด้วยวิธีที่ระบบกำหนด เช่น การสแกนลายนิ้วมือ การป้อนรหัสผ่าน หรือการใช้บัตร หากข้อมูลที่ตรวจสอบตรงกับข้อมูลที่ลงทะเบียนไว้ ระบบจะส่งสัญญาณควบคุมไปยังกลอนประตูไฟฟ้าเพื่อปลดล็อกและอนุญาตให้ผู้ใช้เข้าสู่พื้นที่ได้

ระบบสามารถเชื่อมต่อกับ door sensor เพื่อตรวจสอบสถานะเปิด–ปิดของประตู และใช้สำหรับตรวจจับเหตุการณ์ผิดปกติ เช่น ประตูถูกเปิดโดยไม่ได้รับอนุญาตหรือเปิดค้างเกินเงื่อนไขที่กำหนด นอกจากนี้ ยังสามารถใช้งานร่วมกับ tamper alarm เพื่อแจ้งเตือนเมื่ออุปกรณ์ถูกถอดหรือรื้อถอนจากตำแหน่งติดตั้งโดยไม่ได้รับอนุญาต รวมถึงเชื่อมต่อ exit switch เพื่อให้ผู้ใช้งานสามารถปลดล็อกประตูจากภายใน และเชื่อมต่ออุปกรณ์แจ้งเตือนภายนอกตามรูปแบบการใช้งานของระบบ (เอชไอพี โกลบอล จำกัด, 2015; HIP, n.d.)

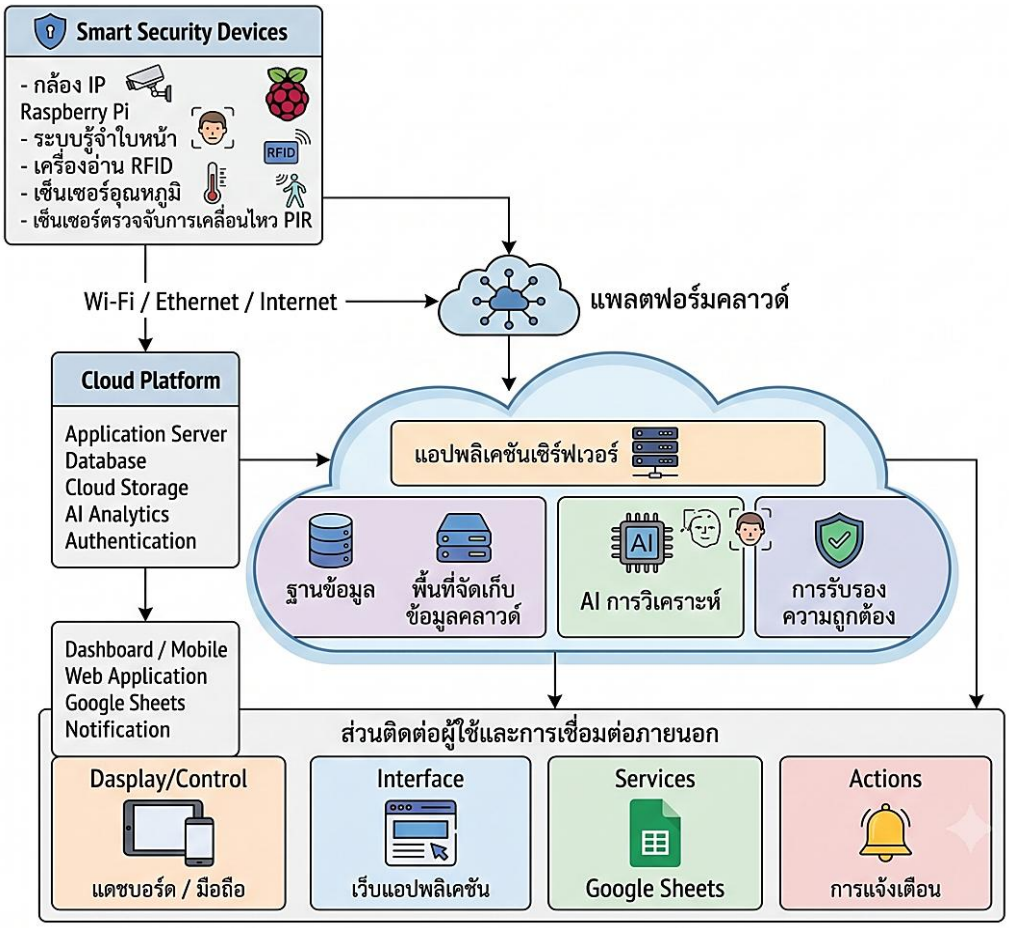
การประยุกต์ใช้อุปกรณ์ลักษณะนี้ช่วยให้ระบบควบคุมการเข้า–ออกสามารถรวมการยืนยันตัวตน การควบคุมประตู การตรวจสอบสถานะ และการแจ้งเตือนไว้ในระบบเดียว เหมาะสำหรับสำนักงาน ห้องปฏิบัติการ ห้องควบคุม หรือพื้นที่ที่ต้องการจำกัดสิทธิ์การเข้าใช้งาน

รายละเอียดการติดตั้ง การเชื่อมต่ออุปกรณ์ การกำหนดค่าระบบ การลงทะเบียนผู้ใช้งาน และการทดสอบการทำงาน แสดงในภาคผนวก ก (ใบงานที่ 10)

9.4 ระบบประตูอัจฉริยะด้วยเทคโนโลยีจดจำใบหน้า

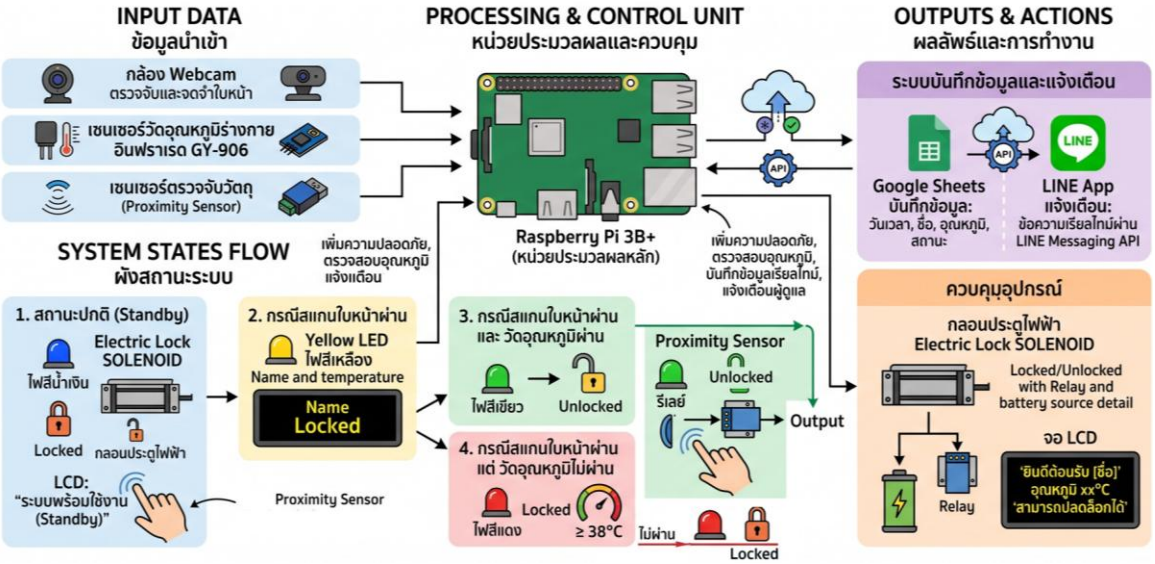
9.4.1 งานออกแบบระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า

ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า (Face Recognition) เป็นการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และการประมวลผลภาพเพื่อยืนยันตัวตนของผู้ใช้งานก่อนอนุญาตให้เข้าสู่พื้นที่ ระบบที่พัฒนาขึ้นใช้ Raspberry Pi 3B+ เป็นหน่วยประมวลผลหลัก ทำงานร่วมกับกล้อง Webcam สำหรับรับภาพใบหน้า เซนเซอร์อินฟราเรด GY-906 สำหรับตรวจวัดอุณหภูมิแบบไม่สัมผัส เซนเซอร์ตรวจจับวัตถุ อุปกรณ์แสดงสถานะ และกลอนประตูไฟฟ้า นอกจากนี้ ระบบยังสามารถบันทึกข้อมูลเหตุการณ์ลงใน Google Sheets และส่งการแจ้งเตือนไปยังผู้ดูแลระบบผ่านบริการของ LINE แนวคิดการออกแบบระบบแสดงดังรูปที่ 9.13



รูปที่ 9.11 การออกแบบระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า

หลักการทำงานโดยภาพรวมประกอบด้วย การรับข้อมูล (input) > การตรวจจับและจดจำใบหน้า (face detection and recognition) > การตรวจสอบเงื่อนไข (verification) > การตัดสินใจ (decision) > การควบคุมประตูและแสดงผล (access control and output) > การบันทึกและแจ้งเตือน (logging and notification) ดังรูปที่ 9.14



รูปที่ 9.12 แนวคิดการทำงานของระบบจดจำใบหน้าสำหรับควบคุมการเข้า–ออกประตู

เมื่อเริ่มต้นการทำงาน ระบบจะเข้าสู่สถานะพร้อมใช้งานและคงกลอนประตูไว้ในสถานะล็อก เมื่อผู้ใช้งานอยู่บริเวณหน้ากล้อง ระบบจะตรวจจับใบหน้า (face detection) จากภาพที่ได้รับ แล้วประมวลผลเพื่อเปรียบเทียบข้อมูลใบหน้ากับข้อมูลอ้างอิงของผู้ใช้ที่ลงทะเบียนไว้ หากผลการเปรียบเทียบเป็นไปตามเกณฑ์ที่กำหนด ระบบจะถือว่าผ่านขั้นตอนการยืนยันตัวตนและดำเนินการตรวจสอบเงื่อนไขถัดไป

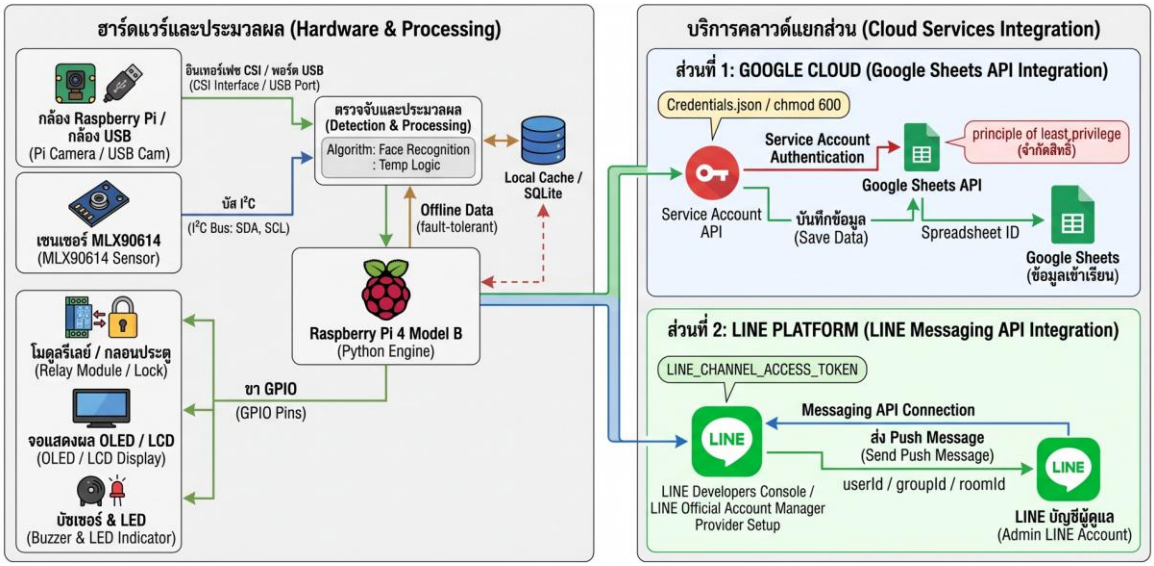
ในระบบต้นแบบนี้ หลังจากยืนยันตัวตนด้วยใบหน้าสำเร็จ ระบบจะตรวจวัดอุณหภูมิด้วยเซนเซอร์ GY-906 และเปรียบเทียบกับ ค่าเกณฑ์ที่กำหนดสำหรับการทดลอง หากผ่านเงื่อนไขระบบจะสั่ง Relay เพื่อควบคุมกลอนประตูให้ปลดล็อกชั่วคราว พร้อมแสดงชื่อผู้ใช้ ค่าอุณหภูมิ และสถานะการอนุญาตผ่านจอแสดงผลและ LED จากนั้นระบบจะบันทึกข้อมูลเหตุการณ์ เช่น วัน เวลา ผู้ใช้งาน ค่าอุณหภูมิ และสถานะการเข้าใช้งานลงใน Google Sheets รวมทั้งส่งการแจ้งเตือนไปยังผู้ดูแลระบบ

ในกรณีที่ระบบจดจำใบหน้าได้ แต่ผลการตรวจสอบอุณหภูมิไม่เป็นไปตามเงื่อนไขที่กำหนด ระบบจะไม่สั่งปลดล็อกประตู พร้อมแสดงสถานะปฏิเสธและบันทึกเหตุการณ์เพื่อให้สามารถตรวจสอบย้อนหลังได้ ส่วนกรณีที่ระบบไม่สามารถยืนยันใบหน้าได้ตามเกณฑ์ที่กำหนด ระบบจะคงประตูไว้ในสถานะล็อกและดำเนินการแจ้งสถานะตามที่ออกแบบไว้

นอกจากนี้ ระบบยังมี เซนเซอร์ตรวจจับวัตถุ สำหรับเป็นอินพุตในการสั่งปลดล็อกจากด้านภายในหรือใช้ตามเงื่อนไขที่กำหนดในระบบต้นแบบ เมื่อเซนเซอร์ตรวจพบวัตถุ ระบบจะส่งข้อมูลไปยัง Raspberry Pi เพื่อประมวลผลและสั่งปลดล็อกประตูชั่วคราว ก่อนกลับเข้าสู่สถานะล็อกและรอการใช้งานครั้งถัดไป ทั้งนี้ ในการนำไปใช้กับระบบควบคุมการเข้า–ออกจริง ควรออกแบบอุปกรณ์สำหรับการออกจากพื้นที่และการปลดล็อกฉุกเฉินให้เหมาะสมกับข้อกำหนดด้านความปลอดภัยของสถานที่

9.4.2 งานประยุกต์ใช้ Google Cloud และ Google Sheets

ข้อมูลเหตุการณ์ที่เกิดขึ้นสามารถบันทึกลงใน Google Sheets เพื่อใช้เป็นประวัติการเข้า–ออกและสนับสนุนการตรวจสอบย้อนหลัง ข้อมูลที่บันทึกอาจประกอบด้วย วันและเวลา ผู้ใช้งาน ผลการยืนยันตัวตน ค่าอุณหภูมิ สถานะการอนุญาต และวิธีการปลดล็อกประตู ขณะเดียวกัน การแจ้งเตือนผ่าน LINE Messaging API (Google Cloud, 2026; Google for Developers, 2026; Google for Developers, 2026; Google Cloud. 2026; LINE Developers, n.d.; LINE Developers, 2024) ช่วยให้ผู้ดูแลระบบได้รับข้อมูลเหตุการณ์จากระยะไกล ทำให้สามารถติดตามสถานะของระบบได้สะดวกยิ่งขึ้น (Halvorsen, 2026; Mathe et al., 2024)



รูปที่ 9.13 สถาปัตยกรรมการเชื่อมต่อระบบตรวจจับและรู้จำใบหน้ากับ Google Sheets API และ LINE Messaging API

1) การเชื่อมต่อ Google Cloud

จากรูปที่ 9.13 Google Sheets API ทำหน้าที่รับข้อมูลจากโปรแกรมบน Raspberry Pi และบันทึกลงใน Google Sheets เช่น ชื่อผู้ใช้งาน รหัสประจำตัว วัน เวลา ค่าอุณหภูมิ และผลการตรวจสอบ ระบบใช้บัญชีบริการ (service account) สำหรับยืนยันตัวตนของโปรแกรมแทนการเข้าสู่ระบบด้วยบัญชีผู้ใช้ทั่วไป แนวทางการนำไปปฏิบัติมีดังนี้

1.1) สร้างโปรเจกต์ใน Google Cloud และเปิดใช้งาน Google Sheets API

1.2) สร้าง Service Account สำหรับระบบตรวจจับใบหน้า

1.3) สร้างกุญแจของบัญชีบริการเป็นไฟล์ JSON และจัดเก็บไว้ใน Raspberry Pi อย่างปลอดภัย

1.4) คัดลอกค่า client_email จากไฟล์ JSON แล้วแชร์ Google Sheets ให้กับอีเมลดังกล่าว

1.5) กำหนดสิทธิ์เป็น Editor เฉพาะสเปรดชีตที่โปรแกรมต้องบันทึกข้อมูล โดยไม่จำเป็นต้องให้บทบาท Editor แก่ Service Account ทั้งโปรเจกต์

1.6)กำหนด Spreadsheet ID และชื่อแผ่นงานในโปรแกรม Python

1.7) เมื่อระบบรู้จำใบหน้าได้สำเร็จ โปรแกรมจะสร้างระเบียนข้อมูลและส่งไปยัง Google Sheets ผ่านการเชื่อมต่อ HTTPS ตัวอย่างข้อมูลที่ควรบันทึก ได้แก่

วันและเวลา	รหัสผู้ใช้	ชื่อ–นามสกุล	อุณหภูมิ	ผลการตรวจสอบ
17/09/2026 08:15	6501001	ผู้เรียน A	36.5 °C	บันทึกสำเร็จ

ไฟล์ JSON มี private key ซึ่งถือเป็นข้อมูลลับ จึงไม่ควรบันทึกไว้ในซอร์สโค้ด GitHub รายงาน หรือภาพหน้าจอ ควรจำกัดสิทธิ์ของไฟล์ เช่น chmod 600 และกำหนดตำแหน่งไฟล์ผ่านตัวแปรสภาพแวดล้อม GOOGLE_APPLICATION_CREDENTIALS การกำหนดสิทธิ์ดังกล่าวสอดคล้องกับหลักการให้สิทธิ์เท่าที่จำเป็น หรือ principle of least privilege

2) การเชื่อมต่อ LINE Messaging API

LINE Messaging API ทำหน้าที่ส่งข้อความแจ้งเตือนจาก Raspberry Pi ไปยังบัญชี LINE ของผู้ดูแล เช่น แจ้งว่าระบบบันทึกการเข้าเรียนสำเร็จ ตรวจพบอุณหภูมิสูง ไม่สามารถรู้จำใบหน้า หรือระบบเชื่อมต่อ Google Sheets ไม่สำเร็จ แนวทางการนำไปปฏิบัติมีดังนี้

2.1) สร้างหรือเลือก LINE Official Account สำหรับระบบ

2.2) เปิดใช้งาน Messaging API ผ่าน LINE Official Account Manager

2.3) ตรวจสอบ Messaging API Channel ใน LINE Developers Console

2.4) ออก Channel Access Token และจัดเก็บไว้ในตัวแปรสภาพแวดล้อม เช่น LINE_CHANNEL_ACCESS_TOKEN

2.5) เพิ่ม LINE Official Account เป็นเพื่อน หรือเพิ่มเข้ากลุ่มที่ต้องการรับข้อความ

2.6) กำหนดรหัสปลายทางเป็น userId, groupId หรือ roomId โดยไม่สามารถใช้ชื่อผู้ใช้หรือชื่อกลุ่มแทนได้

2.7) ให้โปรแกรม Python ส่ง Push Message เมื่อเกิดเหตุการณ์ตามเงื่อนไขที่กำหนด

2.8) ตรวจสอบ HTTP status code หากได้รับ 200 OK แสดงว่าคำขอได้รับการประมวลผลสำเร็จ ตัวอย่างข้อความแจ้งเตือน ได้แก่ ระบบบันทึกการเข้าเรียน

ชื่อ: ผู้เรียน A
เวลา: 08:15 น.
อุณหภูมิ: 36.5 °C
สถานะ: บันทึกข้อมูลสำเร็จ

Channel Access Token เป็นข้อมูลลับเช่นเดียวกับกุญแจของ Service Account จึงไม่ควรเขียนลงในโปรแกรมโดยตรงหรือแสดงในรายงานและภาพหน้าจอ

โดยสรุป ระบบนี้เป็นการบูรณาการ การจดจำใบหน้า การตรวจวัดอุณหภูมิ การควบคุมกลอนประตู การบันทึกข้อมูลบน Cloud และการแจ้งเตือนผ่านเครือข่าย เข้าด้วยกัน เพื่อแสดงแนว

ทางการพัฒนาระบบควบคุมการเข้า–ออกอัจฉริยะที่สามารถตรวจสอบตัวตน ตัดสินใจ ควบคุมอุปกรณ์ และบันทึกเหตุการณ์ได้โดยอัตโนมัติ

รายละเอียดการเชื่อมต่ออุปกรณ์ การลงทะเบียนข้อมูลใบหน้า การพัฒนาโปรแกรมจดจำใบหน้า การกำหนดเงื่อนไขการควบคุมประตู การเชื่อมต่อ Google Cloud Platform และ Google Sheets การแจ้งเตือนผ่าน LINE Messaging API และการทดสอบการทำงานของระบบ แสดงในภาคผนวก ก (ใบงานที่ 11)

9.5 งานประยุกต์ใช้เซนเซอร์ตรวจจับก๊าซ MQ–2 ในระบบความปลอดภัย

9.5.1 งานตรวจจับก๊าซและควบคุมวาล์วก๊าซอัตโนมัติด้วยเซนเซอร์ MQ–2 และ NodeMCU ESP8266

ระบบตัวอย่างเป็นการประยุกต์ใช้เซนเซอร์ MQ-2 ร่วมกับบอร์ด NodeMCU ESP8266 สำหรับตรวจจับการเปลี่ยนแปลงของระดับก๊าซไวไฟและควบคุมอุปกรณ์ตัดการจ่ายก๊าซ องค์ประกอบหลักประกอบด้วยเซนเซอร์ MQ-2, NodeMCU ESP8266, relay module, วาล์วตัดก๊าซที่ขับด้วยมอเตอร์ (motorized gas shut-off valve), แหล่งจ่ายไฟที่เหมาะสมกับอุปกรณ์ และ Push Button สำหรับการควบคุมหรือรีเซตระบบตามเงื่อนไขที่กำหนด

เซนเซอร์ MQ-2 เป็นเซนเซอร์ก๊าซชนิดสารกึ่งตัวนำโลหะออกไซด์ (Metal-Oxide Semiconductor: MOS) ที่มีความไวต่อก๊าซและไอระเหยไวไฟหลายชนิด เช่น LPG โพรเพน (propane) มีเทน (methane) ไฮโดรเจน (hydrogen) รวมถึงควัน ทั้งนี้ MQ-2 มีการตอบสนองต่อก๊าซหลายชนิด จึง ไม่ใช่เซนเซอร์ที่สามารถจำแนกชนิดของก๊าซได้อย่างจำเพาะ และค่าที่อ่านได้จากเอาต์พุตแอนะล็อกเป็นสัญญาณที่สัมพันธ์กับการเปลี่ยนแปลงของก๊าซ หากต้องการแสดงผลเป็นค่าความเข้มข้นเชิงปริมาณ เช่น ppm จำเป็นต้องมีการสอบเทียบและพิจารณาคุณลักษณะการตอบสนองของเซนเซอร์เพิ่มเติม

1) หลักการตรวจจับก๊าซและควบคุมวาล์วก๊าซอัตโนมัติ

หลักการทำงานของระบบสามารถแบ่งออกเป็น 4 ขั้นตอนสำคัญ ดังนี้

1.1) การตรวจจับก๊าซ

เมื่อเริ่มต้นระบบ ชุดทำความร้อน (heater) ภายในเซนเซอร์ MQ-2 จะได้รับพลังงานและทำให้วัสดุไวต่อก๊าซอยู่ในสภาวะที่เหมาะสมต่อการตรวจจับ เมื่อมีก๊าซที่เซนเซอร์มีความไวอยู่ในบริเวณตรวจวัด คุณสมบัติทางไฟฟ้าของวัสดุไวต่อก๊าซจะเปลี่ยนแปลง ส่งผลให้ความต้านทานของเซนเซอร์และแรงดันเอาต์พุตของวงจรตรวจวัดเปลี่ยนแปลงตามไปด้วย ระบบจึงสามารถใช้การเปลี่ยนแปลงของสัญญาณดังกล่าวเป็นข้อมูลสำหรับตรวจสอบสภาวะก๊าซในบริเวณที่เฝ้าระวัง

1.2) การประมวลผลและเปรียบเทียบกับค่าเกณฑ์

NodeMCU ESP8266 รับสัญญาณจากเซนเซอร์ผ่านอินพุตแอนะล็อกและแปลงเป็นค่าดิจิทัลด้วยตัวแปลงแอนะล็อกเป็นดิจิทัล (Analog-to-Digital Converter: ADC) จากนั้นโปรแกรมจะนำค่าที่อ่านได้ไปเปรียบเทียบกับ ค่าเกณฑ์ (Threshold) ที่กำหนดสำหรับระบบต้นแบบ หากค่าที่ตรวจวัดยังอยู่ในช่วงปกติ ระบบจะคงวาล์วก๊าซไว้ในสถานะการทำงานตามที่กำหนดและเฝ้าระวังสัญญาณจากเซนเซอร์อย่างต่อเนื่อง

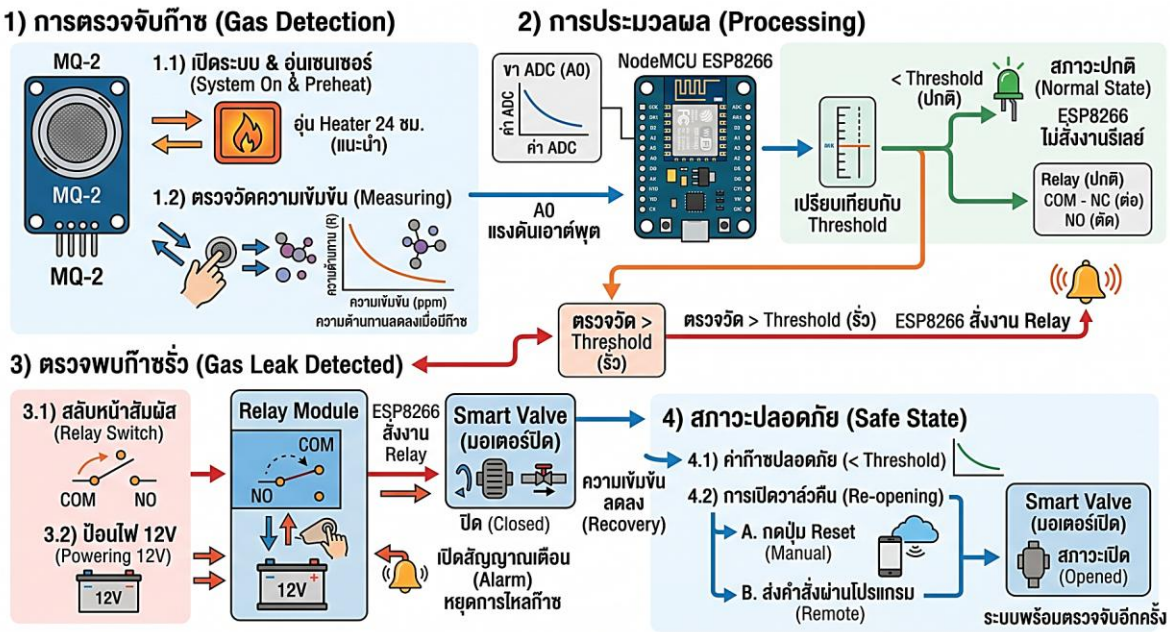
1.3) การตอบสนองเมื่อตรวจพบสภาวะผิดปกติ

เมื่อค่าที่ตรวจวัดสูงกว่าเกณฑ์ที่กำหนด ระบบจะถือว่าเกิดสภาวะที่ต้องแจ้งเตือน NodeMCU จะสั่งงานอุปกรณ์แจ้งเตือนตามที่ออกแบบไว้ และส่งสัญญาณควบคุมไปยัง Relay Module ซึ่งทำหน้าที่เป็นส่วนเชื่อมต่อระหว่างวงจรควบคุมแรงดันต่ำกับวงจรกำลังของวาล์ว

สำหรับวาล์วที่ใช้มอเตอร์และต้องควบคุมทิศทางการหมุน relay module สามารถใช้สลับการจ่ายไฟตามวงจรที่ออกแบบ เพื่อขับวาล์วไปยัง ตำแหน่งปิด (closed position) ทำให้แหล่งจ่ายก๊าซถูกตัดและช่วยลดการจ่ายก๊าซเพิ่มเติมเข้าสู่บริเวณที่ตรวจพบความผิดปกติ

1.4) การเข้าสู่สถานะปลอดภัยและการคืนระบบ

หลังจากสั่งปิดวาล์วก๊าซ ระบบควรคงวาล์วไว้ในสถานะปิดและแจ้งสถานะความผิดปกติ แม้ว่าค่าที่ตรวจวัดจากเซนเซอร์จะลดลงแล้วก็ตาม การเปิดวาล์วกลับควรดำเนินการหลังจากตรวจสอบและแก้ไขสาเหตุของการรั่วไหล รวมทั้งยืนยันว่าบริเวณดังกล่าวอยู่ในสภาวะปลอดภัยแล้ว จากนั้นจึงสั่ง Reset หรือคืนระบบตามขั้นตอนที่กำหนด เพื่อป้องกันการเปิดจ่ายก๊าซกลับโดยอัตโนมัติในขณะที่สาเหตุของการรั่วไหลยังไม่ได้รับการแก้ไข



รูปที่ 9.14 แนวคิดการออกแบบระบบตรวจจับก๊าซและควบคุมวาล์วก๊าซอัตโนมัติด้วยเซนเซอร์ MQ-2 และ NodeMCU ESP8266

โดยสรุป ระบบนี้ทำงานตามกระบวนการ การตรวจจับ (sensing) > การประมวลผล (processing) > การตัดสินใจ (decision) > การแจ้งเตือนและควบคุมวาล์ว (alarm and actuation) > สถานะปลอดภัย (safe state) ซึ่งแสดงให้เห็นแนวทางการประยุกต์ใช้เซนเซอร์ ไมโครคอนโทรลเลอร์ และอุปกรณ์ควบคุมร่วมกันในระบบรักษาความปลอดภัยอัจฉริยะ

รายละเอียดการเชื่อมต่อวงจร การกำหนดค่า Threshold การควบคุม Relay และวาล์วก๊าซ การเขียนโปรแกรม และการทดสอบการทำงานของระบบ แสดงในภาคผนวก ก (ใบงานที่ 12)

บรรณานุกรมบทที่ 9

ชลดา ปานสง, เกียรติศักดิ์ สมฤทธิ์, จิรพงษ์ จิตตะโคตร์, พัชราวรรณ พูลใจ, ศิวกร รัตนวราหะ, และธนพล แก้วคำแจ้ง. (2566). การพัฒนาสื่อบทเรียนออนไลน์มูเดิลคลาวด์ สำหรับการฝึกอบรมการติดตั้งและบำรุงรักษาระบบกล้องวงจรปิด ตามมาตรฐานกรมพัฒนาฝีมือแรงงาน. *วารสารวิจัยและนวัตกรรมการอาชีวศึกษา*, *7*(2), 66-75.

ชลดา ปานสง, ปรียานุช จันหนู, และวัฒนา ภูสูง. (2561). การพัฒนาชุดฝึกอบรมการติดตั้งและบำรุงรักษากล้องวงจรปิด ตามสมรรถนะของกรมพัฒนาฝีมือแรงงาน. ใน: *การประชุมวิชาการครุศาสตร์อุตสาหกรรมระดับนานาชาติและระดับชาติ (The 6th International Conference on Learning Innovation in Science and Technology (ICLIST 2018) and the 2nd National Conference on Learning Innovation in Science and Technology (NCLIST 2018): ICLIST & NCLIST 2018*. วันที่ 21-24 มีนาคม 2561,710-723.

ชลดา ปานสง, ศราวุธ พลรักษา, ชาญณรงค์ บุตรทา, อุดมศักดิ์ จันทรทาโพ, และ บัญชา แสนโสดา. (2565). การพัฒนาชุดฝึกอบรมฐานสมรรถนะ เรื่อง การติดตั้งและเขียนโปรแกรมควบคุมอัตโนมัติในงานอุตสาหกรรม ตามมาตรฐานของ Thai-Meister. *วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น, 19*(2). 1-14.

เอชไอพี โกลบอล จำกัด. (2015). *คู่มือการใช้งาน CMG 280* [คู่มือผลิตภัณฑ์]. https://hip-servicecenter.com/newpro/download/คู่มือการใช้งาน%20Standalone%20Access%20Control%20CMG%20280.pdf

HIP. (ม.ป.ป.). *คู่มือการใช้งาน Standalone Access Control CMG 280* [คู่มือการใช้งาน]. HIP Service Center. https://hip-servicecenter.com/newpro/download/คู่มือการใช้งาน%20Standalone%20Access%20Control%20CMG%20280.pdf.

Aqib, M. (2018). *RFID and keypad based door lock using Arduino*. Hackster.io. https://www.hackster.io/muhammad-aqib/rfid-and-keypad-based-door-lock-using-arduino-89e1d5.

Google Cloud. (2026). *Set up Application Default Credentials*. https://docs.cloud.google.com/docs/authentication/provide-credentials-adc

Google for Developers. (2026). *Create access credentials*. https://developers.google.com/workspace/guides/create-credentials

Google for Developers. (2026). *Enable Google Workspace APIs*. https://developers.google.com/workspace/guides/enable-apis

Google Cloud. (2026). *Create and delete service account keys*. https://docs.cloud.google.com/iam/docs/keys-create-delete.

Global Column Limited. (2016). *VStarcam C7824WIP HD wireless IP security camera with audio night vision pan & tilt*. HobbyKing. https://hobbyking.com/vstarcam-c7824wip-hd-wireless-hd-ip-security-camera-with-audio-night-vision-pan-tilt.html.

Halvorsen, H.-P. (2026). *Raspberry Pi and Python*. https://www.halvorsen.blog/documents/programming/python/.

LINE Developers. (2024). *Get started with the Messaging API*. https://developers.line.biz/en/docs/messaging-api/getting-started/

LINE Developers. (n.d.). *Messaging API reference*. https://developers.line.biz/en/reference/messaging-api/.

Mathe, S. E., Kondaveeti, H. K., Vappangi, S., Vanambathina, S. D., & Kumaravelu, N. K. (2024). A comprehensive review on applications of Raspberry Pi. *Computer Science Review, 52*, 100636.

Mohanan, V. (2021). *Interfacing R307 optical fingerprint scanner with Arduino boards for biometric authentication*. Circuitstate Electronics. https://www.circuitstate.com/tutorials/interfacing-r307-optical-fingerprint-scanner-with-arduino-boards-for-biometric-authentication/.

Yu, L. (2016). *How to distinguish T568A and T568B of RJ45 Ethernet cable wiring?* LinkedIn. https://www.linkedin.com/pulse/how-distinguish-t568a-t568b-rj45-ethernet-cable-wiring-laura-yu.

ภาคผนวก ก
ใบงาน

	ใบงานที่ 1 เรื่อง งานออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้องตามมาตรฐานที่กำหนด

วัตถุประสงค์

1. สำรวจพื้นที่สำหรับติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
2. ใช้แอพพลิเคชั่นวัดระยะการเดินสายติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
3. เลือกชนิดของกล้องโทรทัศน์วงจรปิดได้เหมาะสมกับงาน
4. คำนวณระยะเลนส์กล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
5. คำนวณความยาวโฟกัสได้อย่างถูกต้อง
6. คำนวณหาฮาร์ดดิสก์ไดร์ฟได้อย่างถูกต้อง
7. คำนวณหาแบนด์วิธได้อย่างถูกต้อง
8. เขียนแบบงานติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง

เครื่องมือและอุปกรณ์

1. ดินสอ/ปากกา/กระดาษ
2. เครื่องคำนวณ
4. แอพพลิเคชั่นวัดระยะ
4. โปรแกรมการออกแบบงานติดตั้งระบบกล้องโทรทัศน์วงจรปิด

ความรู้พื้นฐานในการปฏิบัติงาน

ก่อนดำเนินการติดตั้งระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV) ปฏิบัติงานควรมีความรู้พื้นฐานเกี่ยวกับการสำรวจพื้นที่ การกำหนดวัตถุประสงค์ในการเฝ้าระวัง การเลือกชนิดและคุณสมบัติของกล้อง การกำหนดตำแหน่งติดตั้ง ตลอดจนการออกแบบระบบส่งสัญญาณ ระบบบันทึกภาพ เครือข่าย และแหล่งจ่ายไฟ เพื่อให้ระบบสามารถครอบคลุมพื้นที่เป้าหมายและให้ข้อมูลภาพที่เหมาะสมกับวัตถุประสงค์ในการรักษาความปลอดภัย ประกอบด้วย

1. การวิเคราะห์วัตถุประสงค์ของการเฝ้าระวัง

ต้องกำหนดว่าต้องการใช้กล้องเพื่อวัตถุประสงค์ใด เช่น ตรวจสอบภาพรวมของพื้นที่ ตรวจจับบุคคลหรือยานพาหนะ สังเกตเหตุการณ์ หรือใช้ภาพเพื่อช่วยระบุตัวบุคคล เนื่องจากวัตถุประสงค์ที่แตกต่างกันมีผลต่อการเลือกความละเอียด เลนส์ ตำแหน่ง และมุมมองของกล้อง

2. การสำรวจและวิเคราะห์พื้นที่ติดตั้ง

3. ควรสำรวจขนาดและลักษณะของพื้นที่

จุดเข้า–ออก ตำแหน่งที่ต้องเฝ้าระวัง สิ่งกีดขวาง จุดอับ ระดับความสูงในการติดตั้ง สภาพแสง และสภาพแวดล้อม รวมถึงตำแหน่งของระบบไฟฟ้าและระบบเครือข่ายที่มีอยู่ เพื่อนำข้อมูลมาใช้จัดทำแผนผังการติดตั้ง

4. มุมมองและพื้นที่ครอบคลุมของกล้อง

ผู้ปฏิบัติงานควรเข้าใจ Field of View (FOV) ซึ่งเป็นขอบเขตพื้นที่ที่กล้องสามารถมองเห็นได้ โดยสัมพันธ์กับความยาวโฟกัสของเลนส์ ขนาดเซนเซอร์รับภาพ ระยะห่างระหว่างกล้องกับวัตถุ และตำแหน่งติดตั้ง เลนส์มุมกว้างช่วยให้เห็นพื้นที่กว้าง แต่รายละเอียดของวัตถุในระยะไกลอาจลดลง

5. การเลือกกล้องและเลนส์ให้เหมาะสมกับงาน

ควรพิจารณาชนิดของกล้อง ความละเอียดของภาพ ความยาวโฟกัสของเลนส์ ความสามารถในการทำงานในสภาวะแสงน้อย ระบบอินฟราเรด ช่วงไดนามิก เช่น WDR และระดับการป้องกันฝุ่นและน้ำสำหรับการติดตั้งภายนอกอาคาร ทั้งนี้ การเลือกกล้องไม่ควรพิจารณาจากความละเอียดหรือความยาวโฟกัสเพียงอย่างเดียว แต่ควรสัมพันธ์กับวัตถุประสงค์และพื้นที่จริง

6. การกำหนดตำแหน่งและทิศทางของกล้อง

ตำแหน่งติดตั้งควรทำให้กล้องสามารถมองเห็นพื้นที่เป้าหมายได้อย่างเหมาะสม ลดจุดอับและหลีกเลี่ยงสิ่งกีดขวาง แสงย้อน หรือแหล่งกำเนิดแสงที่ส่องเข้าสู่เลนส์โดยตรง นอกจากนี้ควรคำนึงถึงความสูง มุมก้ม–เงย และความสะดวกในการบำรุงรักษา

7. การออกแบบระบบส่งสัญญาณและเครือข่าย

ระบบกล้องแอนะล็อกและระบบ IP camera มีโครงสร้างการส่งข้อมูลแตกต่างกัน ระบบแอนะล็อกอาจใช้สายโคแอกเชียลเชื่อมต่อกับ DVR ขณะที่ระบบ IP ใช้เครือข่าย Ethernet เชื่อมต่อกล้องกับ Network Switch หรือ PoE Switch และ NVR/VMS ดังนั้นผู้ปฏิบัติงานควรเข้าใจชนิดสายสัญญาณ ระยะทาง การเดินสาย และความต้องการแบนด์วิดท์ของระบบ

8. การออกแบบระบบบันทึกและจัดเก็บข้อมูล

ควรกำหนดจำนวนกล้อง ความละเอียด อัตราเฟรม รูปแบบการบีบอัด ระยะเวลาที่ต้องการเก็บภาพ และรูปแบบการบันทึก เพื่อใช้ประมาณความจุของอุปกรณ์จัดเก็บข้อมูล รวมถึงเลือก DVR, NVR หรือระบบจัดเก็บข้อมูลให้เหมาะสม

9. การออกแบบแหล่งจ่ายไฟ

ต้องพิจารณาแรงดัน กระแส และกำลังไฟฟ้าที่กล้องและอุปกรณ์ต้องการ รวมถึงระยะทางของสายและแรงดันตก สำหรับระบบ IP camera อาจใช้ Power over Ethernet (PoE) เพื่อส่งข้อมูลและจ่ายพลังงานผ่านสาย Ethernet เส้นเดียว หากอุปกรณ์รองรับมาตรฐานที่สอดคล้องกัน

10. ความมั่นคงปลอดภัยของระบบ IP camera

สำหรับกล้องที่เชื่อมต่อเครือข่าย ควรคำนึงถึงการกำหนด IP Address การเปลี่ยนรหัสผ่านเริ่มต้น การกำหนดสิทธิ์ผู้ใช้งาน การอัปเดต Firmware การแบ่งเครือข่าย เช่น VLAN และการจำกัดการเข้าถึงกล้องจากเครือข่ายที่ไม่จำเป็น เพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต

11. ความปลอดภัยในการติดตั้งและการบำรุงรักษา

ผู้ปฏิบัติงานต้องคำนึงถึงความปลอดภัยทางไฟฟ้า การใช้เครื่องมือ การทำงานบนที่สูง การยึดกล้องและอุปกรณ์ให้แข็งแรง การป้องกันสายและจุดต่อจากสภาพแวดล้อม รวมทั้งจัดวางอุปกรณ์ให้สามารถตรวจสอบและบำรุงรักษาได้สะดวก

สำหรับ ใบงานที่ 1: การออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิดบริเวณโรงจอดรถ ที่คุณมีพื้นที่ตัวอย่าง 5.50 × 5.50 × 3 เมตร ความรู้พื้นฐานข้างต้นถือว่าเพียงพอมากแล้วค่ะ จากนั้นส่วน “งานที่กำหนด” จึงค่อยให้นักศึกษา สำรวจพื้นที่ > กำหนดพื้นที่เฝ้าระวัง > เลือกกล้องและเลนส์ > กำหนดตำแหน่งติดตั้ง > กำหนด FOV > เขียนแผนผัง > ตรวจสอบจุดอับ > สรุปเหตุผลในการออกแบบ รายละเอียดในบทที่ 3 ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

ขั้นตอนการปฏิบัติงาน

1. จากแผนผังโรงจอดรถในรูปที่ 1.1 โดยลูกค้ากำหนดมาให้ดังนี้

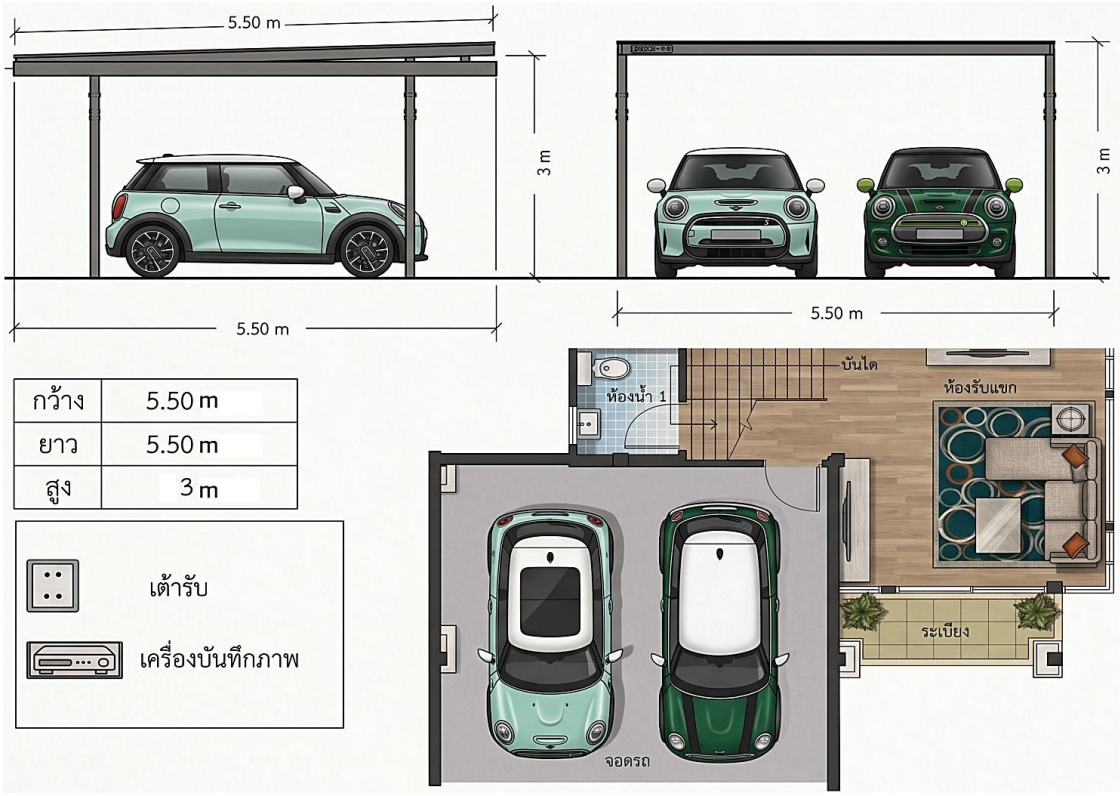
1.1 โรงรถมีขนาด 5.50 x 5.50 x 3 m

1.2 กำหนดให้ติดตั้งกล้องโทรทัศน์วงจรปิดเพียง 1 ตัว

1.3 กล้องสามารถจับภาพรถขณะเข้า – ออก ภายในโรงรถ

1.4 กล้องสามารถจับภาพได้ในพื้นที่ที่มีแสงน้อย

	ใบงานที่ 1 เรื่อง งานออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)



รูปที่ 1.1 แผนผังโรงจอดรถสำหรับออกแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด

2. เลือกใช้อุปกรณ์ในการติดตั้งกล้องโทรทัศน์วงจรปิดให้เหมาะสมกับงาน

2.1 เลือกชนิดของกล้องที่ใช้ และจำนวนกล้อง

.....

.....

.....

.....

.....

2.2 เลือกเลนส์ที่ใช้

.....

.....

.....

.....

.....

2.2.1 คำนวณระยะเลนส์กล้องโทรทัศน์วงจรปิด โดยกำหนดระยะห่างของวัตถุ 6 เมตร ใช้ CCD 1/3”

2.2.2 คำนวณความยาวโฟกัส โดยกำหนดให้จับภาพระยะ 10 ฟุต

2.3 เครื่องบันทึกภาพและแสดงภาพ

2.4 คำนวณหาฮาร์ดดิสก์ไดร์ฟ โดยกำหนดให้ กล้องความละเอียด 2 ล้านพิกเซล จำนวนความจุ Hard disk 1 TB

2.5 คำนวณหาแบนด์วิธ โดยกำหนดให้ใช้อัตราการบันทึกที่ 512 kbps

2.6 เลือกสายสัญญาณที่ใช้

---

3. เขียนแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด

สรุปผลการทดลอง

เอกสารอ้างอิง

กิตติศักดิ์ เฮงสว่าง. (2553). *การจัดการระบบเครือข่ายกล้องวงจรปิดเอซิต*. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีมหานคร.

ชลดา ปานสง, เกียรติศักดิ์ สมฤทธิ์, จิรพงษ์ จิตตะโคตร์, พัชราวรรณ พูลใจ, ศิวกร รัตนวราหะ, และธนพล แก้วคำแจ้ง. (2566). การพัฒนาสื่อบทเรียนออนไลน์มูเดิลคลาวด์สำหรับการฝึกอบรมการติดตั้งและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด ตามมาตรฐานกรมพัฒนาฝีมือแรงงาน. *วารสารวิจัยและนวัตกรรมการอาชีวศึกษา*, *7*(2), 66-75.

ชลดา ปานสง, ปรียานุช จันหนู, และวัฒนา ภูสูง. (2561). การพัฒนาชุดฝึกอบรมการติดตั้งและบำรุงรักษากล้องโทรทัศน์วงจรปิด ตามสมรรถนะของกรมพัฒนาฝีมือแรงงาน. ใน: *การประชุมวิชาการครุศาสตร์อุตสาหกรรมระดับนานาชาติและระดับชาติ (The 6th International Conference on Learning Innovation in Science and Technology (ICLIST 2018) and the 2nd National Conference on Learning Innovation in Science and Technology (NCLIST 2018): ICLIST & NCLIST 2018*. วันที่ 21-24 มีนาคม 2561,710-723.

พกิจ สุวัตถิ์. (2557). *การปฏิบัติงานด้านระบบกล้องวงจรปิด CCTV*. กรุงเทพฯ: ภาควิชาวิศวกรรมศาสตร์และอุตสาหกรรมวิจัย คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสยาม.

CS Odessa. (2025a). *CCTV network example*. https://www.conceptdraw.com/How-To-Guide/cctv-network-example.

Ideal Quality Solutions Co., Ltd. (2560). *ระบบกล้องวงจรปิด*. https://www.ideal-solutions.co.th/products/cctv-closed-circuit-television-system/

JVSG.com. (2024). *Video surveillance design apps*. https://www.jvsg.com/.

Kruegle, H. (2011). *CCTV surveillance: Video practices and technology*. Butterworth-Heinemann.

Samsung CCTV Thai. (2024). *การดูแลและบำรุงรักษากล้องวงจรปิด CCTV*. https://www.samsungcctvthai.com/การดูแลและบำรุงรักษา/.

	ใบงานที่ 2 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ติดตั้งกล้องโทรทัศน์วงจรปิดแบบแอนะล็อกได้อย่างถูกต้องตามมาตรฐาน

วัตถุประสงค์

1. อ่านแบบงานติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
2. เลือกใช้อุปกรณ์ของกล้องโทรทัศน์วงจรปิดได้เหมาะสมกับงาน
3. ติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
4. เดินสายสัญญาณได้เหมาะสมกับหน้างาน
5. เข้าหัวสายสัญญาณโคแอกซ์เชียลได้อย่างถูกต้อง
6. เชื่อมต่อระบบกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
7. ตรวจสอบระบบกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง

เครื่องมือและอุปกรณ์

1. กล้องโทรทัศน์วงจรปิดแบบแอนะล็อก
2. กล่องพักสาย
3. เครื่องบันทึกภาพ DVR
4. สายไฟ
5. สาย RG-6
6. ข้อต่อท่อ
7. หัว BNC
8. ตลับเมตร หรือไม้บรรทัด
9. ครีมย้ำหัว
10. สว่าน
11. คีมตัดท่อ
12. ถุงมือ
13. โฮลซอ
14. ดินสอ
15. คัทเตอร์

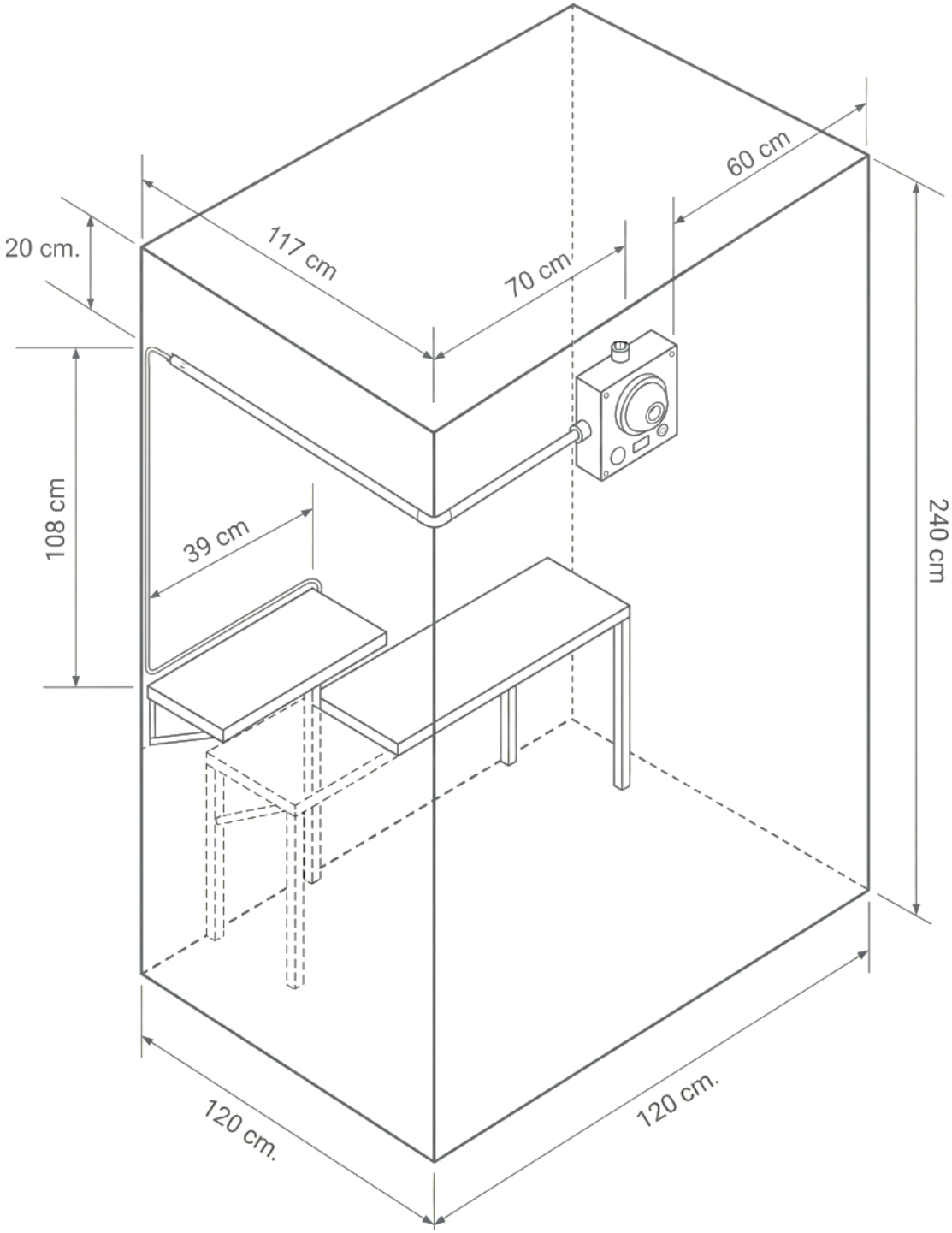
ความรู้พื้นฐานในการปฏิบัติงาน

การติดตั้งกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก (Analog CCTV) ผู้ปฏิบัติงานควรมีความรู้เกี่ยวกับ หลักการทำงานของกล้อง การเลือกตำแหน่งและมุมติดตั้ง การเดินสายสัญญาณและสายไฟ ตลอดจนการเชื่อมต่อกล้องกับเครื่องบันทึกภาพ DVR (Digital Video Recorder) โดยทั่วไปกล้องจะส่งสัญญาณภาพผ่านสายโคแอกเชียลไปยัง DVR เพื่อประมวลผล บันทึก และแสดงภาพบนจอภาพ นอกจากนี้ ควรมีความรู้เกี่ยวกับ แหล่งจ่ายไฟ ขั้วต่อสายสัญญาณ การตรวจสอบคุณภาพของภาพ และความปลอดภัยในการติดตั้ง เพื่อให้ระบบสามารถทำงานได้อย่างถูกต้อง มีเสถียรภาพ และครอบคลุมพื้นที่ รายละเอียดในบทที่ 3 ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

	ใบงานที่ 2 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ขั้นตอนการปฏิบัติงาน

1. อ่านแบบงานติดตั้งกล้องวงจรปิดแบบแอนะล็อก ดังรูปที่ 2.1



รูปที่ 2.1 แบบจำลองการติดตั้งและเดินสายระบบกล้องโทรทัศน์วงจรปิด

	ใบงานที่ 2 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

การอ่านแบบเป็นความรู้พื้นฐานของงานช่างอุตสาหกรรมที่จะต้องรู้จักสัญลักษณ์ในการเขียนแบบ จากรูปที่ 2.1 เป็นการติดตั้งกล้องโทรทัศน์วงจรปิดบริเวณมุมด้านบนของชุดฝึกปฏิบัติที่ระดับความสูงประมาณ 240 cm โดยยึดกล้องเข้ากับผนังด้านข้างของโครงสร้าง และหันมุมกล้องลงสู่พื้นที่ปฏิบัติงานภายใน เพื่อให้สามารถมองเห็นพื้นที่ได้อย่างครอบคลุมและลดจุดอับของภาพ ตำแหน่งการติดตั้งกล้องอยู่ห่างจากมุมผนังด้านหน้าประมาณ 70 cm และห่างจากด้านข้างประมาณ 60 cm (ชลดา ปานสง และคณะ, 256; ชลดา ปานสง และคณะ, 2566)

2. การเลือกใช้อุปกรณ์ในงานกล้องโทรทัศน์วงจรปิด

2.1 กล้องโทรทัศน์วงจรปิด ใช้กล้องโทรทัศน์วงจรปิดแบบแอนะล็อก 1 ตัว รุ่น HA36513

2.2 เลนส์กล้องโทรทัศน์วงจรปิด ใช้เลนส์ที่ใช้ ขนาด 4 mm

2.3 เครื่องบันทึกภาพ เลือกใช้เป็นเครื่องบันทึกภาพ DVR รุ่น HA-5504 แบบ 4 พอร์ท

2.4 สายสัญญาณเชื่อมต่อ ใช้สายสัญญาณเลือกใช้สายโคแอคเชียล ชนิด RG59 เหมาะสมกับระยะในการเดินสาย 0-200 m สายไฟเลี้ยงกล้องโทรทัศน์วงจรปิด 12 V และสาย VGA

3. ขั้นตอนการติดตั้งกล้องโทรทัศน์วงจรปิด

ขั้นตอนการติดตั้งกล้องโทรทัศน์วงจรปิดแบบแอนะล็อก มีขั้นตอนในการติดตั้งดังนี้

3.1 เตรียมเครื่องมือ วัสดุ อุปกรณ์ การติดตั้งกล้องโทรทัศน์วงจรปิดให้ครบถ้วน

3.2 นำฝากล่องพักสายไฟ (junction box) กำหนดจุดที่ต้องการติดตั้งกล้องโทรทัศน์วงจรปิด โดยให้กล้องโทรทัศน์วงจรปิดอยู่ในกึ่งกลางฝาเพื่อความสวยงาม ดังรูปที่ 2.2

รูปที่ 2.2 กำหนดจุดติดตั้งกล้องโทรทัศน์วงจรปิดบนกล่อง

3.3 ใส่ก้านข้อต่อโฮลซอลงในหัวจับของสว่านไฟฟ้า จรดปลายของดอกสว่านลงที่จุดศูนย์กลางของรูที่จะเจาะ กดไกสว่านแล้วค่อย ๆกดสว่านลงในเนื้อวัสดุ ก่อนจะเร่งความเร็วตามลำดับ ดังรูปที่ 2.3

รูปที่ 2.3 การเจาะรูของฐานของกล้อง

3.4 ติดตั้งฐานยึดกล้องโทรทัศน์วงจรปิดเข้ากับกล่องพักสายไฟ หรือฐานรองกล้อง โดยใช้สกรูขันยึดเพื่อเพิ่มความแข็งแรงและความมั่นคงในการติดตั้ง ช่วยให้สามารถจัดเก็บสายสัญญาณและสายไฟได้อย่างเป็นระเบียบ รวมทั้งป้องกันความเสียหายที่อาจเกิดกับสายเชื่อมต่อของกล้องโทรทัศน์วงจรปิด ดังรูปที่ 2.4

รูปที่ 2.4 ขั้นตอนการใช้ไขควงขันสกรูเพื่อยึดฐานของกล้องให้แน่นกับแผ่นฐานรอง

3.5 อ่านแบบแล้วทำการกำหนดจุดติดตั้งกล้องโทรทัศน์วงจรปิดบนพื้นที่ติดตั้งกล้อง โดยใช้ตลับmวัดให้ได้ระยะตามแบบ ดังรูปที่ 2.5

รูปที่ 2.5 การกำหนดจุดติดตั้งกล้องโทรทัศน์วงจรปิด

3.6 นำตัวกล่องพักสาย กำหนดจุดที่จะทำใส่ข้อต่อ ดังรูปที่ 2.6

รูปที่ 2.6 การวัดระยะรูที่จะเจาะบนกล่องพักสายไฟ

3.7 ใส่ก้านข้อต่อของโฮลซอลงในหัวจับของสว่านไฟฟ้า จรดปลายของดอกสว่านลงที่จุดศูนย์กลางของรูที่จะเจาะ กดไกสว่านแล้วค่อยๆกดสว่านลงในเนื้อวัสดุ ก่อนจะเร่งความเร็วตามลำดับ ดังรูปที่ 2.7

3.8 ประกอบข้อต่อเข้ากล่องพักสาย ดังรูปที่ 2.8

3.9 เมื่อทำการวัดระยะที่จะทำการติดกล่องพักสายไฟลงแล้ว จากนั้นใช้ดอกไขควงหัวแฉกใส่หัวจับของสว่านไฟฟ้า ไขตะปูเกลียวยึดกล่องเข้ากับผนังให้แน่น ดังรูปที่ 2.9

รูปที่ 2.7 การใช้ดอกสว่านเจาะรูของกล่องพักสายไฟ

รูปที่ 2.8 การประกอบข้อต่อเข้ากล่องพักสายไฟ

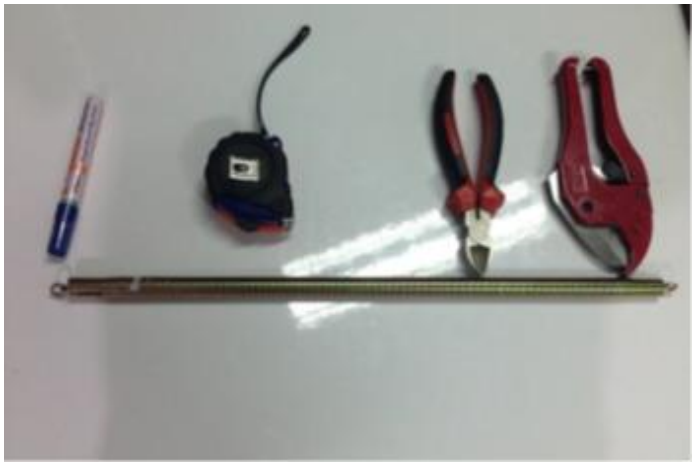
รูปที่ 2.9 การใช้ตะปูเกลียวยึดกล่องพักสายไฟเข้ากับผนัง

2. การเดินสายนำสัญญาณ

การเดินสายนำสัญญาณ มี 2 แบบ ได้แก่การเดินสายในท่อพีวีซี และการเดินสายด้วยเข็มขัดรัดสาย

2.1 ขั้นตอนการเดินสายในท่อพีวีซี

2.1.1 เตรียมเครื่องมือการเดินสายสัญญาณด้วยท่อพีวีซี ให้เรียบร้อย รูปที่ 2.10



รูปที่ 2.10 เครื่องมือสำหรับการเดินสายในท่อพีวีซี

2.1.2 อ่านแบบ ทำการวัดระยะเพื่อนำไปกำหนดจุดติดแคลมป์กล้ามปู รูปที่ 2.11

รูปที่ 2.11 การวัดระยะการวางท่อพีวีซีตามแบบ

2.1.3 กำหนดระยะจุดติดแคลมป์กล้ามปู เพื่อที่จะวางท่อโดยห่างกันประมาณ 60 - 80 cm รูปที่ 2.12

รูปที่ 2.12 การกำหนดระยะแคล้มกล้ามปู

2.1.4 ใช้ดอกไขควงหัวแฉกใส่หัวจับของสว่านไฟฟ้า ไขตะปูเกลียวยึดทำการเจาะยึด แคลมป์กล้ามปูกับผนังให้แน่น ดังรูปที่ 2.13

รูปที่ 2.13 การเจาะยึดแคลมป์กล้ามปูกับผนัง

2.1.5 อ่านแบบและใช้กรรไกรตัดท่อพีวีซี ตัดตามความยาวที่ต้องการ ดังรูปที่ 2.14

รูปที่ 2.14 การใช้กรรไกรตัดท่อพีวีซี

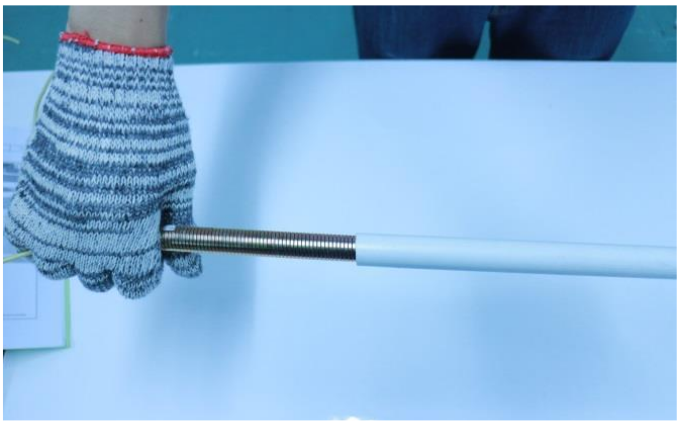
2.1.6 นำท่อที่ตัดเรียบร้อยแล้วมาทำการวัดระยะที่ต้องการตัดจากนั้นทำเครื่องหมายไว้ ดังรูปที่ 2.15

รูปที่ 2.15 การกำหนดระยะท่อ

2.1.7 ใช้ลวดผูกไว้ที่ปลายสปริงเพื่อใช้เป็นตัวกำหนดตำแหน่งของสปริง รูปที่ 2.16

รูปที่ 2.16 การกำหนดตำแหน่งของสปริง

2.1.8 ใส่สปริงเข้าไปตามตำแหน่งที่ต้องการ ดังรูปที่ 2.17



รูปที่ 2.17 การใส่สปริงตามตำแหน่ง

2.1.9 ให้ความร้อนกับท่อพีวีซี โดยใช้เครื่องเป่าลมร้อนให้ความร้อนกับท่ออย่างทั่วถึงและสม่ำเสมอ ดังรูปที่ 2.18

รูปที่ 2.18 การเป่าลมร้อนท่อ PVC

2.1.10 นำท่อไปดัดเข้ากับโค้งไม้แบบโดยให้จุดที่กำหนดอยู่ตรงกลางโค้งเพื่อให้ได้ 90 องศา ดังรูปที่ 2.19

รูปที่ 2.19 การดัดท่อตามแบบไม้

2.1.11 นำผ้าเปียกหรือฟองน้ำหล่อเย็นให้ที่ PVC แข็งตัว จากนั้นนำสปริงดัดท่อออกจากท่อ PVC ที่ดัดเรียบร้อยแล้ว และตรวจสอบความโค้งและความสวยงามของท่อ ดังรูปที่ 2.20

รูปที่ 2.20 การตรวจสอบความโค้งของท่อพีวีซี

2.1.12 ในกรณีที่ไม่ได้ดัดท่อพีวีซี สามารถใช้ข้อต่อต่อพีวีซีใช้แทนกันได้ เพื่อความสะดวกรวดเร็วและเป็นตัวช่วยในการทำงานให้ง่ายขึ้น ดังรูปที่ 2.21

รูปที่ 2.21 การใช้งานข้อต่อต่อพีวีซี

2.1.13 ทำการวางท่อพีวีซีเข้ากับแคลมป์กล้ามปู โดยใช้แรงกดท่อลงไปในแคลมป์กล้ามปูให้แน่น ดังรูปที่ 2.22

รูปที่ 2.22 การวางท่อพีวีซีเข้ากับแคลมป์กล้ามปู

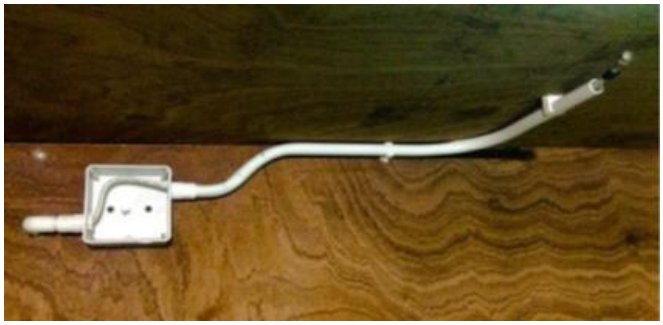
2.1.14 ตัดสายไฟและสาย RG-6 ให้ได้ความยาวที่พอเหมาะกับการเดินท่อพีวีซี ดังรูปที่ 2.23

รูปที่ 2.23 การตัดสายไฟและสาย RG-6 ตามระยะที่วัดไว้

2.1.15 ทำการร้อยสายไฟ และสาย RG-6 เข้าไปในท่อพีวีซีให้เรียบร้อย ดังรูปที่ 2.24

รูปที่ 2.24 การร้อยสายเข้าไปในท่อพีวีซี

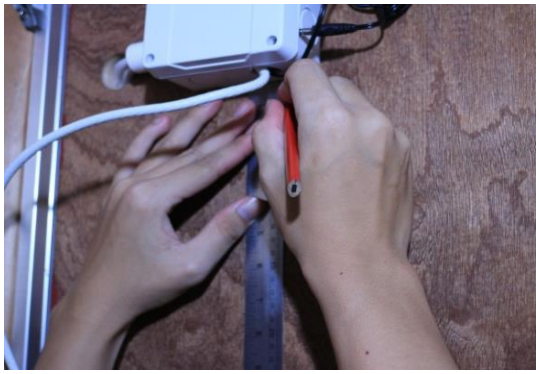
2.1.16 เสร็จสิ้นการเดินสายสัญญาณด้วยท่อพีวีซี ดังรูปที่ 2.25



รูปที่ 2.25 การเดินสายสัญญาณด้วยท่อพีวีซี

2.2 ขั้นตอนการเดินสายด้วยเข็มขัดรัดสาย

2.2.1 ใช้ไม้บรรทัดวัดขอบฝ้าเพดาน คาน และกำหนดจุดไว้ โดยห่างกัน 10 cm ดังรูปที่ 2.26

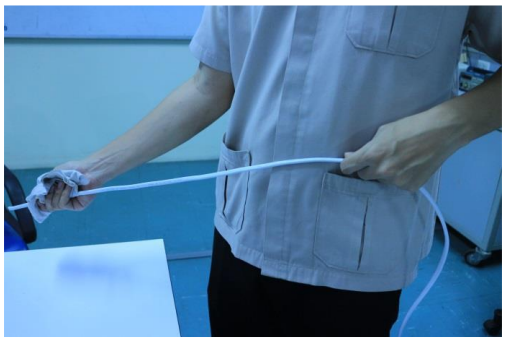


รูปที่ 2.26 การกำหนดตำแหน่งการเดินสาย

2.2.2 ให้เริ่มตอกเข็มขัดรัดสายรัดสายไฟตามเส้น หรือตามจุดที่คุณขีดทำตำแหน่งไว้ ดังรูปที่ 2.27

รูปที่ 2.27 การการตอกเข็มรัดสายไฟ

2.2.3 ใช้ผ้าห่อกับตัวสายจากต้นทาง หรือจากจุดที่สายเริ่มบิดตัว แล้วกระชับอุ้งมือให้แน่น จากนั้นรูดพลางเดินถอยหลังไปเรื่อย ๆ จนกว่าจะสุดปลายสาย ดังรูปที่ 2.28



รูปที่ 2.28 การรูดสายที่บิดตัวให้ตรง

2.2.4 จากนั้นให้เริ่มเดินสายไฟจากบนลงล่าง ยกสายไฟขึ้นรัดกับตัวเข็มขัดรัดสายที่ตอกเอาไว้ ค่อยรัดเข็มขัดรัดสายให้แน่นสนิทรัดรอบสายไฟ ดังรูปที่ 2.29

รูปที่ 2.29 การตอกเข็มขัดรัดสายกลม

3. การเข้าหัวสายสัญญาณโคแอกเชียล

การเข้าหัวสายสัญญาณโคแอกเชียลจะเข้าเป็นการเข้าทั้งหัวสายสัญญาณโคแอกเชียลสายต้นทางเข้าตัวกล้องโทรทัศน์วงจรปิด และสายปลายทางเข้าตัวเครื่อง DVR มีขั้นตอนดังนี้

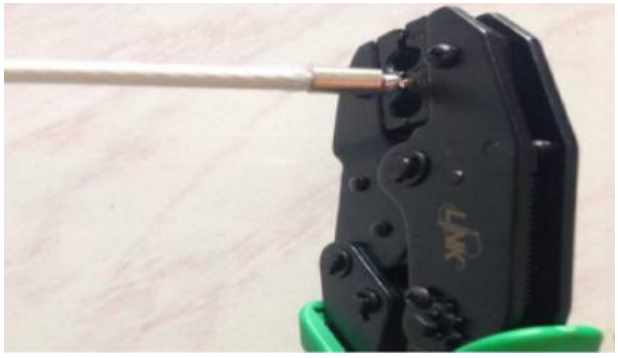
3.1 ใช้มีดปอกสายนำสัญญาณ RG-6 หลังจากปลอกแล้วจะเหลือแกนทองแดง ทำการปลอกฉนวนหุ้มชั้นนอก และสวมแหวนเข้าไปดังรูปที่ 2.30

รูปที่ 2.30 การปลอกสายนำสัญญาณ RG-6

3.2 ใส่เข็ม BNC เข้าที่ปลายสายนำสัญญาณ และสวมแหวนเข้าไป ดังรูปที่ 2.31

รูปที่ 2.31 การใส่เข็ม BNC ที่ปลายสายและสวมแหวน

3.3 ใช้คีมย้ำเข็ม BNC ดังรูปที่ 2.32



รูปที่ 2.32 การใช้คีมย้ำเข็ม BNC

3.4 ใส่ Jack BNC ตามเข้าไป ดังรูปที่ 2.33

รูปที่ 2.33 การใส่ Jack BNC

3.5 ดันแหวนไปให้ชนกับหัว Jack BNC ดังรูปที่ 2.34

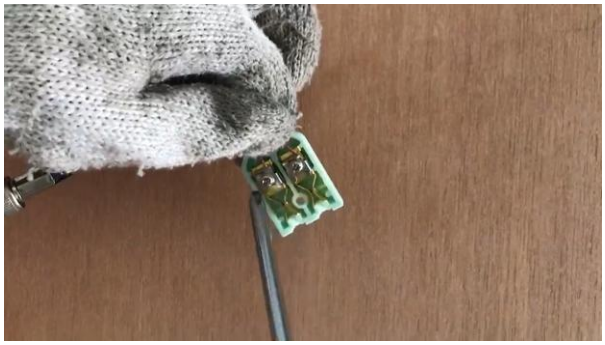
รูปที่ 2.34 การดันแหวนไปให้ชนกับหัว Jack BNC

3.6 สุดท้ายใช้คีมบีบ ย้ำหัวสายให้แน่นเป็นหกเหลี่ยม ดังรูปที่ 2.35

รูปที่ 2.35 การบีบหัวสายโคแอกเชียล

4. การเชื่อมต่อระบบกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก มีขั้นตอนดังนี้

4.1 ปอกสายไฟและทำการเข้าหัวปลั๊กไฟตัวเมีย การเข้าหัวปลั๊กตัวเมียจะเข้าสายต้นทางตัวกล้อง เพื่อที่จะสามารถเสียบกับอะแดปเตอร์ได้ ดังรูปที่ 2.36



รูปที่ 2.36 การเข้าหัวปลั๊กไฟตัวเมีย

4.2 ปอกสายไฟและทำการเข้าหัวปลั๊กไฟตัวผู้ การเข้าหัวปลั๊กตัวผู้จะเข้าสายปลายทาง จะสามารถเสียบกับแหล่งจ่ายไฟไปเลี้ยงตัวกล้องโทรทัศน์วงจรปิดได้ ดังรูปที่ 2.37

รูปที่ 2.37 การเข้าหัวปลั๊กไฟตัวผู้

4.3 ต่อสายสัญญาณภาพและสายไฟเลี้ยงกล้องเข้าด้วยกัน เพื่อเชื่อมต่อระบบกล้องโทรทัศน์วงจรปิด ดังรูปที่ 2.38

รูปที่ 2.38 การต่อสายสัญญาณภาพและสายไฟเลี้ยงกล้องโทรทัศน์วงจรปิด

4.4 เมื่อต่อสายไฟเลี้ยงกล้องและสายสัญญาณภาพแล้ว นำสายสัญญาณภาพต่อเข้ากับด้านหลังของเครื่องบันทึกภาพ เสียบสาย VGA เข้ากับจอทีวี ดังรูปที่ 2.39

รูปที่ 2.39 การต่อสาย VGA เข้ากับ DVR

4.5 ปรับองศาของกล้องโทรทัศน์วงจรปิดให้เรียบร้อย ดังรูปที่ 2.40

รูปที่ 2.40 การปรับองศาของกล้องโทรทัศน์วงจรปิด

4.6 เก็บสายสัญญาณภาพและสายไฟเลี้ยงกล้องให้เรียบร้อย ดังรูปที่ 2.41

รูปที่ 2.41 การเก็บสายสัญญาณภาพให้เรียบร้อย

5. การตรวจสอบระบบกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก มีดังนี้

5.1 เตรียมเครื่องตรวจสอบสัญญาณภาพ ดังรูปที่ 2.42

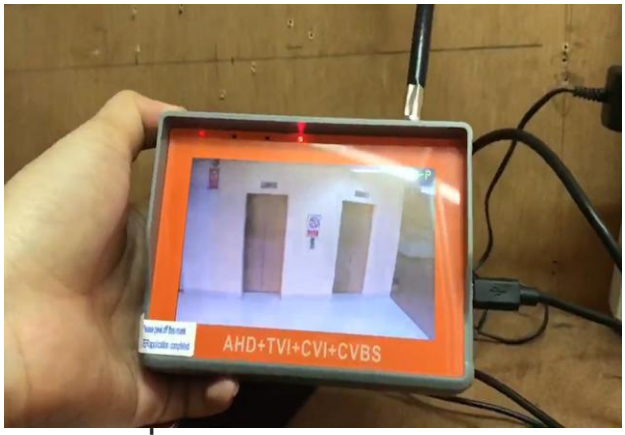
รูปที่ 2.42 เครื่องตรวจสอบสัญญาณภาพ

5.2 เปิดเครื่องตรวจสอบสัญญาณภาพ ต่อสายสัญญาณภาพเข้ากับเครื่องตรวจสัญญาณกล้องโทรทัศน์วงจรปิด ดังรูปที่ 2.43

รูปที่ 2.43 การตรวจสายสัญญาณและไฟเลี้ยง

	ใบงานที่ 2 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

5.3 ตรวจดูสัญญาณภาพถ้าภาพสั่นให้ขยับสายนำสัญญาณ ดังรูปที่ 2.44



รูปที่ 2.44 การตรวจดูสัญญาณภาพ

6 เก็บเครื่องมือ วัสดุ/อุปกรณ์และทำความสะอาดสถานที่ติดตั้งให้เรียบร้อย

ตารางที่ 2.1 บันทึกผลการตรวจสอบ/ทดสอบการติดตั้งกล้องโทรทะศน์วงจรปิด

รายการตรวจสอบ/ทดสอบ	วิธีหรือเกณฑ์การทดสอบ	ผลที่ตรวจวัดหรือสังเกตได้	ผลประเมิน	หมายเหตุ
สายโคแอกเชียล	ตรวจความต่อเนื่องและการลัดวงจร	สายต่อเนื่องและไม่ลัดวงจร		
หัวต่อ BNC	ตรวจสภาพและความแน่น	เชื่อมต่อแน่นหนา		
แรงดันที่แหล่งจ่าย	วัดด้วยมัลติมิเตอร์	12.1 VDC		
แรงดันที่ปลายสายกล้อง	วัดขณะกล้องทำงาน	11.8 VDC		
สัญญาณภาพ	ตรวจจากจอภาพผ่าน DVR	ภาพคมชัดและไม่มีสัญญาณรบกวน		
มุมมองของกล้อง	ตรวจพื้นที่ครอบคลุม	ครอบคลุมทางเข้าและไม่มี จุดบอดสำคัญ		
ภาพกลางคืน	ทดสอบในสภาพแสงน้อย	IR LED ทำงานและเห็นภาพชัดเจน		
การบันทึกของ DVR	บันทึกและเปิดดูย้อนหลัง	บันทึกและค้นคืนได้ถูกต้อง		
การสำรองข้อมูล	ส่งออกไฟล์ไปยัง USB	สำรองและเปิดไฟล์ได้		

	ใบงานที่ 2 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบแอนะล็อก	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

สรุปผลการทดลอง

เอกสารอ้างอิง

กิตติศักดิ์ เฮงสว่าง. (2553). *การจัดการระบบเครือข่ายกล้องวงจรปิดเอซิต*. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีมหานคร.

ชลดา ปานสง, เกียรติศักดิ์ สมฤทธิ์, จิรพงษ์ จิตตะโคตร์, พัชราวรรณ พูลใจ, ศิวกร รัตนวราหะ, และธนพล แก้วคำแจ้ง. (2566). การพัฒนาสื่อบทเรียนออนไลน์มูเดิลคลาวด์สำหรับการฝึกอบรมการติดตั้งและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด ตามมาตรฐานกรมพัฒนาฝีมือแรงงาน. *วารสารวิจัยและนวัตกรรมการอาชีวศึกษา*, *7*(2), 66-75.

ชลดา ปานสง, ปรียานุช จันหนู, และวัฒนา ภูสูง. (2561). การพัฒนาชุดฝึกอบรมการติดตั้งและบำรุงรักษากล้องโทรทัศน์วงจรปิด ตามสมรรถนะของกรมพัฒนาฝีมือแรงงาน. ใน: *การประชุมวิชาการครุศาสตร์อุตสาหกรรมระดับนานาชาติและระดับชาติ (The 6th International Conference on Learning Innovation in Science and Technology (ICLIST 2018) and the 2nd National Conference on Learning Innovation in Science and Technology (NCLIST 2018): ICLIST & NCLIST 2018*. วันที่ 21-24 มีนาคม 2561,710-723.

พกิจ สุวัตถิ์. (2557). *การปฏิบัติงานด้านระบบกล้องวงจรปิด CCTV*. กรุงเทพฯ: ภาควิชาวิศวกรรมศาสตร์และอุตสาหกรรมวิจัย คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสยาม.

CS Odessa. (2025a). *CCTV network example*. https://www.conceptdraw.com/How-To-Guide/cctv-network-example.

Ideal Quality Solutions Co., Ltd. (2560). *ระบบกล้องวงจรปิด*. https://www.ideal-solutions.co.th/products/cctv-closed-circuit-television-system/

Kruegle, H. (2011). *CCTV surveillance: Video practices and technology*. Butterworth-Heinemann.

Samsung CCTV Thai. (2024). *การดูแลและบำรุงรักษากล้องวงจรปิด CCTV*. https://www.samsungcctvthai.com/การดูแลและบำรุงรักษา/.

	ใบงานที่ 3 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network ได้อย่างถูกต้องตามมาตรฐาน

วัตถุประสงค์

1. อ่านแบบงานติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
2. เลือกใช้อุปกรณ์ของกล้องโทรทัศน์วงจรปิดได้เหมาะสมกับงาน
3. ติดตั้งกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
4. เดินสายสัญญาณได้เหมาะสมกับหน้างาน
5. เข้าหัวสายสัญญาณ UTP ได้อย่างถูกต้อง
6. เชื่อมต่อระบบกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง
7. ตรวจสอบระบบกล้องโทรทัศน์วงจรปิดได้อย่างถูกต้อง

เครื่องมือและอุปกรณ์

1. กล้องโทรทัศน์วงจรปิดระบบ IP/Network
2. กล่องพักสาย
3. เครื่องบันทึกภาพ NVR
4. สายไฟ
5. สาย UTP
6. ข้อต่อท่อ
7. หัว RJ-45
8. ตลับเมตร ไม้บรรทัด ระดับน้ำ
9. ครีมย้ำหัวสายเครือข่าย
10. สว่าน
11. คีมตัดท่อ
12. ถุงมือ
13. โฮลซอ
14. ดินสอ
15. เครื่องทดสอบสายเคเบิลเครือข่าย LAN (LAN Cable Tester)
16. คัทเตอร์

ความรู้พื้นฐานในการปฏิบัติงาน

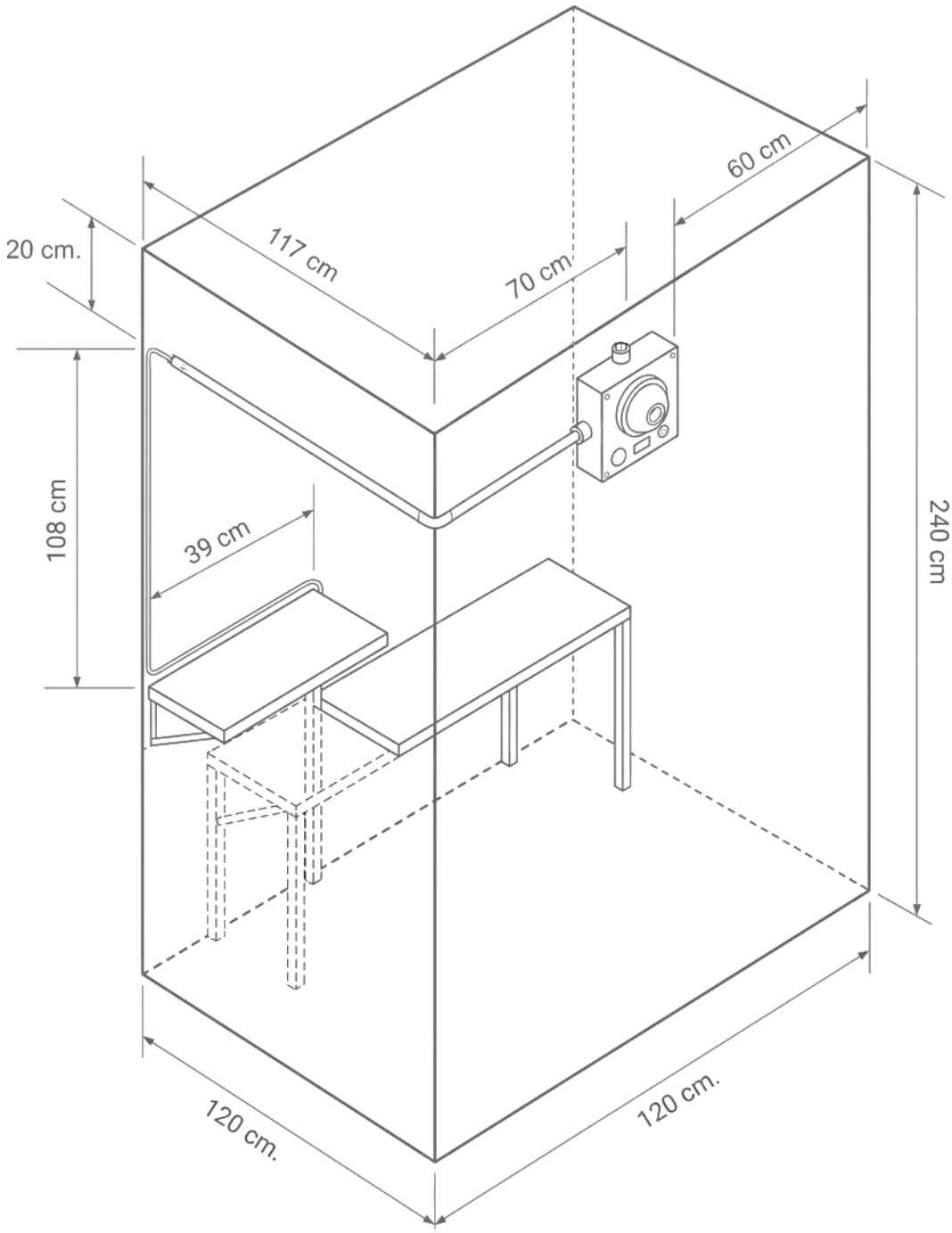
การติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network ผู้ปฏิบัติงานควรมีความรู้เกี่ยวกับหลักการทำงานของ IP camera การเลือกตำแหน่งและมุมติดตั้ง การเดินสายเครือข่าย การเข้าหัวสาย UTP การเชื่อมต่อกล้องกับ Network Switch หรือ PoE Switch และเครื่องบันทึกภาพ NVR (Network Video Recorder) รวมถึงการกำหนด IP address และค่าพื้นฐานของเครือข่าย เพื่อให้อุปกรณ์สามารถสื่อสารกันได้อย่างถูกต้อง นอกจากนี้ ควรสามารถตรวจสอบการเชื่อมต่อ คุณภาพของภาพ การบันทึกข้อมูล และคำนึงถึงความปลอดภัยในการติดตั้ง เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและมีเสถียรภาพ รายละเอียดในบทที่ 3 ระบบกล้องโทรทัศน์วงจรปิดอัจฉริยะ

	ใบงานที่ 3 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ขั้นตอนการปฏิบัติงาน

ตอนที่ 1 งานติดตั้งและทดสอบระบบกล้องโทรทัศน์วงจรปิด IP/Network

1. การอ่านแบบงานติดตั้งกล้องโทรทัศน์วงจรปิด IP/Network ดังรูปที่ 3.1



รูปที่ 3.1 แบบจำลองการติดตั้งและเดินสายระบบกล้องโทรทัศน์วงจรปิด

2. การเลือกใช้อุปกรณ์ระบบ IP/Network

2.1 ใช้กล้องโทรทัศน์วงจรปิดแบบ IP1 ตัว รุ่น HMP 88B10

2.2 ใช้เลนส์มาตรฐานที่มาพร้อมกับกล้อง ขนาด 3.6 mm

2.3 เครื่องบันทึกภาพ เลือกเป็นเครื่องบันทึกภาพ NVR รุ่น 8804A

2.4 สายสัญญาณสายที่ใช้เป็นสายสัญญาณชนิดสายคู่บิดเกลียว หรือสาย UTP แบบ CAT5e สายไฟเลี้ยงกล้อง 12 V

3. การติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network

การติดตั้งกล้องโทรทัศน์วงจรปิดแบบ IP/Network จำเป็นต้องเตรียมเครื่องมือ วัสดุ และอุปกรณ์ต่าง ๆ ให้พร้อมก่อนเริ่มปฏิบัติงาน เพื่อให้การติดตั้งเป็นไปอย่างถูกต้อง ดังนี้

3.1 เตรียมเครื่องมือและอุปกรณ์สำหรับการติดตั้งกล้องโทรทัศน์วงจรปิดให้ครบถ้วน เช่น กล้องโทรทัศน์วงจรปิด เครื่อง NVR สายสัญญาณเครือข่าย อุปกรณ์ PoE กล่องพักสายไฟ และเครื่องมือช่างที่ใช้ในการติดตั้ง

3.2 กำหนดตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดให้เหมาะสมกับพื้นที่ใช้งาน โดยนำฝากล่องพักสายมาวางกำหนดจุดติดตั้ง และจัดตำแหน่งให้ตัวกล้องอยู่กึ่งกลางของฝากล่องพักสาย เพื่อความแข็งแรง ความเป็นระเบียบ และความสวยงามของงานติดตั้ง โดยยึดกล่องพักสายและฐานกล้องเข้ากับผนังหรือโครงสร้างให้แน่นหนา พร้อมตรวจสอบระดับและมุมมองของกล้องให้สามารถครอบคลุมพื้นที่ที่ต้องการเฝ้าระวังได้อย่างเหมาะสม

4. การเดินสายนำสัญญาณ

การเดินสายนำสัญญาณสำหรับระบบกล้องโทรทัศน์วงจรปิดแบบ IP/Network สามารถแบ่งได้เป็น 2 รูปแบบ ได้แก่ การเดินสายด้วยท่อพีวีซี และการเดินสายด้วยเข็มขัดรัดสาย ซึ่งทั้งสองวิธีมีหลักการติดตั้งคล้ายกัน โดยต้องจัดเก็บสายสัญญาณให้เรียบร้อย แข็งแรง และปลอดภัยต่อการใช้งาน

4.1 การเดินสายด้วยท่อพีวีซี

เป็นวิธีที่นิยมใช้ในการติดตั้งถาวร โดยนำสายสัญญาณร้อยภายในท่อพีวีซี เพื่อช่วยป้องกันสายจากแรงกระแทก ความชื้น และสภาพแวดล้อมภายนอก ทำให้งานติดตั้งมีความเรียบร้อยและช่วยยืดอายุการใช้งานของสายสัญญาณ

4.2 การเดินสายด้วยเข็มขัดรัดสาย

เป็นวิธีที่เหมาะสำหรับพื้นที่ที่ไม่สะดวกในการเดินท่อพีวีซี โดยใช้เข็มขัดรัดสายยึดสายสัญญาณเข้ากับโครงสร้างหรือแนวเดินสาย ช่วยให้ติดตั้งได้รวดเร็ว ประหยัดเวลา และสามารถจัดเก็บสายได้อย่างเป็นระเบียบ

5. การเข้าหัวสาย UTP

สาย UTP เป็นสายสัญญาณที่นิยมใช้ในระบบกล้องโทรทัศน์วงจรปิดแบบ IP camera ภายในสายประกอบด้วยสายทองแดงจำนวน 4 คู่ หรือ 8 เส้น ซึ่งมีการตีเกลียวเพื่อลดสัญญาณรบกวน การเชื่อมต่อสาย UTP ใช้หัวเชื่อมต่อแบบ RJ-45 และต้องจัดเรียงลำดับสีของสายให้ถูกต้องตามมาตรฐาน TIA/EIA-568A หรือ TIA/EIA-568B เพื่อให้สามารถรับส่งข้อมูลได้อย่างมีประสิทธิภาพ โดยเลือกใช้สาย CAT ในการติดตั้งนิยมใช้การเข้าหัวสายแบบตรง (straight-through cable) โดยปลายสายทั้งสองด้านจะเรียงสีเหมือนกัน ซึ่งเหมาะสำหรับการเชื่อมต่ออุปกรณ์ต่างชนิดกัน เช่น กล้อง IP กับสวิตช์เครือข่าย (switch) หรือคอมพิวเตอร์กับสวิตช์เครือข่าย

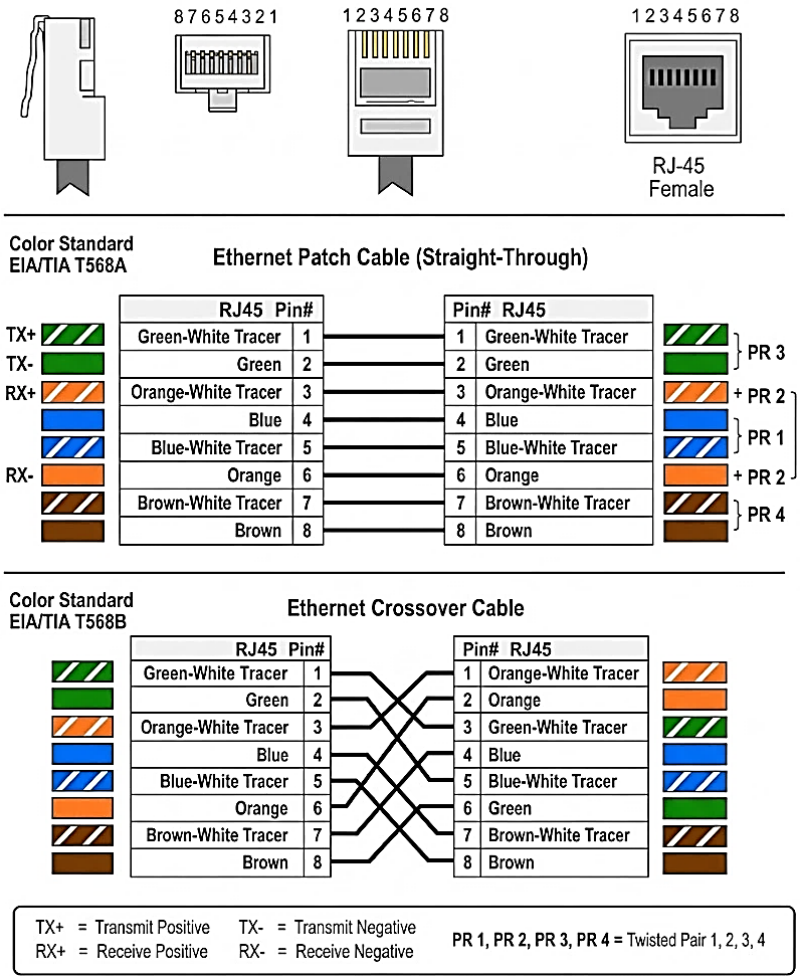
5.1 เตรียมสาย UTP

รูปที่ 3.2 การตัดใช้สาย UTP ความยาวตามที่แบบกำหนด

5.2 ปลอกเปลือกนอกของสาย CAT 5 ประมาณ 2-3 cm ดังรูปที่ 3.3

รูปที่ 3.3 การปลอกเปลือกนอกของสาย UTP

5.3 แยกและจัดเรียงสายสัญญาณทั้ง 8 เส้นตามลำดับสีของมาตรฐาน TIA/EIA-568A ลำดับสีดังนี้ ขาว-เขียว, เขียว, ขาว-ส้ม, น้ำเงิน, ขาว-น้ำเงิน, ส้ม, ขาว-น้ำตาล และน้ำตาล

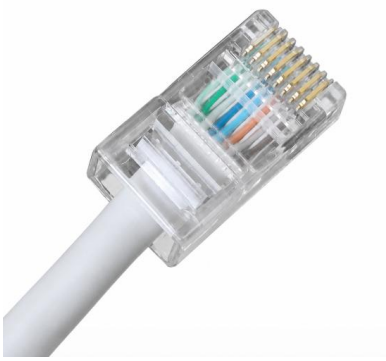


รูปที่ 3.4 การจัดเรียงสีของสายตามมาตรฐาน TIA/EIA-568A และ TIA/EIA-568B (Yu, 2016)

รูปที่ 3.5 การลำดับสีของสายตามมาตรฐาน T568A

5.4 จัดสายให้เรียงตรงและตัดปลายสายให้มีความยาวเท่ากัน โดยให้เหลือความยาวประมาณ 1.5 cm

5.5) สอดสายเข้าสู่หัว RJ-45 โดยให้สายทุกเส้นเข้าไปจนสุดปลายหัวต่อ



รูปที่ 3.6 การนำหัว RJ-45 สวมลงไปจนสุด

5.6 ใช้คีมย้ำหัวต่อสายเครือข่าย (network cable crimping tool) ย้ำหัว RJ-45 ให้แน่น เพื่อให้ขั้วทองแดงภายในหัวต่อสัมผัสกับสายสัญญาณอย่างสมบูรณ์

3.7 การใช้คีมย้ำหัวสายสัญญาณ

5.7 ตรวจสอบความถูกต้องของสายด้วยเครื่องทดสอบสายเคเบิลเครือข่าย (network cable tester) เพื่อทดสอบการเชื่อมต่อและลำดับสายก่อนนำไปใช้งานจริง

รูปที่ 3.8 การตรวจสอบความถูกต้องของสายเครื่องทดสอบสายเคเบิลเครือข่าย

6. การเชื่อมต่อระบบกล้องโทรทัศน์วงจรปิดระบบ IP/Network

หลังจากเข้าหัวสาย UTP เรียบร้อยแล้ว ขจากนั้นเชื่อมต่อระบบกล้องโทรทัศน์วงจรปิด โดยมีขั้นตอนดังนี้

6.1 ปอกสายไฟและเข้าหัวปลั๊กไฟตัวเมีย ใช้สำหรับเชื่อมต่อสายไฟของกล้องเข้ากับอะแดปเตอร์ จ่ายกระแสไฟฟ้าให้กับกล้องโทรทัศน์วงจรปิด รูปที่ 3.9 (ก)

6.2 ทำการปลอกสายไฟและเข้าหัวปลั๊กไฟตัวผู้ ซึ่งใช้สำหรับเชื่อมต่อสายไฟเข้ากับแหล่งจ่ายไฟ เพื่อจ่ายกระแสไฟฟ้าให้กับกล้องโทรทัศน์วงจรปิด ดังรูปที่ 3.10 (ข)

(ก) การเข้าหัวปลั๊กไฟตัวเมีย

(ข) การเข้าหัวปลั๊กไฟตัวผู้

รูปที่ 3.10 การเข้าหัวปลั๊กไฟ

6.3 ทำการเชื่อมต่อสายสัญญาณภาพและสายไฟเลี้ยงของกล้องโทรทัศน์วงจรปิดเข้าด้วยกัน เพื่อให้ระบบกล้องโทรทัศน์วงจรปิดสามารถทำงานได้ ดังรูปที่ 3.11

รูปที่ 3.11 การต่อสายสัญญาณภาพและสายไฟเลี้ยงกล้องโทรทัศน์วงจรปิด

6.4 เก็บสายสัญญาณภาพและสายไฟเลี้ยงกล้องให้เรียบร้อย ดังรูปที่ 3.12

รูปที่ 3.12 การเก็บสายสัญญาณภาพให้เรียบร้อย

6.5 ด้านหลังของเครื่องบันทึกภาพ ต่อสาย VGA และสายสัญญาณเครือข่าย เข้ากับเครื่องบันทึกภาพเพื่อตรวจสอบการทำงานของกล้อง ดังรูปที่ 3.13

รูปที่ 3.13 การต่อสายนำสัญญาณเข้ากับเครื่องบันทึกภาพ NVR

6.6 ใช้หกเหลี่ยมไขปรับมุมกล้องโทรทัศน์วงจรปิด ดังรูปที่ 3.14

รูปที่ 3.14 การใช้หกเหลี่ยมไขปรับมุมกล้องโทรทัศน์วงจรปิดตามมุมมองที่ต้องการ

7. การตรวจสอบระบบกล้องโทรทัศน์วงจรปิดระบบ IP/Network มีดังนี้

7.1 เตรียมสายสัญญาณภาพ และสายปล่อยไฟเลี้ยงกล้อง สำหรับต่อเข้าเครื่องตรวจสอบสัญญาณภาพ ดังรูปที่ 3.15

รูปที่ 3.15 เครื่องตรวจสอบสัญญาณภาพ

7.2 ต่อสายสัญญาณภาพ สายไฟเลี้ยงกล้องเข้ากับเครื่องตรวจสัญญาณกล้องโทรทัศน์วงจรปิด ดังรูปที่ 3.16

รูปที่ 3.16 การตรวจสายสัญญาณและไฟเลี้ยง

7.3 ต่อสายไฟเลี้ยง 12 V ให้กับกล้องโทรทัศน์วงจรปิดและต่อสายสัญญาณภาพ ดังรูปที่ 3.17

รูปที่ 3.17 การต่อสายไฟเลี้ยงและสายสัญญาณ

7.4 เปิดเครื่องทดสอบและกดปุ่ม AV ตรวจดูสัญญาณภาพ ถ้าภาพสั่นให้ขยับสายนำสัญญาณ ดังรูปที่ 3.18

รูปที่ 3.18 การตรวจดูสัญญาณภาพ

ตอนที่ 2 งานตั้งค่าให้ภาพจากกล้องโทรทัศน์วงจรปิดแสดงผลผ่านเว็บไซต์

การตั้งค่าให้สามารถดูภาพจากกล้องโทรทัศน์วงจรปิดผ่านเว็บเบราว์เซอร์ เป็นขั้นตอนที่ให้ผู้ใช้งานสามารถตรวจสอบภาพจากกล้องได้ผ่านระบบเครือข่ายอินเทอร์เน็ต มีขั้นตอนดังนี้

1. ติดตั้งและเปิดโปรแกรม CMS บนเครื่องคอมพิวเตอร์ จากนั้นเข้าสู่ระบบ
2. เลือกเมนู “Device Management” หรือ “Add Device” เพื่อทำการเพิ่มอุปกรณ์เครื่องบันทึกภาพเข้าสู่ระบบ
3. กำหนดข้อมูลของเครื่องบันทึกภาพ ได้แก่
   - 3.1 ชื่ออุปกรณ์ (Device Name)
   - 3.2 หมายเลข IP Address
   - 3.3 Port
   - 3.4 Username
   - 3.5 Password
4. ตรวจสอบการเชื่อมต่อเครือข่ายของเครื่องบันทึกภาพ โดยเครื่องบันทึกจะต้องเชื่อมต่อกับระบบอินเทอร์เน็ต หรือระบบเครือข่าย LAN ให้เรียบร้อย

5. ทำการตั้งค่า port forwarding ที่ router เพื่อเปิดช่องทางการรับส่งข้อมูลจากเครื่องบันทึกภาพไปยังเครือข่ายภายนอก โดยทั่วไปจะกำหนดพอร์ตที่ใช้สำหรับ HTTP หรือ media port ตามที่ระบุในเครื่องบันทึกภาพ

6. เปิดเว็บเบราว์เซอร์ เช่น Internet Explorer หรือ Google Chrome จากนั้นพิมพ์หมายเลข IP address หรือ domain name ของเครื่องบันทึกภาพลงในแถบ address

7. เมื่อเข้าสู่หน้าเว็บของระบบกล้องโทรทัศน์วงจรปิด ให้กรอกชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบ

8. หลังจากเข้าสู่ระบบเรียบร้อย ผู้ใช้งานจะสามารถดูภาพสด (live view) ดูภาพย้อนหลัง (playback) และควบคุมการทำงานของกล้องโทรทัศน์วงจรปิดผ่านหน้าเว็บได้ ทั้งนี้หากไม่สามารถแสดงผลภาพผ่านเว็บได้ ควรตรวจสอบการตั้งค่าเครือข่าย หมายเลข IP address การเชื่อมต่ออินเทอร์เน็ต และการเปิดพอร์ตของ router ให้ถูกต้อง

รูปที่ 3.19 ขั้นตอนการตั้งค่าให้ภาพจากกล้องโทรทัศน์วงจรปิดแสดงผลผ่านเว็บ

	ใบงานที่ 3 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ตารางที่ 3.1 บันทึกผลรายการทดสอบ

รายการทดสอบ	ค่าที่กำหนด/วิธีทดสอบ	ผลที่ตรวจวัดได้	ผลการประเมิน	หมายเหตุ
การทดสอบสาย UTP	ทดสอบสาย 1–8 ด้วย Network Cable Tester	ลำดับ 1–8 ถูกต้อง		
การเชื่อมต่อกล้อง	ใช้คำสั่ง ping ไปยัง IP address ของกล้อง	ตอบสนองครบ ไม่มี Packet Loss		
การแสดงภาพสด	เปิดดูผ่านแอปพลิเคชัน	ภาพต่อเนื่องและคมชัด		
ภาพเวลากลางคืน	ปิดแสงและตรวจสอบ IR LED	มองเห็นวัตถุได้ชัดเจน		
การตรวจจับการเคลื่อนไหว	เคลื่อนที่ผ่านพื้นที่ตรวจจับ	ตรวจจับและแจ้งเตือนได้		
การบันทึกวิดีโอ	บันทึกลง microSD/NVR	บันทึกและเปิดดูย้อนหลังได้		
การดูภาพระยะไกล	ทดสอบผ่านอินเทอร์เน็ตมือถือ	ดูภาพสดได้ มีความล่าช้าเล็กน้อย		

สรุปผลการทดลอง

	ใบงานที่ 3 เรื่อง งานติดตั้งกล้องโทรทัศน์วงจรปิดระบบ IP/Network	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

เอกสารอ้างอิง

กิตติศักดิ์ เฮงสว่าง. (2553). *การจัดการระบบเครือข่ายกล้องวงจรปิดเอชิต*. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีมหานคร.

ชลดา ปานสง, เกียรติศักดิ์ สมฤทธิ์, จิรพงษ์ จิตตะโคตร์, พัชราวรรณ พูลใจ, ศิวกร รัตนวราหะ, และธนพล แก้วคำแจ้ง. (2566). การพัฒนาสื่อบทเรียนออนไลน์มูเดิลคลาวด์สำหรับการฝึกอบรมการติดตั้งและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด ตามมาตรฐานกรมพัฒนาฝีมือแรงงาน. *วารสารวิจัยและนวัตกรรมการอาชีวศึกษา*, *7*(2), 66-75.

ชลดา ปานสง, ปรียานุช จันหนู, และวัฒนา ภูสูง. (2561). การพัฒนาชุดฝึกอบรมการติดตั้งและบำรุงรักษากล้องโทรทัศน์วงจรปิด ตามสมรรถนะของกรมพัฒนาฝีมือแรงงาน. ใน: *การประชุมวิชาการครุศาสตร์อุตสาหกรรมระดับนานาชาติและระดับชาติ (The 6th International Conference on Learning Innovation in Science and Technology (ICLIST 2018) and the 2nd National Conference on Learning Innovation in Science and Technology (NCLIST 2018): ICLIST & NCLIST 2018*. วันที่ 21-24 มีนาคม 2561,710-723.

บริษัท มีเดีย เสิร์ช จำกัด. (2021). *กล้องวงจรปิดระบบ WiFi กับการออกแบบระบบเครือข่าย*. https://www.cctvbangkok.com/cctv-wifi-system/.

พกิจ สุวัตถิ์. (2557). *การปฏิบัติงานด้านระบบกล้องวงจรปิด CCTV*. กรุงเทพฯ: ภาควิชาวิศวกรรมศาสตร์และอุตสาหกรรมวิจัย คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสยาม.

CS Odessa. (2025a). *CCTV network example*. https://www.conceptdraw.com/How-To-Guide/cctv-network-example.

Ideal Quality Solutions Co., Ltd. (2560). *ระบบกล้องวงจรปิด*. https://www.ideal-solutions.co.th/products/cctv-closed-circuit-television-system/

JVSG.com. (2024). *Video surveillance design apps*. https://www.jvsg.com/.

Kruegle, H. (2011). *CCTV surveillance: Video practices and technology*. Butterworth-Heinemann.

Samsung CCTV Thai. (2024). *การดูแลและบำรุงรักษากล้องวงจรปิด CCTV*. https://www.samsungcctvthai.com/การดูแลและบำรุงรักษา/.

Yu, L. (2016). *How to distinguish T568A and T568B of RJ45 Ethernet cable wiring?* LinkedIn. https://www.linkedin.com/pulse/how-distinguish-t568a-t568b-rj45-ethernet-cable-wiring-laura-yu.

	ใบงานที่ 4 เรื่อง งานติดตั้งกล้อง Internet Protocol Camera (IP camera)	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ติดตั้งกล้องโทรทัศน์วงจรปิดแบบ IP camera ได้อย่างถูกต้อง

วัตถุประสงค์

1. ต่อสายไฟและสายเครือข่ายโดยไม่ทำให้อุปกรณ์เสียหาย
2. เชื่อมต่อสมาร์ตโฟน คอมพิวเตอร์ และกล้องเข้ากับเราเตอร์เดียวกัน
3. เพิ่มกล้องในแอป Eye4 โดยใช้ Device ID หรือ QR code ของกล้อง
4. เปลี่ยนรหัสผ่านเริ่มต้นของกล้องได้
5. ระบุ IP address ของกล้องและอุปกรณ์ที่ใช้ทดสอบได้
6. ใช้คำสั่ง ping ทดสอบการเชื่อมต่อได้
7. ดูภาพสดและตรวจสอบการตอบสนองของภาพได้
8. บันทึกผลการทดลองอย่างเป็นระบบ

เครื่องมือและอุปกรณ์

1.	กล้อง IP camera รุ่น Vstarcam C7824WIP	1 ตัว
2.	อะแดปเตอร์ของกล้องตามพิกัดที่ผู้ผลิตกำหนด	1 ชุด
3.	เราเตอร์หรือ Access Point แบบ Wi-Fi 2.4 GHz	1 เครื่อง
4.	สาย LAN ชนิดตรง Cat5e หรือสูงกว่า	1 เส้น
5.	คอมพิวเตอร์หรือโน้ตบุ๊ก	1 เครื่อง
6.	สมาร์ตโฟนติดตั้งแอป Eye4	1 เครื่อง
7.	โปรแกรมค้นหา IP address หรือหน้าจัดการเราเตอร์	1 โปรแกรม
8.	เครื่องทดสอบสาย LAN – LAN Cable Tester	1 เครื่อง

ความรู้พื้นฐานในการปฏิบัติงาน

กล้อง IP camera เป็นกล้องที่รับ–ส่งข้อมูลภาพผ่านระบบเครือข่าย โดยกล้องแต่ละตัวจะได้รับหมายเลข IP address เพื่อใช้ระบุตำแหน่งและติดต่อสื่อสารกับอุปกรณ์อื่น เช่น คอมพิวเตอร์ สมาร์ตโฟน และเราเตอร์ ใบงานนี้ใช้กล้อง Vstarcam C7824WIP เชื่อมต่อกับเครือข่ายภายใน หรือ LAN ผ่านสาย Ethernet หรือ Wi-Fi จากนั้นตรวจสอบ IP address และทดสอบดูภาพจากอุปกรณ์ที่เชื่อมต่ออยู่ในเครือข่ายเดียวกัน กล้องรุ่นนี้รองรับภาพความละเอียดสูงสุด 1280 × 720 พิกเซล การบีบอัด H.264/MJPEG/JPEG การเชื่อมต่อ Wi-Fi ย่าน 2.4 GHz และพอร์ตเครือข่าย RJ45 ตามข้อมูลจำเพาะของผู้ผลิต

1. ส่วนประกอบของกล้อง IP camera รุ่น Vstarcam C7824WIP

กล้อง IP camera รุ่น Vstarcam C7824WIP เป็นกล้องโทรทัศน์วงจรปิดแบบไร้สายที่รองรับการเชื่อมต่อผ่านเครือข่าย Wi-Fi โดยมีความละเอียดระดับ HD 720P สามารถควบคุมและตรวจสอบภาพผ่านแอปพลิเคชันบนอุปกรณ์พกพา เช่น สมาร์ตโฟนหรือแท็บเล็ต ทั้งระบบปฏิบัติการ Android และ iOS ได้อย่างสะดวก กล้องรุ่นนี้สามารถปรับหมุนได้ทั้งแนวนอนและแนวตั้ง ช่วยเพิ่มมุมมองในการตรวจสอบพื้นที่ได้อย่างครอบคลุม อีกทั้งยังรองรับการบันทึกวิดีโอลง micro SD card ได้สูงสุด 64 GB ทำให้สามารถดูภาพย้อนหลังได้โดยไม่จำเป็นต้องใช้อุปกรณ์บันทึกภาพเพิ่มเติม นอกจากนี้ กล้องยังมีระบบอินฟราเรดสำหรับการมองเห็นในเวลากลางคืน พร้อมไมโครโฟนและลำโพงภายในตัวเครื่อง ทำให้สามารถสนทนาโต้ตอบแบบสองทางได้ รวมถึงรองรับมาตรฐาน ONVIF ซึ่งช่วยให้สามารถเชื่อมต่อร่วมกับอุปกรณ์หรือซอฟต์แวร์ระบบกล้องโทรทัศน์วงจรปิดอื่น ๆ ได้อย่างมีประสิทธิภาพ

รูปที่ 4.1 กล้อง IP camera รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

ส่วนประกอบของกล้อง IP camera รุ่น Vstarcam C7824WIP ประกอบด้วยด้านหน้าของกล้องประกอบด้วยเลนส์กล้องสำหรับบันทึกภาพ ไฟอินฟราเรดสำหรับมองเห็นในที่มืด ไมโครโฟนรับเสียง และเซ็นเซอร์ตรวจจับแสง ซึ่งช่วยให้กล้องสามารถปรับโหมดการทำงานระหว่างกลางวันและกลางคืนได้โดยอัตโนมัติ

รูปที่ 4.2 ภายนอกกล้อง IP รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

ด้านหลังของกล้องประกอบด้วยพอร์ตเชื่อมต่อสายสัญญาณเครือข่าย ช่องเสียบไฟเลี้ยง ปุ่มรีเซ็ต ช่องใส่ micro SD card เสาอากาศ Wi-Fi สำหรับรับส่งสัญญาณเครือข่ายไร้สาย

รูปที่ 4.3 ด้านหลังกล้อง IP รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

2. คุณสมบัติของกล้อง IP camera รุ่น Vstarcam C7824WIP

2.1 คุณสมบัติของกล้อง IP camera รุ่น Vstarcam C7824WIP มีคุณสมบัติ ดังนี้

2.1.1 ภาพคมชัดระดับ HD 720P

กล้องรองรับความละเอียดระดับ HD 720P หรือประมาณ 1 MP พร้อมรองรับการบีบอัดวิดีโอแบบ H.264 ช่วยให้ภาพมีความคมชัดและประหยัดพื้นที่จัดเก็บข้อมูล เลนส์ขนาด 3.6 mm และระบบ IR-cut ช่วยให้ภาพสีมีความสมจริงและคมชัดทั้งในเวลากลางวันและกลางคืน

รูปที่ 4.4 ความคมชัดของกล้อง IP รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

2.1.2 รองรับการเชื่อมต่อ Wi-Fi

กล้องสามารถเชื่อมต่อเครือข่ายแบบไร้สายผ่าน Wi-Fi ทำให้ติดตั้งและใช้งานได้สะดวก รองรับการใช้งานผ่านแอปพลิเคชัน EYE4 และ VSCAM บนอุปกรณ์ Android และ iOS

รูปที่ 4.5 การเชื่อมต่อของกล้อง IP รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

2.1.3 รองรับการบันทึกวิดีโอและสนทนาแบบสองทาง

กล้องรองรับการบันทึกวิดีโอด้วยรูปแบบ H.264 ลงบน micro SD card ได้สูงสุด 64 GB พร้อมไมโครโฟนและลำโพงในตัว ทำให้สามารถสนทนาโต้ตอบระหว่างผู้ใช้งานกับปลายทางได้แบบสองทาง

รูปที่ 4.6 คุณสมบัติด้านการบันทึกและสนทนาของกล้อง IP รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

2.1.4 สามารถหมุนกล้องได้รอบทิศทาง

กล้องสามารถควบคุมการหมุนในแนวนอนได้สูงสุด 355 องศา และแนวตั้งได้ประมาณ 120 องศา ช่วยเพิ่มพื้นที่ในการตรวจสอบและลดจุดอับของกล้อง

รูปที่ 4.7 คุณสมบัติด้านการหมุนของกล้อง IP camera รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

2.1.5 รองรับระบบตรวจจับความเคลื่อนไหว

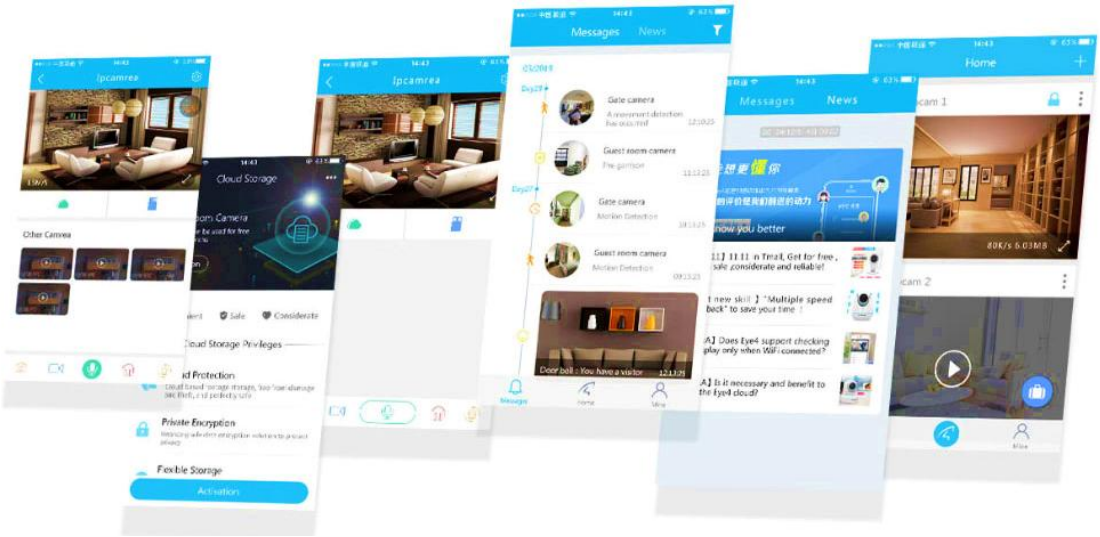
กล้องมีระบบ motion detection สำหรับตรวจจับความเคลื่อนไหวโดยอัตโนมัติ และมีไฟอินฟราเรดจำนวน 12 ดวง ช่วยให้สามารถมองเห็นภาพในเวลากลางคืนหรือในพื้นที่ที่มีแสงน้อยได้อย่างชัดเจน

รูปที่ 4.8 คุณสมบัติด้านบตรวจจับความเคลื่อนไหวของกล้อง IP รุ่น Vstarcam C7824WIP (Global Column Limited, 2016)

3. การเชื่อมต่อกล้อง IP camera

การเชื่อมต่อของกล้อง IP รุ่น Vstarcam 7824WIP สามารถเชื่อมต่อได้หลากหลาย

3.1 การเชื่อมต่อกล้องIP camera รุ่น Vstarcam 7824WIP ผ่าน APP Ere4

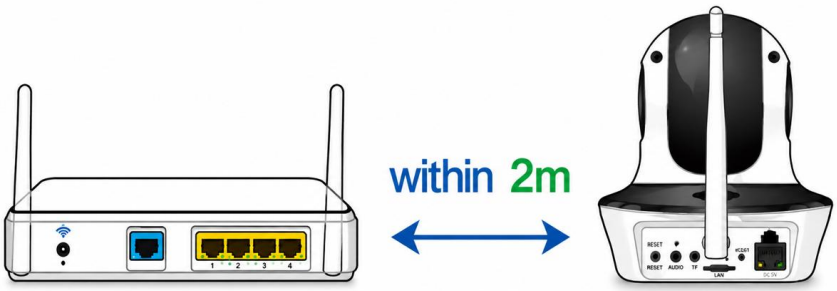


รูปที่ 4.9 ขั้นตอนการเชื่อมต่อของกล้อง IP รุ่น Vstarcam 7824WIP (Global Column Limited, 2016)

3.1.1 ขั้นตอนที่ 1 การเตรียมความพร้อมก่อนติดตั้ง

	ใบงานที่ 4 เรื่อง งานติดตั้งกล้อง Internet Protocol Camera (IP camera)	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ก่อนเริ่มติดตั้งกล้อง IP camera รุ่น Vstarcam C7824WIP ให้เชื่อมต่อสมาร์ตโฟนเข้ากับเครือข่าย Wi-Fi ที่ใช้งาน โดยเครือข่ายต้องเป็นย่านความถี่ 2.4 GHz เท่านั้น เนื่องจากกล้องไม่รองรับเครือข่าย 5 GHz ในระหว่างการตั้งค่า วางกล้องให้อยู่ห่างจากเราเตอร์ประมาณ 2 m เพื่อให้การรับ–ส่งสัญญาณมีความเสถียร จากนั้นเสียบปลั๊กไฟให้กับกล้องและรอประมาณ 30 s เพื่อให้ระบบบูตและเริ่มต้นการทำงานจนสมบูรณ์



รูปที่ 4.10 การจัดวางกล้อง IP camera รุ่น Vstarcam C7824WIP ก่อนติดตั้ง

หากเป็นการเชื่อมต่อกล้องครั้งแรก ไม่จำเป็นต้องทำการรีเซตอุปกรณ์ แต่หากเคยมีการตั้งค่าหรือใช้งานมาก่อน ควรทำการรีเซตกล้องก่อนเริ่มติดตั้งใหม่ โดยใช้เข็มหรือก็บกดปุ่ม reset ค้างไว้ประมาณ 5 s หรือจนได้ยินเสียงแจ้งว่า “Reset completed”

3.1.2 ขั้นตอนที่ 2 ดาวน์โหลดแอปพลิเคชัน Eye4 และลงทะเบียน

ให้ค้นหาแอปพลิเคชัน “Eye4” ผ่าน App Store สำหรับระบบ iOS หรือ Google Play Store สำหรับระบบ Android หรือสามารถสแกน QR code ที่อยู่บนกล่องผลิตภัณฑ์เพื่อดาวน์โหลดแอปพลิเคชันได้โดยตรง หลังจากติดตั้งแอปพลิเคชันเรียบร้อยแล้ว ให้เปิดแอปและเลือก “ลงทะเบียน” จากนั้นกรอกชื่อผู้ใช้และรหัสผ่านเพื่อสร้างบัญชีผู้ใช้งาน นอกจากนี้ยังรองรับการเข้าสู่ระบบผ่านบัญชี Facebook ได้อีกด้วย

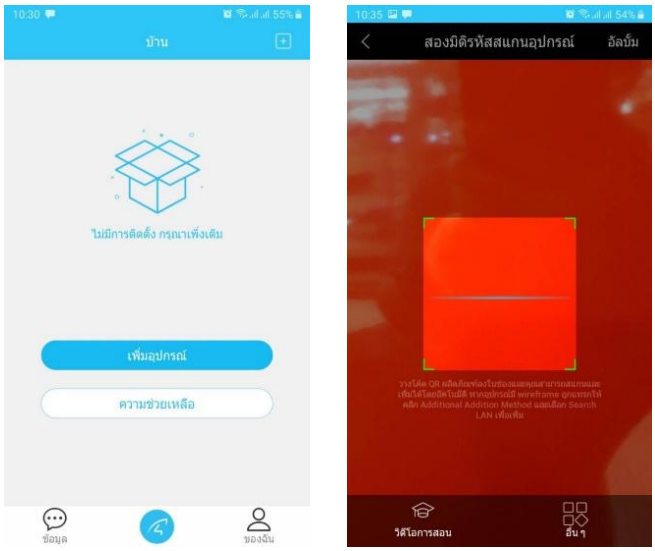
รูปที่ 4.13 การดาวน์โหลดแอปพลิเคชัน Eye4

3.1.3 ขั้นตอนที่ 3 การเพิ่มอุปกรณ์และสแกน QR code ของกล้อง Vstarcam

เปิดแอปพลิเคชัน Eye4 แล้วกดเครื่องหมาย “+” ที่มุมขวาบน จากนั้นทำการสแกน QR code ที่อยู่บนตัวกล้อง IP camera แล้วปฏิบัติตามคำแนะนำบนหน้าจอเพื่อดำเนินการติดตั้งให้เสร็จสมบูรณ์

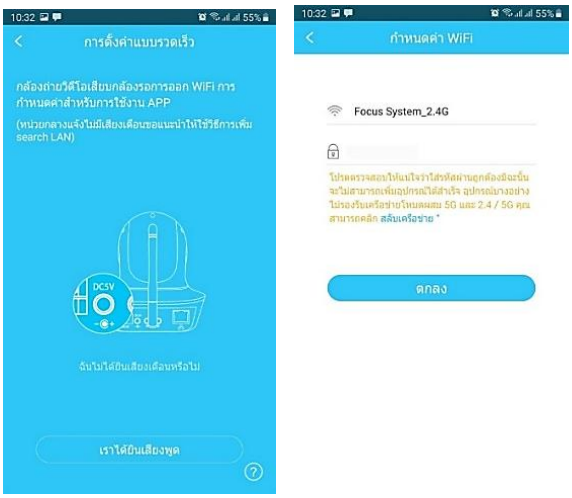
รูปที่ 4.14 การสแกน QR code เพื่อเพิ่มอุปกรณ์ (Global Column Limited, 2016)

3.1.4 เมื่อระบบค้นพบกล้องเรียบร้อยแล้ว ให้กำหนดชื่ออุปกรณ์ตามต้องการ แล้วกดปุ่ม “+” ที่มุมขวาบน แล้วทำการสแกนโค้ด QR ที่ตัวกล้องจากนั้นทำตามคำแนะนำบนแอปฟลิเคชั่นเพื่อดำเนินการให้เสร็จสิ้น สำหรับอุปกรณ์ Android หากระบบร้องขอสิทธิ์การเข้าถึง ควรเลือก “อนุญาต” เพื่อให้แอปสามารถทำงานได้อย่างสมบูรณ์



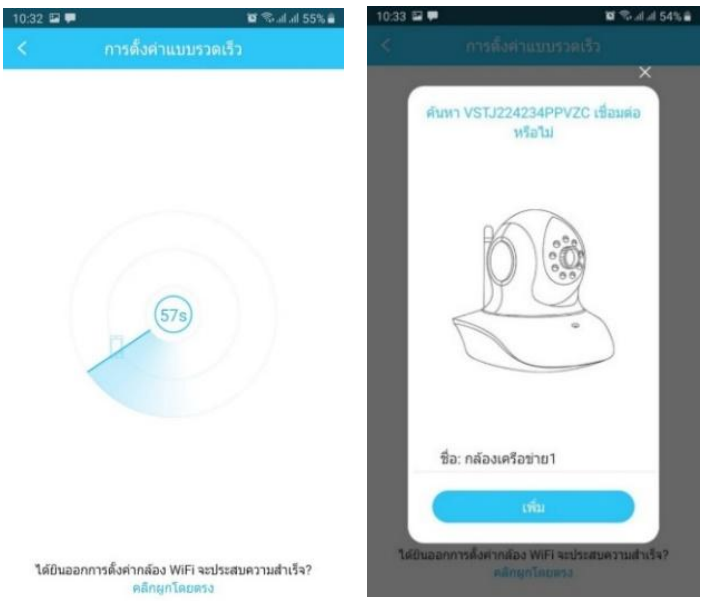
รูปที่ 4.15 การสแกนโค้ด QR ที่ตัวกล้องเพื่อดำเนินการตามคำแนะนำบนแอปฟลิเคชั่น (Global Column Limited, 2016)

3.1.5 หลังจากนั้นให้กรอกรหัสผ่านของเครือข่าย Wi-Fi ที่ต้องการเชื่อมต่อ พร้อมตรวจสอบความถูกต้องของชื่อเครือข่ายและรหัสผ่าน ก่อนกดปุ่ม “ตกลง” เพื่อยืนยันการเชื่อมต่อ โดยชื่อ Wi-Fi จะถูกเลือกให้อัตโนมัติ หากไม่ปรากฏชื่อเครือข่าย ควรตรวจสอบการเชื่อมต่อ Wi-Fi ของสมาร์ตโฟนอีกครั้ง ทั้งนี้เครือข่ายที่ใช้งานต้องเป็นย่านความถี่ 2.4 GHz เท่านั้น



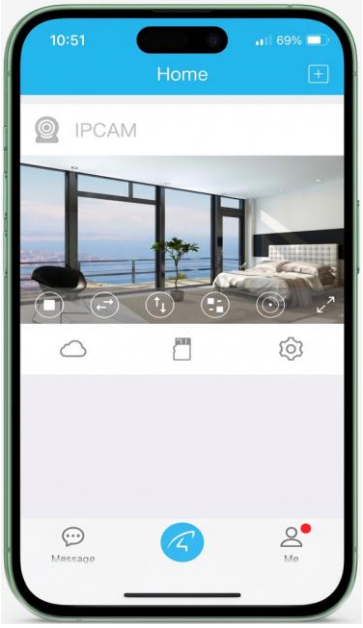
รูปที่ 4.16 การกรอกรหัสผ่าน Wi-Fi เพื่อเชื่อมต่อกล้อง (Global Column Limited, 2016)

3.1.6 จากนั้นรอจนกว่าจะพบกล้องไอพี ทำการตั้งชื่อแล้วกดเพิ่ม



รูปที่ 4.17 การตั้งชื่อกล้องหลังเชื่อมต่อสำเร็จ (Global Column Limited, 2016)

3.1.7 หลังจากติดตั้งเสร็จสมบูรณ์ ควรเปลี่ยนรหัสผ่านเริ่มต้นของกล้องเพื่อเพิ่มความปลอดภัยในการใช้งาน



รูปที่ 4.18 หน้าจอแอปพลิเคชันหลังติดตั้งเสร็จสมบูรณ์

4. IP address

IP address คือหมายเลขที่ใช้ระบุอุปกรณ์ในเครือข่าย ตัวอย่างเช่น 192.168.1.105 โดยอุปกรณ์ที่ต้องการติดต่อกันภายใน LAN โดยตรงควรอยู่ในเครือข่ายย่อยเดียวกัน เช่น

อุปกรณ์	**ตัวอย่าง IP address**
เราเตอร์	192.168.1.1
กล้อง IP camera	192.168.1.105
คอมพิวเตอร์	192.168.1.20
สมาร์ตโฟน	192.168.1.35

เมื่อใช้ subnet mask 255.255.255.0 อุปกรณ์ตัวอย่างทั้งหมดอยู่ในเครือข่าย 192.168.1.0/24 จึงสามารถติดต่อกันภายใน LAN ได้ หากเราเตอร์และกล้องของสถานศึกษากำหนดหมายเลขชุดอื่น ให้ใช้ค่าจริงของเครือข่ายนั้น

5. DHCP

DHCP เป็นบริการของเราเตอร์ที่แจก IP address ให้กับอุปกรณ์โดยอัตโนมัติ เมื่อเชื่อมต่อกล้องเข้ากับเราเตอร์ กล้องมักได้รับ IP address จาก DHCP ก่อน

เพื่อป้องกัน IP address ของกล้องเปลี่ยนภายหลัง สามารถใช้ฟังก์ชัน DHCP Reservation ของเราเตอร์ผูก IP address ไว้กับ MAC address ของกล้อง

6. Default gateway

Default gateway โดยทั่วไปคือ IP address ของเราเตอร์ ทำหน้าที่เป็นทางออกจากเครือข่ายภายในไปยังเครือข่ายอื่นหรืออินเทอร์เน็ต เช่น 192.168.1.1

6. การเชื่อมต่อแบบสายและไร้สาย

- Ethernet หรือ LAN: มีความเสถียร เหมาะสำหรับการตั้งค่าครั้งแรกและการตรวจสอบปัญหา
- Wi-Fi: ติดตั้งสะดวก แต่คุณภาพสัญญาณอาจได้รับผลกระทบจากระยะทาง ผนัง และสัญญาณรบกวน
- กล้องรุ่นนี้ใช้ Wi-Fi ย่าน 2.4 GHz จึงควรตรวจสอบว่าเราเตอร์เปิดใช้งานย่านดังกล่าว

7. การดูภาพภายในเครือข่าย

การดูภาพภายในเครือข่าย หมายถึงกล้องและอุปกรณ์ที่ใช้ดูภาพเชื่อมต่อกับเราเตอร์หรือ LAN เดียวกัน ไม่จำเป็นต้องเปิดพอร์ตกล้องออกสู่อินเทอร์เน็ต

IP address แบบ 192.168.x.x, 10.x.x.x หรือ 172.16–31.x.x เป็น Private IP address ใช้งานภายในเครือข่าย และไม่ใช่ Cloud URL

ขั้นตอนการปฏิบัติงาน

1. ขั้นตอนที่ 1 ตรวจสอบอุปกรณ์ก่อนติดตั้ง
   1) ตรวจสอบชื่อรุ่นบนตัวกล้องว่าเป็น Vstarcam C7824WIP
   2) ตรวจสอบสภาพตัวกล้อง เลนส์ เสาอากาศ สายไฟ และขั้วต่อ
   3) อ่านค่าพิกัดแรงดันและกระแสจากป้ายกำกับของกล้อง
   4) ตรวจสอบว่าอะแดปเตอร์มีแรงดันและขั้วตรงกับกล้อง
   5) ตรวจสอบสาย LAN ว่าไม่มีรอยแตกหรือขั้ว RJ45 เสียหาย
   6) ใช้ LAN Cable Tester ทดสอบสาย LAN
   7) ตรวจสอบว่าลำดับสาย 1–8 แสดงต่อเนื่องและตรงกันทั้งสองด้าน
   8) บันทึกผลการตรวจสอบลงในตาราง
2. ขั้นตอนที่ 2 เตรียมเครือข่าย
   1) เปิดเราเตอร์หรือ Access Point
   2) ตรวจสอบว่าเราเตอร์เปิด DHCP Server
   3) ตรวจสอบว่าเราเตอร์เปิด Wi-Fi ย่าน 2.4 GHz
   4) บันทึก SSID ที่ใช้ในการทดลอง
   5) เชื่อมต่อคอมพิวเตอร์กับเราเตอร์ด้วยสาย LAN หรือ Wi-Fi
   6) เชื่อมต่อสมาร์ตโฟนกับ SSID เดียวกัน
   7) ตรวจสอบว่าคอมพิวเตอร์และสมาร์ตโฟนได้รับ IP address
   8) บันทึก IP address ของเราเตอร์ คอมพิวเตอร์ และสมาร์ตโฟน

9) วิธีตรวจสอบ IP address ของคอมพิวเตอร์ Windows

- กด Windows + R
- พิมพ์ cmd
- กด Enter
- พิมพ์คำสั่ง

  ipconfig

10) บันทึกค่า IPv4 Address, Subnet Mask และ Default Gateway

ตารางที่ 4.1 ข้อมูลเครือข่ายก่อนติดตั้งกล้อง

รายการ	ค่าที่ตรวจพบ
SSID	
ย่านความถี่	2.4 GHz / 5 GHz
IP address ของเราเตอร์	
Subnet mask	
IP address ของคอมพิวเตอร์	
IP address ของสมาร์ตโฟน	
DHCP Server	เปิด/ปิด

3. ตอนที่ 3 เชื่อมต่อกล้องด้วยสาย LAN

การตั้งค่าครั้งแรกควรใช้สาย LAN เพราะช่วยลดปัญหาจากรหัสผ่าน Wi-Fi หรือระดับสัญญาณ

1) ตรวจสอบว่าอะแดปเตอร์กล้องยังไม่ได้เสียบปลั๊ก
2) ต่อสาย LAN ด้านหนึ่งเข้าพอร์ต RJ45 ของกล้อง
3) ต่อปลายอีกด้านเข้าพอร์ต LAN ของเราเตอร์
4) ตรวจสอบว่าสายเสียบแน่นทั้งสองด้าน
5) ต่ออะแดปเตอร์เข้ากับกล้อง
6) เสียบอะแดปเตอร์เข้ากับแหล่งจ่ายไฟ
7) รอประมาณ 1-2 นาทีให้กล้องเริ่มทำงาน
8) สังเกตไฟแสดงสถานะหรือเสียงแจ้งเตือนของกล้อง
9) ตรวจสอบไฟ Link/Activity ที่พอร์ตเราเตอร์ หากเราเตอร์มีไฟแสดงสถานะ
10) ห้ามถอดไฟระหว่างกล้องกำลังเริ่มต้นระบบ

4. ตอนที่ 4 ติดตั้งและเพิ่มกล้องในแอป Eye4

คู่มือ Vstarcam ระบุวิธีเพิ่มกล้องหลายรูปแบบ เช่น การค้นหาใน LAN การเพิ่มด้วยตนเอง การสแกน QR code และการตั้งค่า Wi-Fi ทั้งนี้ชื่อเมนูอาจแตกต่างกันตามรุ่นและเวอร์ชันแอปพลิเคชั่น (https://www.vstarcam.com/support/wp-content/uploads/2019/06/User-Manual-for-Smart-Cameras-1.pdf?utm_source=chatgpt.com)

1) ติดตั้งแอป Eye4 จากแหล่งดาวน์โหลดที่เชื่อถือได้
2) เปิดแอปและเข้าสู่ระบบ หากแอปกำหนดให้ลงทะเบียน
3) อนุญาตสิทธิ์การเข้าถึงเครือข่ายภายในหรือกล้องถ่ายภาพเท่าที่จำเป็น
4) กดเครื่องหมายเพิ่มอุปกรณ์ +
5) เลือกประเภทอุปกรณ์ IP camera
6) เลือกวิธีเพิ่มอุปกรณ์อย่างใดอย่างหนึ่ง
   - ค้นหาอุปกรณ์ใน LAN
   - สแกน QR code บนตัวกล้อง
   - ป้อน Device ID ด้วยตนเอง
7) เลือกกล้องที่ตรวจพบ
8) ป้อนชื่อผู้ใช้และรหัสผ่านตามข้อมูลของกล้อง
9) หากกล้องยังใช้รหัสผ่านเริ่มต้น ให้เปลี่ยนเป็นรหัสผ่านใหม่ทันที
10) ตั้งชื่ออุปกรณ์ เช่น LAB-IPCAM-01
11) กดบันทึก
12) เลือกกล้องเพื่อเปิด Live View
13) สังเกตว่าภาพปรากฏต่อเนื่องหรือไม่
14) เลื่อนวัตถุผ่านหน้ากล้อง เพื่อตรวจสอบว่าภาพมีการเปลี่ยนแปลงจริง
15) หากกล้องรองรับการหมุน ให้ทดลองควบคุมในระยะที่ไม่ทำให้กล้องชนสิ่งกีดขวาง
16) บันทึกผลการดูภาพ
17) หากเพิ่มกล้องไม่สำเร็จ ให้เลือก “ค้นหาใน LAN” ขณะที่กล้องต่อสาย LAN และสมาร์ตโฟนเชื่อมต่อเราเตอร์เดียวกันก่อน

5. ขั้นตอนที่ 5 ตรวจสอบ IP address ของกล้อง เลือกใช้วิธีใดวิธีหนึ่งต่อไปนี้

1) วิธีที่ 1 ตรวจสอบจากหน้าจัดการเราเตอร์
   1.1) เปิดเว็บเบราว์เซอร์
   1.2) ป้อน IP address ของเราเตอร์ เช่น 192.168.1.1
   1.3) เข้าสู่ระบบด้วยบัญชีผู้ดูแลที่ผู้สอนกำหนด
   1.4) เปิดเมนู DHCP Client List, Connected Devices หรือ LAN Clients
   1.5) ค้นหาอุปกรณ์ที่มีชื่อเกี่ยวข้องกับ Vstarcam หรือเปรียบเทียบ MAC address
   1.6) บันทึก IP address และ MAC address ของกล้อง
   1.7) ห้ามเปลี่ยนการตั้งค่าอื่นของเราเตอร์โดยไม่ได้รับอนุญาต
2) วิธีที่ 2 ใช้โปรแกรมค้นหาอุปกรณ์
   2.1) เปิดโปรแกรมค้นหากล้องหรือโปรแกรมสแกนเครือข่ายที่ผู้สอนกำหนด
   2.2) เลือก Network Interface ที่เชื่อมต่อกับเราเตอร์
   2.3) กด Search หรือ Scan

2.4) รอจนโปรแกรมแสดงรายการอุปกรณ์

2.5) ระบุกล้องจากชื่ออุปกรณ์ IP address หรือ MAC address

2.6) บันทึกข้อมูลที่ตรวจพบ

3) วิธีที่ 3 ตรวจสอบจากแอป

3.1)เปิดรายละเอียดอุปกรณ์ในแอป Eye4

3.2)เปิด Device Information หรือ Network Information

3.3)ตรวจสอบว่ามีการแสดง Local IP address หรือไม่

3.4)บันทึกค่าที่พบ

ตารางที่ 4.2 ข้อมูลประจำตัวของกล้อง

รายการ	ค่าที่ตรวจพบ
ชื่อกล้อง	
รุ่นกล้อง	
Device ID	
MAC address	
IP address	
Subnet mask	
Default gateway	
วิธีได้รับ IP	DHCP/Static
วิธีค้นพบ IP	Router/App/โปรแกรมค้นหา

6. ขั้นตอนที่ 6 ทดสอบการติดต่อด้วยคำสั่ง Ping

1) ตรวจสอบว่าคอมพิวเตอร์กับกล้องอยู่ในเครือข่ายเดียวกัน

2) เปิด Command Prompt

3) ใช้คำสั่ง โดยแทนค่าด้วย IP address จริงของกล้อง

```
ping 192.168.1.105
```

4) ตรวจสอบผลที่ปรากฏ

5) หากได้รับข้อความ Reply from... แสดงว่ากล้องตอบสนองต่อ Ping

6) บันทึกค่าเวลาเฉลี่ยและจำนวน packet ที่สูญหาย

7) หากขึ้น Request timed out แต่ยังดูภาพได้ ไม่ควรสรุปทันทีว่ากล้องเสีย เพราะอุปกรณ์หรือไฟร์วอลล์อาจปิดการตอบ ICMP

8) ใช้ผลการดูภาพร่วมกับผล Ping ในการตัดสิน

	ใบงานที่ 4 เรื่อง งานติดตั้งกล้อง Internet Protocol Camera (IP camera)	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ตารางที่ 4.3 ข้อมูลประจำตัวของกล้อง

ครั้งที่	IP ของกล้อง	ส่ง	รับ	สูญหาย	เวลาเฉลี่ย	ผล (ผ่าน/ไม่ผ่าน)
1		4				
2		4				
3		4				

7. ขั้นตอนที่ 7 ทดสอบดูภาพภายในเครือข่าย

7.1 ทดสอบผ่านสมาร์ตโฟน

1) ตรวจสอบว่าสมาร์ตโฟนเชื่อมต่อ Wi-Fi เดียวกับกล้อง

2) ปิด Mobile Data ชั่วคราวเพื่อยืนยันว่ากำลังทดสอบผ่าน LAN

3) เปิดแอป Eye4

4) เลือกกล้องที่เพิ่มไว้

5) เปิด Live View

6) ให้สมาชิกในกลุ่มเดินผ่านหน้ากล้อง

7) ตรวจสอบว่าภาพในแอปเปลี่ยนแปลงตามเหตุการณ์จริง

8) บันทึกความต่อเนื่อง ความล่าช้า และความคมชัดของภาพ

9) จับภาพหน้าจอประกอบรายงาน โดยหลีกเลี่ยงการถ่ายติดบุคคลที่ไม่ยินยอม

7.2 ทดสอบผ่านคอมพิวเตอร์

1) ตรวจสอบว่าคอมพิวเตอร์อยู่ในเครือข่ายเดียวกับกล้อง

2) เปิดโปรแกรมหรือเว็บอินเทอร์เฟซที่กล้องรองรับ

3) ป้อน IP address หรือเลือกกล้องจากรายการ

4) เข้าสู่ระบบด้วยบัญชีของกล้อง

5) เปิด Live View

6) ตรวจสอบว่าภาพตรงกับภาพในแอป

7) หากเว็บเบราว์เซอร์ไม่แสดงภาพ แต่แอปแสดงภาพได้ ให้ตรวจสอบว่าเฟิร์มแวร์หรือเว็บอินเทอร์เฟซต้องใช้ซอฟต์แวร์เฉพาะหรือไม่

8) ห้ามติดตั้งปลั๊กอินที่ไม่ทราบแหล่งที่มา

8. ขั้นตอนที่ 8 ตั้งค่ากล้องให้เชื่อมต่อ Wi-Fi ให้ทำตอนนี้หลังจากยืนยันแล้วว่ากล้องทำงานผ่านสาย LAN ได้

8.1 เปิดการตั้งค่ากล้องในแอป Eye4

8.2 เลือกเมนู Network Settings หรือ Wi-Fi Settings

8.3 เลือก SSID ย่าน 2.4 GHz ที่ใช้ในการทดลอง

8.4 ป้อนรหัสผ่าน Wi-Fi อย่างระมัดระวัง

8.5 ตรวจสอบตัวพิมพ์ใหญ่-เล็กและอักขระพิเศษ

8.6 กดบันทึกหรือ Apply

8.7 รอให้กล้องบันทึกค่าและเชื่อมต่อ Wi-Fi

8.8 ห้ามตัดไฟระหว่างการบันทึกค่า

8.9 ตรวจสอบจากเราเตอร์ว่ากล้องปรากฏในรายการอุปกรณ์ไร้สาย

8.10 ปิดภาพสดในแอปอีกครั้งขณะที่ยังต่อสาย LAN

8.11 เมื่อยืนยันว่าตั้งค่า Wi-Fi สำเร็จ ให้ปิดไฟเลี้ยงกล้อง

8.12 ถอดสาย LAN ออกจากกล้อง

8.13 จ่ายไฟให้กล้องอีกครั้ง

8.14 รอประมาณ 1-2 นาที

8.15 เปิด Live View ในแอป

8.16 ตรวจสอบว่ายังดูภาพได้

8.17 ตรวจสอบ IP address อีกครั้ง เพราะ IP อาจเปลี่ยนเมื่อเปลี่ยนจาก LAN เป็น Wi-Fi

8.18 บันทึก IP address ใหม่ หากมีการเปลี่ยนแปลง

9. ขั้นตอนที่ 9 พิสูจน์ว่าเป็นการดูภาพภายในเครือข่าย

9.1 ให้กล้อง สมาร์ตโฟน และคอมพิวเตอร์เชื่อมต่อกับเราเตอร์เดียวกัน

9.2 ปิด Mobile Data ของสมาร์ตโฟน

9.3 ตัดการเชื่อมต่ออินเทอร์เน็ตด้าน WAN ของเราเตอร์ชั่วคราว โดยได้รับอนุญาตจากผู้สอน

9.4 ไม่ต้องปิดเราเตอร์หรือ Wi-Fi

9.5 ทดลอง Ping กล้องจากคอมพิวเตอร์

9.6 ทดลองดูภาพด้วยวิธี Local/LAN ที่ซอฟต์แวร์รองรับ

9.7 หากยังดูภาพได้ แสดงว่าการรับส่งภาพเกิดขึ้นภายใน LAN

9.8 ต่ออินเทอร์เน็ตกลับเมื่อทดสอบเสร็จ

แอปบางรุ่นอาจต้องตรวจสอบบัญชีผ่าน Cloud ก่อนเปิดภาพ แม้กล้องกับโทรศัพท์อยู่ใน LAN เดียวกัน หากแอปดูภาพไม่ได้หลังตัดอินเทอร์เน็ต แต่เปิดภาพผ่าน Local Client ได้ ให้บันทึกข้อจำกัดนี้ตามจริง

10. วิธีแก้ปัญหาในการติดตั้งเบื้องต้น

10.1 หากติดตั้งกล้องตามขั้นตอนแล้ว แต่กล้องยังไม่สามารถออนไลน์ได้ สามารถตรวจสอบเบื้องต้นได้ดังนี้

1) ตรวจสอบสัญญาณ Wi-Fi ว่าสามารถใช้งานได้ตามปกติ

2) ตรวจสอบแหล่งจ่ายไฟและปลั๊กไฟของกล้อง

3) ตรวจสอบว่าหลังเสียบปลั๊ก กล้องมีการหมุนปรับตำแหน่งอัตโนมัติหรือไม่

4) กดปุ่ม Reset ค้างไว้ประมาณ 5 s หรือจนได้ยินเสียงแจ้งเตือน แล้วดำเนินการติดตั้งใหม่อีกครั้ง

10.2 กรณีเปลี่ยนเราเตอร์ใหม่แล้วไม่สามารถใช้งานกล้องได้ สามารถแก้ไขได้ดังนี้

1) วิธีที่ 1 ให้กำหนดชื่อ Wi-Fi รหัสผ่านของเราเตอร์ใหม่ให้เหมือนกับเราเตอร์เดิมทุกประการ

2) วิธีที่ 2 เชื่อมต่อสายสัญญาณเครือข่าย ระหว่างกล้องกับเราเตอร์ใหม่ จากนั้นเปิดแอป Eye4 รอจนกล้องออนไลน์ แล้วเข้าไปที่เมนู “ตั้งค่า Wi-Fi” เลือกเครือข่าย Wi-Fi ใหม่ กรอกรหัสผ่าน และกดตกลง รอประมาณ 1 นาที จนกล้องรีบูตเสร็จ จากนั้นจึงถอดสายสัญญาณเครือข่ายออก

3) วิธีที่ 3 ทำการรีเซตกล้อง IP camera แล้วติดตั้งใหม่ทั้งหมด

10.3 กรณีลืมรหัสผ่านกล้อง IP camera หากผู้ใช้งานเปลี่ยนรหัสผ่านของกล้องแล้วลืมรหัสผ่าน สามารถแก้ไขได้โดยกดปุ่ม reset ค้างไว้ประมาณ 5 s หรือจนได้ยินเสียงแจ้งเตือน จากนั้นทำการติดตั้งใหม่อีกครั้ง โดยระบบจะกลับไปใช้รหัสผ่านเริ่มต้นคือ 888888 ซึ่งเป็นรหัสผ่านเริ่มต้นจากโรงงานของกล้อง Vstarcam

11. บันทึกผลการปฏิบัติงานในตารางที่ 4.4

ตารางที่ 4.4 บันทึกผลการติดตั้งและทดสอบกล้อง

ลำดับ	รายการทดสอบ	ผลที่คาดหวัง	ผลที่ตรวจพบ	ผ่าน/ไม่ผ่าน	หมายเหตุ
1	กล้องเริ่มทำงาน	มีไฟหรือเสียงแสดงสถานะ			
2	พอร์ต LAN ทำงาน	ไฟ Link/Activity ติดหรือกะพริบ			
3	เพิ่มกล้องใน Eye4	แอปพบและบันทึกกล้องได้			
4	ดูภาพผ่านสาย LAN	ภาพสดแสดงต่อเนื่อง			
5	ตรวจพบ IP address	พบ IP ของกล้องใน LAN			
6	ทดสอบ Ping	ติดต่อกล้องได้หรือบันทึกข้อจำกัด			
7	ตั้งค่า Wi-Fi	กล้องเชื่อมต่อ 2.4 GHz ได้			
8	ดูภาพหลังถอด LAN	ภาพสดแสดงผ่าน Wi-Fi			
9	ทดสอบการเคลื่อนไหว	ภาพเปลี่ยนตามเหตุการณ์จริง			
10	ทดสอบภายใน LAN	ดูภาพจากเครือข่ายเดียวกันได้			
11	เปลี่ยนรหัสผ่าน	ไม่ใช้รหัสผ่านเริ่มต้น			
12	ตรวจสอบความร้อน	กล้องและอะแดปเตอร์ไม่ร้อนผิดปกติ			

	ใบงานที่ 4 เรื่อง งานติดตั้งกล้อง Internet Protocol Camera (IP camera)	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

สรุปผลการทดลอง

เอกสารอ้างอิง

กิตติศักดิ์ เฮงสว่าง. (2553). *การจัดการระบบเครือข่ายกล้องวงจรปิดเอซิต*. สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีมหานคร.

ชลดา ปานสง, เกียรติศักดิ์ สมฤทธิ์, จิรพงษ์ จิตตะโคตร์, พัชราวรรณ พูลใจ, ศิวกร รัตนวราหะ, และธนพล แก้วคำแจ้ง. (2566). การพัฒนาสื่อบทเรียนออนไลน์มูเดิลคลาวด์สำหรับการฝึกอบรมการติดตั้งและบำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด ตามมาตรฐานกรมพัฒนาฝีมือแรงงาน. *วารสารวิจัยและนวัตกรรมการอาชีวศึกษา*, 7(2), 66-75.

บริษัท มีเดีย เสิร์ช จำกัด. (2021). *กล้องวงจรปิดระบบ WiFi กับการออกแบบระบบเครือข่าย*. https://www.cctvbangkok.com/cctv-wifi-system/.

พกิจ สุวัตถิ์. (2557). *การปฏิบัติงานด้านระบบกล้องวงจรปิด CCTV*. กรุงเทพฯ: ภาควิชาวิศวกรรมศาสตร์และอุตสาหกรรมวิจัย คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสยาม.

CS Odessa. (2025a). *CCTV network example*. https://www.conceptdraw.com/How-To-Guide/cctv-network-example.

Global Column Limited. (2016). *VStarcam C7824WIP HD wireless IP security camera with audio night vision pan & tilt*. HobbyKing. https://hobbyking.com/vstarcam-c7824wip-hd-wireless-hd-ip-security-camera-with-audio-night-vision-pan-tilt.html.

Ideal Quality Solutions Co., Ltd. (2560). *ระบบกล้องวงจรปิด*. https://www.ideal-solutions.co.th/products/cctv-closed-circuit-television-system/

Kruegle, H. (2011). *CCTV surveillance: Video practices and technology*. Butterworth-Heinemann.

Yu, L. (2016). *How to distinguish T568A and T568B of RJ45 Ethernet cable wiring?* LinkedIn. https://www.linkedin.com/pulse/how-distinguish-t568a-t568b-rj45-ethernet-cable-wiring-laura-yu.

	ใบงานที่ 5 เรื่อง ระบบควบคุมประตูอัจฉริยะ ด้วยเทคโนโลยี RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ออกแบบ ต่อวงจร เขียนโปรแกรมควบคุม และทดสอบระบบควบคุมประตูอัจฉริยะด้วยเทคโนโลยี RFID ได้อย่างถูกต้องเหมาะสม

วัตถุประสงค์

1. อธิบายหลักการทำงานของระบบควบคุมการเข้า–ออกประตูด้วย RFID ได้อย่างถูกต้อง
2. อธิบายการสื่อสารแบบ SPI, I²C และการสแกนแป้นกดแบบเมทริกซ์ได้อย่างถูกต้อง
3. เชื่อมต่อ Arduino UNO กับโมดูล RFID-RC522 จอ LCD แบบ I²C แป้นกด เซอร์โวมอเตอร์ LED และ Buzzer ได้อย่างถูกต้อง
4. อ่านค่า UID ของบัตรหรือแท็ก RFID และบันทึกลงในโปรแกรมได้
5. เขียนและอัปโหลดโปรแกรมตรวจสอบบัตร RFID ร่วมกับรหัสผ่านได้
6. ทดสอบการอนุญาตและปฏิเสธการเข้าใช้งานได้
7. ตรวจสอบ แก้ไข และบันทึกข้อขัดข้องของระบบได้
8. ปฏิบัติงานโดยคำนึงถึงความปลอดภัยและการป้องกันข้อมูลส่วนบุคคลได้

เครื่องมือและอุปกรณ์

1. บอร์ด Arduino UNO พร้อมสาย USB	1 ชุด
2. โมดูลอ่านบัตร RFID-RC522 ความถี่ 13.56 MHz	1 โมดูล
3. บัตรหรือแท็ก RFID ที่ใช้งานร่วมกับ RC522 ได้	2 ใบ
4. จอ LCD 16×2 พร้อมโมดูล I²C	1 ชุด
5. Keypad แบบ 4×4 หรือ 4×3	1 ชุด
6. เซอร์โวมอเตอร์ขนาดเล็ก	1 ตัว
7. LED สีเขียว น้ำเงิน และสีแดง	1 ดวง
8. ตัวต้านทานจำกัดกระแส LED 220–330 Ω	2 ตัว
9. Active Buzzer 5 V	1 ตัว
10. แหล่งจ่ายไฟ DC 5 V ที่จ่ายกระแสได้เพียงพอ	1 ชุด
11. เบรดบอร์ดและสายต่อวงจร	1 ชุด
12. ดิจิทัลมัลติมิเตอร์	1 เครื่อง
13. คอมพิวเตอร์ที่ติดตั้ง Arduino IDE	1 เครื่อง

	ใบงานที่ 5 เรื่อง ระบบควบคุมประตูอัจฉริยะ ด้วยเทคโนโลยี RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความรู้พื้นฐานในการปฏิบัติงาน

1. การออกแบบระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino

ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยี RFID เป็นระบบรักษาความปลอดภัยที่ใช้คลื่นความถี่วิทยุในการอ่านข้อมูลจากบัตรหรือแท็ก เพื่อใช้ประกอบการตรวจสอบสิทธิ์ของผู้ใช้งานแทนกุญแจแบบดั้งเดิม ระบบช่วยเพิ่มความสะดวกและรวดเร็วในการเข้า–ออก รวมทั้งสามารถเพิ่ม ยกเลิก หรือเปลี่ยนแปลงสิทธิ์ได้ผ่านโปรแกรม จึงเหมาะสำหรับประยุกต์ใช้กับห้องเรียน ห้องปฏิบัติการ สำนักงาน ตู้เก็บอุปกรณ์ และประตูอัตโนมัติ ในการทดลองนี้ ระบบประกอบด้วยโมดูล RFID-RC522 บอร์ด Arduino UNO แป้นกดแบบเมทริกซ์ จอแสดงผล LCD 16×2 แบบ I²C หลอด LED อุปกรณ์กำเนิดเสียง Buzzer และเซอร์โวมอเตอร์ โดย Arduino UNO ทำหน้าที่เป็นหน่วยควบคุมหลักในการรับข้อมูล ประมวลผล ตรวจสอบสิทธิ์ และสั่งงานอุปกรณ์เอาต์พุตของระบบ

1.1 หลักการทำงานของระบบ

โมดูล RFID-RC522 ทำหน้าที่อ่านข้อมูลจากบัตรหรือแท็ก RFID ที่ทำงานในย่านความถี่ 13.56 MHz เมื่อผู้ใช้นำบัตรเข้าใกล้ตัวอ่าน โมดูลจะอ่านหมายเลขประจำบัตรหรือ UID (Unique Identifier) แล้วส่งข้อมูลไปยัง Arduino UNO ผ่านการสื่อสารแบบ SPI เพื่อเปรียบเทียบกับรายการ UID ที่กำหนดไว้ในโปรแกรม

หาก UID ตรงกับรายการบัตรที่ได้รับอนุญาต ระบบจะเข้าสู่ขั้นตอนการรับรหัสผ่านจาก Keypad ผู้ใช้งานต้องป้อนรหัสผ่านให้ถูกต้องภายในเงื่อนไขที่กำหนด เมื่อทั้ง UID และรหัสผ่านถูกต้อง Arduino จะดำเนินการดังนี้

- แสดงข้อความ “Access Granted” และ “Door Opened” บนจอ LCD
- เปิด LED สีเขียวเพื่อแสดงสถานะอนุญาต
- สั่งให้เซอร์โวมอเตอร์หมุนไปยังตำแหน่งปลดล็อก
- หน่วงเวลาตามที่กำหนด แล้วสั่งให้เซอร์โวมอเตอร์กลับสู่ตำแหน่งล็อก

หาก UID ไม่อยู่ในรายการที่ได้รับอนุญาต หรือผู้ใช้ป้อนรหัสผ่านไม่ถูกต้อง ระบบจะไม่สั่งปลดล็อกประตู พร้อมแสดงข้อความ “Access Denied” เปิด LED สีแดง และส่งเสียงเตือนจาก Buzzer

การใช้บัตร RFID ร่วมกับรหัสผ่านถือเป็นการยืนยันตัวตนสองปัจจัย เมื่อบัตรเป็นปัจจัยประเภท “สิ่งที่ผู้ใช้มี” และรหัสผ่านเป็นปัจจัยประเภท “สิ่งที่ผู้ใช้รู้” อย่างไรก็ตาม การทดลองนี้ตรวจสอบสิทธิ์จากค่า UID เป็นหลัก จึงเหมาะสำหรับการศึกษาและระบบต้นแบบ เนื่องจาก UID ของบัตรบางประเภทอาจถูกอ่านหรือคัดลอกได้ ระบบที่นำไปใช้งานจริงจึงควรเพิ่มกลไกการพิสูจน์ตัวตนที่ปลอดภัย การจัดการสิทธิ์ผู้ใช้ และการบันทึกเหตุการณ์เข้า–ออก

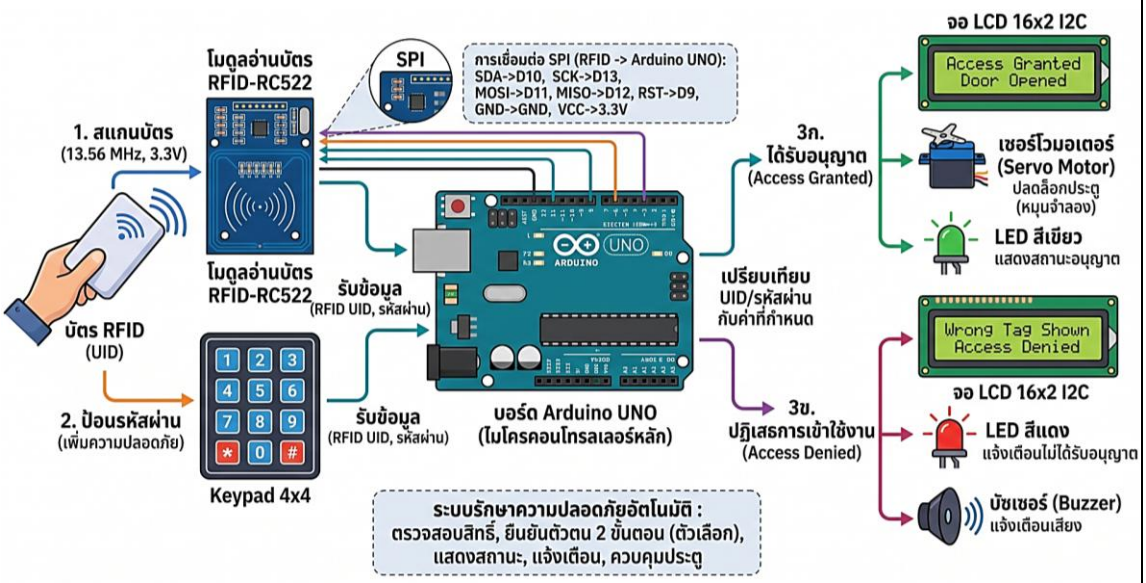
1.2 การเชื่อมต่อโมดูล RFID-RC522

โมดูล RFID-RC522 สื่อสารกับ Arduino UNO ผ่านบัส SPI โดยเชื่อมต่อดังนี้

ตารางที่ 5.1 การเชื่อมโมดูล RFID-RC522 สื่อสารกับ Arduino UNO ผ่านบัส SPI

ขา RFID-RC522	ขา Arduino UNO	หน้าที่
SDA/SS	D10	เลือกอุปกรณ์บนบัส SPI
SCK	D13	สัญญาณนาฬิกา
MOSI	D11	ส่งข้อมูลจาก Arduino ไปยัง RC522
MISO	D12	ส่งข้อมูลจาก RC522 ไปยัง Arduino
RST	D9	รีเซตโมดูล
3.3V	3.3V	แหล่งจ่ายไฟ
GND	GND	จุดอ้างอิงศักย์ไฟฟ้า
IRQ	ไม่เชื่อมต่อ	ไม่ใช้ในการทดลองนี้

โมดูล RFID-RC522 ใช้แรงดันไฟฟ้า 3.3 V จึงห้ามต่อขา VCC เข้ากับแหล่งจ่าย 5 V เพราะอาจทำให้โมดูลเสียหายได้ ก่อนประกอบวงจรทั้งหมดควรทดสอบ RC522 แยกจากอุปกรณ์อื่น โดยอัปโหลดโปรแกรมตัวอย่าง DumpInfo จากไลบรารี MFRC522 แล้วเปิด Serial Monitor เพื่อตรวจสอบว่าสามารถอ่าน UID และข้อมูลจากบัตรได้อย่างถูกต้อง



รูปที่ 5.1 หลักการทำงานของระบบควบคุมการเข้า–ออกประตูด้วย RFID และ Arduino

2. การออกแบบวงจรควบคุมระบบประตูด้วย RFID และ Arduino

ระบบควบคุมประกอบด้วยอุปกรณ์อินพุต ได้แก่ โมดูล RFID-RC522 และ Keypad ส่วนอุปกรณ์เอาต์พุต ได้แก่ จอ LCD หลอด LED, Buzzer และเซอร์โวมอเตอร์ การออกแบบวงจรต้องกำหนดขาเชื่อมต่อให้สอดคล้องกับโปรแกรม และต้องตรวจสอบไม่ให้ขาของอุปกรณ์แต่ละชนิดซ้ำกัน

2.1 การเชื่อมต่อจอ LCD แบบ I²C

จอ LCD 16×2 แบบ I²C ใช้แสดงคำแนะนำและสถานะของระบบ เช่น “Scan Your Card,” “Enter Password,” “Access Granted” และ “Access Denied” การสื่อสารแบบ I²C ใช้สายสัญญาณหลักเพียงสองเส้น ได้แก่ SDA และ SCL สำหรับ Arduino UNO และ Arduino Nano เชื่อมต่อดังนี้

- SDA เชื่อมต่อกับขา A4
- SCL เชื่อมต่อกับขา A5
- VCC เชื่อมต่อกับแหล่งจ่ายตามพิกัดของโมดูล LCD
- GND เชื่อมต่อกับ GND ของระบบ

ก่อนใช้งานควรตรวจสอบที่อยู่ I²C ของจอ ซึ่งมักเป็น 0x27 หรือ 0x3F แต่ต้องยืนยันด้วยโปรแกรม I²C Scanner หรือข้อมูลของโมดูลที่ใช้จริง

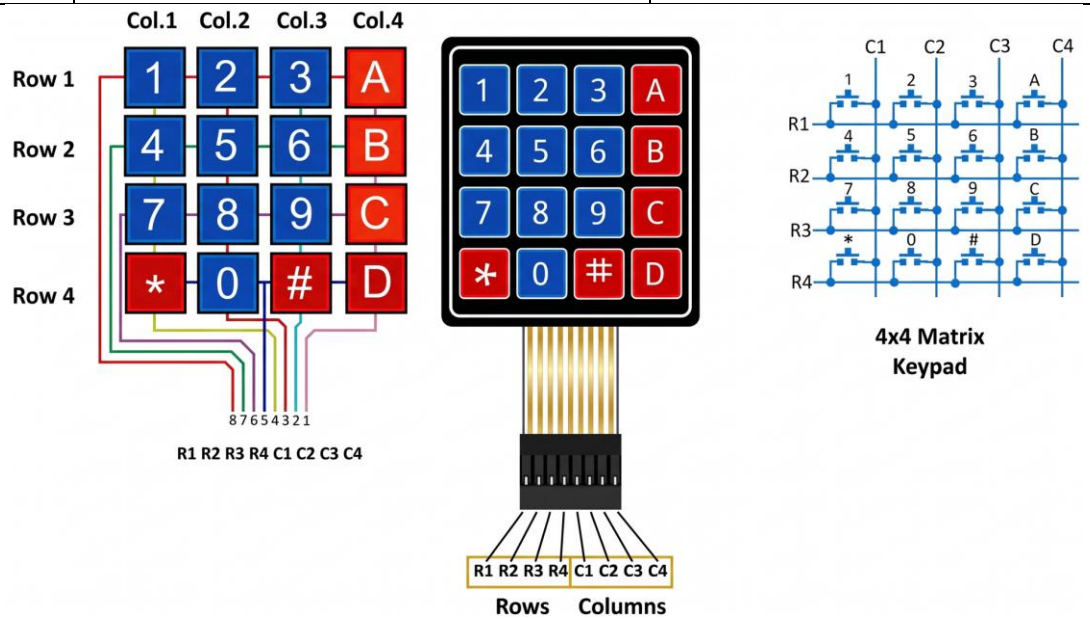
2.2 หลักการทำงานของ Keypad แบบเมทริกซ์

Keypad แบบ 4×4 ประกอบด้วยปุ่ม 16 ปุ่ม เชื่อมต่อกันในลักษณะเมทริกซ์จำนวน 4 แถวและ 4 คอลัมน์ ได้แก่ R1–R4 และ C1–C4 จึงใช้สายเชื่อมต่อทั้งหมด 8 เส้น เมื่อผู้ใช้กดปุ่มวงจรภายในจะเชื่อมแถวและคอลัมน์ที่สัมพันธ์กับปุ่มนั้นเข้าด้วยกัน ตัวอย่างเช่น

- ปุ่ม 1 อยู่ที่ R1 และ C1
- ปุ่ม 5 อยู่ที่ R2 และ C2
- ปุ่ม 9 อยู่ที่ R3 และ C3
- ปุ่ม # อยู่ที่ R4 และ C3

Arduino ตรวจสอบการกดปุ่มด้วยวิธีสแกนเมทริกซ์ (matrix scanning) โดยกระตุ้นสัญญาณทีละแถวและอ่านสถานะของแต่ละคอลัมน์ หากพบการเชื่อมต่อระหว่าง R2 และ C2 โปรแกรมจะระบุว่าผู้ใช้กดปุ่มเลข 5 วิธีนี้ช่วยลดจำนวนขาอินพุต/เอาต์พุตเมื่อเทียบกับการต่อปุ่มแต่ละปุ่มแยกกัน

หากการทดลองใช้เฉพาะตัวเลข 0–9 รวมถึงเครื่องหมาย * และ # สามารถใช้ Keypad แบบ 4×3 ได้โดยตรง ซึ่งใช้สายเชื่อมต่อเพียง 7 เส้น หากเลือกใช้ Keypad แบบ 4×4 แต่ไม่ใช้คอลัมน์ C4 ซึ่งประกอบด้วยปุ่ม A–D ต้องกำหนดจำนวนคอลัมน์และผังปุ่มในโปรแกรมให้ตรงกับการต่อวงจรจริง



รูปที่ 5.2 ตำแหน่งแถวและคอลัมน์ของ Keypad แบบ 4×4

2.3 การเชื่อมต่อ LED, Buzzer และเซอร์โวมอเตอร์

LED สีเขียวใช้แสดงสถานะอนุญาตให้เข้าใช้งาน ส่วน LED สีแดงใช้แสดงสถานะปฏิเสธ LED แต่ละดวงต้องต่ออนุกรมกับตัวต้านทานจำกัดกระแสประมาณ 220–330 Ω เพื่อป้องกันความเสียหายต่อ LED และขาเอาต์พุตของ Arduino

Buzzer ใช้แจ้งเตือนเมื่อบัตรหรือรหัสผ่านไม่ถูกต้อง หากเป็น active Buzzer ที่ใช้กระแสไม่เกินพิกัดของขา Arduino อาจควบคุมจากขาดิจิทัลได้ แต่หากอุปกรณ์ใช้กระแสสูง ควรควบคุมผ่านทรานซิสเตอร์หรือวงจรขับที่เหมาะสม

เซอร์โวมอเตอร์ใช้จำลองกลไกล็อกและปลดล็อกประตู โดย Arduino ส่งสัญญาณควบคุมตำแหน่งผ่านขาดิจิทัลที่กำหนด เนื่องจากเซอร์โวมอเตอร์อาจดึงกระแสสูงขณะเริ่มหมุนหรือรับภาระ จึงควรใช้แหล่งจ่ายไฟภายนอก 5 V ที่สามารถจ่ายกระแสได้เพียงพอ และต้องต่อ GND ของแหล่งจ่ายภายนอกร่วมกับ GND ของ Arduino ไม่ควรจ่ายไฟให้เซอร์โวมอเตอร์จากขา 3.3 V หรือจากขาเอาต์พุตดิจิทัลของ Arduino

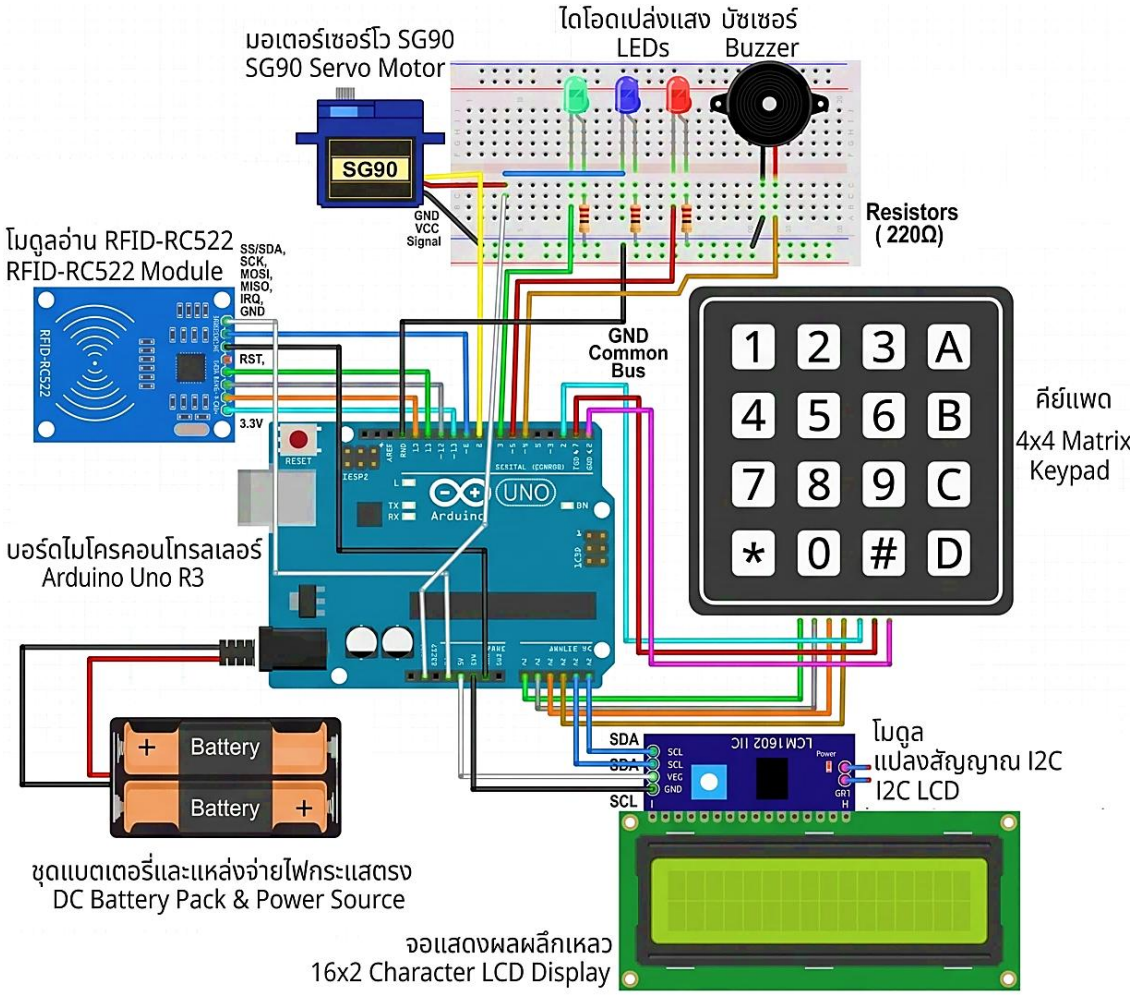
2.4 การจ่ายไฟให้ระบบ

Arduino UNO สามารถรับพลังงานผ่านสาย USB หรือรับแรงดันภายนอกผ่านแจ็ก DC หรือขา VIN ตามข้อกำหนดของบอร์ด หากใช้แบตเตอรี่หรือแหล่งจ่าย 6–12 V ต้องต่อเข้าที่วงจรรับไฟของ Arduino เท่านั้น ห้ามต่อแรงดันดังกล่าวเข้ากับ RC522, LCD, Keypad หรือเซอร์โวมอเตอร์โดยตรง

สำหรับการทดลอง ควรจ่ายไฟให้ Arduino ผ่าน USB และใช้แหล่งจ่าย 5 V ภายนอกสำหรับเซอร์โวมอเตอร์ วิธีนี้ช่วยลดปัญหาแรงดันตก สัญญาณรบกวน และการรีเซตของ Arduino ขณะที่เซอร์โวมอเตอร์ทำงาน

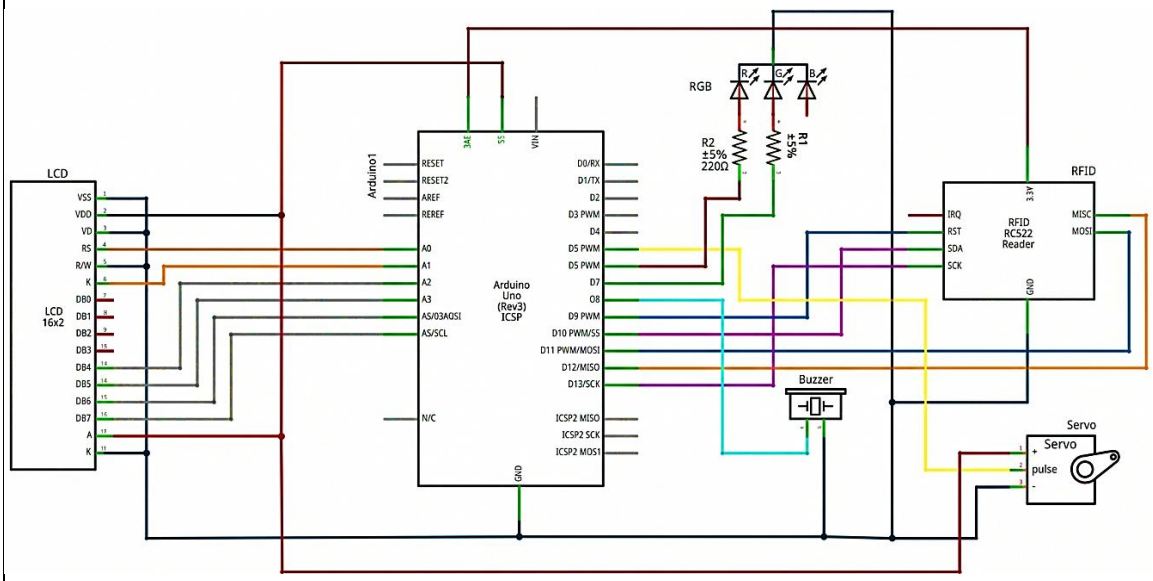
ขั้นตอนการปฏิบัติงาน

1. เชื่อมต่อวงจรดังรูปที่ 5.3



รูปที่ 5.3 ผังการเชื่อมต่ออุปกรณ์ระบบ RFID ร่วมกับ จอ LCD, Keypad, และ Servo motor (ดัดแปลงจาก Aqib, 2018)

	ใบงานที่ 5 เรื่อง ระบบควบคุมประตูอัจฉริยะ ด้วยเทคโนโลยี RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)



รูปที่ 5.4 วงจรควบคุมการเข้าออกประตูด้วย RFID และ Arduino (ดัดแปลงจาก Aqib, 2018)

ตารางที่ 5.2 ตารางตรวจสอบวงจรก่อนจ่ายไฟ

รายการตรวจสอบ	**ผลการตรวจสอบ** (ผ่าน/ไม่ผ่าน)	**หมายเหตุ**
RC522 ต่อกับแหล่งจ่าย 3.3 V		
ขา SPI เชื่อมต่อถูกต้อง		
LCD แสดงข้อความได้		
Keypad อ่านปุ่มได้ครบถ้วน		
LED มีตัวต้านทานจำกัดกระแส		
เซอร์โวมอเตอร์ใช้แหล่งจ่ายเหมาะสม		
กราวด์ของทุกวงจรเชื่อมต่อร่วมกัน		
ไม่มีขาสัญญาณกำหนดซ้ำกัน		

2. เขียนโปรแกรมควบคุมการทำงานตามเงื่อนไขที่กำหนด

(ดังภาคผนวก ข Arduino Code: 6) เพื่อให้ตรวจสอบข้อผิดพลาดได้ง่าย ควรพัฒนาและทดสอบโปรแกรมเป็นลำดับดังนี้

1) ทดสอบการอ่าน UID จาก RFID-RC522 ด้วยโปรแกรม DumpInfo

2) ทดสอบการแสดงข้อความบนจอ LCD

3) ทดสอบการอ่านปุ่มจาก Keypad

4) ทดสอบการเปิด–ปิด LED และ Buzzer

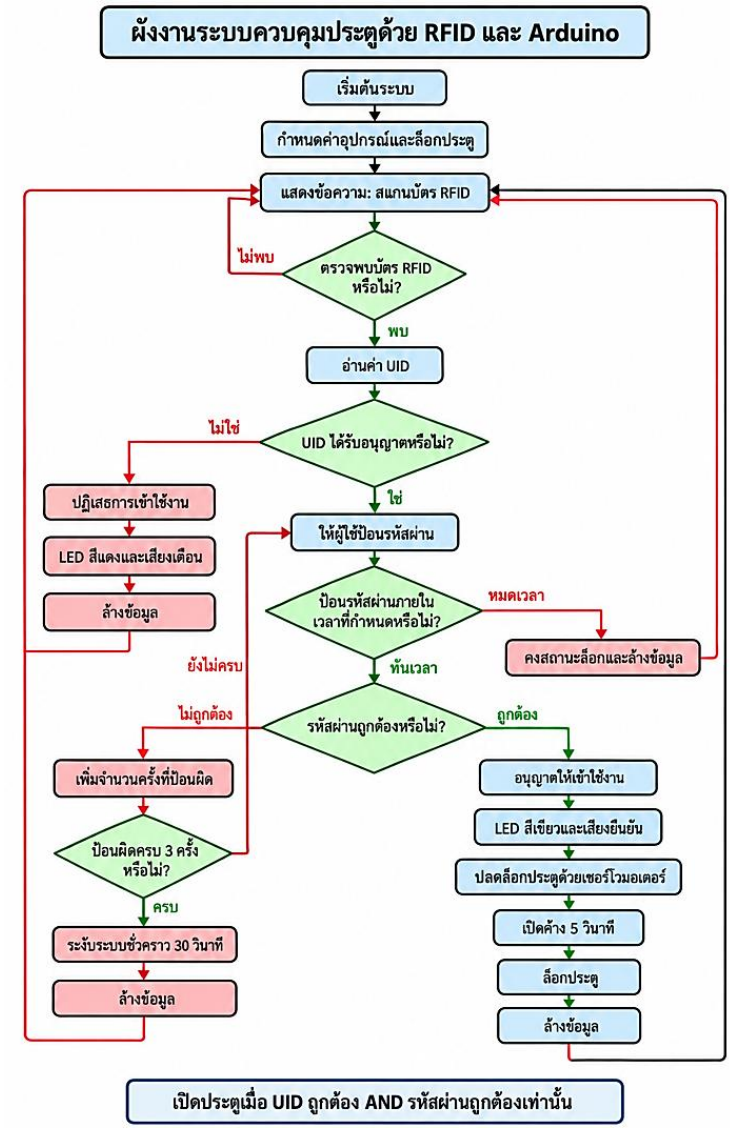
5) ทดสอบตำแหน่งล็อกและปลดล็อกของเซอร์โวมอเตอร์

6) รวมโปรแกรมตรวจสอบ UID และรหัสผ่าน

7) ทดสอบกรณีบัตรถูกต้อง บัตรไม่ถูกต้อง รหัสผ่านถูกต้อง และรหัสผ่านไม่ถูกต้อง

8) ตรวจสอบให้ระบบกลับสู่สถานะล็อกเมื่อเริ่มทำงานหรือเกิดการรีเซต

เมื่อ UID และรหัสผ่านถูกต้อง Arduino จะสั่งปลดล็อกประตู แสดงข้อความอนุญาต และเปิด LED สีเขียว แต่หากข้อมูลส่วนใดไม่ถูกต้อง ระบบจะคงสถานะล็อก แสดงข้อความปฏิเสธ เปิด LED สีแดง และส่งเสียงเตือน ทั้งนี้ โปรแกรมควรกำหนดจำนวนครั้งที่อนุญาตให้ป้อนรหัสผ่านผิด ระยะเวลาเปิดประตู และวิธีกลับเข้าสู่สถานะรอรับบัตรไว้อย่างชัดเจน (Aqib, 2018)



รูปที่ 5.5 ผังลำดับการเขียนโปรแกรม

3. ทดสอบการทำงานของโปรแกรมควบคุม

3.1 ขั้นตอนที่ 1 การตรวจสอบโมดูล RFID-RC522

1) ตรวจสอบสภาพของ Arduino UNO และ RFID-RC522
2) ต่อวงจร RC522 ตามตารางการเชื่อมต่อ
3) เชื่อมต่อ Arduino UNO เข้ากับคอมพิวเตอร์
4) เปิด Arduino IDE และติดตั้งไลบรารี MFRC522
5) เปิดโปรแกรมตัวอย่าง DumpInfo
6) เลือกชนิดบอร์ดและพอร์ตให้ถูกต้อง แล้วอัปโหลดโปรแกรม
7) เปิด Serial Monitor และกำหนดอัตราบอดให้ตรงกับโปรแกรม
8) นำบัตรแต่ละใบเข้าใกล้ตัวอ่าน แล้วบันทึกค่า UID

ตารางที่ 5.3 ตารางบันทึกค่า UID

บัตร/แท็ก	ค่า UID ที่อ่านได้	สถานะที่กำหนด	ผลการอ่าน
บัตรใบที่ 1		อนุญาต	
บัตรใบที่ 2		ไม่อนุญาต	
บัตรใบที่ 3		อื่น ๆ	

3.2 ขั้นตอนที่ 2 การติดตั้งจอ LCD และ Keypad

1) ต่อจอ LCD แบบ I²C เข้ากับ Arduino
2) ตรวจสอบ I²C address ของจอ เช่น 0x27 หรือ 0x3F
3) อัปโหลดโปรแกรมทดสอบการแสดงข้อความ
4) เชื่อมต่อ Keypad ตามลำดับขาแถวและคอลัมน์
5) อัปโหลดโปรแกรมทดสอบ Keypad
6) กดปุ่มทุกปุ่มและตรวจสอบค่าที่แสดงบน Serial Monitor

3.3 ตอนที่ 3 การติดตั้งอุปกรณ์แสดงผลและกลไกเปิดประตู

1) ต่อ LED แต่ละดวงผ่านตัวต้านทาน 220–330 Ω
2) ต่อ Buzzer ตามประเภทและพิกัดกระแสของอุปกรณ์
3) ต่อสายสัญญาณของเซอร์โวมอเตอร์เข้ากับขาที่กำหนด
4) ต่อแหล่งจ่ายไฟ 5 V ภายนอกให้เซอร์โวมอเตอร์
5) เชื่อมต่อ GND ของแหล่งจ่ายภายนอกเข้ากับ GND ของ Arduino
6) ทดสอบตำแหน่งล็อกและปลดล็อกของเซอร์โวมอเตอร์

3.4 ตอนที่ 4 การรวมวงจรและเขียนโปรแกรม

1) ตรวจสอบว่าไม่มีการกำหนดขาซ้ำกัน
2) เพิ่ม UID ของบัตรที่ได้รับอนุญาตลงในโปรแกรม

3) กำหนดรหัสผ่านสำหรับ Keypad
4) กำหนดตำแหน่งล็อกและปลดล็อกของเซอร์โวมอเตอร์
5) อัปโหลดโปรแกรมควบคุมระบบฉบับสมบูรณ์
6) ทดสอบระบบตามกรณีทดสอบที่กำหนด
7) บันทึกผล ปัญหา และวิธีแก้ไข

ตารางที่ 5.4 ตารางบันทึกผลการทดสอบระบบ

กรณีทดสอบ	**ผลที่คาดหวัง**	**ผลที่สังเกตได้**	**ประเมินผล** (ผ่าน/ไม่ผ่าน)
บัตรถูกต้องและรหัสผ่านถูกต้อง	ปลดล็อก เปิด LED สีเขียว และแสดง “Access Granted”		
บัตรถูกต้องแต่รหัสผ่านไม่ถูกต้อง	ไม่ปลดล็อก เปิด LED สีแดงและ Buzzer		
บัตรไม่ถูกต้อง	ปฏิเสธทันทีและไม่ให้ป้อนรหัสผ่าน		
ไม่มีบัตรอยู่ในระยะอ่าน	ระบบรอรับบัตรและประตูยังล็อก		
กดรหัสผ่านไม่ครบ	ระบบยังไม่ตรวจสอบหรือรอรับข้อมูลต่อ		
กดปุ่มล้างข้อมูล	ลบรหัสที่ป้อนและให้เริ่มป้อนใหม่		
เปิดประตูครบเวลาที่กำหนด	เซอร์โวมอเตอร์กลับสู่ตำแหน่งล็อก		
รีเซตหรือเปิดระบบใหม่	ระบบเริ่มต้นในสถานะล็อก		
สแกนบัตรไม่ถูกต้องติดต่อกัน	ระบบแจ้งเตือนตามเงื่อนไขที่กำหนด		

ตารางที่ 5.5 ตารางบันทึกค่าที่ตรวจวัด

รายการ	**ค่าที่กำหนด**	**ค่าที่วัดได้**	**ผลประเมิน** (ผ่าน/ไม่ผ่าน)
แรงดันที่ขา VCC ของ RC522	3.3 V	V	
แรงดันแหล่งจ่ายเซอร์โวมอเตอร์	5 V ตามพิกัดอุปกรณ์	 V	
มุมตำแหน่งล็อก	.....°	.....°	
มุมตำแหน่งปลดล็อก	.....°	.....°	
เวลาที่ประตูเปิดค้าง	.....s	.....s	
ระยะอ่านบัตร	ตามสภาพการทดลอง	.....cm	
จำนวนครั้งที่ทดสอบบัตรถูกต้อง	10 ครั้ง	สำเร็จ.....ครั้ง	

	ใบงานที่ 5 เรื่อง ระบบควบคุมประตูอัจฉริยะ ด้วยเทคโนโลยี RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ตารางที่ 5.6 การบันทึกปัญหาและแนวทางแก้ไข

ปัญหาที่พบ	สาเหตุที่เป็นไปได้	วิธีแก้ไข	ผลหลังแก้ไข
อ่านบัตร RFID ไม่ได้			
LCD ไม่แสดงข้อความ			
Keypad แสดงปุ่มไม่ตรง			
เซอร์โวมอเตอร์สั่นหรือ Arduino รีเซต			
Buzzer หรือ LED ไม่ทำงาน			
ระบบอนุญาตบัตรผิดใบ			

สรุปผลการทดลอง

เอกสารอ้างอิง

ปิยะ โควินท์ทวีวัฒน์, วีระศักดิ์ ชื่นตา, สัญญา ควรคิด, วิโรจน์ บัวงาม, และ หฤทัย ดิ้นสกุล. (2551). *ระบบบ่งชี้ด้วยคลื่นความถี่วิทยุ.* มหาวิทยาลัยราชภัฏนครปฐม.

Aqib, M. (2018). *RFID and Keypad based door lock using Arduino*. Hackster.io. https://www.hackster.io/muhammad-aqib/rfid-and-Keypad-based-door-lock-using-arduino-89e1d5.

Duroc, Y. (2022). From Identification to Sensing: RFID Is One of the Key Technologies in the IoT Field. *Sensors*, *22*(19), 7523. https://doi.org/10.3390/s22197523.

Hunt, V. D., Puglia, A., & Puglia, M. (2007). *RFID: A guide to radio frequency identification*. John Wiley & Sons.

Prabhu, S. (2026). *What is RFID? How it works? Interface RC522 RFID module with Arduino*. Last Minute Engineers. https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/.

Finkenzeller, K. (2010). *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication* (3rd ed.). Wiley.

Instructables. (2017, January 25). *Create an access control system with an 4x3 keypad & RFID-RC522!* https://www.instructables.com/Create-an-Access-Control-System-With-an-4x3-Keypad/.

Violino, B. (2005). *A summary of RFID standards*. RFID Journal. https://www.rfidjournal.com/expert-views/a-summary-of-rfid-standards/76205/.

3prabhakar. (2023, October 3). *How to write data in RFID tag using 4x4 keypad* [Online forum post]. Arduino Forum. https://forum.arduino.cc/t/how-to-write-data-in-rfid-tag-using-4x4-keypad/1174618.

	ใบงานที่ 6 เรื่อง งานออกแบบระบบควบคุมการเข้า-ออกประตูด้วย RFID โดยใช้ NodeMCU ESP8266	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

มีความรู้และทักษะในการออกแบบ ประกอบ และทดสอบระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยี RFID โดยใช้ NodeMCU ESP8266 ได้

วัตถุประสงค์

1. อธิบายหลักการทำงานของระบบควบคุมการเข้า–ออกด้วย RFID ได้อย่างถูกต้อง
2. อธิบายหน้าที่ของ NodeMCU ESP8266, RFID-RC522, LCD 16×2 แบบ I²C และ MCP23017 ได้อย่างถูกต้อง
3. อธิบายการสื่อสารแบบ SPI และ I²C ที่ใช้ในระบบได้อย่างถูกต้อง
4. เลือกและกำหนดขาเชื่อมต่อของอุปกรณ์ให้เหมาะสมกับ NodeMCU ESP8266 ได้
5. เชื่อมต่อ NodeMCU ESP8266 กับ RFID-RC522 และจอ LCD ได้อย่างถูกต้องและปลอดภัย
6. อ่านและบันทึกค่า UID ของบัตรหรือแท็ก RFID ได้อย่างถูกต้อง
7. เขียนโปรแกรมเปรียบเทียบ UID กับรายการบัตรที่ได้รับอนุญาตได้อย่างถูกต้อง
8. เขียนโปรแกรมแสดงข้อความและควบคุม LED ตามผลการตรวจสอบสิทธิ์ได้อย่างถูกต้อง
9. ทดสอบ วิเคราะห์ และแก้ไขข้อขัดข้องเบื้องต้นของวงจรได้อย่างถูกต้อง
10. ปฏิบัติงานโดยคำนึงถึงความปลอดภัยทางไฟฟ้าและการคุ้มครองข้อมูลผู้ใช้งานได้

เครื่องมือและอุปกรณ์

1.	บอร์ด NodeMCU ESP8266	1 บอร์ด
2.	สาย Micro-USB พร้อมสายรับส่งข้อมูล	1 เส้น
3.	โมดูล RFID-RC522 ความถี่ 13.56 MHz	1 โมดูล
4.	บัตรหรือแท็ก RFID ที่รองรับ RC522 อย่างน้อย	2 ใบ
5.	จอ LCD 16×2 พร้อมโมดูล I²C	1 ชุด
6.	ไอซีหรือโมดูล MCP23017	1 ชุด
7.	LED สีเขียว	1 ดวง
8.	LED สีแดง	1 ดวง
9.	ตัวต้านทาน 220–330 Ω	2 ตัว
10.	เบรดบอร์ด	1 แผง
11.	สายต่อวงจรแบบจัมเปอร์	ตามความเหมาะสม
12.	ดิจิทัลมัลติมิเตอร์	1 เครื่อง
13.	คอมพิวเตอร์ที่ติดตั้ง Arduino IDE	1 เครื่อง

14. โปรแกรม Serial Monitor 1 โปรแกรม
15. แหล่งจ่ายไฟ DC ที่มีแรงดันและกระแสเหมาะสม 1 ชุด

ความรู้พื้นฐานในการปฏิบัติงาน

1. หลักการของระบบควบคุมการเข้า–ออกด้วย RFID

RFID หรือ Radio Frequency Identification เป็นเทคโนโลยีระบุตัวตนด้วยคลื่นความถี่วิทยุ ระบบประกอบด้วยตัวอ่าน RFID และบัตรหรือแท็ก เมื่อผู้ใช้นำบัตรเข้าใกล้ตัวอ่าน พลังงานจากสนามแม่เหล็กไฟฟ้าของตัวอ่านจะทำให้บัตรแบบพาสซีฟสามารถตอบสนองและส่งข้อมูลกลับมา

ในการทดลองนี้ โมดูล RFID-RC522 อ่านค่า UID จากบัตรหรือแท็กที่ทำงานในย่านความถี่ 13.56 MHz แล้วส่งข้อมูลไปยัง NodeMCU ESP8266 ผ่านบัส SPI จากนั้นโปรแกรมจะเปรียบเทียบ UID ที่อ่านได้กับรายการ UID ที่ได้รับอนุญาต

- ถ้า UID ตรงกับรายการที่กำหนด ระบบจะแสดงข้อความอนุญาตและเปิด LED สีเขียว
- ถ้า UID ไม่ตรงกับรายการที่กำหนด ระบบจะแสดงข้อความปฏิเสธและเปิด LED สีแดง
- หลังแสดงผลตามเวลาที่กำหนด ระบบจะปิด LED และกลับเข้าสู่สถานะรอรับบัตรใบถัดไป

การตรวจสอบ UID เหมาะสำหรับการเรียนรู้และการสร้างระบบต้นแบบ แต่ระบบรักษาความปลอดภัยที่นำไปใช้งานจริงไม่ควรอาศัย UID เพียงอย่างเดียว เนื่องจาก UID ของบัตรบางประเภทอาจถูกอ่านหรือคัดลอกได้

2. หน้าที่ของ NodeMCU ESP8266

NodeMCU ESP8266 เป็นบอร์ดพัฒนาที่ใช้ไมโครคอนโทรลเลอร์ ESP8266 และรองรับการเชื่อมต่อ Wi-Fi ภายในตัว บอร์ดทำหน้าที่เป็นหน่วยควบคุมหลักของระบบ โดย

1) รับค่า UID จาก RFID-RC522
2) เปรียบเทียบ UID กับข้อมูลที่กำหนดไว้ในโปรแกรม
3) ส่งข้อความไปยังจอ LCD
4) ควบคุม LED และอุปกรณ์แจ้งเตือน
5) เชื่อมต่อเครือข่ายเพื่อส่งหรือบันทึกข้อมูลได้ หากมีการพัฒนาระบบ IoT เพิ่มเติม

ขา GPIO ของ ESP8266 ทำงานด้วยระดับลอจิก 3.3 V และไม่ทนต่อสัญญาณ 5 V จึงต้องระมัดระวังไม่ให้สัญญาณที่มีแรงดัน 5 V ป้อนเข้าสู่ขา GPIO โดยตรง

3. การเชื่อมต่อ RFID-RC522 ผ่านบัส SPI

SPI หรือ Serial Peripheral Interface เป็นการสื่อสารแบบอนุกรมที่ใช้สายสัญญาณหลัก ได้แก่ SCK, MOSI, MISO และ SS/SDA โดยมีสาย RST สำหรับรีเซตโมดูล การกำหนดขาที่นิยมใช้กับ NodeMCU ESP8266 มีดังนี้

ตารางที่ 6.1 การเชื่อมต่อวงจร ขา RFID-RC522 กับ ขา NodeMCU

ขา RFID-RC522	ขา NodeMCU	GPIO	หน้าที่
SDA/SS	D8	GPIO15	เลือกอุปกรณ์ SPI
SCK	D5	GPIO14	สัญญาณนาฬิกา
MOSI	D7	GPIO13	ส่งข้อมูลจาก NodeMCU ไปยัง RC522
MISO	D6	GPIO12	รับข้อมูลจาก RC522
RST	D0	GPIO16	รีเซตโมดูล
3.3V	3V3	–	แหล่งจ่ายไฟ 3.3 V
GND	GND	–	กราวด์ร่วม
IRQ	ไม่เชื่อมต่อ	–	ไม่ใช้ในการทดลอง

คำว่า SDA บนโมดูล RC522 ในการเชื่อมต่อแบบ SPI ทำหน้าที่เป็นขา SS หรือ Chip Select ไม่ใช่ขา SDA ของบัส I²C

โมดูล RC522 ต้องรับไฟเลี้ยง 3.3 V ห้ามต่อขา VCC เข้ากับ 5 V เนื่องจากอาจทำให้โมดูลเสียหายได้

4.การเชื่อมต่อจอ LCD 16×2 แบบ I²C

จอ LCD 16×2 แบบ I²C ใช้แสดงคำแนะนำ ค่า UID และผลการตรวจสอบสิทธิ์ เช่น

- "Scan Your Card"
- "Access Granted"
- "Access Denied"
- "Welcome"

การสื่อสารแบบ I²C ใช้สายสัญญาณ SDA และ SCL โดยการกำหนดขามาตรฐานที่นิยมใช้กับ NodeMCU ESP8266 ดังนี้

ตารางที่ 6.2 การเชื่อมต่อจอ LCD 16×2 แบบ I²C

ขาจอ LCD I²C	ขา NodeMCU	GPIO
SDA	D2	GPIO4
SCL	D1	GPIO5
GND	GND	–
VCC	ตามพิกัดของโมดูล	–

ก่อนใช้งานต้องตรวจสอบที่อยู่ I²C ของจอ ซึ่งมักเป็น 0x27 หรือ 0x3F ด้วยโปรแกรม I²C Scanner

จอ LCD 16×2 โดยทั่วไปต้องการไฟเลี้ยง 5 V เพื่อให้แสดงผลได้ชัดเจน แต่ NodeMCU ใช้ลอจิก 3.3 V หากโมดูล LCD มีตัวต้านทาน pull-up ของสาย SDA และ SCL ต่อกับ 5 V อาจทำให้แรงดัน 5 V ป้อนเข้าสู่ขา GPIO ของ ESP8266 ดังนั้นควรใช้วงจรแปลงระดับแรงดัน I²C หรือปรับตัวต้านทาน pull-up ให้ต่อกับ 3.3 V ตามคุณลักษณะของโมดูลที่ใช้

5. หน้าที่ของ MCP23017

MCP23017 เป็นไอซีขยายขาอินพุตและเอาต์พุตแบบดิจิทัลจำนวน 16 ขา โดยสื่อสารกับ NodeMCU ผ่านบัส I²C จึงใช้สาย SDA และ SCL ร่วมกับจอ LCD ได้ แต่ต้องกำหนด I²C address ของอุปกรณ์แต่ละตัวไม่ให้ซ้ำกัน

MCP23017 เหมาะสำหรับใช้เพิ่มขาควบคุม LED, Buzzer, Relay, Keypad หรืออุปกรณ์อื่นเมื่อขา GPIO ของ NodeMCU ไม่เพียงพอ อย่างไรก็ตาม หากระบบมีเพียง RC522, LCD I²C และ LED สองดวง อาจยังไม่จำเป็นต้องใช้ MCP23017 เพราะ NodeMCU อาจมีขาที่เพียงพอหลังจากวางแผนการใช้งานอย่างเหมาะสม

หากใช้ MCP23017 กับ NodeMCU ควรจ่ายไฟให้ MCP23017 ด้วย 3.3 V เพื่อให้ระดับลอจิก I²C สอดคล้องกับ ESP8266 และต้องกำหนดขา A0–A2 เพื่อเลือก I²C address อย่างชัดเจน ไม่ควรปล่อยขากำหนด address ให้ลอย

6. การควบคุม LED แสดงสถานะ

LED สีเขียวและสีแดงทำหน้าที่แสดงผลการตรวจสอบสิทธิ์ โดย LED แต่ละดวงต้องต่ออนุกรมกับตัวต้านทานประมาณ 220–330 Ω เพื่อจำกัดกระแส

ตารางที่ 6.3 แสดงสถานะ LED สำหรับการควบคุมระบบ

สถานะ	**LCD**	**LED สีเขียว** (ติด/ดับ)	**LED สีแดง** (ติด/ดับ)
รอรับบัตร	Scan Your Card		
UID ถูกต้อง	Access Granted		
UID ไม่ถูกต้อง	Access Denied		
ระบบกลับสู่สถานะเริ่มต้น	Scan Your Card		

7. ลำดับการทำงานของโปรแกรม โปรแกรมควบคุมควรทำงานตามลำดับดังนี้

1) เริ่มต้นระบบและกำหนดค่าขาอุปกรณ์
2) เริ่มต้นการสื่อสาร SPI และ I²C
3) ตรวจสอบการทำงานของ RC522 และ LCD
4) ปิด LED ทุกดวง
5) แสดงข้อความ “Scan Your Card”
6) ตรวจสอบว่ามีบัตรอยู่ในระยะอ่านหรือไม่

7) อ่านค่า UID และแปลงให้อยู่ในรูปแบบเดียวกับข้อมูลที่บันทึกไว้

8) เปรียบเทียบ UID กับรายการที่ได้รับอนุญาต

9) แสดงผลอนุญาตหรือปฏิเสธผ่าน LCD และ LED

10) หยุดการสื่อสารกับบัตรเพื่อป้องกันการอ่านซ้ำ

11) หน่วงเวลาตามที่กำหนดและล้างสถานะ

12) กลับเข้าสู่สถานะรอรับบัตรใบต่อไป

8. ข้อควรระวังในการปฏิบัติงาน

1) ปิดแหล่งจ่ายไฟก่อนประกอบหรือเปลี่ยนแปลงวงจร

2) ต่อ RC522 เข้ากับแหล่งจ่าย 3.3 V เท่านั้น

3) ห้ามป้อนสัญญาณ 5 V เข้าขา GPIO ของ ESP8266

4) ตรวจสอบการต่อ SDA และ SCL ไม่ให้สลับกัน

5) ตรวจสอบหมายเลขขา D และหมายเลข GPIO ให้ถูกต้อง เนื่องจากไม่ใช่หมายเลขเดียวกัน

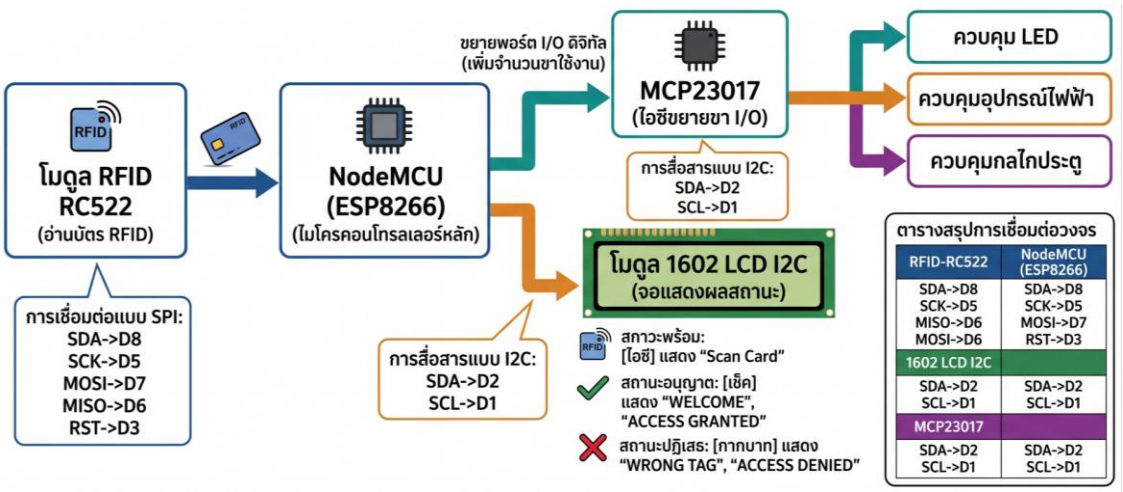
6) กำหนด I²C address ของ LCD และ MCP23017 ไม่ให้ซ้ำกัน

7) ต่อ GND ของอุปกรณ์ทุกส่วนร่วมกัน

8) ตรวจสอบการลัดวงจรด้วยมัลติมิเตอร์ก่อนจ่ายไฟ

9) ไม่ควรบันทึกหรือเผยแพร่ UID จริงพร้อมข้อมูลระบุตัวบุคคลโดยไม่มีมาตรการคุ้มครองข้อมูล

10) เมื่อนำไปควบคุมกลอนไฟฟ้าจริง ต้องเพิ่มวงจรขับ รีเลย์หรือ MOSFET ไดโอดป้องกันแรงดันย้อน และแหล่งจ่ายไฟแยกที่เหมาะสม



รูปที่ 6.1 หลักการควบคุมการเข้า-ออกประตูด้วย RFID, NodeMCU ESP8266, และ LCD

	ใบงานที่ 6 เรื่อง งานออกแบบระบบควบคุมการเข้า-ออกประตูด้วย RFID โดยใช้ NodeMCU ESP8266	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ลำดับขั้นตอนการปฏิบัติงาน

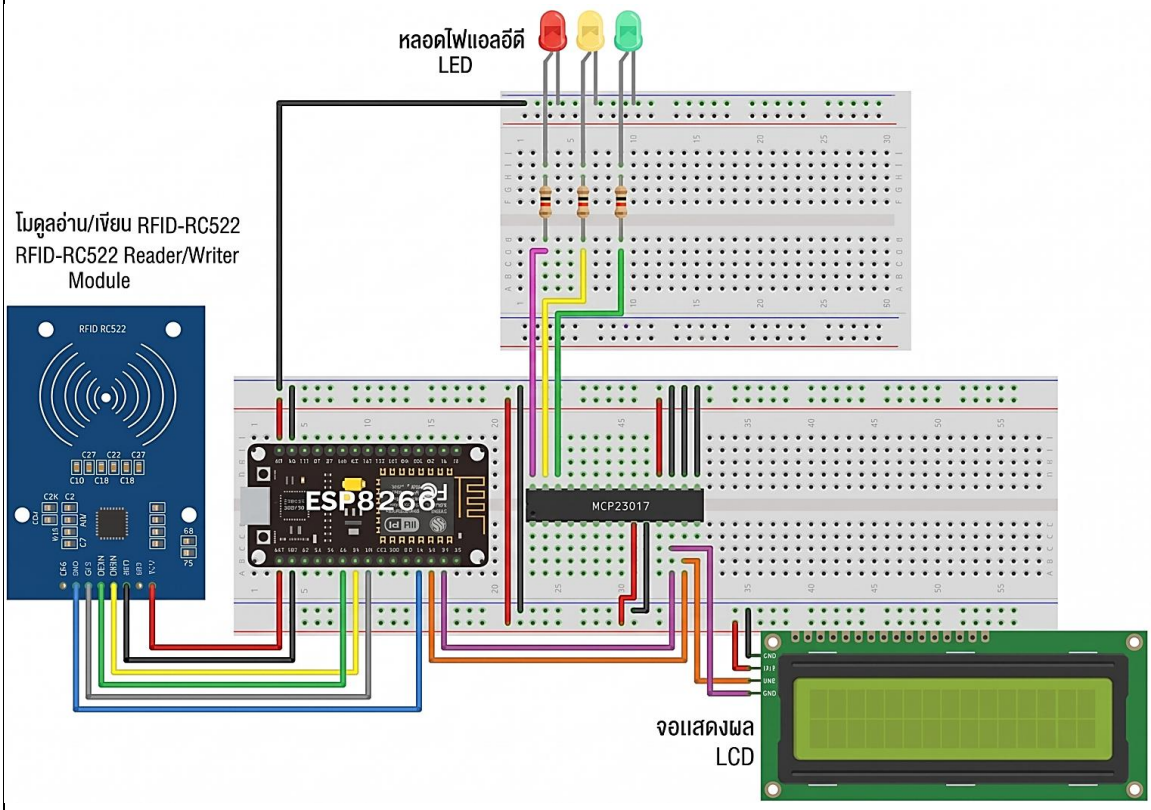
1. กำหนดเงื่อนไขการทำงานของระบบ ได้แก่
   1) UID ที่ได้รับอนุญาต
   2) ข้อความที่แสดงบนจอ LCD
   3) สถานะของ LED สีเขียวและสีแดง
   4) ระยะเวลาแสดงผลก่อนกลับสู่สถานะเริ่มต้น
2. ออกแบบผังงานและผังการเชื่อมต่อวงจรก่อนประกอบจริง
3. ติดตั้งโปรแกรมและไลบรารี
   1) เปิดโปรแกรม Arduino IDE
   2) ติดตั้งชุดข้อมูลบอร์ด ESP8266 และเลือกบอร์ด NodeMCU ที่ใช้งาน
   3) ติดตั้งไลบรารีที่จำเป็น ได้แก่ SPI, MFRC522, LiquidCrystal_I^{2}C, MCP23017
   4) เชื่อมต่อ NodeMCU กับคอมพิวเตอร์
   5) เลือกหมายเลขพอร์ตและชนิดบอร์ดให้ถูกต้อง
4. ทดสอบบอร์ด NodeMCU ESP8266
   1) อัปโหลดโปรแกรมตัวอย่างสำหรับกะพริบ LED หรือแสดงข้อความผ่าน Serial Monitor
   2) ตรวจสอบว่าสามารถอัปโหลดโปรแกรมลงบอร์ดได้
   3) เปิด Serial Monitor และตรวจสอบการเริ่มต้นทำงานของบอร์ด
   4) หากอัปโหลดไม่ได้ ให้ตรวจสอบสาย USB พอร์ต ไดรเวอร์ และการเลือกบอร์ด
5. เชื่อมต่อวงจรดังรูปที่ 6.2 ตารางที่ 6.4

ตารางที่ 6.4 การต่อ RFID-RC522 และ LCD I²C เข้ากับ NodeMCU

RFID-RC522 และ LCD I²C		**NodeMCU ESP8266**
RFID-RC522	SDA/SS	D8
	SCK	D5
	MOSI	D7
	MISO	D6
	RST	D0
	3.3V	3V3
	GND	GND
	IRQ	ไม่เชื่อมต่อ

ตารางที่ 6.4 การต่อ RFID-RC522 และ LCD I²C เข้ากับ NodeMCU(ต่อ)

RFID-RC522 และ LCD I²C		NodeMCU ESP8266
LCD I²C	SDA	D2
	SCL	D1
	GND	GND
	VCC	ตามพิกัดของโมดูล



รูปที่ 6.2 วงจรของโมดูล RFID ร่วมกับโมดูล 1602 LCD I²C

6. ตารางตรวจสอบการเชื่อมต่อวงจร และบันทึกผลในตารางที่ 6.5

ตารางที่ 6.5 ตารางตรวจสอบการเชื่อมต่อวงจร

ลำดับ	อุปกรณ์/สัญญาณ	ขาที่อุปกรณ์	ขา NodeMCU/ ขา MCP23017	ผลตรวจสอบ (ผ่าน/ไม่ผ่าน)	หมายเหตุ
1.	RFID-RC522: SDA/SS	SDA/SS	D8 (GPIO15)		
2.	RFID-RC522: SCK	SCK	D5 (GPIO14)		

ตารางที่ 6.5 ตารางตรวจสอบการเชื่อมต่อวงจร (ต่อ)

ลำดับ	อุปกรณ์/สัญญาณ	ขาที่อุปกรณ์	ขา NodeMCU/ ขา MCP23017	ผลตรวจสอบ (ผ่าน/ไม่ผ่าน)	หมายเหตุ
3.	RFID-RC522: MOSI	MOSI	D7 (GPIO13)		
4.	RFID-RC522: MISO	MISO	D6 (GPIO12)		
5.	RFID-RC522: RST	RST	D0 (GPIO16)		
6.	RFID-RC522: VCC	3.3 V	3V3		
7.	LCD I²C: SDA	SDA	D2 (GPIO4)		
8.	LCD I²C: SCL	SCL	D1 (GPIO5)		
9.	LED สีเขียว	ขาแอโนด	----------		
10.	LED สีแดง	ขาแอโนด	----------		
11.	กราวด์ร่วม	GND	GND		

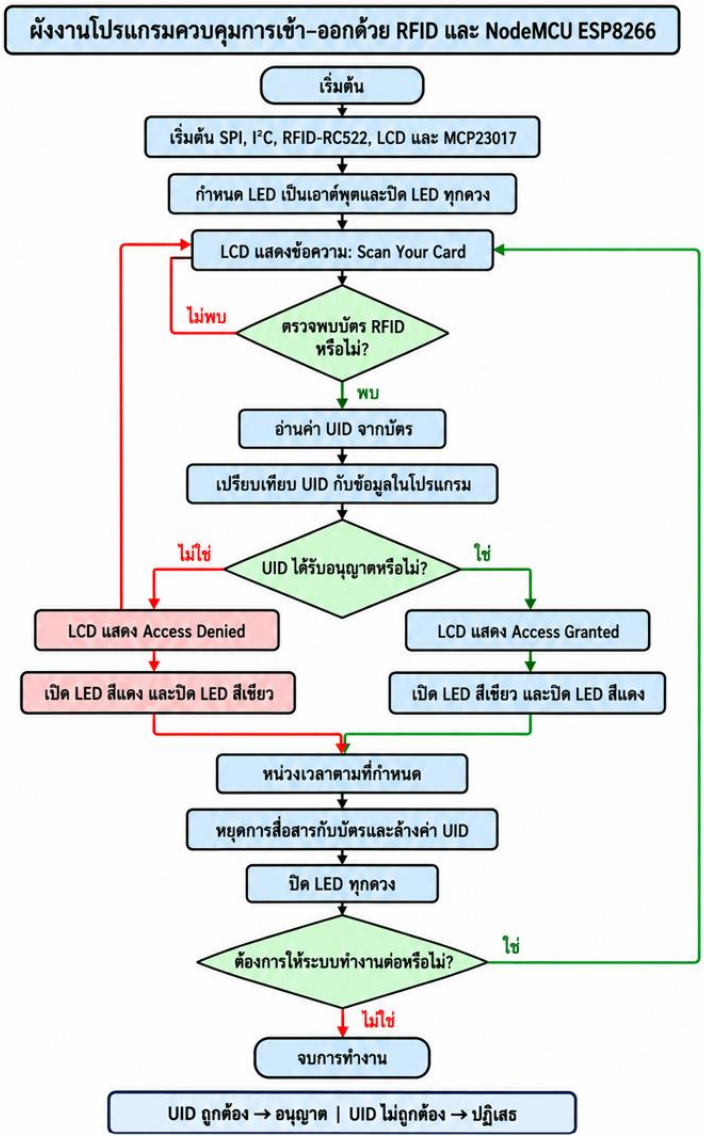
6. เขียนโปรแกรมควบคุมระบบ (ดังภาคผนวก ข Arduino Code: 7)

กำหนดให้โปรแกรมทำงานตามลำดับต่อไปนี้

1) เริ่มต้นการสื่อสารผ่าน Serial, SPI และ I²C
2) เริ่มต้น RFID-RC522, LCD และ MCP23017 หากมี
3) กำหนดขา LED เป็นเอาต์พุต
4) ปิด LED ทุกดวง
5) แสดงข้อความ “Scan Your Card”
6) ตรวจสอบว่ามีบัตรอยู่ในระยะอ่านหรือไม่
7) อ่านค่า UID จากบัตร
8) เปรียบเทียบ UID กับรายการที่ได้รับอนุญาต
9) แสดงผลตามเงื่อนไข ได้แก่
   - UID ถูกต้อง: แสดง “Access Granted” และเปิด LED สีเขียว
   - UID ไม่ถูกต้อง: แสดง “Access Denied” และเปิด LED สีแดง
10) หน่วงเวลาตามที่กำหนด เช่น 2–3 วินาที
11) ปิด LED และล้างข้อความสถานะ
12) ยุติการสื่อสารกับบัตรเพื่อป้องกันการอ่านซ้ำ
13) กลับไปแสดงข้อความ “Scan Your Card”

7. อัปโหลดและทดสอบระบบ ทดสอบระบบตามกรณีต่อไปนี้

	ใบงานที่ 6 เรื่อง งานออกแบบระบบควบคุมการเข้า-ออกประตูด้วย RFID โดยใช้ NodeMCU ESP8266	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)



รูปที่ 6.3 ฝังการทำงานของโปรแกรม

ตารางที่ 6.6 อัปโหลดและทดสอบระบบ

กรณีทดสอบ	ผลที่คาดหวัง
ยังไม่มีบัตรอยู่ใกล้ตัวอ่าน	LCD แสดง “Scan Your Card” และ LED ปิด
ใช้บัตรที่ได้รับอนุญาต	LCD แสดง “Access Granted” และ LED สีเขียวติด
ใช้บัตรที่ไม่ได้รับอนุญาต	LCD แสดง “Access Denied” และ LED สีแดงติด
วางบัตรค้างบนตัวอ่าน	ระบบไม่ควรประมวลผลซ้ำอย่างต่อเนื่อง
นำบัตรออกแล้วแตะใหม่	ระบบสามารถอ่านและตรวจสอบบัตรได้อีกครั้ง
รีเซต NodeMCU	ระบบเริ่มต้นใหม่และกลับสู่สถานะรอรับบัตร
ถอดอุปกรณ์ I²C	โปรแกรมควรแจ้งหรือตรวจพบความผิดปกติ

8. บันทึกผลการปฏิบัติงานในตารางที่ 6.7

ตารางที่ 6.7 ตารางทดสอบการทำงานตามเงื่อนไข

กรณีทดสอบ	ผลที่คาดหวัง	ข้อความบน LCD ที่ปรากฏจริง	LED สีเขียว	LED สีแดง	ผลประเมิน (ผ่าน/ไม่ผ่าน)
เปิดหรือรีเซตระบบ	ระบบพร้อมรับบัตร		ปิด	ปิด	
ไม่มีบัตรอยู่ในระยะอ่าน	แสดงข้อความรอรับบัตร		ปิด	ปิด	
ใช้บัตรที่ได้รับอนุญาต	อนุญาตให้เข้าใช้งาน		เปิด	ปิด	
ใช้บัตรที่ไม่ได้รับอนุญาต	ปฏิเสธการเข้าใช้งาน		ปิด	เปิด	
วางบัตรค้างบนตัวอ่าน	ไม่ประมวลผลซ้ำต่อเนื่อง		ตามเงื่อนไข	ตามเงื่อนไข	
นำบัตรออกแล้วสแกนใหม่	อ่านบัตรได้อีกครั้ง		ตาม UID	ตาม UID	
ครบเวลาการแสดงผล	กลับสู่สถานะรอรับบัตร		ปิด	ปิด	
ไม่พบอุปกรณ์ I²C	แจ้งข้อผิดพลาด/ไม่อนุญาต		ปิด	เปิด/กะพริบ	
RFID-RC522 ขัดข้อง	ไม่แสดงผลอนุญาต		ปิด	ตามที่กำหนด	

สรุปผลการทดลอง

เอกสารอ้างอิง

สิทธา ชูหีบ, ณิชานาฎ เกตุอู่ทอง, และ ธิดาพร พัดเพ็ง. (2562). *แบบจำลองระบบความปลอดภัยการเข้าออกด้วยอาร์เอฟไอดีและไอโอที*. ปริญญานิพนธ์หลักสูตรครุศาสตร์อุตสาหกรรมบัณฑิต สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์และโทรคมนาคม, ภาควิชาครุศาสตร์อุตสาหกรรม, คณะครุศาสตร์อุตสาหกรรม, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี, ปทุมธานี.

Ayeni, P. O., & Adesoba, O. C. (2025). IoT-based home control system using NodeMCU and Firebase. *Journal of Edge Computing, 4*(1), 17–34. https://doi.org/10.55056/jec.814.

Santos, R., & Santos, S. (2016). *ESP8266 web server with Arduino IDE: Step-by-step project guide*. Random Nerd Tutorials.

Santos, R., & Santos, S. (2025). *Learn ESP32 with Arduino IDE* (3rd ed., Version 3.2). Random Nerd Tutorials. https://randomnerdtutorials.com/learn-esp32-with-arduino-ide/

	ใบงานที่ 7 เรื่อง งานออกแบบการควบคุมกลอนประตูโซลิ-นอยด์ ด้วย RFID และ NodeMCU ESP8266	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

การออกแบบ ประกอบ เขียนโปรแกรม และทดสอบระบบควบคุมกลอนประตูโซลินอยด์ด้วยเทคโนโลยี RFID โดยใช้ NodeMCU ESP8266 ได้

วัตถุประสงค์

1. อธิบายหลักการทำงานของระบบควบคุมกลอนประตูด้วย RFID ได้
2. อธิบายหน้าที่ของ NodeMCU ESP8266, RFID-RC522, MCP23017, LCD, Relay และกลอนประตูโซลินอยด์ได้
3. ออกแบบผังการทำงานและวงจรควบคุมระบบได้
4. เชื่อมต่อ RFID-RC522 กับ NodeMCU ผ่านบัส SPI ได้
5. เชื่อมต่อ LCD และ MCP23017 ผ่านบัส I²C ได้
6. เชื่อมต่อโมดูลรีเลย์กับกลอนประตูและแหล่งจ่ายไฟแยกได้อย่างถูกต้อง
7. เขียนโปรแกรมตรวจสอบ UID และควบคุมการล็อก–ปลดล็อกประตูได้
8. เขียนโปรแกรมควบคุม LED และแสดงข้อความบนจอ LCD ตามสถานะระบบได้
9. ทดสอบการเปิดประตูด้วยสวิตช์กดจากภายในได้
10. ตรวจสอบ วิเคราะห์ และแก้ไขข้อขัดข้องเบื้องต้นของระบบได้
11. ปฏิบัติงานโดยคำนึงถึงความปลอดภัยทางไฟฟ้าและการป้องกันข้อมูลผู้ใช้งานได้

เครื่องมือและอุปกรณ์

1. NodeMCU ESP8266	1 บอร์ด
2. RFID-RC522	1 โมดูล
3. บัตรหรือแท็ก RFID 13.56 MHz อย่างน้อย	2 ใบ
4. จอ LCD 16×2 แบบ I²C	1 ชุด
5. MCP23017	1 ชุด
6. โมดูลรีเลย์ที่ควบคุมด้วยลอจิก 3.3 V ได้	1 โมดูล
7. กลอนประตูโซลินอยด์ DC	1 ชุด
8. แหล่งจ่ายไฟ DC ตามพิกัดของกลอน	1 ชุด
9. LED สีเหลือง สีเขียว และสีแดง สีละ	1 ดวง
10. ตัวต้านทาน 220–330 Ω	3 ตัว
11. สวิตช์กดแบบชั่วขณะ	1 ตัว
12. ไดโอดป้องกันแรงดันย้อน	1 ตัว
13. ฟิวส์และฐานฟิวส์	1 ชุด
14. เบรดบอร์ดและสายจัมเปอร์	1 ชุด

15. สาย Micro-USB ชนิดรับส่งข้อมูลได้ 1 เส้น
16. ดิจิทัลมัลติมิเตอร์ 1 เครื่อง
17. คอมพิวเตอร์ที่ติดตั้ง Arduino IDE 1 เครื่อง

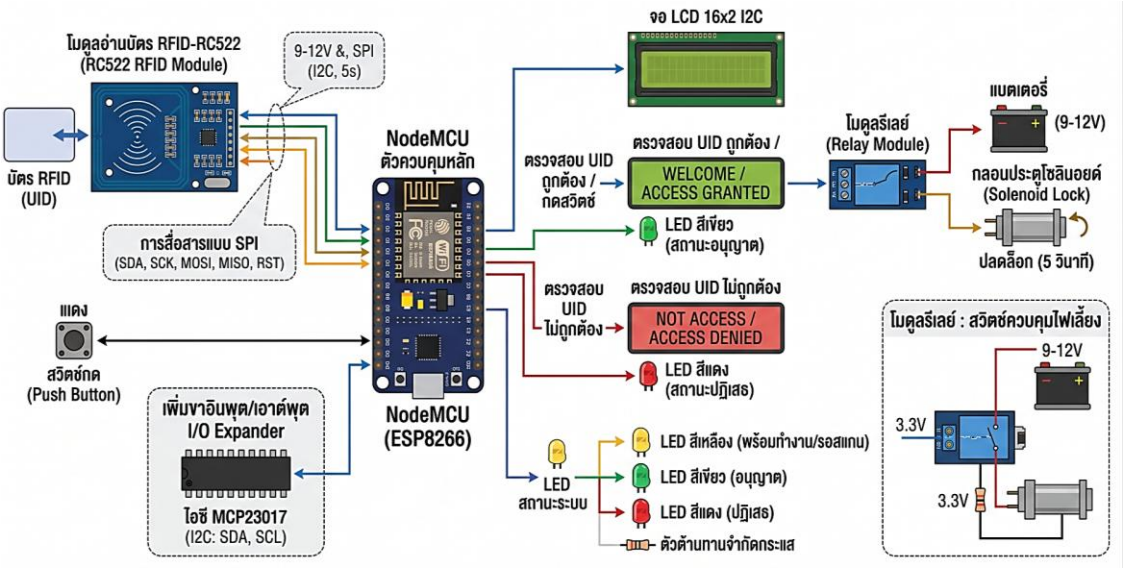
ความรู้พื้นฐานในการปฏิบัติงาน

1. หลักการทำงานของระบบ

NodeMCU ESP8266 ทำหน้าที่เป็นหน่วยควบคุมหลัก รับค่า UID จาก RFID-RC522 ผ่านบัส SPI แล้วเปรียบเทียบกับรายการ UID ที่ได้รับอนุญาตในโปรแกรม หาก UID ถูกต้อง ระบบจะ

1) แสดงข้อความ WELCOME หรือ ACCESS GRANTED
2) ปิด LED สีเหลือง
3) เปิด LED สีเขียว
4) สั่งให้รีเลย์ทำงาน
5) จ่ายไฟให้กลอนประตูเพื่อปลดล็อก
6) เปิดประตูค้างไว้ประมาณ 5 วินาที
7) หยุดการทำงานของรีเลย์
8) ทำให้กลอนกลับสู่สถานะล็อก
9) กลับไปแสดงข้อความ PRESS TAG! และเปิด LED สีเหลือง

หาก UID ไม่ถูกต้อง ระบบจะไม่สั่งให้รีเลย์ทำงาน กลอนประตูยังคงล็อก พร้อมแสดง ACCESS DENIED และเปิด LED สีแดง



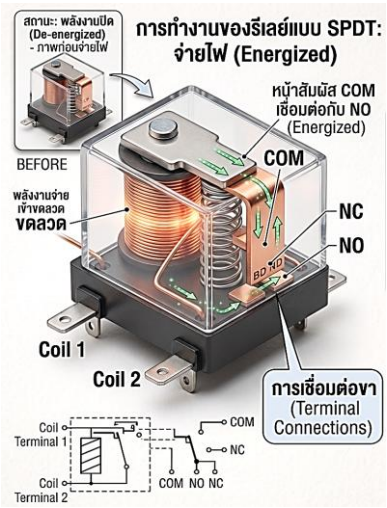
รูปที่ 7.1 หลักการควบคุมกลอนประตูโซลินอยด์ด้วย RFID โดยใช้ NodeMCU ESP8266

2. การควบคุมกลอนประตูผ่านรีเลย์

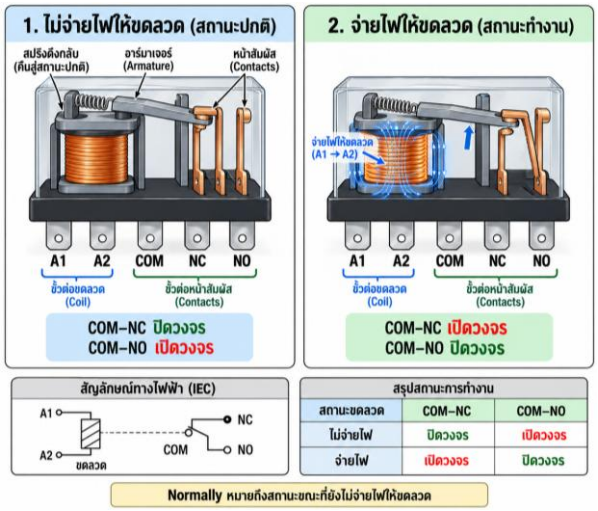
NodeMCU ไม่สามารถจ่ายกระแสให้กลอนโซลินอยด์โดยตรงได้ เนื่องจากขา GPIO มีระดับลอจิก 3.3 V และจ่ายกระแสได้จำกัด ขณะที่กลอนประตูต้องการกระแสสูงกว่า จึงต้องใช้โมดูลรีเลย์เป็นตัวกลางในการควบคุมแหล่งจ่ายไฟของกลอน วงจรหน้าสัมผัสของรีเลย์ควรต่อโดยพิจารณาจากประเภทของกลอนและพฤติกรรมที่ต้องการ ได้แก่

- COM เป็นขั้วร่วมของหน้าสัมผัส
- NO เชื่อมต่อกับ COM เมื่อรีเลย์ทำงาน
- NC เชื่อมต่อกับ COM เมื่อรีเลย์ไม่ทำงาน

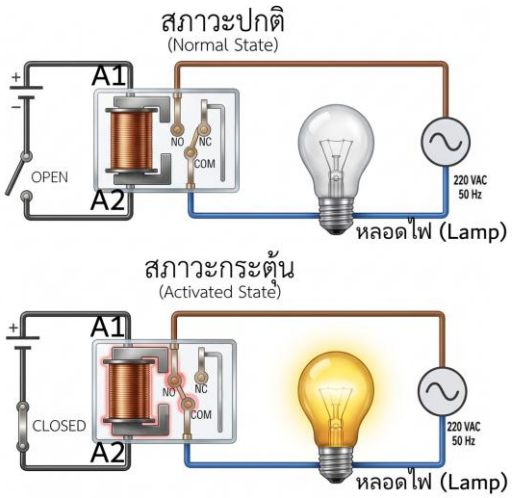
หากกลอนเป็นชนิด จ่ายไฟเพื่อปลดล็อก โดยทั่วไปสามารถใช้หน้าสัมผัส COM และ NO เพื่อให้กลอนรับไฟเฉพาะช่วงที่อนุญาต แต่ต้องตรวจสอบหลักการทำงานของกลอนจริงก่อนต่อ



(ก) โครงสร้างรีเลย์



(ข) หลักการทำงานรีเลย์



(ค) การต่อวงจรใช้งานรีเลย์

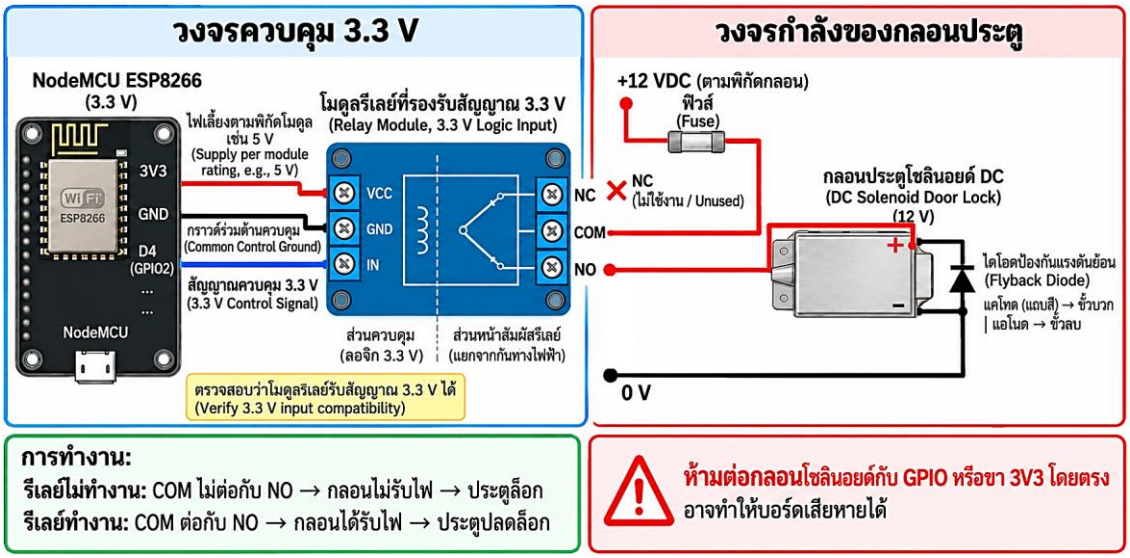
รูปที่ 7.2 โครงสร้างและหลักการทำงานของรีเลย์

3. การป้องกันแรงดันย้อน

กลอนโซลินอยด์เป็นโหลดชนิดเหนี่ยวนำ เมื่อหยุดจ่ายกระแสอาจเกิดแรงดันย้อนซึ่งทำให้หน้าสัมผัสรีเลย์เกิดประกายไฟและรบกวนวงจรควบคุมได้ สำหรับกลอน DC ควรต่อไดโอดป้องกันแรงดันย้อนขนานกับขดลวดของกลอน โดยต่อ

- ➲ แคโทดของไดโอดเข้ากับขั้วบวก
- ➲ แอโนดของไดโอดเข้ากับขั้วลบ

ต้องต่อไดโอดให้ถูกขั้ว เพราะหากกลับขั้วจะทำให้แหล่งจ่ายลัดวงจรเมื่อจ่ายไฟ



รูปที่ 7.3 การต่อวงจรควบคุมกลอนประตูโซลินอยด์ด้วย NodeMCU

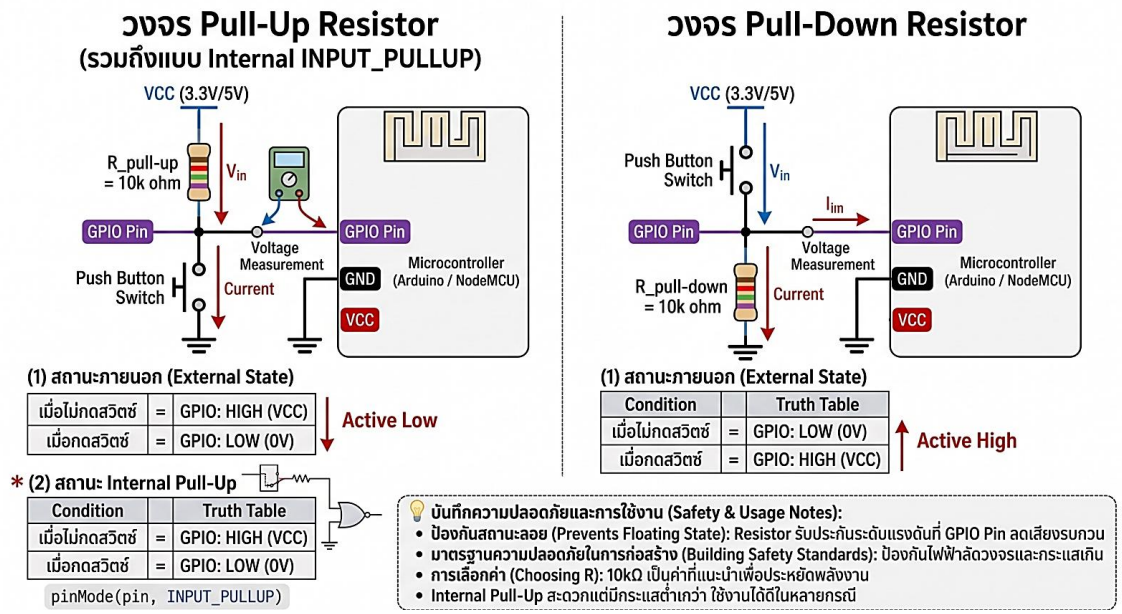
4. การใช้ MCP23017

MCP23017 เป็นไอซีขยายขาอินพุตและเอาต์พุตจำนวน 16 ขา สื่อสารกับ NodeMCU ผ่านบัส I²C ในใบงานนี้สามารถใช้ควบคุม LED และรับสถานะจากสวิตช์กดได้ ทำให้ลดจำนวน GPIO ที่ใช้บน NodeMCU MCP23017 และ LCD สามารถใช้สาย SDA และ SCL ร่วมกันได้ แต่ต้องกำหนด I²C address ไม่ให้ซ้ำกัน และควรจ่ายไฟให้ MCP23017 ด้วย 3.3 V เพื่อให้ระดับลอจิกสอดคล้องกับ ESP8266

5. สวิตช์เปิดประตูจากภายใน

สวิตช์กดทำหน้าที่ขอเปิดประตูจากภายใน เมื่อโปรแกรมตรวจพบการกดสวิตช์ จะสั่งรีเลย์ให้ทำงานเช่นเดียวกับกรณีบัตร RFID ถูกต้อง โดยไม่ต้องตรวจสอบ UID

ควรกำหนดอินพุตด้วยตัวต้านทาน pull-up หรือ pull-down เพื่อป้องกันสถานะลอย หากใช้ INPUT_PULLUP สวิตช์จะอ่านค่าเป็น LOW เมื่อถูกกดและ HIGH เมื่อไม่ถูกกด



รูปที่ 7.4 หลักการต่ออินพุตด้วยต้านทาน pull-up หรือ pull-down

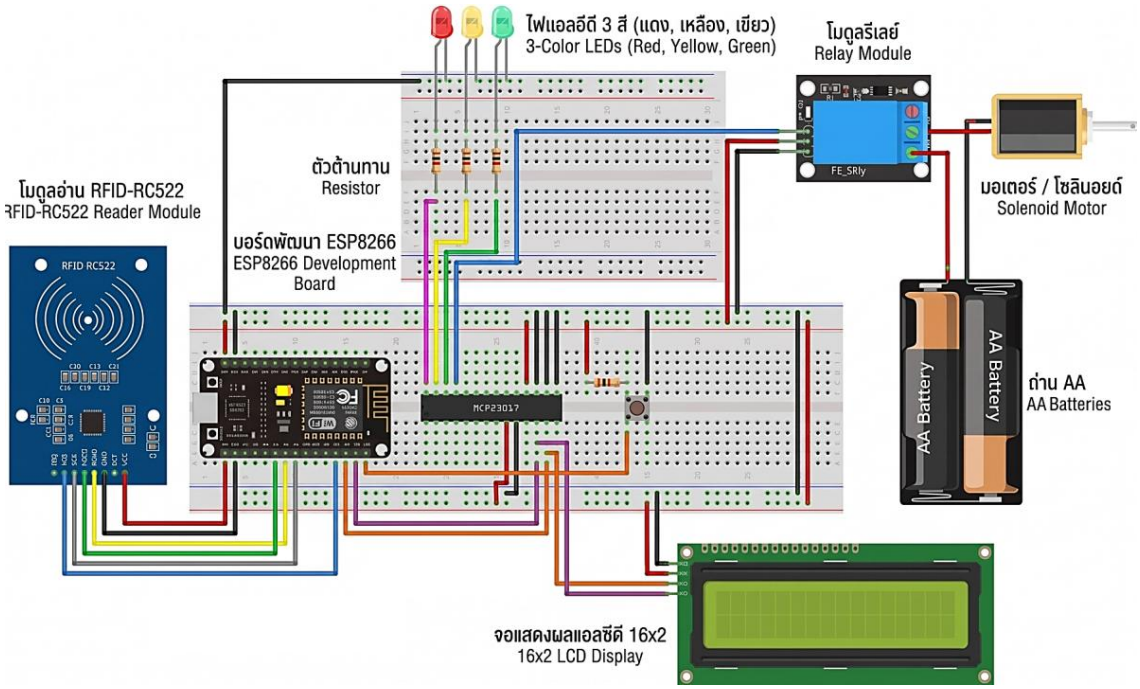
5. ข้อควรระวัง

1) ห้ามต่อกลอนโซลินอยด์เข้ากับขา GPIO หรือขา 3V3 ของ NodeMCU โดยตรง
2) ตรวจสอบพิกัดแรงดันและกระแสของกลอนก่อนจ่ายไฟ
3) เลือกรีเลย์ที่หน้าสัมผัสรองรับแรงดันและกระแสของกลอนได้
4) ตรวจสอบว่าโมดูลรีเลย์รับสัญญาณลอจิก 3.3 V จาก ESP8266 ได้
5) ติดตั้งฟิวส์ที่วงจรแหล่งจ่ายของกลอนเพื่อป้องกันกระแสเกิน
6) ต่อไดโอดป้องกันแรงดันย้อนให้ถูกขั้ว
7) ต่อ RFID-RC522 กับแหล่งจ่าย 3.3 V เท่านั้น
8) ห้ามป้อนสัญญาณ 5 V เข้าขา GPIO ของ ESP8266
9) ปิดแหล่งจ่ายไฟก่อนต่อหรือเปลี่ยนแปลงวงจร
10) ตรวจสอบการลัดวงจรระหว่างขั้วบวกกับ GND ก่อนจ่ายไฟ
11) กลอนและรีเลย์อาจเกิดความร้อนเมื่อทำงานต่อเนื่อง ไม่ควรจ่ายไฟให้กลอนนานเกินความจำเป็น
12) ขณะทดสอบกลไกต้องระวังนิ้วมือและสิ่งของติดอยู่ในส่วนเคลื่อนที่

ลำดับขั้นตอนการปฏิบัติงาน

1. ต่อวงจรดังรูปที่ 7.5 และตำแหน่งขาตามตารางที่ 7.1

	ใบงานที่ 7 เรื่อง งานออกแบบการควบคุมกลอนประตูโซลิ-นอยด์ ด้วย RFID และ NodeMCU ESP8266	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)



รูปที่ 7.5 วงจรควบคุมกลอนประตูโซลินอยด์ด้วย RFID และ Relay

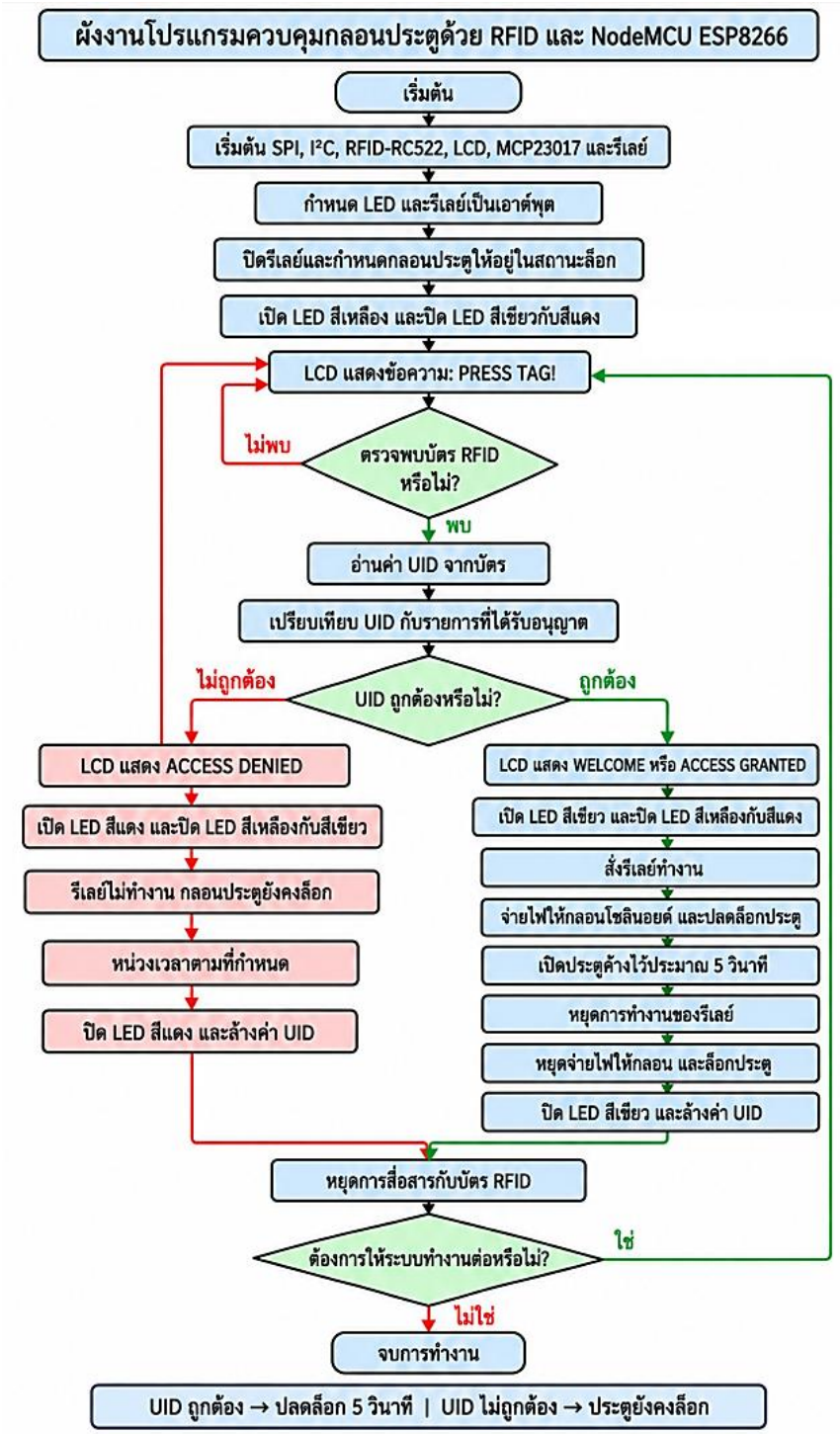
ตารางที่ 7.1 ตารางตรวจสอบการเชื่อมต่อวงจร

ลำดับ	อุปกรณ์/สัญญาณ	ขาอุปกรณ์	ขา NodeMCU/ ขา MCP23017	หมายเหตุ
1	RFID-RC522: SDA/SS	SDA/SS	D3 (GPIO0)	ตรงกับ SS_PIN D3
2	RFID-RC522: SCK	SCK	D5 (GPIO14)	ขา SPI ของ ESP8266
3	RFID-RC522: MOSI	MOSI	D7 (GPIO13)	ขา SPI ของ ESP8266
4	RFID-RC522: MISO	MISO	D6 (GPIO12)	ขา SPI ของ ESP8266
5	RFID-RC522: RST	RST	D8 (GPIO15)	ตรงกับ RST_PIN D8
6	RFID-RC522: VCC	3.3V	3V3	ห้ามต่อกับ 5 V
7	RFID-RC522: GND	GND	GND	กราวด์ร่วม
8	RFID-RC522: IRQ	IRQ	ไม่เชื่อมต่อ	โปรแกรมไม่ได้ใช้งาน
9	LCD I²C: SDA	SDA	D2 (GPIO4)	บัส I²C
10	LCD I²C: SCL	SCL	D1 (GPIO5)	บัส I²C
11	LCD I²C: VCC	VCC	ตามพิกัดโมดูล LCD	ตรวจสอบระดับแรงดัน I²C
12	LCD I²C: GND	GND	GND	กราวด์ร่วม
13	MCP23017: SDA	SDA	D2 (GPIO4)	ใช้บัสร่วมกับ LCD
14	MCP23017: SCL	SCL	D1 (GPIO5)	ใช้บัสร่วมกับ LCD
15	MCP23017: VDD	VDD	3V3	ใช้ลอจิก 3.3 V

ตารางที่ 7.1 ตารางตรวจสอบการเชื่อมต่อวงจร (ต่อ)

ลำดับ	อุปกรณ์/สัญญาณ	ขาอุปกรณ์	ขา NodeMCU/ ขา MCP23017	หมายเหตุ
16	MCP23017: VSS	VSS	GND	กราวด์ร่วม
17	MCP23017: A0–A2	A0, A1, A2	GND	ที่อยู่ I²C เป็น 0x20
18	MCP23017: RESET	RESET	3V3 ผ่าน R 10 kΩ	ไม่ควรปล่อยขาลอย
19	LED สีแดง	แอโนด	MCP23017 หมายเลข 7: GPA7 (ขาจริง 28)	ตรงกับ LED_R 7
20	LED สีเหลือง	แอโนด	MCP23017 หมายเลข 6: GPA6 (ขาจริง 27)	ตรงกับ LED_Y 6
21	LED สีเขียว	แอโนด	MCP23017 หมายเลข 5: GPA5 (ขาจริง 26)	ตรงกับ LED_G 5
22	LED ทั้งสามดวง	แคโทด	GND	แต่ละดวงต่อผ่าน R 220–330 Ω
23	โมดูลรีเลย์: IN	IN	MCP23017 หมายเลข 4: GPA4 (ขาจริง 25)	ตรงกับ RELAY 4
24	โมดูลรีเลย์: VCC	VCC	แหล่งจ่ายตามพิกัดโมดูล	ต้องรองรับสัญญาณ IN 3.3V
25	โมดูลรีเลย์: GND	GND	GND ด้านวงจรควบคุม	กราวด์ร่วมกับ NodeMCU
26	สวิตช์เปิดประตู	ขาที่ 1	D0 (GPIO16)	ตรงกับ SW D0
27	สวิตช์เปิดประตู	ขาที่ 2	GND	เมื่อกด โปรแกรมอ่านค่า LOW
28	ตัวต้านทานสวิตช์	10 kΩ	ระหว่าง D0 กับ 3V3	ตัวต้านทาน pull-up ภายนอก
29	รีเลย์: COM	COM	ขั้วบวกแหล่งจ่ายกลอนผ่านฟิวส์	ภาคกำลัง
30	รีเลย์: NO	NO	ขั้วบวกกลอนโซลินอยด์	จ่ายไฟเมื่อรีเลย์ทำงาน
31	รีเลย์: NC	NC	ไม่เชื่อมต่อ	ไม่ใช้ในระบบนี้
32	กลอนโซลินอยด์	ขั้วบวก	NO ของรีเลย์	ใช้แรงดันตามพิกัดกลอน
33	กลอนโซลินอยด์	ขั้วลบ	0 V ของแหล่งจ่ายกลอน	ไม่ต่อกับ GPIO
34	ไดโอดป้องกันแรงดันย้อน	แคโทด/ ด้านแถบสี	ขั้วบวกของกลอน	ต่อขนานกับกลอน
35	ไดโอดป้องกันแรงดันย้อน	แอโนด	ขั้วลบของกลอน	ตรวจสอบขั้วให้ถูกต้อง

2. เขียนโปรแกรมควบคุมการทำงานตามเงื่อนไขที่กำหนด (ดังภาคผนวก ข Arduino Code: 8) เพื่อให้ตรวจสอบข้อผิดพลาดได้ง่าย ควรพัฒนาและทดสอบโปรแกรมเป็นลำดับดังนี้



รูปที่ 7.5 ผังการเขียนโปรแกรมควบคุมกลอนประตูโซลินอยด์

1) อัปโหลดโปรแกรมควบคุมฉบับสมบูรณ์
2) เปิดระบบและตรวจสอบข้อความเริ่มต้น
3) ทดสอบบัตรที่ได้รับอนุญาต
4) ทดสอบบัตรที่ไม่ได้รับอนุญาต
5) ทดสอบสวิตช์เปิดประตูจากภายใน
6) ตรวจสอบการหน่วงเวลา 5 วินาที
7) ตรวจสอบว่าประตูกลับสู่สถานะล็อกทุกครั้ง
8) ทดสอบการเปิดหรือรีเซตระบบ โดยกลอนต้องเริ่มในสถานะล็อก
9) บันทึกผล ปัญหา และแนวทางแก้ไข

3. บันทึกผลการปฏิบัติงานในตารางที่ 7.2 และ 7.3

ตารางที่ 7.2 ตารางบันทึกผลการทดลองการตรวจสอบบัตร

ลำดับ	บัตร/แท็ก	UID	สิทธิ์ที่กำหนด	ผลตรวจสอบ (ถูกต้อง/ไม่ถูกต้อง)
1	บัตร A	----------	อนุญาต	
2	บัตร B	----------	ไม่อนุญาต	
3	บัตร C	----------	อนุญาต/ไม่อนุญาต	

ตารางที่ 7.3 ตารางบันทึกผลการทดลองระบบ

กรณีทดสอบ	ผลที่คาดหวัง	ผลที่เกิดขึ้นจริง	ประเมินผล (ผ่าน/ไม่ผ่าน)
เปิดหรือรีเซตระบบ	กลอนล็อกและ LED สีเหลืองติด		
ไม่มีบัตร	LCD แสดง PRESS TAG!		
บัตรได้รับอนุญาต	รีเลย์ทำงานและประตูปลดล็อก		
บัตรไม่ได้รับอนุญาต	รีเลย์ไม่ทำงานและประตูยังล็อก		
UID ถูกต้อง	LCD แสดง ACCESS GRANTED และ LED สีเขียวติด		
UID ไม่ถูกต้อง	LCD แสดง ACCESS DENIED และ LED สีแดงติด		
กดสวิตช์จากภายใน	รีเลย์ทำงานและประตูปลดล็อก		
ครบเวลา 5 วินาที	รีเลย์หยุดและประตูกลับมาล็อก		
วางบัตรค้างบนตัวอ่าน	ระบบไม่สั่งรีเลย์ซ้ำต่อเนื่อง		
ถอด RFID-RC522	ระบบไม่อนุญาตให้เปิดด้วยบัตร		

	ใบงานที่ 7 เรื่อง งานออกแบบการควบคุมกลอนประตูโซลิ-นอยด์ ด้วย RFID และ NodeMCU ESP8266	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

สรุปผลการทดลอง

เอกสารอ้างอิง

สิทธา ชูหีบ, ณิชานาฎ เกตุอู่ทอง, และ ธิดาพร พัดเพ็ง. (2562). *แบบจำลองระบบความปลอดภัยการเข้าออกด้วยอาร์เอฟไอดีและไอโอที*. ปริญญานิพนธ์หลักสูตรครุศาสตร์อุตสาหกรรมบัณฑิต สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์และโทรคมนาคม, ภาควิชาครุศาสตร์อุตสาหกรรม, คณะครุศาสตร์อุตสาหกรรม, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี, ปทุมธานี.

Ayeni, P. O., & Adesoba, O. C. (2025). IoT-based home control system using NodeMCU and Firebase. *Journal of Edge Computing, 4*(1), 17–34. https://doi.org/10.55056/jec.814.

Sahasika, M. P., Pratiwi, D., & Santoso, G. B. (2023, May 8). Visualization of home security sensor system based on IoT server. *Qeios, Preprint*, 1-19. https://doi.org/10.32388/ZC810D.

Santos, R., & Santos, S. (2016). *ESP8266 web server with Arduino IDE: Step-by-step project guide*. Random Nerd Tutorials.

Santos, R., & Santos, S. (2025). *Learn ESP32 with Arduino IDE* (3rd ed., Version 3.2). Random Nerd Tutorials. https://randomnerdtutorials.com/learn-esp32-with-arduino-ide/.

	ใบงานที่ 8 เรื่อง งานประยุกต์ใช้ RFID ร่วมกับ IP Camera และ LINE Messaging API	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ประยุกต์ใช้ระบบควบคุมการเข้า–ออกประตูด้วย RFID ร่วมกับ NodeMCU ESP8266 กล้อง IP camera รุ่น Vstarcam C7824WIP และ LINE Messaging API เพื่อสร้างระบบรักษาความปลอดภัย

วัตถุประสงค์

1. อธิบายหลักการทำงานร่วมกันของ RFID, ESP8266, IP camera และ LINE Messaging API ได้อย่างถูกต้อง
2. เชื่อมต่อ RFID-RC522, LCD, MCP23017, LED, Relay และสวิตช์กับ NodeMCU ESP8266 ได้อย่างถูกต้อง
3. เชื่อมต่อกล้อง Vstarcam C7824WIP กับเครือข่าย Wi-Fi 2.4 GHz และแอปพลิเคชัน Eye4 ได้
4. ตรวจสอบ IP address และการเข้าถึงกล้องภายในเครือข่ายได้
5. แยกความแตกต่างระหว่าง URL ภายในเครือข่ายกับ URL สาธารณะแบบ HTTPS ได้
6. สร้าง LINE Official Account และเปิดใช้งาน Messaging API ได้อย่างถูกต้อง
7. กำหนด Channel access token และรหัสผู้รับข้อความได้อย่างปลอดภัย
8. เขียนโปรแกรมตรวจสอบ UID และควบคุมกลอนประตูได้
9. ส่งข้อความแจ้งเตือนผ่าน LINE Messaging API ได้
10. ทดสอบการแจ้งเตือนเมื่อใช้บัตรถูกต้อง บัตรไม่ถูกต้อง และสวิตช์เปิดประตูได้
11. บันทึก วิเคราะห์ และแก้ไขข้อขัดข้องของระบบได้
12. ปฏิบัติงานโดยคำนึงถึงความปลอดภัยทางไฟฟ้า เครือข่าย และข้อมูลส่วนบุคคลได้

เครื่องมือและอุปกรณ์

1. NodeMCU ESP8266	1 บอร์ด
2. RFID-RC522	1 โมดูล
3. บัตรหรือแท็ก RFID อย่างน้อย	2 ใบ
4. LCD 16×2 แบบ I²C	1 ชุด
5. MCP23017	1 ชุด
6. LED สีแดง สีเหลือง และสีเขียว สีละ	1 ดวง
7. ตัวต้านทาน 220–330 Ω	3 ตัว
8. โมดูลรีเลย์ที่รับสัญญาณลอจิก 3.3 V ได้	1 ชุด
9. กลอนประตูโซลินอยด์ DC	1 ชุด
10. ไดโอดป้องกันแรงดันย้อน	1 ตัว

11. ฟิวส์และฐานฟิวส์ 1 ชุด
12. สวิตช์กดเปิดประตู 1 ตัว
13. แหล่งจ่ายไฟตามพิกัดกลอน 1 ชุด
14. กล้อง Vstarcam C7824WIP 1 ชุด
15. เราเตอร์ Wi-Fi 2.4 GHz 1 ชุด
16. สมาร์ตโฟนที่ติดตั้ง Eye4 และ LINE 1 เครื่อง
17. คอมพิวเตอร์ที่ติดตั้ง Arduino IDE 1 เครื่อง
18. ดิจิทัลมัลติมิเตอร์ 1 เครื่อง
19. เบรดบอร์ดและสายจัมเปอร์ 1 ชุด
20. บัญชี LINE Official Account และ Messaging API channel 1 บัญชี

การปฏิบัติงานที่ 8.1

การส่งข้อความแจ้งเตือนด้วย LINE Messaging API โดยใช้ NodeMCU ESP8266

ความรู้พื้นฐานในการปฏิบัติงาน

1. ความรู้พื้นฐานในการปฏิบัติงาน

1.1 LINE Official Account

LINE Official Account เป็นบัญชีที่ใช้สื่อสารกับผู้ใช้ในฐานะองค์กร หน่วยงาน ร้านค้า หรือระบบอัตโนมัติ เมื่อเปิดใช้ Messaging API บัญชีนี้จะทำหน้าที่เป็นบอตที่รับหรือส่งข้อความผ่านโปรแกรมได้

1.2 Messaging API channel

Channel เป็นช่องทางที่โปรแกรมใช้ติดต่อกับ LINE Platform ภายใน Channel จะมีข้อมูลสำคัญ เช่น

- Channel ID
- Channel secret
- Channel access token
- User ID ของนักพัฒนา
- Webhook URL หากใช้รับเหตุการณ์จาก LINE

ใบงานนี้ใช้เฉพาะการส่ง Push message จึงยังไม่จำเป็นต้องสร้าง Webhook server หากส่งข้อความไปยัง User ID ของผู้เรียนเอง

1.3 Push message

Push message คือข้อความที่บอตเป็นผู้เริ่มส่งไปยังผู้รับ โดยไม่จำเป็นต้องรอให้ผู้ใช้ส่งข้อความมาก่อนในขณะนั้น คำขอจะถูกส่งไปยัง endpoint

`https://api.line.me/v2/bot/message/push`

ส่วนหัวของคำขอต้องมีข้อมูลสำคัญดังนี้

```
Content-Type: application/json
Authorization: Bearer CHANNEL_ACCESS_TOKEN
```

และข้อมูล JSON ต้องระบุผู้รับในฟิลด์ to กับข้อความในฟิลด์ messages ตาม (https://developers.line.biz/en/reference/messaging-api/)

1.4 Channel access token

Channel access token เปรียบเสมือนกุญแจที่อนุญาตให้โปรแกรมใช้ Messaging API ของ Channel นั้น หากบุคคลอื่นได้รับ token อาจสามารถส่งข้อความในนามของบัญชีได้

LINE รองรับ token หลายประเภท สำหรับการเรียนพื้นฐานสามารถออก Long-lived channel access token จากแท็บ Messaging API ใน LINE Developers Console ได้ แต่สำหรับระบบจริง LINE แนะนำ token ที่กำหนดอายุได้หรือ Channel access token v2.1 รายละเอียดอยู่ใน (https://developers.line.biz/en/docs/basics/channel-access-token/)

1.5 User ID

User ID ของ LINE Messaging API ไม่ใช่ชื่อผู้ใช้ ไม่ใช่ชื่อแสดงผล และไม่ใช่ LINE ID ที่ใช้ค้นหาเพื่อน โดยทั่วไปมีรูปแบบดังนี้

```
Uxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

User ID ของนักพัฒนาสามารถตรวจสอบได้จากหัวข้อ Your user ID ในแท็บ Basic settings ของ Channel หากไม่ปรากฏ ต้องเชื่อม Business ID กับบัญชี LINE ก่อน ตาม (https://developers.line.biz/en/docs/messaging-api/getting-user-ids/)

1.6 HTTPS และ JSON

- HTTPS เป็นการสื่อสารผ่านเครือข่ายที่เข้ารหัส
- JSON เป็นรูปแบบข้อมูลที่ใช้ส่งคำสั่งไปยัง LINE API
- ESP8266 ต้องเชื่อมต่ออินเทอร์เน็ตจึงจะเรียก LINE API ได้
- การส่ง API สำเร็จโดยทั่วไปจะได้รับ HTTP status code 200 ตัวอย่าง JSON สำหรับส่งข้อความหนึ่งข้อความ คือ

```
{
  "to": "Uxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "messages": [
    {
      "type": "text",
      "text": "ทดสอบส่งข้อความจาก ESP8266"
    }
  ]
}
```

1.7 ข้อควรระวังด้านความปลอดภัย

1) ห้ามถ่ายภาพหรือเผยแพร่ Channel access token

2) ห้ามนำ token จริงใส่ในรายงานหรือส่งในกลุ่มสนทนา

3) ห้ามอัปโหลดโปรแกรมที่มี token จริงไปยัง GitHub หรือพื้นที่สาธารณะ

4) ห้ามส่ง token ผ่านอีเมลหรือข้อความที่ไม่มีการป้องกัน

5) หากสงสัยว่า token รั่วไหล ให้ Revoke หรือ Issue token ใหม่ทันที

6) เมื่อออก token ใหม่ Long-lived token เดิมอาจถูกยกเลิก

7) ควรใช้ LINE Official Account สำหรับการทดลอง ไม่ควรใช้บัญชีของหน่วยงานจริง

8) ไม่ควรส่งข้อความทดสอบจำนวนมาก เพราะมีข้อจำกัดอัตราการเรียก API และโควตาข้อความ

9) ไม่ควรแสดงรหัสผ่าน Wi-Fi บน Serial Monitor

10) ตัวอย่างที่ใช้ setInsecure() เหมาะเฉพาะการทดลองในห้องปฏิบัติการ เพราะไม่ได้ตรวจสอบใบรับรองเซิร์ฟเวอร์อย่างสมบูรณ์ ระบบจริงควรใช้ Root CA หรือใช้เซิร์ฟเวอร์กลางที่ปลอดภัย

ลำดับขั้นตอนการปฏิบัติงาน

1. ขั้นตอนที่ 1 เตรียมบัญชีสำหรับการทดลอง
   1) เปิดแอป LINE บนสมาร์ตโฟน
   2) ตรวจสอบว่าสามารถเข้าสู่ระบบได้
   3) ตรวจสอบว่าบัญชี LINE เชื่อมโยงกับหมายเลขโทรศัพท์หรืออีเมลตามที่ระบบกำหนด
   4) เปิดเว็บเบราว์เซอร์ในคอมพิวเตอร์
   5) เตรียมอีเมลสำหรับใช้สมัคร LINE Business ID
   6) ไม่ควรใช้บัญชีส่วนตัวของบุคคลอื่น
   7) หากเป็นการทำงานกลุ่ม ให้กำหนดสมาชิกหนึ่งคนเป็นผู้ดูแลบัญชี
   8) บันทึกชื่อผู้ดูแลบัญชี แต่ไม่บันทึกรหัสผ่านลงในใบงาน
2. ขั้นตอนที่ 2 สร้าง LINE Official Account
   1) เปิดหน้า LINE Official Account
   2) เลือกสร้าง LINE Official Account
   3) เข้าสู่ระบบด้วย LINE Business ID
   4) หากยังไม่มี Business ID ให้สมัครด้วยบัญชี LINE หรืออีเมล
   5) กรอกข้อมูลที่ระบบกำหนด เช่น
      - ชื่อบัญชี
      - ประเภทธุรกิจหรือการใช้งาน
      - ประเทศหรือภูมิภาค
      - ชื่อผู้รับผิดชอบ
      - อีเมลติดต่อ

6) ตั้งชื่อสำหรับการทดลอง เช่น
RFID LAB GROUP 1

7) ตรวจสอบข้อมูลก่อนยืนยัน

8) กดยอมรับข้อกำหนดเมื่อได้อ่านและเข้าใจแล้ว

9) เมื่อสร้างสำเร็จ ให้เปิด LINE Official Account Manager

10) ตรวจสอบว่าบัญชีที่สร้างปรากฏในรายการ

11) คลิกบัญชีที่ต้องการใช้

12) บันทึกชื่อบัญชีและ Basic ID ลงในตาราง โดยไม่บันทึกรหัสผ่าน

13) บัยทึกผลการปฏิบัติงานลงในตาราง 8.1

ตารางที่ 8.1 ข้อมูล LINE Official Account

รายการ	ข้อมูลที่ตรวจพบ
ชื่อ LINE Official Account	
Basic ID	
ผู้ดูแลบัญชี	
วันที่สร้าง	
สถานะบัญชี	พร้อมใช้งาน/ไม่พร้อมใช้งาน

3. ตอนที่ 3 เปิดใช้งาน Messaging API

ปัจจุบันต้องเปิดใช้ Messaging API ผ่าน LINE Official Account Manager ไม่สามารถสร้าง Messaging API channel โดยตรงจาก LINE Developers Console ได้

1) เข้าสู่ LINE Official Account Manager

2) เลือก LINE Official Account ที่สร้างไว้

3) เปิดเมนู Settings

4) เลือกหัวข้อ Messaging API

5) กด Enable Messaging API

6) หากระบบให้ลงทะเบียนข้อมูลนักพัฒนา ให้กรอกชื่อและอีเมล

7) เลือก Provider สำหรับจัดเก็บ Channel โดยการเลือก Provider ดังนี้

- หากเป็นงานของสถานศึกษา ให้ใช้ Provider ที่ผู้สอนกำหนด
- หากเป็นการทดลองส่วนบุคคล สามารถสร้าง Provider ใหม่โดยใช้ชื่อที่ระบุเจ้าของชัดเจน
- ห้ามเลือก Provider ของหน่วยงานอื่น
- ต้องตรวจสอบให้ถูกต้องก่อนยืนยัน เพราะ LINE ระบุว่าเมื่อกำหนด Provider ให้บัญชีแล้ว จะไม่สามารถย้ายหรือยกเลิกการผูก Provider ได้โดยง่าย

8) ยืนยันการเปิดใช้ Messaging API

9) เปิด LINE Developers Console

10) เข้าสู่ระบบด้วยบัญชีเดียวกับที่ใช้ใน LINE Official Account Manager

11) เลือก Provider ที่กำหนดไว้

12) ตรวจสอบว่ามี Messaging API channel ของบัญชีที่สร้างไว้

13) คลิกเข้าไปใน Channel

14) ตรวจสอบแท็บต่อไปนี้

- Basic settings
- Messaging API
- Security หรือแท็บอื่นตามสิทธิ์ของบัญชี

15) บันทึกเฉพาะ Channel ID ลงในตาราง

16) ห้ามบันทึก Channel secret ลงในใบงานฉบับที่เผยแพร่

ตารางที่ 8.2 ข้อมูล Messaging API channel

รายการ	ข้อมูลที่ตรวจพบ
Provider	
Channel name	
Channel ID	
Channel type	Messaging API
สถานะ	พร้อมใช้งาน/ไม่พร้อมใช้งาน

4. ขั้นตอนที่ 4 ปรับการตอบกลับอัตโนมัติ

บัญชีที่สร้างใหม่อาจเปิด Greeting message และ Auto-response message ไว้ หากไม่ปิด ผู้เรียนอาจสับสนว่าข้อความใดมาจากโปรแกรมและข้อความใดมาจากระบบอัตโนมัติ

1) เปิด LINE Official Account Manager

2) เลือกบัญชีที่ใช้ทดลอง

3) เปิดเมนูตั้งค่าการตอบกลับ

4) ปิด Auto-response messages ชั่วคราว

5) จะเปิดหรือปิด Greeting message ก็ได้ แต่ต้องบันทึกสถานะไว้

6) ตรวจสอบว่าโหมดการตอบกลับอนุญาตให้ใช้ Messaging API

7) บันทึกการตั้งค่า

ตารางที่ 8.3 ข้อมูล Messaging API channel

รายการ	สถานะ (เปิด/ปิด)
Greeting message	
Auto-response message	
Messaging API	

5. ขั้นตอนที่ 5 เพิ่ม LINE Official Account เป็นเพื่อน

ผู้รับต้องเพิ่ม LINE Official Account เป็นเพื่อนก่อนจึงจะเหมาะสำหรับการทดสอบ Push message

1) เปิด LINE Developers Console
2) เลือก Provider และ Messaging API channel
3) เปิดแท็บ Messaging API
4) ค้นหา QR code สำหรับเพิ่มบัญชีเป็นเพื่อน
5) เปิดแอป LINE บนสมาร์ตโฟน
6) เลือกเพิ่มเพื่อนด้วย QR code
7) สแกน QR code ที่ปรากฏบนหน้าจอ
8) กดเพิ่มเพื่อน
9) เปิดห้องสนทนาของ LINE Official Account
10) ส่งข้อความทดสอบ เช่น “Hello”
11) ตรวจสอบว่าบัญชีไม่อยู่ในรายการที่ถูกบล็อก
12) หากเปิด Greeting message ไว้ อาจมีข้อความต้อนรับปรากฏขึ้น ซึ่งยังไม่ใช่ข้อความจาก ESP8266

6. ขั้นตอนที่ 6 ออก Channel access token

สำหรับผู้เริ่มต้น ให้ใช้ Long-lived channel access token ในการทดลอง เนื่องจากออกจากหน้า Console ได้ง่าย แต่ต้องเก็บรักษาอย่างเข้มงวด

1) เปิด LINE Developers Console
2) เลือก Provider
3) เลือก Messaging API channel
4) เปิดแท็บ Messaging API
5) เลื่อนไปยังหัวข้อ Channel access token
6) หากยังไม่มี token ให้กด Issue
7) ยืนยันการออก token
8) กดคัดลอก token
9) นำ token ไปเก็บไว้ในไฟล์ลับเฉพาะเครื่องทดลอง
10) ห้ามเขียน token เต็มลงในตาราง
11) บันทึกเพียง 4 ตัวแรกและ 4 ตัวท้าย เช่น “AbCd**********Wxyz”
12) หาก token ปรากฏในภาพหน้าจอ ให้ปิดบัง token ก่อนนำภาพไปใช้ในงาน

ตารางที่ 8.4 การตรวจสอบ Token

รายการ	ข้อมูล
ประเภท Token	Long-lived/ประเภทอื่น
วันที่ออก Token	
อักขระ 4 ตัวแรก	
อักขระ 4 ตัวท้าย	
ผู้ดูแล Token	
เก็บ Token ในที่ปลอดภัย	ใช่/ไม่ใช่

7. ตอนที่ 7 ตรวจสอบ User ID ของผู้รับ

วิธีที่ง่ายที่สุดสำหรับใบงานนี้คือใช้ User ID ของผู้สร้าง Channel เอง

1) เปิด LINE Developers Console
2) เลือก Provider และ Channel ที่ใช้ทดลอง
3) เปิดแท็บ Basic settings
4) เลื่อนไปยังหัวข้อ Your user ID
5) คัดลอก User ID
6) ตรวจสอบว่าขึ้นต้นด้วยอักษร U
7) ตรวจสอบว่าค่าดังกล่าวไม่ใช่ Basic ID และไม่ใช่ชื่อแสดงผล
8) หากไม่พบ Your user ID ให้ตรวจสอบว่า LINE Business ID เชื่อมกับบัญชี LINE แล้วหรือไม่
9) ตรวจสอบว่าบัญชี LINE เดียวกันเพิ่ม Official Account เป็นเพื่อนแล้ว
10) เก็บ User ID ไว้ในไฟล์การตั้งค่าของกลุ่ม
11) ในรายงานควรปิดบังบางส่วน เช่น “U1234**********abcd”

8. ขั้นตอนที่ 8 ทดสอบส่งข้อความจากคอมพิวเตอร์ก่อน

ควรทดสอบ token และ User ID จากคอมพิวเตอร์ก่อนใช้ ESP8266 เพื่อแยกปัญหาบัญชี LINE ออกจากปัญหาโปรแกรมไมโครคอนโทรลเลอร์

8.1 เตรียมข้อมูล เตรียมข้อมูลต่อไปนี้โดยไม่เปิดเผยให้บุคคลอื่น

```
CHANNEL_ACCESS_TOKEN
USER_ID
```

8.2 ทดสอบด้วย Postman

1) เปิดโปรแกรม Postman
2) สร้าง HTTP Request ใหม่
3) เลือก Method เป็น POST
4) กำหนด URL เป็น
   https://api.line.me/v2/bot/message/push

5) เปิดแท็บ Headers

6) เพิ่ม Header รายการที่ 1 และ เพิ่ม Header รายการที่ 2

Header	Key	Value
รายการที่ 1	Content-Type	application/json
รายการที่ 2	Authorization	Bearer ตามด้วยเว้นวรรคและ Channel access token

ตัวอย่างรูปแบบ:

```
Bearer AbCdEf123456...
```

7) เปิดแท็บ Body

8) เลือก raw

9) เลือกชนิดข้อมูล JSON

10) ป้อนข้อมูลต่อไปนี้ โดยแทน User ID ด้วยค่าจริง

```
{
  "to": "Uxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "messages": [
    {
      "type": "text",
      "text": "ทดสอบ LINE Messaging API จากคอมพิวเตอร์"
    }
  ]
}
```

11) ตรวจสอบเครื่องหมายปีกกา วงเล็บ เครื่องหมายคำพูด และเครื่องหมายจุลภาค

12) กด Send

13) ตรวจสอบ HTTP status code

14) เปิดแอป LINE บนสมาร์ตโฟน

15) ตรวจสอบว่ามีข้อความจาก LINE Official Account

16) บันทึกเวลาและผลการทดลอง

17) ห้ามนำภาพหน้าจอที่มี token ไปใส่รายงาน

8.3 ตัวอย่างทดสอบด้วยคำสั่ง curl

ผู้เรียนที่ใช้ Command Prompt หรือ Terminal สามารถใช้รูปแบบต่อไปนี้

```
curl -X POST https://api.line.me/v2/bot/message/push \
-H "Content-Type: application/json" \
-H "Authorization: Bearer CHANNEL_ACCESS_TOKEN" \
-d "{\"to\":\"USER_ID\",\"messages\":[{\"type\":\"text\",\"text\":\"Test LINE Messaging API\"}]}"
```

ให้แทน CHANNEL_ACCESS_TOKEN และ USER_ID ด้วยค่าจริง การใช้คำสั่งนี้อาจทำให้ token ถูกบันทึกในประวัติคำสั่ง จึงควรใช้เฉพาะเครื่องทดลองและล้างประวัติตามนโยบายของห้องปฏิบัติการ

9. ตอนที่ 9 ติดตั้ง Arduino IDE และ ESP8266
   1) เปิด Arduino IDE
   2) เลือกเมนู File > Preferences
   3) เพิ่ม URL ของ ESP8266 Board Manager ตามคู่มือ ESP8266 Arduino Core
   4) เปิด Tools > Board > Boards Manager
   5) ค้นหา esp8266
   6) ติดตั้งแพ็กเกจ ESP8266 by ESP8266 Community
   7) เชื่อมต่อ NodeMCU กับคอมพิวเตอร์ด้วยสาย USB
   8) ตรวจสอบว่าไฟบนบอร์ดติด
   9) เลือกเมนู Tools > Board
   10) เลือก NodeMCU 1.0 (ESP-12E Module)
   11) เลือก Port ให้ตรงกับบอร์ด
   12) เปิดตัวอย่าง Blink หรือโปรแกรมทดสอบ
   13) กด Verify
   14) กด Upload
   15) หากอัปโหลดสำเร็จ ให้ดำเนินขั้นตอนต่อไป
   16) หากไม่พบ Port ให้ตรวจสาย USB และไดรเวอร์ USB-to-Serial
10. ตอนที่ 10 ทดสอบการเชื่อมต่อ Wi-Fi ของ ESP8266
   1) เปิด Arduino IDE
   2) สร้าง Sketch ใหม่
   3) ป้อนโปรแกรมทดสอบต่อไปนี้
   4) เปลี่ยนชื่อและรหัสผ่าน Wi-Fi ให้ตรงกับเครือข่ายทดลอง

```
#include <ESP8266WiFi.h>

const char* WIFI_SSID = "YOUR_WIFI_NAME";
const char* WIFI_PASSWORD = "YOUR_WIFI_PASSWORD";
```

```
void setup() {
  Serial.begin(115200);
  delay(100);

  WiFi.mode(WIFI_STA);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);

  Serial.print("Connecting to Wi-Fi");

  unsigned long startTime = millis();

  while (WiFi.status() != WL_CONNECTED &&
         millis() - startTime < 20000) {
    Serial.print(".");
    delay(500);
  }

  Serial.println();

  if (WiFi.status() == WL_CONNECTED) {
    Serial.println("Wi-Fi connected");
    Serial.print("ESP8266 IP address: ");
    Serial.println(WiFi.localIP());
  } else {
    Serial.println("Wi-Fi connection failed");
  }
}

void loop() {
}
```

11. ขั้นตอนที่ 11 เขียนโปรแกรมส่งข้อความจาก ESP8266

11.1 โปรแกรมสำหรับการทดลอง

โปรแกรมนี้ใช้ client.setInsecure() เพื่อให้การทดลองเริ่มต้นทำได้ง่าย แต่ไม่ตรวจสอบใบรับรองของเซิร์ฟเวอร์

```
#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <ESP8266HTTPClient.h>

// ------------------------------
// ข้อมูลเครือข่าย Wi-Fi
// ------------------------------
const char* WIFI_SSID = "YOUR_WIFI_NAME";
const char* WIFI_PASSWORD = "YOUR_WIFI_PASSWORD";

// ------------------------------
// ข้อมูล LINE Messaging API
// ห้ามเผยแพร่ข้อมูลจริง
// ------------------------------
const char* LINE_ACCESS_TOKEN =
  "YOUR_CHANNEL_ACCESS_TOKEN";
```

```
const char* LINE_TO_ID =
  "YOUR_USER_ID";

// Endpoint สำหรับส่ง Push message
const char* LINE_API_URL =
  "https://api.line.me/v2/bot/message/push";

// ป้องกันการส่งข้อความซ้ำ
bool messageSent = false;

// แปลงอักขระพิเศษให้ใช้ใน JSON ได้
String jsonEscape(String text) {
  text.replace("\\", "\\\\");
  text.replace("\"", "\\\"");
  text.replace("\n", "\\n");
  text.replace("\r", "");
  text.replace("\t", "\\t");
  return text;
}

// เชื่อมต่อ Wi-Fi โดยกำหนดเวลารอสูงสุด
bool connectWiFi(unsigned long timeoutMs) {
  WiFi.mode(WIFI_STA);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);

  Serial.print("Connecting to Wi-Fi");

  unsigned long startTime = millis();

  while (WiFi.status() != WL_CONNECTED &&
         millis() - startTime < timeoutMs) {
    Serial.print(".");
    delay(500);
  }

  Serial.println();

  if (WiFi.status() == WL_CONNECTED) {
    Serial.println("Wi-Fi connected");
    Serial.print("IP address: ");
    Serial.println(WiFi.localIP());
    return true;
  }

  Serial.println("Wi-Fi connection failed");
  return false;
}

// ส่งข้อความไปยัง LINE Messaging API
bool sendLineMessage(String message) {
  if (WiFi.status() != WL_CONNECTED) {
    Serial.println("Cannot send: Wi-Fi disconnected");
    return false;
  }
```

```
  WiFiClientSecure client;

  // ใช้เฉพาะการทดลองในห้องปฏิบัติการ
  client.setInsecure();
  client.setTimeout(15000);

  HTTPClient https;
  https.setTimeout(15000);

  if (!https.begin(client, LINE_API_URL)) {
    Serial.println("Cannot start HTTPS connection");
    return false;
  }

  https.addHeader("Content-Type", "application/json");
  https.addHeader(
    "Authorization",
    String("Bearer ") + LINE_ACCESS_TOKEN
  );

  String safeMessage = jsonEscape(message);

  String payload = "{";
  payload += "\"to\":\"";
  payload += LINE_TO_ID;
  payload += "\",";
  payload += "\"messages\":[{";
  payload += "\"type\":\"text\",";
  payload += "\"text\":\"";
  payload += safeMessage;
  payload += "\"";
  payload += "}]}";

  Serial.println("Sending LINE message...");

  int httpCode = https.POST(payload);
  String response = https.getString();

  Serial.print("HTTP response code: ");
  Serial.println(httpCode);

  if (response.length() > 0) {
    Serial.print("Response: ");
    Serial.println(response);
  }

  https.end();

  if (httpCode == 200) {
    Serial.println("LINE message sent successfully");
    return true;
  }

  Serial.println("LINE message failed");
  return false;
}
```

```
void setup() {
  Serial.begin(115200);
  delay(100);

  if (!connectWiFi(20000)) {
    return;
  }

  if (!messageSent) {
    String message =
      "ทดสอบส่งข้อความจาก NodeMCU ESP8266\n"
      "สถานะ: เชื่อมต่อ LINE Messaging API สำเร็จ";

    messageSent = sendLineMessage(message);
  }
}

void loop() {
  // ใบงานนี้ส่งข้อความหนึ่งครั้งหลังเปิดเครื่อง
}
```

11.2 ค่าที่ต้องแก้ไข ให้ผู้เรียนต้องแก้ไขเพียง 4 ค่า ได้แก่

```
const char* WIFI_SSID = "ชื่อ Wi-Fi";
const char* WIFI_PASSWORD = "รหัสผ่าน Wi-Fi";
const char* LINE_ACCESS_TOKEN = "Channel access token";
const char* LINE_TO_ID = "User ID";
```

ห้ามแก้ URL ของ LINE API เป็นลิงก์ Markdown และห้ามเขียนในลักษณะต่อไปนี้

```
"[https://api.line.me/...](https://api.line.me/...)"
```

ค่าที่ถูกต้องต้องเป็น URL ธรรมดาเท่านั้น

```
"https://api.line.me/v2/bot/message/push"
```

12. ตอนที่ 12 อัปโหลดและทดสอบโปรแกรม

1) ตรวจสอบว่าได้แทนค่า Wi-Fi, token และ User ID แล้ว
2) ตรวจสอบว่าไม่มีช่องว่างเพิ่มก่อนหรือหลัง token
3) ตรวจสอบว่า User ID ขึ้นต้นด้วย U
4) กด Verify
5) หากพบข้อผิดพลาด ให้ตรวจสอบวงเล็บ เครื่องหมายคำพูด และเครื่องหมายอัฒภาค
6) เลือกบอร์ด NodeMCU 1.0
7) เลือก Port ให้ถูกต้อง
8) กด Upload
9) รอจนแสดงข้อความอัปโหลดสำเร็จ
10) เปิด Serial Monitor ที่ 115200 baud

11) กดปุ่ม Reset บน NodeMCU หนึ่งครั้ง

12) ตรวจสอบข้อความตามลำดับ

```
Connecting to Wi-Fi
Wi-Fi connected
IP address: ...
Sending LINE message...
HTTP response code: 200
LINE message sent successfully
```

13) เปิดแอป LINE บนสมาร์ตโฟน

14) เปิดห้องสนทนาของ LINE Official Account

15) ตรวจสอบข้อความที่ได้รับ

16) เปรียบเทียบเวลาบน Serial Monitor กับเวลาที่ข้อความมาถึง

17) บันทึกผล

18) ไม่ควรกด Reset ซ้ำหลายครั้ง เพราะจะทำให้ส่งข้อความซ้ำและใช้โควตา

13. ขั้นตอนที่ 13 ทดสอบข้อความหลายสถานะ แก้เฉพาะข้อความแล้วทดสอบทีละกรณี

1) กรณีที่ 1 ระบบพร้อมทำงาน

```
String message =
  "RFID Door Lock\n"
   "สถานะ: ระบบพร้อมทำงาน";
```

2) กรณีที่ 2 อนุญาตให้เข้าใช้งาน

```
String message =
   "อนุญาตให้เข้าใช้งาน\n"
   "สถานะ: เปิดประตู";
```

3) กรณีที่ 3 ปฏิเสธการเข้าใช้งาน

```
String message =
   "แจ้งเตือน\n"
   "สถานะ: ตรวจพบบัตรที่ไม่ได้รับอนุญาต";
```

4) กรณีที่ 4 เปิดประตูด้วยสวิตช์

```
String message =
   "มีการเปิดประตูจากด้านใน\n"
   "สาเหตุ: กดสวิตช์เปิดประตู";
```

ทดสอบแต่ละข้อความเพียงหนึ่งครั้งและบันทึกผล

14. ขั้นตอนที่ 14 ทดสอบสภาวะผิดปกติ

14.1 ทดสอบเมื่อรหัสผ่าน Wi-Fi ไม่ถูกต้อง

1) เปลี่ยน WIFI_PASSWORD เป็นค่าทดสอบที่ไม่ถูกต้อง
2) อัปโหลดโปรแกรม
3) เปิด Serial Monitor
4) ตรวจสอบว่าแสดง Wi-Fi connection failed
5) ตรวจสอบว่าโปรแกรมไม่พยายามส่ง LINE
6) เปลี่ยนกลับเป็นค่าที่ถูกต้องทันที

14.2 ทดสอบเมื่อ User ID ไม่ถูกต้อง

1) สำรอง User ID ที่ถูกต้อง
2) เปลี่ยนอักขระท้าย User ID หนึ่งตัว
3) อัปโหลดและทดสอบ
4) บันทึก HTTP response code และข้อความตอบกลับ
5) คืนค่า User ID ที่ถูกต้อง

14.3 ทดสอบเมื่อ Token ไม่ถูกต้อง

เพื่อความปลอดภัย ไม่จำเป็นต้องนำ token จริงไปแก้ไข ให้แทนค่าด้วยข้อความ เช่น INVALID_TOKEN

1) อัปโหลดและทดสอบ
2) ตรวจสอบว่า LINE ปฏิเสธคำขอ
3) บันทึก HTTP response code
4) คืนค่า token ที่ถูกต้อง
5) ห้ามเผยแพร่ token จริงในตารางผล

14.4 ทดสอบเมื่ออินเทอร์เน็ตขัดข้อง

1) ปิดการเชื่อมต่ออินเทอร์เน็ตด้าน WAN ของเราเตอร์ โดยได้รับอนุญาตจากผู้สอน
2) เปิด NodeMCU
3) ตรวจสอบว่า NodeMCU อาจเชื่อมต่อ Wi-Fi ได้ แต่ไม่สามารถติดต่อ LINE API
4) บันทึกผล
5) ต่ออินเทอร์เน็ตกลับ
6) ทดสอบอีกครั้ง

15. การแปลผล HTTP response code

โดยเมื่อเกิดข้อผิดพลาด ต้องอ่านทั้ง HTTP response code และ response body ไม่ควรตัดสินจากรหัสเพียงอย่างเดียว

16. จากนั้นตารางบันทึกผลการทดลองในตารางที่ 8.6, 8.7, และ 8.8

ตารางที่ 8.5 สรุปรายการแปลผล HTTP response code

รหัส	ความหมายทั่วไป	แนวทางตรวจสอบ
200	LINE รับคำขอสำเร็จ	ตรวจสอบข้อความในแอป LINE
400	รูปแบบคำขอหรือ JSON ไม่ถูกต้อง	ตรวจ to, messages, วงเล็บและเครื่องหมายคำพูด
401	การยืนยันตัวตนไม่สำเร็จ	ตรวจ token และคำว่า Bearer
403	ไม่มีสิทธิ์ดำเนินการ	ตรวจสิทธิ์ Channel และผู้รับ
404	URL หรือ endpoint ไม่ถูกต้อง	ตรวจ URL ของ LINE API
409	สถานะคำขอขัดแย้งในบาง API	ตรวจ response body
429	ส่งคำขอถี่หรือเกินข้อจำกัด	หยุดส่งและรอก่อนทดลองใหม่
ค่าติดลบ	ESP8266 เชื่อมต่อเซิร์ฟเวอร์ไม่ได้	ตรวจ Wi-Fi, DNS, HTTPS และเวลา timeout

ตารางที่ 8.6 ผลการเตรียมระบบ LINE

รายการตรวจสอบ	ผลที่ตรวจพบ	ผ่าน/ไม่ผ่าน	หมายเหตุ
สร้าง LINE Official Account ได้			
เปิด Messaging API ได้			
พบ Channel ใน Developers Console			
ออก Channel access token ได้			
ตรวจพบ Your user ID			
เพิ่ม Official Account เป็นเพื่อนแล้ว			
ทดสอบจาก Postman/curl สำเร็จ			

ตารางที่ 8.7 ผลการส่งข้อความจาก ESP8266

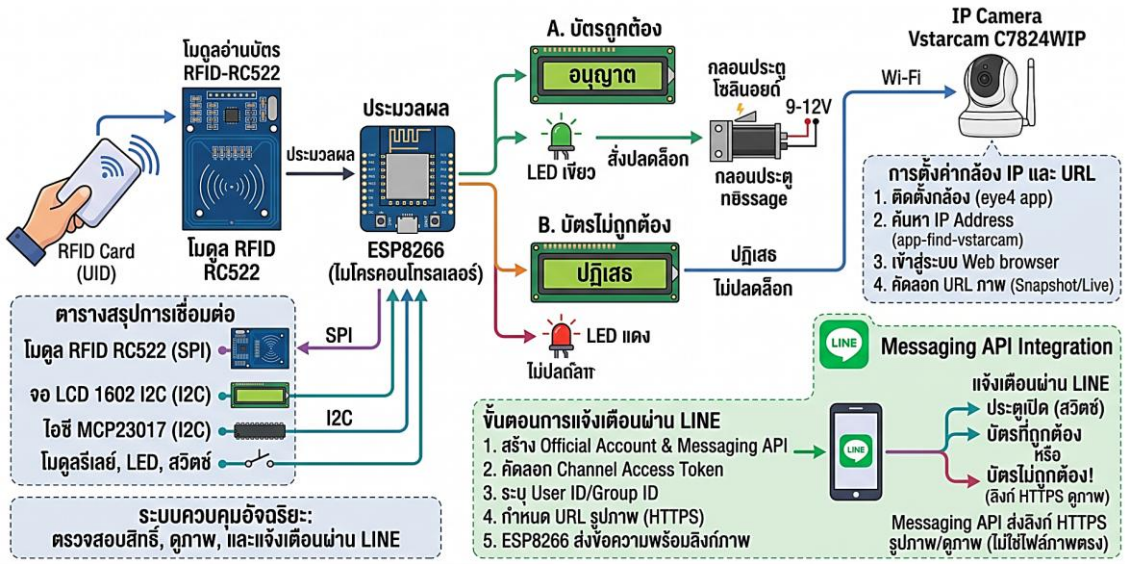
ครั้งที่	ข้อความทดสอบ	Wi-Fi	HTTP code	ได้รับข้อความ	เวลาตอบสนอง	ผล
1	ระบบพร้อมทำงาน					
2	อนุญาตให้เข้าใช้งาน					
3	ปฏิเสธการเข้าใช้งาน					
4	เปิดประตูด้วยสวิตช์					

ตารางที่ 8.8 ผลการทดสอบข้อผิดพลาด

กรณีทดสอบ	ผลที่คาดหวัง	HTTP code/ข้อความ	ผลที่เกิดขึ้นจริง	ผ่าน/ไม่ผ่าน
รหัสผ่าน Wi-Fi ผิด	เชื่อมต่อ Wi-Fi ไม่ได้			
User ID ผิด	LINE ปฏิเสธหรือส่งไม่ได้			
Token ผิด	ยืนยันตัวตนไม่สำเร็จ			
อินเทอร์เน็ตขัดข้อง	ติดต่อ LINE API ไม่ได้			
ข้อความมีภาษาไทย	แสดงภาษาไทยได้ถูกต้อง			
ข้อความมีหลายบรรทัด	ขึ้นบรรทัดใหม่ถูกต้อง			

การปฏิบัติงานที่ 8.2

ระบบ RFID ควบคุมกลอนประตูด้วย NodeMCU ESP8266



รูปที่ 8.1 การประยุกต์ใช้งาน RFID ร่วมกับ IP camera และ LINE Messaging API

ความรู้พื้นฐานในการปฏิบัติงาน

1.การทำงานของ RFID

RFID-RC522 ทำงานที่ความถี่ 13.56 MHz เมื่อบัตรเข้าใกล้ตัวอ่าน โมดูลจะอ่านหมายเลข UID และส่งไปยัง NodeMCU ผ่านบัส SPI

UID เป็นรหัสประจำบัตร แต่ไม่ควรถือว่า UID เพียงอย่างเดียวเป็นระบบรักษาความปลอดภัยระดับสูง เพราะบัตรบางประเภทอาจถูกทำสำเนาได้ ใบงานนี้ใช้ UID เพื่อศึกษาหลักการตรวจสอบสิทธิ์เบื้องต้น

2. การสื่อสาร SPI ขาสำคัญของ SPI ได้แก่

- SCK: สัญญาณนาฬิกา
- MOSI: ข้อมูลจาก NodeMCU ไปยัง RC522
- MISO: ข้อมูลจาก RC522 กลับมายัง NodeMCU
- SS/SDA: เลือกอุปกรณ์
- RST: รีเซตโมดูล

3. การสื่อสาร I²C

LCD และ MCP23017 ใช้สาย SDA และ SCL ร่วมกันได้ แต่ต้องมี I²C address ไม่ซ้ำกัน ตัวอย่างในใบงานกำหนด ต้องตรวจสอบ address จริงด้วยโปรแกรม I²C Scanner ก่อนใช้งาน

- LCD I²C: 0x27
- MCP23017: 0x20

4. รีเลย์และกลอนประตู

NodeMCU และ MCP23017 ไม่สามารถจ่ายกระแสให้กลอนหรือขดลวดรีเลย์เปล่าโดยตรง จึงต้องใช้โมดูลรีเลย์ที่มีวงจรขับภายในและรองรับสัญญาณควบคุม 3.3 V หน้าสัมผัสรีเลย์ประกอบด้วย

- COM: ขั้วร่วม
- NO: ต่อกับ COM เมื่อรีเลย์ทำงาน
- NC: ต่อกับ COM เมื่อรีเลย์ไม่ทำงาน

สำหรับกลอนชนิดจ่ายไฟเพื่อปลดล็อก ใช้ COM และ NO เพื่อให้กลอนได้รับไฟเฉพาะช่วงที่อนุญาต

5. ไดโอดป้องกันแรงดันย้อน

กลอนโซลินอยด์เป็นโหลดเหนี่ยวนำ เมื่อหยุดจ่ายไฟจะเกิดแรงดันย้อน จึงต้องต่อไดโอดคร่อมกลอน (หากต่อไดโอดกลับขั้ว จะทำให้เกิดกระแสลัดวงจรเมื่อจ่ายไฟ) โดย

- แคโทดหรือด้านที่มีแถบ ต่อกับขั้วบวกของกลอน
- แอโนด ต่อกับขั้วลบของกลอน

6. ลอจิก Active LOW โดยตัวอย่างโปรแกรมกำหนดให้รีเลย์เป็น Active LOW

คำสั่ง	**สถานะรีเลย์**	**สถานะกลอน**
HIGH	หยุดทำงาน	ล็อก
LOW	ทำงาน	ปลดล็อก

ต้องตรวจสอบโมดูลจริง เพราะรีเลย์บางรุ่นเป็น Active HIGH

ขั้นตอนการปฏิบัติงาน

1. ขั้นตอนที่ 1 เชื่อมต่อกล้อง IP camera

เชื่อมต่อกล้อง Vstarcam C7824WIP กับแอป Eye4 โดยใช้เครือข่าย Wi-Fi ย่าน 2.4 GHz จากนั้นเพิ่มอุปกรณ์ด้วยการสแกน QR code ที่ตัวกล้อง ตั้งชื่อกล้อง และเปลี่ยนรหัสผ่านเพื่อความปลอดภัย

2. ขั้นตอนที่ 2 ตรวจสอบ IP address ของกล้อง

ใช้โปรแกรมค้นหากล้อง เช่น app-find-vstarcam เพื่อตรวจสอบหมายเลข IP address ของกล้อง จากนั้นเปิดกล้องผ่าน Web browser และคัดลอก URL สำหรับดูภาพหรือ snapshot ของกล้องไว้ใช้ในโปรแกรม

3. ขั้นตอนที่ 3 สร้าง LINE Messaging API

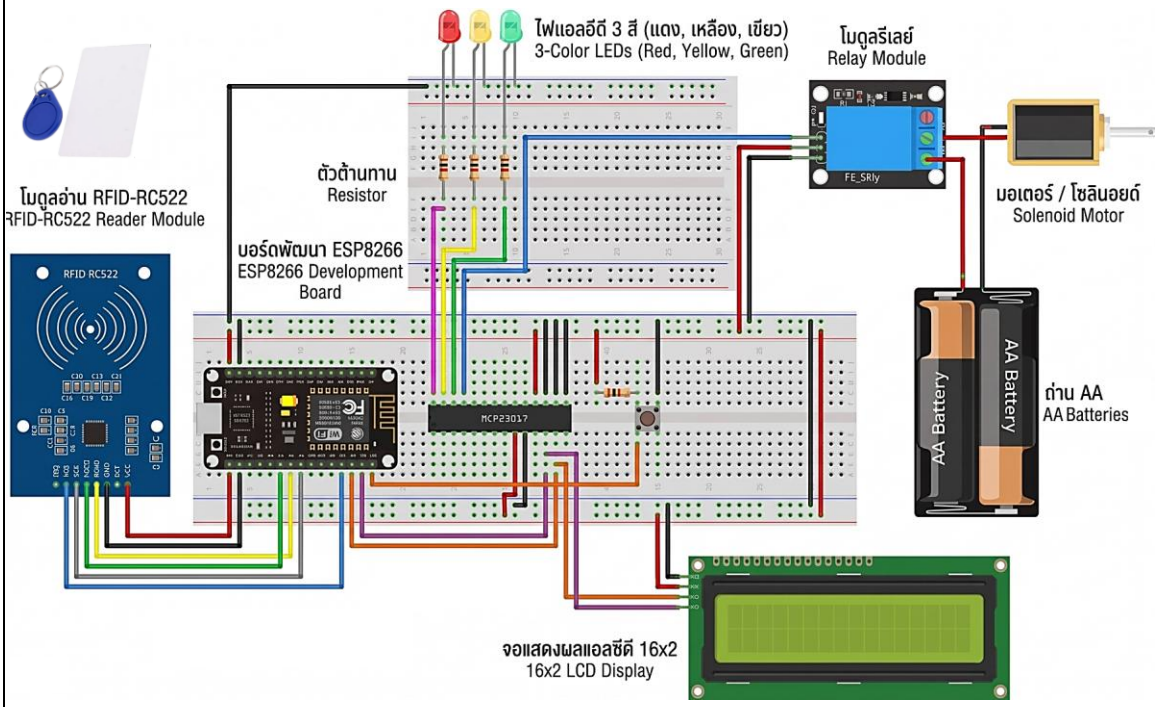
สร้าง LINE Official Account และเปิดใช้งาน Messaging API เพื่อรับค่า channel access token จาก LINE Developers Console จากนั้นเพิ่มบัญชี LINE Official Account เป็นเพื่อน และเตรียม user ID หรือ group ID สำหรับรับข้อความแจ้งเตือน

4. ขั้นตอนที่ 4 ติดตั้งไลบรารีใน Arduino IDE

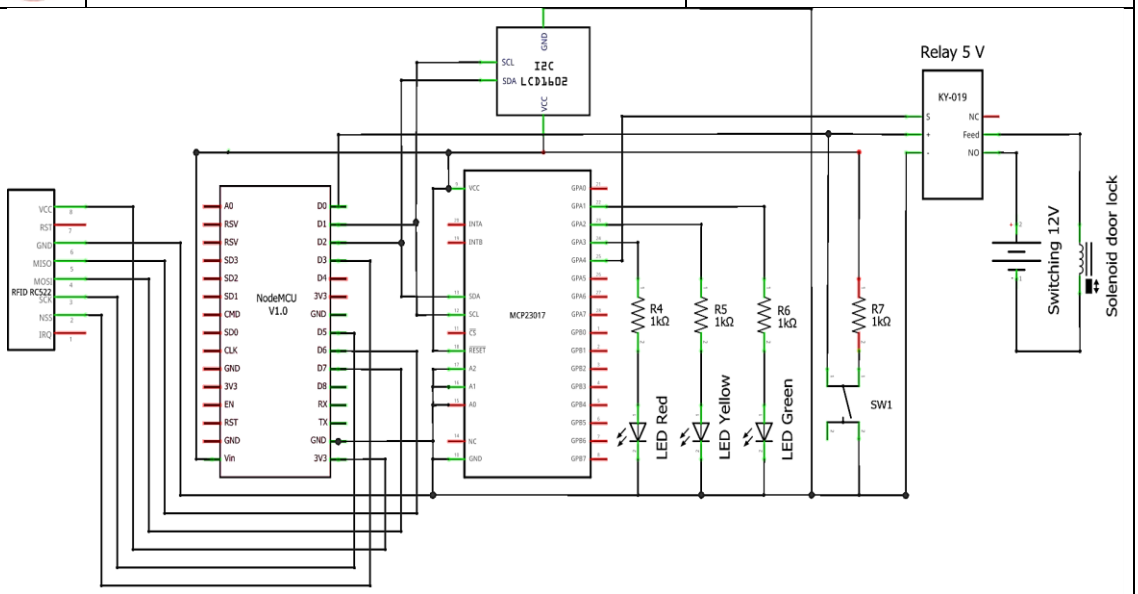
ติดตั้งไลบรารีที่จำเป็น เช่น ESP8266WiFi.h, WiFiClientSecure.h, ESP8266HTTPClient.h, MFRC522.h, LiquidCrystal_I²C.h และ Adafruit_MCP23017.h

5. ขั้นตอนที่ 5 เชื่อมต่อวงจร

ต่อโมดูล RFID RC522 เข้ากับ ESP8266 ผ่านการสื่อสารแบบ SPI ต่อ LCD และ MCP23017 ผ่าน I²C จากนั้นต่อ LED, Relay และสวิตช์เข้ากับขาที่กำหนด โดย Relay ทำหน้าที่ควบคุมกลอนประตูโซลินอยด์ ซึ่งต้องใช้แหล่งจ่ายไฟแยก 9–12 V ดังรูปที่ 8.2 หรือ 8.3 และตารางที่ 8.8, 8.9, 8.10, 8.11, และ 8.12



รูปที่ 8.2 วงจรการประยุกต์ใช้ RFID ร่วมกับ IP camera และ LINE Messaging API



รูปที่ 8.3 แผนภาพเค้าร่างการประยุกต์ใช้ RFID ร่วมกับ IP camera โดยใช้ ESP8266

ตารางที่ 8.8 การเชื่อมต่อขาขาอุปกรณ์ RFID-RC522 กับ NodeMCU

ขา RFID-RC522	ขา NodeMCU	GPIO	หน้าที่
SDA/SS	D3	GPIO0	เลือก RC522
SCK	D5	GPIO14	นาฬิกา SPI
MOSI	D7	GPIO13	ส่งข้อมูลไป RC522
MISO	D6	GPIO12	รับข้อมูลจาก RC522
RST	D8	GPIO15	รีเซต RC522
3.3V	3V3	–	ไฟเลี้ยง
GND	GND	–	กราวด์
IRQ	ไม่ต่อ	–	ไม่ใช้ในใบงาน

ตารางที่ 8.9 การเชื่อมต่อขาอุปกรณ์ LCD และ MCP23017 กับ NodeMCU

อุปกรณ์	ขาอุปกรณ์	ขา NodeMCU	GPIO
LCD I²C	SDA	D2	GPIO4
LCD I²C	SCL	D1	GPIO5
MCP23017	SDA	D2	GPIO4
MCP23017	SCL	D1	GPIO5
MCP23017	VDD	3V3	–
MCP23017	VSS	GND	–
MCP23017	A0, A1, A2	GND	–
MCP23017	RESET (ดึงขึ้น)	3.3 V	–

○ การต่อ A0, A1 และ A2 ลง GND ทำให้ MCP23017 มี address 0x20

○ หากโมดูล LCD ใช้ไฟ 5 V และมีตัวต้านทาน Pull-up บน SDA/SCL ไปที่ 5 V ต้องใช้ตัวแปลงระดับลอจิก I²C หรือแก้ไขวงจร Pull-up เพื่อไม่ให้แรงดัน 5 V เข้าขา ESP8266

ตารางที่ 8.10 การเชื่อมต่อขาอุปกรณ์ LED และรีเลย์กับ MCP23017

อุปกรณ์	หมายเลขในโปรแกรม	พอร์ต MCP23017	ขา DIP
LED สีแดง	7	GPA7	28
LED สีเหลือง	6	GPA6	27
LED สีเขียว	5	GPA5	26
สัญญาณควบคุมรีเลย์	4	GPA4	25

ตารางที่ 8.11 การเชื่อมต่อสวิตช์เปิดประตู

จุดต่อ	การเชื่อมต่อ
ขาหนึ่งของสวิตช์	D0 หรือ GPIO16
อีกขาของสวิตช์	GND
ตัวต้านทาน 10 kΩ	ระหว่าง D0 กับ 3.3 V

○ สถานะที่โปรแกรมอ่านได้คือ ไม่กดสวิตช์: HIGH และถ้ากดสวิตช์: LOW

ตารางที่ 8.12 การเชื่อมต่อสวิตช์เปิดประตู

จุดเริ่มต้น	จุดปลายทาง
ขั้วบวกแหล่งจ่ายกลอน	ฟิวส์
ฟิวส์	COM ของรีเลย์
NO ของรีเลย์	ขั้วบวกของกลอน
ขั้วลบของกลอน	0 V ของแหล่งจ่ายกลอน
แคโทดของไดโอด	ขั้วบวกของกลอน
แอโนดของไดโอด	ขั้วลบของกลอน

6. ขั้นตอนที่ 6 อัปโหลดโปรแกรมลง ESP8266

เขียนโปรแกรมใน Arduino IDE โดยกำหนดค่า Wi-Fi, channel access token, user ID หรือ group ID, UID ของบัตร RFID ที่อนุญาต และ URL ของกล้อง IP camera จากนั้นกด verify เพื่อตรวจสอบความถูกต้อง และ upload โปรแกรมลงบอร์ด

7. ขั้นตอนที่ 7 ทดสอบการทำงานของระบบ

เมื่อระบบเริ่มทำงาน จอ LCD จะแสดงข้อความให้แตะบัตร หากแตะบัตร RFID ที่ถูกต้อง ESP8266 จะสั่งให้ Relay ทำงานเพื่อปลดล็อกกลอนประตู พร้อมส่งข้อความแจ้งเตือนผ่าน LINE Messaging API และแนบลิงก์ภาพจากกล้อง IP camera

9. ขั้นตอนที่ 9 กรณีบัตรไม่ถูกต้อง

หากแตะบัตร RFID ที่ไม่ได้รับอนุญาต ระบบจะไม่สั่งให้ Relay ทำงาน กลอนประตูยังคงล็อกอยู่ พร้อมแสดงข้อความปฏิเสธบนจอ LCD เปิดไฟ LED สีแดง และส่งข้อความแจ้งเตือนไปยัง LINE ว่ามีการใช้บัตรที่ไม่ถูกต้อง

10. ขั้นตอนที่ 10 การเปิดประตูด้วยสวิตช์

เมื่อกดสวิตช์เปิดประตูจากด้านใน ESP8266 จะสั่งให้ Relay ทำงานเพื่อปลดล็อกกลอนประตูชั่วคราว และส่งข้อความแจ้งเตือนผ่าน LINE ว่ามีการเปิดประตูจากสวิตช์

หากต้องการให้รูปแสดงใน LINE โดยตรง ต้องอัปโหลดภาพจากกล้องไปยังเซิร์ฟเวอร์หรือ URL แบบ HTTPS ที่เข้าถึงได้ก่อน แล้วจึงส่งภาพผ่าน LINE Messaging API

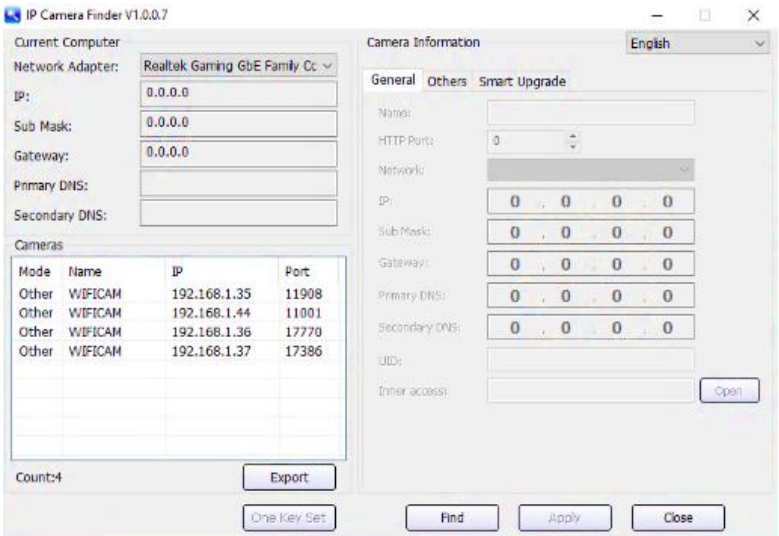
11. ขั้นตอนการเขียนโปรแกรมควบคุม snapshot ด้วย IP camera และแจ้งเตือนผ่าน LINE Messaging API

ระบบนี้เป็นการนำ ESP8266 มาใช้งานร่วมกับ IP camera รุ่น Vstarcam C7824WIP และ LINE Messaging API เพื่อส่งข้อความแจ้งเตือนเมื่อมีเหตุการณ์เกิดขึ้น เช่น การกดสวิตช์ หรือการอ่านบัตร RFID โดยกล้อง IP camera จะใช้สำหรับดูภาพหรือ snapshot ผ่าน URL ของกล้อง ส่วน LINE Messaging API จะใช้ส่งข้อความแจ้งเตือนไปยังผู้ใช้ผ่าน LINE Official Account

11.1) การเชื่อมต่อ cloud ของ IP camera บน Web browser

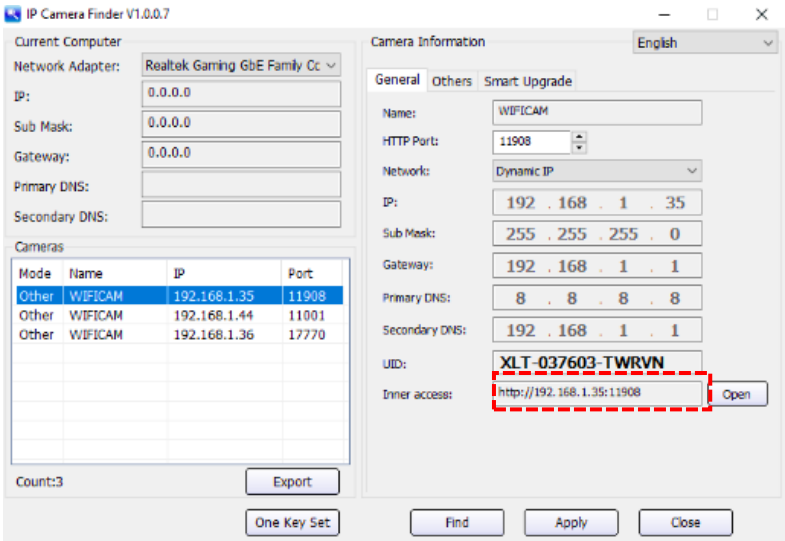
มีการเชื่อมต่อ cloud ของ IP camera บน Web browser มีขั้นตอนดังนี้

11.1.1) ขั้นตอนที่ 1 ใช้โปรแกรม app-find-vstarcam” ในการค้นหาหมายเลข IP ของกล้อง ดังรูปที่ 8.4



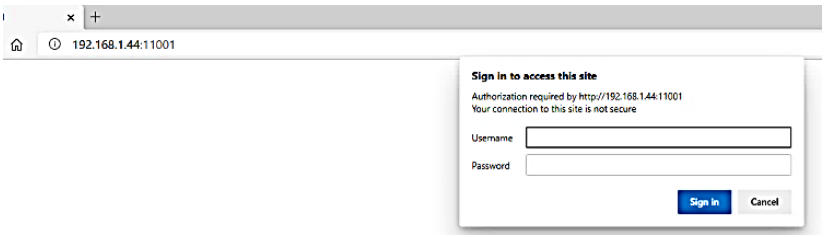
รูปที่ 8.4 หน้าต่างโปรแกรม app-find-vstarcam

11.2.2) ขั้นตอนที่ 2 เมื่อทำการเลือกหมายเลข IP address แล้วจะปรากฏ URL ของกล้องตัวนั้น ที่ช่อง Inner accress ให้ทำการกดคำสั่ง Open ดังรูปที่ 8.5



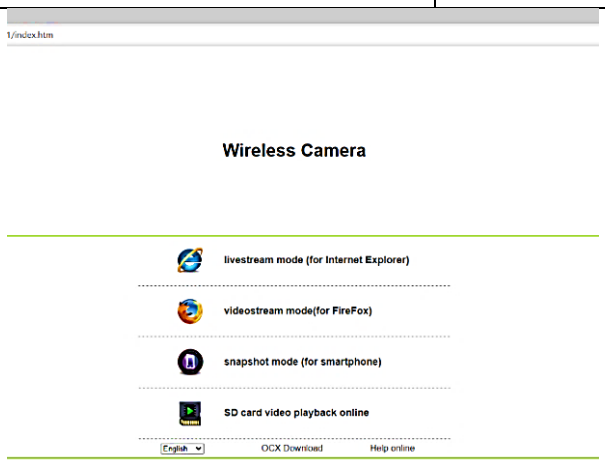
รูปที่ 8.5 การค้นหา URL ของกล้อง IP

11.2.3) ขั้นตอนที่ 3 เว็บเบราเซอร์ จะปรากฏหน้าต่างขึ้นมาดังรูปที่ 8.6 ให้ใส่ Username, Password ที่ตั้งค่าไว้กับที่ตัวกล้อง แล้วทำการเข้าสู่ระบบ (Sign in)



รูปที่ 8.6 Web browser สำหรับการเปิดหน้าจอ URL ของกล้อง

11.2.4) ขั้นตอนที่ 4 เมื่อเข้าสู่ระบบเรียบร้อย จะปรากฏหน้าต่างขึ้นมา ให้เราทำการเลือกเว็บเบราเวอร์ที่ใช้ในการเปิด URL ของกล้อง ดังรูปที่ 8.7

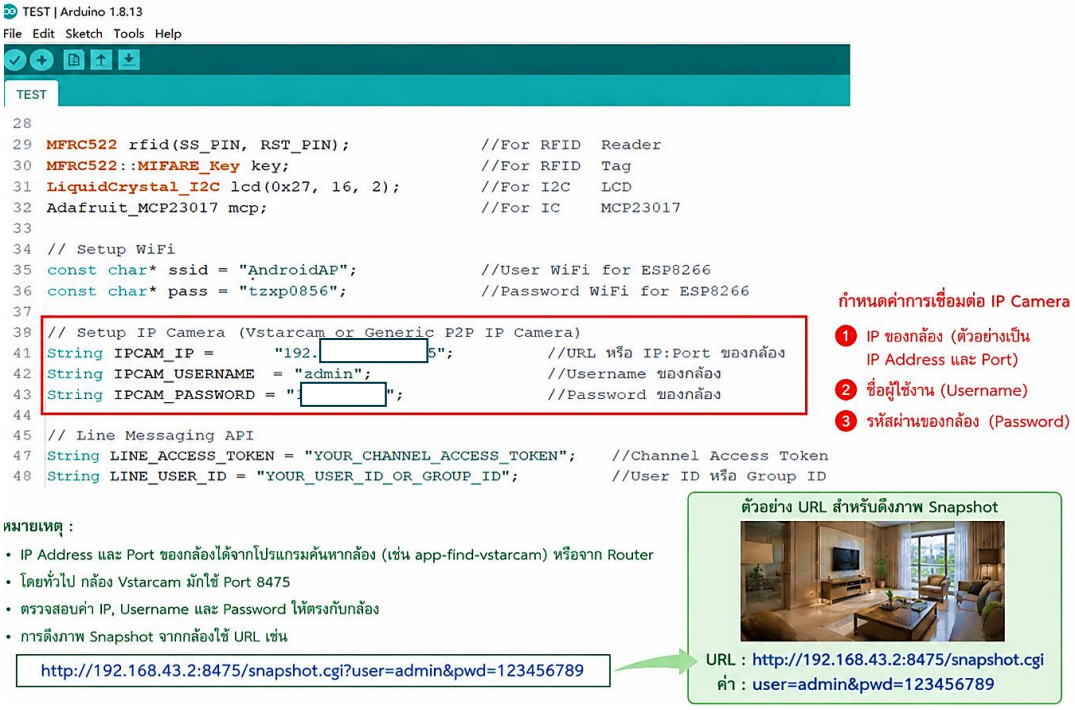


รูปที่ 8.7 การเลือกเว็บเบราเซอร์ ที่ใช้เปิด URL ของกล้อง

2.2.5) ขั้นตอนที่ 5 เมื่อทำการเลือกเว็บเบราเซอร์ แล้วจะปรากฏหน้าต่างที่แสดงภาพวงจรปิดของกล้องที่เลือกขึ้นมา โดยให้ทำการคัดลอกช่อง URL เอาไว้ด้วย ดังรูปที่ 8.8

รูปที่ 8.8 หน้าต่างแสดงภาพวงจรปิดของกล้อง

2.2.6) การเชื่อมต่อคลาวด์ของกล้องร่วมกับ ESP8266 ให้นำ URL ที่คัดลอกไว้ มาใส่ไว้ในโค้ดที่โปรแกรมไว้ดังรูปที่ 8.9



รูปที่ 8.9 การกำหนดค่า IP camera และ LINE Messaging API บน ESP8266

จากรูปที่ 8.9 การเชื่อมต่อ cloud ของ IP camera บน Web browser เมื่อทำการเลือกเว็บเบราเซอร์ แล้วจะปรากฏหน้าต่างที่แสดงภาพวงจรปิดของกล้องที่เลือกขึ้นมา โดยให้ทำการคัดลอกช่อง URL เอาไว้ด้วยการเชื่อมต่อคลาวด์ของกล้องร่วมกับ ESP8266 ให้นำ URL ที่คัดลอกไว้ มาใส่ไว้ในโค้ดที่โปรแกรม

- String IPCAM_IP “XXXX” ; ให้ทำการใส่หมายเลข IP Address ของกล้อง
- String IPCAM_USERNAME = "XXXX" ; ให้ทำการใส่ Username ของกล้อง
- String IPCAM_PASSWORD = "XXXX" ; ให้ทำการใส่ Password ของกล้อง

เมื่อผู้ใช้นำบัตร RFID มาแตะที่โมดูล RC522 ระบบจะอ่านค่า UID แล้วส่งให้ ESP8266 ตรวจสอบ หาก UID ตรงกับค่าที่กำหนดไว้ ระบบจะแสดงข้อความอนุญาตบนจอ LCD เปิดไฟ LED สีเขียว และสั่งให้ Relay ทำงานเพื่อปลดล็อกกลอนประตูโซลินอยด์ พร้อมส่งข้อความแจ้งเตือนผ่าน LINE Messaging API หาก UID ไม่ตรงกับค่าที่กำหนดไว้ ระบบจะแสดงข้อความปฏิเสธบนจอ LCD เปิดไฟ LED สีแดง และส่งข้อความแจ้งเตือนไปยัง LINE เพื่อแจ้งว่ามีการใช้บัตรที่ไม่ได้รับอนุญาต

ในส่วนของ IP camera รุ่น Vstarcam C7824WIP จะใช้สำหรับตรวจสอบภาพเหตุการณ์ผ่าน URL snapshot ของกล้อง โดย ESP8266 จะส่งลิงก์ snapshot ไปพร้อมข้อความแจ้งเตือนผ่าน LINE Messaging API แทนการส่งไฟล์ภาพโดยตรง เนื่องจาก LINE Messaging

API ต้องใช้ URL รูปภาพแบบ HTTPS ที่ LINE สามารถเข้าถึงได้ หากเป็น URL ภายในเครือข่าย เช่น http://192.168.x.x จะเหมาะสำหรับแนบเป็นลิงก์ให้ผู้ใช้เปิดดูในเครือข่ายเดียวกันเท่านั้น รายละเอียดการเขียนโปรแกรมควบคุมการทำงานของระบบดังภาคผนวก ก (Arduino Code: 10)

สรุปผลการทดลอง

เอกสารอ้างอิง

สิทธา ชูหีบ, ณิชานาฎ เกตุอู่ทอง, และ ธิดาพร พัดเพ็ง. (2562). *แบบจำลองระบบความปลอดภัยการเข้าออกด้วยอาร์เอฟไอดีและไอโอที*. ปริญญานิพนธ์หลักสูตรครุศาสตร์อุตสาหกรรมบัณฑิต สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์และโทรคมนาคม, ภาควิชาครุศาสตร์อุตสาหกรรม, คณะครุศาสตร์อุตสาหกรรม, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี, ปทุมธานี.

Ayeni, P. O., & Adesoba, O. C. (2025). IoT-based home control system using NodeMCU and Firebase. *Journal of Edge Computing, 4*(1), 17–34. https://doi.org/10.55056/jec.814.

LINE Developers. (2024). *Get started with the Messaging API*. LINE Developers Documentation. https://developers.line.biz/en/docs/messaging-api/getting-started/.

LINE Developers. (n.d.). *Messaging API reference*. https://developers.line.biz/en/reference/messaging-api/

Sahasika, M. P., Pratiwi, D., & Santoso, G. B. (2023, May 8). Visualization of home security sensor system based on IoT server. *Qeios, Preprint*, 1-19. https://doi.org/10.32388/ZC810D.

Santos, R., & Santos, S. (2016). *ESP8266 web server with Arduino IDE: Step-by-step project guide*. Random Nerd Tutorials.

Santos, R., & Santos, S. (2025). *Learn ESP32 with Arduino IDE* (3rd ed., Version 3.2). Random Nerd Tutorials. https://randomnerdtutorials.com/learn-esp32-with-arduino-ide/

	ใบงานที่ 9 เรื่อง ระบบประตูอัจฉริยะด้วยเทคโนโลยี ตรวจสอบลายนิ้วมือร่วมกับ RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ประยุกต์ใช้เทคโนโลยีตรวจสอบลายนิ้วมือร่วมกับ RFID เพื่อสร้างระบบรักษาความปลอดภัยได้

วัตถุประสงค์

1. ตรวจสอบรุ่นและพิกัดแรงดันของเซนเซอร์ลายนิ้วมือได้
2. ต่อสาย TX และ RX แบบไขว้ได้ถูกต้อง
3. ใช้โปรแกรมตัวอย่างเพื่อลงทะเบียนลายนิ้วมือได้
4. กำหนดหมายเลข ID ให้ลายนิ้วมือได้
5. ตรวจสอบลายนิ้วมือที่ลงทะเบียนและไม่ได้ลงทะเบียนได้
6. ต่อและทดสอบ RFID-RC522 ได้
7. ทดสอบรีเลย์โดยยังไม่ต่อกลอนประตูได้
8. ต่อกลอนประตูพร้อมฟิวส์และไดโอดป้องกันแรงดันย้อนได้
9. ตรวจสอบว่าประตูเปิดเฉพาะเมื่อได้รับอนุญาตได้
10. ทำให้ระบบกลับเข้าสู่สถานะรอหลังครบเวลาที่กำหนดได้

เครื่องมือและอุปกรณ์

1.	Arduino UNO R3	1 บอร์ด
2.	เซนเซอร์ลายนิ้วมือ JM101B หรือ R307	1 ตัว
3.	โมดูล RFID-RC522	1 โมดูล
4.	บัตรหรือแท็ก RFID 13.56 MHz อย่างน้อย	2 ใบ
5.	จอ LCD 16×2 พร้อมโมดูล I²C	1 ชุด
6.	โมดูลรีเลย์ 5 V	1 โมดูล
7.	กลอนประตูโซลินอยด์ DC	1 ตัว
8.	แหล่งจ่ายไฟสำหรับกลอนตามพิกัด	1 ชุด
9.	ฟิวส์และฐานฟิวส์	1 ชุด
10.	ไดโอดป้องกันแรงดันย้อน เช่น 1N4007	1 ตัว
11.	LED สีแดง สีเหลือง และสีเขียว สีละ	1 ดวง
12.	ตัวต้านทาน 220–330 Ω	3 ตัว
13.	Active Buzzer 5 V หรือวงจรขับ Buzzer	1 ชุด
14.	Push button	1 ตัว
15.	Breadboard และสาย Jumper	1 ชุด
16.	มัลติมิเตอร์	1 เครื่อง

17. คอมพิวเตอร์ติดตั้ง Arduino IDE 1 เครื่อง
18. สาย USB สำหรับ Arduino UNO 1 เส้น
19. แหล่งจ่ายไฟ 5 V แบบควบคุมแรงดัน 1 ชุด
20. ซอฟต์แวร์และไลบรารี ติดตั้งไลบรารีใน Arduino IDE
    1) Adafruit Fingerprint Sensor Library
    2) MFRC522
    3) LiquidCrystal I2C
    4) SoftwareSerial ซึ่งมากับ Arduino IDE
    5) SPI ซึ่งมากับ Arduino IDE
    6) Wire ซึ่งมากับ Arduino IDE

ความรู้พื้นฐานในการปฏิบัติงาน

1. การทำงานของเซนเซอร์ลายนิ้วมือ เซนเซอร์ลายนิ้วมือทำหน้าที่หลักดังนี้
   1) ถ่ายภาพลายนิ้วมือ
   2) ประมวลผลลักษณะเฉพาะของลายนิ้วมือ
   3) สร้างแม่แบบหรือ Template
   4) บันทึก Template ไว้ในหน่วยความจำภายใน
   5) เปรียบเทียบลายนิ้วมือที่สแกนกับ Template
   6) ส่ง Fingerprint ID และค่าความเชื่อมั่นกลับไปยัง Arduino

   Arduino ไม่ได้รับภาพลายนิ้วมือโดยตรงในการทดลองนี้ แต่ได้รับผลการค้นหา เช่น หมายเลข ID และค่าความเชื่อมั่น

2. การลงทะเบียนลายนิ้วมือ

   การลงทะเบียนต้องสแกนนิ้วเดียวกันอย่างน้อย 2 ครั้ง เพื่อให้เซนเซอร์สร้าง Template และตรวจว่าภาพทั้งสองเป็นนิ้วเดียวกัน จากนั้นจึงบันทึก Template ไว้ในตำแหน่ง ID ที่กำหนด ตัวอย่างเช่น

ผู้ใช้งาน	**Fingerprint ID**
ผู้ใช้คนที่ 1	1
ผู้ใช้คนที่ 2	2
ผู้ดูแลระบบ	10

3. การสื่อสาร UART

   เซนเซอร์ลายนิ้วมือสื่อสารกับ Arduino ผ่าน UART โดยต่อแบบไขว้ดังนี้

   Sensor TX ➲ Arduino RX

   Sensor RX ➲ Arduino TX

ในการทดลองนี้กำหนด

➲Arduino D2 เป็น RX

➲Arduino D3 เป็น TX

ดังนั้นจึงต่อ

Sensor TX ➲ Arduino D2

Sensor RX ⬅ Arduino D3

4. การทำงานของ RFID

โมดูล RFID-RC522 อ่าน UID ของบัตรหรือแท็ก แล้วส่งให้ Arduino ผ่าน SPI เพื่อเปรียบเทียบกับรายการ UID ที่อนุญาต RC522 ต้องใช้ไฟเลี้ยง 3.3 V เท่านั้น ห้ามต่อ VCC เข้ากับ 5 V

5. วิธีตรวจสอบสิทธิ์ ใบงานนี้ใช้เงื่อนไขแบบ OR ดังนี้

RFID ถูกต้อง OR ลายนิ้วมือถูกต้อง ➲ อนุญาตให้เปิดประตู

ระบบจะปฏิเสธเมื่อ

RFID ไม่ถูกต้อง หรือไม่พบลายนิ้วมือในฐานข้อมูล

หากต้องการ Multi-factor Authentication ต้องเปลี่ยนเงื่อนไขเป็น

RFID ถูกต้อง AND ลายนิ้วมือถูกต้อง ➲ อนุญาตให้เปิดประตู

6. การควบคุมกลอนประตู

Arduino ไม่สามารถจ่ายกระแสให้กลอนโซลินอยด์โดยตรง จึงต้องใช้โมดูลรีเลย์เป็นตัวควบคุมแหล่งจ่ายไฟของกลอน

สำหรับกลอนชนิดจ่ายไฟเพื่อปลดล็อก ให้ต่อผ่าน COM และ NO เพื่อให้กลอนได้รับไฟเฉพาะขณะอนุญาตให้เปิดประตู

ลำดับขั้นตอนการปฏิบัติงาน

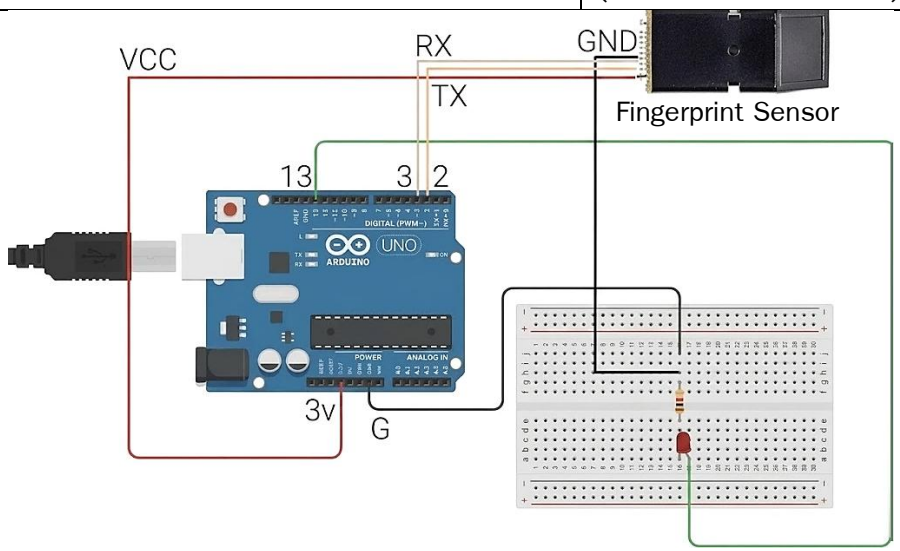
ตอนที่ 9.1

การลงทะเบียนและทดสอบเซนเซอร์ลายนิ้วมือ

1.1 การเชื่อมต่อกับไมโครคอนโทรลเลอร์ Arduino UNO

การเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือ โดยเชื่อมต่อเซนเซอร์ลายนิ้วมือ รุ่นJM101B ประกอบด้วยขาที่ใช้งานที่สำคัญ 4 ขา ได้แก่ VCC, GND, TX, และ RX โดยสามารถเชื่อมต่อกับไมโครคอนโทรลเลอร์ Arduino UNO ดังรูปที่ รูปที่ 9.1 และตารางที่ 9.1

	ใบงานที่ 9 เรื่อง ระบบประตูอัจฉริยะด้วยเทคโนโลยี ตรวจสอบลายนิ้วมือร่วมกับ RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)



รูปที่ 9.1 แผนผังการเชื่อมต่อเซนเซอร์สแกนลายนิ้วมือกับไมโครคอนโทรลเลอร์เบื้องต้น

ตารางที่ 9.1 การเชื่อมต่อขาเซนเซอร์ลายนิ้วมือกับไมโครคอนโทรลเลอร์ Arduino UNO

ขาเซนเซอร์	เชื่อมต่อกับ Arduino UNO	หน้าที่
VCC	5V	จ่ายไฟเลี้ยงให้เซนเซอร์
GND	GND	กราวด์ร่วมของระบบ
TX	ขา Digital 2 (D2)	ส่งข้อมูลจากเซนเซอร์ไปยัง Arduino
RX	ขา Digital 3 (D3)	รับข้อมูลจาก Arduino

1.2. การทำงานของระบบ

1.2.1) ขั้นตอนที่ 1 การเริ่มต้นระบบ

เมื่อเชื่อมต่อ Arduino กับคอมพิวเตอร์ผ่านสาย USB ทำให้ Arduino จะได้รับพลังงานไฟฟ้า 5 V เซนเซอร์ลายนิ้วมือได้รับไฟเลี้ยงจากขา 5 V และโปรแกรมใน Arduino เริ่มทำงานและสร้างการสื่อสารแบบ Serial กับเซนเซอร์

1.2.2) ขั้นตอนที่ 2 การสแกนลายนิ้วมือ

เมื่อผู้ใช้นำปลายนิ้วสัมผัสบนหน้าสแกนของเซนเซอร์ เซนเซอร์จะทำการ (1) ตรวจจับภาพลายนิ้วมือ (2) แปลงภาพเป็นข้อมูลดิจิทัล และ (3) วิเคราะห์จุดลักษณะเฉพาะของลายนิ้วมือ เช่น จุดสิ้นสุดของเส้นลายและจุดแตกแขนงของเส้นลาย

1.2.3) ขั้นตอนที่ 3 การส่งข้อมูลไปยัง Arduino

หลังจากอ่านลายนิ้วมือแล้ว เซนเซอร์จะส่งข้อมูลผ่านขา TX ไปยัง Arduino ผ่านการสื่อสารแบบ UART serial ส่วน Arduino จะรับข้อมูลผ่านขา D2 และนำไปประมวลผลตามโปรแกรมที่กำหนด

1.2.4) ขั้นตอนที่ 4 การเปรียบเทียบลายนิ้วมือ

หากมีการลงทะเบียนลายนิ้วมือไว้ในหน่วยความจำของเซนเซอร์แล้วเซนเซอร์จะทำการ (1) เปรียบเทียบลายนิ้วมือที่อ่านได้ (2) ค้นหารหัสประจำตัว (ID) และ (3) ส่งผลการตรวจสอบกลับมายัง Arduino

1.2.5) บันทึกผลการทดลองในตารางที่ 9.2

ตารางที่ 9.2 การลงทะเบียนลายนิ้วมือ

ID	นิ้วที่ใช้	ครั้งที่ 1	ครั้งที่ 2	บันทึกสำเร็จ	หมายเหตุ
1					
2					
3					

ตารางที่ 9.3 ผลการค้นหาลายนิ้วมือ

ครั้งที่	นิ้วที่ทดสอบ	ID ที่คาดหวัง	ID ที่ตรวจพบ	Confidence	ผล
1	ลงทะเบียนแล้ว				
2	ลงทะเบียนแล้ว				
3	ลงทะเบียนแล้ว				
4	ไม่ได้ลงทะเบียน				
5	ไม่ได้ลงทะเบียน				

1.2.6) ขั้นตอนที่ 5 การแสดงผล เมื่อ Arduino ได้รับผลการตรวจสอบ

กรณีตรวจสอบสำเร็จ ซึ่ง (1) ตรวจพบลายนิ้วมือในฐานข้อมูล (2) แสดงหมายเลข ID ผ่าน Serial Monitor และ (3) LED ที่ต่อกับขา D13 ติดสว่าง

กรณีตรวจสอบไม่สำเร็จ จะ (1) ไม่พบข้อมูลลายนิ้วมือ (2) แสดงข้อความแจ้งเตือนผ่าน serial monitor และ (3) LED ดับ หรือแสดงสถานะตามที่กำหนดในโปรแกรม (โปรแกรมควบวบคุมการทำงานดังภาคผนวก ก, Arduino Code: 11)

โดยสรุปวงจรนี้เป็นระบบตรวจสอบลายนิ้วมือเบื้องต้นที่ใช้เซนเซอร์สแกนลายนิ้วมือเชื่อมต่อกับ Arduino UNO ผ่านการสื่อสารแบบ UART โดยเซนเซอร์ทำหน้าที่อ่านและเปรียบเทียบลายนิ้วมือ ส่วน Arduino ทำหน้าที่รับข้อมูล ประมวลผล และแสดงผลผ่าน Serial Monitor และ LED แสดงสถานะ ซึ่งเป็นพื้นฐานสำคัญของระบบควบคุมการเข้า ออกและระบบรักษาความปลอดภัยด้วยเทคโนโลยีชีวมาตร (biometric security system) ในงานจริงต่อไป

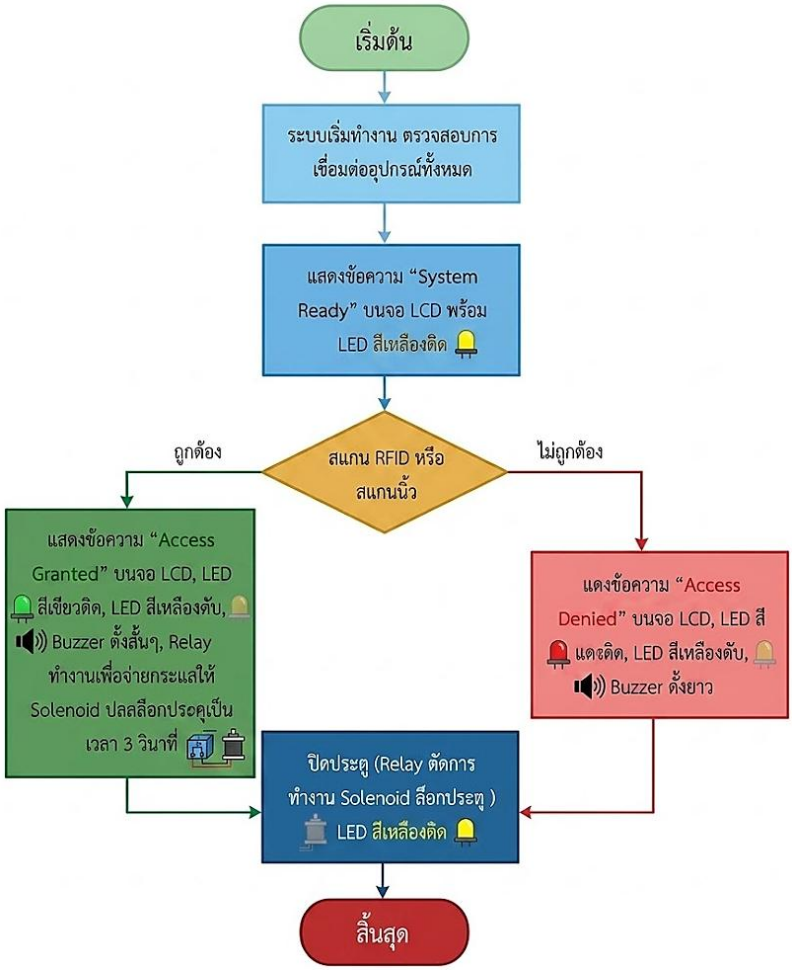
ตอนที่ 9.2

งานควบคุมการเข้า-ออกประตูด้วยการตรวจสอบลายนิ้วมือร่วมกับ RFID

เมื่อเปิดระบบ บอร์ด Arduino จะทำการตรวจสอบการเชื่อมต่อของอุปกรณ์ต่าง ๆ ได้แก่ โมดูล RFID, เซนเซอร์ลายนิ้วมือ, จอแสดงผล, LCD, Relay, LED, และ Buzzer หากอุปกรณ์ทั้งหมดพร้อมใช้งาน ระบบจะแสดงข้อความ “System Ready” บนจอ LCD และไฟ LED สีเหลืองจะติดสว่างเพื่อแสดงสถานะพร้อมทำงาน

จากรูปที่ 9.2 ระบบจะเข้าสู่โหมดรอการยืนยันตัวตน โดยผู้ใช้งานสามารถเลือกใช้ บัตรหรือแท็ก RFID หรือลายนิ้วมือ ในการขออนุญาตเข้าใช้งาน

หากข้อมูลบัตร RFID หรือข้อมูลลายนิ้วมือที่สแกนตรงกับข้อมูลที่บันทึกไว้ในฐานข้อมูล ระบบจะดำเนินการดังนี้



รูปที่ 9.2 แผนผังแสดงการทำงานของระบบการเข้า-ออกประตูด้วยการตรวจสอบลายนิ้วมือร่วมกับ RFID

- แสดงข้อความ “Access Granted” บนจอ LCD
- เปิดไฟ LED สีเขียว และดับไฟ LED สีเหลือง
- ส่งสัญญาณเสียงสั้นจาก Buzzer เพื่อแจ้งผลการอนุญาต
- สั่งงานRelayให้จ่ายกระแสไฟไปยังกลอนไฟฟ้า (solenoid lock) เพื่อปลดล็อก
- ประตูจะเปิดค้างไว้เป็นเวลา 3 s

เมื่อครบเวลาที่กำหนด ระบบจะสั่งปิด Relay ทำให้กลอนไฟฟ้ากลับเข้าสู่สถานะล็อกประตูอีกครั้ง พร้อมเปิดไฟ LED สีเหลืองเพื่อแสดงสถานะรอการใช้งานครั้งถัดไป

ในกรณีที่ข้อมูลบัตร RFID หรือลายนิ้วมือไม่ถูกต้อง ระบบจะดำเนินการดังนี้

- แสดงข้อความ “Access Denied” บนจอ LCD
- เปิดไฟ LED สีแดง และดับไฟ LED สีเหลือง
- ส่งสัญญาณเสียงเตือนยาวจาก Buzzer
- ไม่อนุญาตให้เปิดประตู

ระบบยังรองรับการเปิดประตูด้วย สวิตช์กด (push button) สำหรับการเข้าออกแบบแมนนวล (manual access) เมื่อกดสวิตช์ ระบบจะสั่งปลดล็อกประตูชั่วคราว จนครบเวลาที่กำหนด ระบบจะล็อกประตูโดยอัตโนมัติ จากนั้นกลับเข้าสู่โหมดรอการยืนยันตัวตนต่อไป

ลำดับขั้นตอนการปฏิบัติงาน

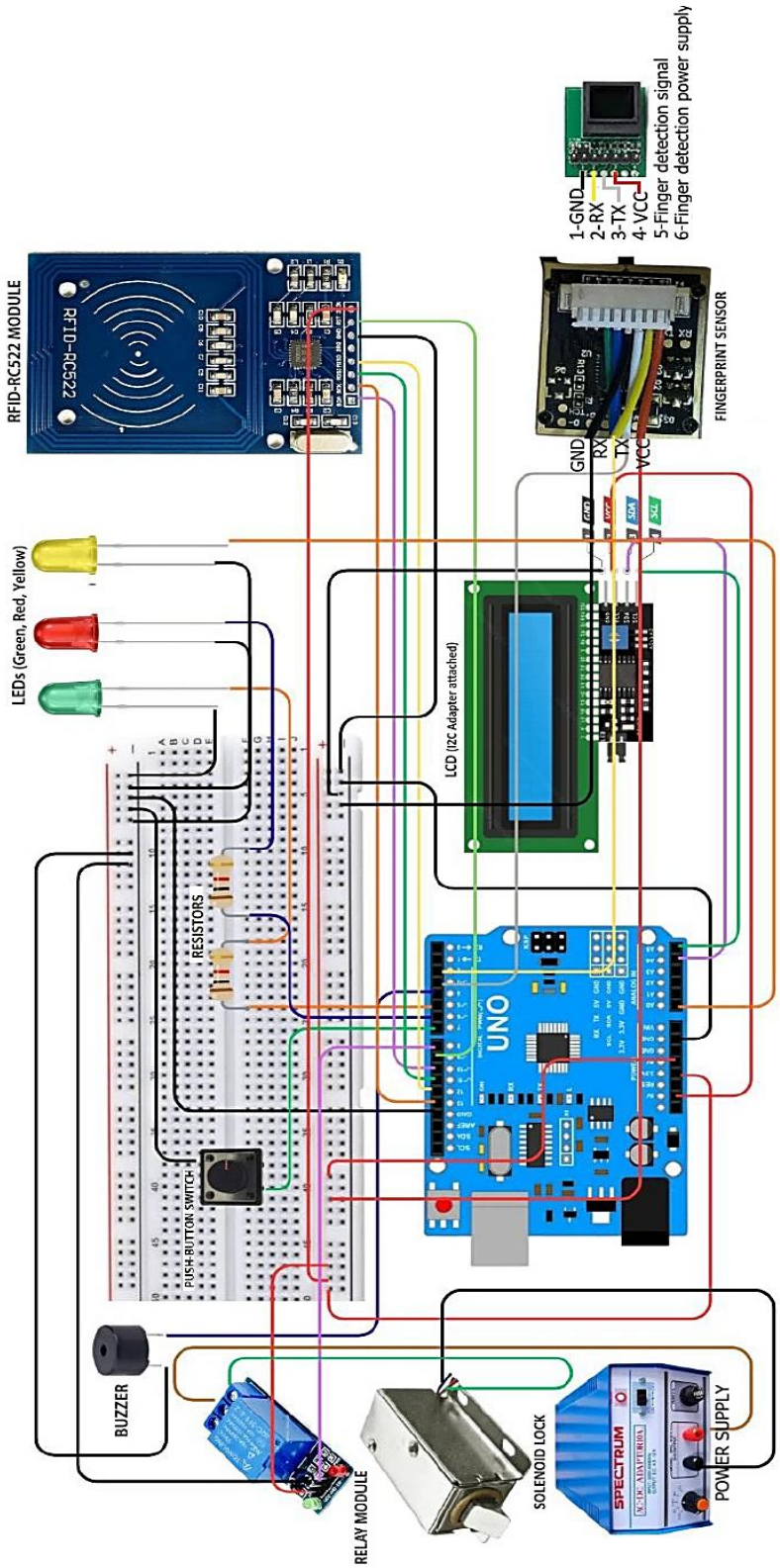
2.1 ต่อวงจรดังรูปที่ 9.3 และ ตารางที่ 9.4 การเชื่อมต่อบอร์ด Arduino UNO กับอุปกรณ์ต่าง ๆ ของระบบ

ตารางที่ 9.4 การเชื่อมต่อบอร์ด Arduino UNO กับอุปกรณ์ต่าง ๆ ของระบบ

ขาอุปกรณ์ / ชื่ออุปกรณ์	ตำแหน่งขา	ตำแหน่งขา Arduino UNO	หน้าที่
RFID (MFRC522)	VCC	3.3V	ใช้แรงดันไฟฟ้า 3.3V เท่านั้น
	GND	GND	ขากราวด์ร่วมของระบบ
	RST	D9	ขารีเซต (Reset) ของโมดูล RFID
	SDA (SS)	D10	ขาเลือกอุปกรณ์ (Slave Select) สำหรับการสื่อสารแบบ SPI
	MOSI	D11	ส่งข้อมูลจาก Arduino ไปยัง RFID (Master Out Slave In)
	MISO	D12	รับข้อมูลจาก RFID มายัง Arduino (Master In Slave Out)
	SCK	D13	ขาสัญญาณ Clock ของการสื่อสารแบบ SPI

ตารางที่ 9.4 การเชื่อมต่อบอร์ด Arduino UNO กับอุปกรณ์ต่าง ๆ ของระบบ (ต่อ)

ขาอุปกรณ์ / ชื่ออุปกรณ์	ตำแหน่งขา	ตำแหน่งขา Arduino UNO	หน้าที่
Fingerprint Sensor	VCC	5V	ใช้ไฟเลี้ยง 5V
	GND	GND	กราวด์ร่วมของระบบ
	TX	D2	ส่งข้อมูลจากเซนเซอร์ไปยัง Arduino (RX)
	RX	D3	รับข้อมูลจาก Arduino (TX) ไปยังเซนเซอร์
LCD (I²C Module)	VCC	5V	จ่ายไฟเลี้ยง 5V ให้จอ LCD
	GND	GND	กราวด์ร่วมของระบบ
	SDA	A4	ขาสื่อสารข้อมูล I²C (Data Line)
	SCL	A5	ขาสัญญาณนาฬิกา I²C (Clock Line)
Relay Module	IN	D8	ใช้ควบคุมการเปิด–ปิดRelay
	VCC	5V	จ่ายไฟเลี้ยงให้Relay
	GND	GND	กราวด์ร่วมกับ Arduino
Switch	ขา 1	D7	ใช้อ่านค่าสถานะของสวิตช์
	ขา 2	GND	เชื่อมต่อกับกราวด์ (GND)
อุปกรณ์อื่น ๆ	LED สีเขียว	D5	แสดงสถานะเมื่อระบบอนุญาตให้เข้าใช้งาน (Access Granted)
	LED สีแดง	D6	แสดงสถานะเมื่อระบบปฏิเสธการเข้าใช้งาน (Access Denied)
	LED สีเหลือง	A0	กระพริบแสดงสถานะขณะรอหรือกำลังสแกนข้อมูล
	Buzzer	D4	ส่งสัญญาณเสียงแจ้งเตือนเมื่อมีการเข้าออกหรือมีเหตุการณ์เกิดขึ้น



รูปที่ 2.98 วงจรการเชื่อมต่อการประยุกต์ใช้งานเทคโนโลยี RFID และการสแกนลายนิ้วมือ

2.2 เขียนโปรแกรมดังภาคผนวก ข (Arduino Code: 12)

1) ตรวจสอบขาที่กำหนดในโปรแกรมให้ตรงกับตาราง
2) กำหนด UID ของบัตรที่ได้รับอนุญาต
3) กำหนด Fingerprint ID ที่ได้รับอนุญาต
4) ตรวจสอบ I²C address ของ LCD
5) ตรวจสอบ Baud rate ของเซนเซอร์
6) ตรวจสอบลอจิก Active LOW หรือ Active HIGH ของรีเลย์
7) ตรวจสอบว่าคำสั่งเริ่มต้นกำหนดให้รีเลย์หยุดทำงาน
8) ตรวจสอบเวลาปลดล็อกเป็น 3 วินาที
9) กด Verify
10) แก้ไขข้อผิดพลาดจนคอมไพล์ผ่าน
11) เลือก Arduino UNO และ Port ให้ถูกต้อง
12) กด Upload
13) เปิด Serial Monitor
14) กด Reset
15) ตรวจสอบสถานะเริ่มต้น

2.3 บันทึกผลการทดลองในตารางที่ 9.5

ตารางที่ 6 ผลการตรวจสอบสิทธิ์

ครั้งที่	วิธีตรวจสอบ	UID/ID	ผลที่คาดหวัง	LCD	LED	Buzzer	Relay	กลอน	ผล
1.	RFID อนุญาต		เปิด						
2.	RFID อนุญาต		เปิด						
3.	RFID ไม่อนุญาต		ไม่เปิด						
4.	Fingerprint อนุญาต		เปิด						
5.	Fingerprint อนุญาต		เปิด						
6.	Fingerprint ไม่อนุญาต		ไม่เปิด						
7.	Push button	–	เปิด						

	ใบงานที่ 9 เรื่อง ระบบประตูอัจฉริยะด้วยเทคโนโลยีตรวจสอบลายนิ้วมือร่วมกับ RFID	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

สรุปผลการทดลอง

เอกสารอ้างอิง

ปิยะ โควินท์ทวีวัฒน์, วีระศักดิ์ ชื่นตา, สัญญา ควรคิด, วิโรจน์ บัวงาม, และ หฤทัย ดิ้นสกุล. (2551). *ระบบบ่งชี้ด้วยคลื่นความถี่วิทยุ.* มหาวิทยาลัยราชภัฏนครปฐม.

Aqib, M. (2018). *RFID and Keypad based door lock using Arduino*. Hackster.io. https://www.hackster.io/muhammad-aqib/rfid-and-Keypad-based-door-lock-using-arduino-89e1d5.

Duroc, Y. (2022). From Identification to Sensing: RFID Is One of the Key Technologies in the IoT Field. *Sensors*, *22*(19), 7523. https://doi.org/10.3390/s22197523.

Hangzhou Grow Technology Co., Ltd. (2011). *R307 fingerprint module user manual* (Version 1.20). Alldatasheet. https://www.alldatasheet.com/datasheet-pdf/view/1756584/GROW/R307.html.

Prabhu, S. (2026). *What is RFID? How it works? Interface RC522 RFID module with Arduino*. Last Minute Engineers. https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/.

Finkenzeller, K. (2010). *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication* (3rd ed.). Wiley.

Instructables. (2017, January 25). *Create an access control system with an 4x3 keypad & RFID-RC522!* https://www.instructables.com/Create-an-Access-Control-System-With-an-4x3-Keypad/.

Mohanan, V. (2021). *Interfacing R307 optical fingerprint scanner with Arduino boards for biometric authentication*. Circuitstate Electronics. https://www.circuitstate.com/tutorials/interfacing-r307-optical-fingerprint-scanner-with-arduino-boards-for-biometric-authentication/.

Violino, B. (2005). *A summary of RFID standards*. RFID Journal. https://www.rfidjournal.com/expert-views/a-summary-of-rfid-standards/76205/.

Samsung Display. (n.d.). *[Learn Display] 60. Fingerprint on Display (FoD).* Samsung Display Newsroom. https://global.samsungdisplay.com/30345/feed/.

3prabhakar. (2023, October 3). *How to write data in RFID tag using 4x4 keypad* [Online forum post]. Arduino Forum. https://forum.arduino.cc/t/how-to-write-data-in-rfid-tag-using-4x4-keypad/1174618.

	ใบงานที่ 10 เรื่อง งานติดตั้งและทดสอบระบบควบคุมการเข้า-ออกประตูด้วยเครื่องสแกนลายนิ้วมือ	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ติดตั้งและทดสอบระบบควบคุมการเข้า-ออกประตูด้วยเครื่องสแกนลายนิ้วมือในระบบรักษาความปลอดภัยได้

วัตถุประสงค์

1. ตรวจสอบพิกัดแรงดันก่อนต่ออุปกรณ์
2. ปิดแหล่งจ่ายไฟก่อนต่อหรือแก้ไขสาย
3. ระบุขั้ว 12V, GND, BUT, SEN, NO, COM และ NC ได้
4. เลือกวงจรควบคุมกลอนตามชนิด Fail-secure หรือ Fail-safe ได้
5. ตรวจสอบหน้าสัมผัสรีเลย์ด้วยมัลติมิเตอร์ได้
6. เปลี่ยนรหัสผู้ดูแลจากค่าเริ่มต้นได้
7. ลงทะเบียนลายนิ้วมืออย่างน้อย 2 ผู้ใช้ได้
8. เพิ่มบัตรและรหัสผ่านสำหรับเปิดประตูได้
9. ทดสอบปุ่มกดออกและเซนเซอร์ประตูได้
10. ตรวจสอบการล็อกกลับหลังครบเวลาที่กำหนดได้

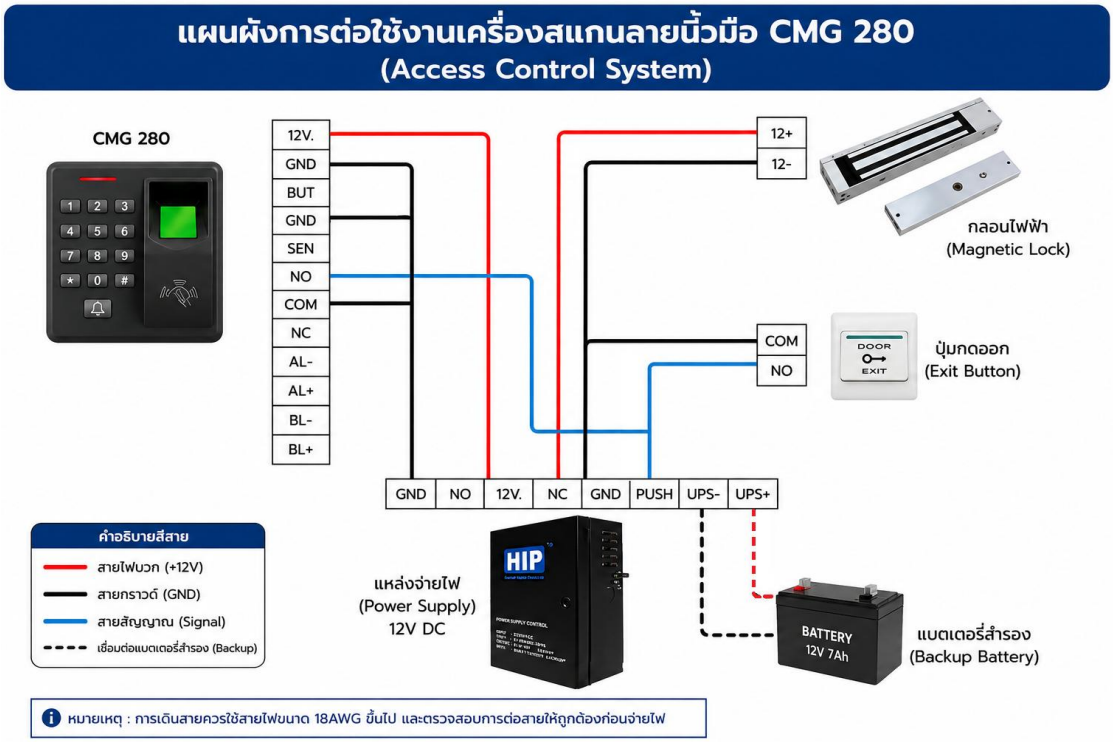
เครื่องมือและอุปกรณ์

1.	เครื่อง CMG 280	1 เครื่อง
2.	แผ่นยึดด้านหลังและสกรู	1 ชุด
3.	แหล่งจ่ายไฟ 12 VDC ตามพิกัดระบบ	1 ชุด
4.	กลอนไฟฟ้าหรือชุดจำลองกลอน	1 ชุด
5.	ปุ่มกดออก Exit Switch	1 ตัว
6.	Magnetic Door Contact หรือ Door Sensor	1 ชุด
7.	อุปกรณ์แจ้งเตือนภายนอก ถ้ามี	1 ชุด
8.	บัตรที่รองรับกับเครื่อง อย่างน้อย	2 ใบ
9.	ฟิวส์และฐานฟิวส์	1 ชุด
10.	ไดโอดป้องกันแรงดันย้อนสำหรับกลอน DC	1 ตัว
11.	สายไฟและขั้วต่อ	1 ชุด
12.	มัลติมิเตอร์	1 เครื่อง
13.	ไขควงปากแบนและปากแฉก	1 ชุด
14.	คีมปอกสายและคีมตัดสาย	1 ชุด
15.	สว่านและอุปกรณ์ยึดผนัง	ตามความเหมาะสม

16. เทปพันสายไฟหรือท่อหด 1 ชุด
17. ป้ายกำกับสายไฟ 1 ชุด

ความรู้พื้นฐานในการปฏิบัติงาน

การติดตั้งและทดสอบเครื่องสแกนลายนิ้วมือ โดยเลือกใช้เครื่องสแกนลายนิ้วมือรุ่น CMG 280 ซึ่งเป็นอุปกรณ์ควบคุมการเข้าออกที่รองรับการตรวจสอบตัวตนด้วยลายนิ้วมือ รหัสผ่าน และบัตรประจำตัว โดยสามารถเชื่อมต่อกับระบบกลอนประตูไฟฟ้าและอุปกรณ์เสริมต่าง ๆ เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยขององค์กร การติดตั้งและการทดสอบระบบอย่างถูกต้องจึงเป็นขั้นตอนสำคัญที่ช่วยให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ ลดความผิดพลาดในการใช้งาน และยืดอายุการใช้งานของอุปกรณ์ เนื้อหาภายในหัวข้อข้อนี้ประกอบด้วยหลักการทำงานของระบบสแกนลายนิ้วมือ รายละเอียดอุปกรณ์และส่วนประกอบ วิธีการติดตั้ง การกำหนดค่าพารามิเตอร์ การลงทะเบียนผู้ใช้งาน การทดสอบการทำงานของระบบ และแนวทางการแก้ไขปัญหาเบื้องต้น



รูปที่ 10.1 ผังการต่อใช้งานเครื่องสแกนลายนิ้วมือรุ่น CMG 280 (HIP, n.d.)

ลำดับขั้นตอนการปฏิบัติงาน

1. หลักการทำงานของเครื่องสแกนลายนิ้วมือ รุ่น CMG 280

เครื่องสแกนลายนิ้วมือ รุ่น CMG 280 เป็นอุปกรณ์ควบคุมการเข้าออก ที่ใช้เทคโนโลยีการตรวจสอบและยืนยันตัวตนด้วยลายนิ้วมือ รหัสผ่าน หรือบัตรประจำตัว เพื่อเพิ่มความปลอดภัยในการควบคุมการเข้าถึงพื้นที่ โดยมีหลักการทำงานดังนี้ (เอชไอพี โกลบอล จำกัด, 2015; HIP, n.d.)

1.1) เมื่อผู้ใช้งานทำการสแกนลายนิ้วมือและระบบสามารถยืนยันตัวตนได้ตรงกับข้อมูลที่บันทึกไว้ในหน่วยความจำ เครื่องจะส่งสัญญาณควบคุมไปยังกลอนประตูไฟฟ้า (electronic door lock) เพื่อปลดล็อกประตูให้สามารถเข้าใช้งานได้

1.2) ระบบสามารถเชื่อมต่อกับเซนเซอร์ตรวจสอบสถานะประตู (door sensor) เพื่อตรวจสอบว่าประตูอยู่ในสถานะเปิดหรือปิด หากประตูถูกเปิดโดยไม่ได้รับอนุญาต หรือปิดไม่สนิท ระบบจะส่งสัญญาณเตือนเพื่อแจ้งให้ผู้ดูแลระบบทราบ

1.3) เครื่องรองรับระบบป้องกันการงัดแงะ (tamper alarm) โดยหากอุปกรณ์ถูกถอดหรือรื้อถอนออกจากตำแหน่งติดตั้งโดยไม่ได้รับอนุญาต ระบบจะส่งสัญญาณเตือนทันที

1.4) ระบบสามารถเชื่อมต่อกับปุ่มกดออก (exit switch) เพื่อให้ผู้ใช้งานสามารถกดปุ่มสำหรับเปิดประตูจากด้านในได้อย่างสะดวกและปลอดภัย

1.5) เครื่องสามารถเชื่อมต่อกับอุปกรณ์สัญญาณเตือนภายนอก (external bell) หรือออดไฟฟ้า เพื่อใช้สำหรับแจ้งเตือนเหตุการณ์ต่าง ๆ ตามการตั้งค่าของระบบ

2. ขั้นตอนการติดตั้งเครื่องสแกนลายนิ้วมือ CMG 280 จากรูปที่ 10.2 ดังนี้

รูปที่ 10.2 ขั้นตอนการติดตั้งเครื่องสแกนลายนิ้วมือ CMG 280

2.1)ใช้ไขควงคลายน็อตยึดที่อยู่บริเวณด้านล่างของตัวเครื่องออก

2.2)ถอดแผ่นยึดด้านหลัง (back plate) ออกจากตัวเครื่องอย่างระมัดระวัง

2.3)นำแผ่นยึดด้านหลังไปกำหนดตำแหน่งติดตั้งบนผนัง จากนั้นเจาะและยึดแผ่นยึดเข้ากับผนังให้แน่นหนาด้วยสกรูที่เหมาะสม

2.4)นำตัวเครื่องสแกนลายนิ้วมือประกอบเข้ากับแผ่นยึดที่ติดตั้งไว้บนผนัง โดยจัดตำแหน่งให้ตรงกับรางหรือจุดล็อกของแผ่นยึด

2.5)ขันน็อตยึดบริเวณด้านล่างของตัวเครื่องให้แน่น เพื่อป้องกันการเคลื่อนตัวหรือการถอดเครื่องออกโดยไม่ได้รับอนุญาต

2.6)ตรวจสอบความแข็งแรงของการติดตั้งและความเรียบร้อยของตัวเครื่องก่อนดำเนินการเชื่อมต่อระบบไฟฟ้าและอุปกรณ์ต่าง ๆ

3. การตั้งค่าตัวเครื่อง

3.1) การเข้าสู่ระบบผู้ดูแล (Administrator Mode) การเข้าสู่ระบบผู้ดูแลระบบมีขั้นตอนดังนี้

3.3.1) กดปุ่ม * ตามด้วยปุ่ม #

3.3.2) ป้อนรหัสผ่านผู้ดูแลระบบ (ค่าเริ่มต้นจากโรงงานคือ 123456)

3.3.3) หากเข้าสู่ระบบสำเร็จ ไฟแสดงสถานะสีเขียวจะติดสว่าง และเครื่องจะส่งเสียงสัญญาณ (beep) จำนวน 1 ครั้ง

3.3.4) หากป้อนรหัสผ่านไม่ถูกต้อง ไฟแสดงสถานะสีแดงจะติดสว่าง และเครื่องจะส่งเสียงสัญญาณจำนวน 2 ครั้ง

เมื่อต้องการออกจากระบบ ให้กดปุ่ม * หรือหากไม่มีการใช้งานเครื่องเป็นเวลานานกว่า 20 s ระบบจะออกจากโหมดผู้ดูแลโดยอัตโนมัติ

3.2) การเปลี่ยนรหัสผ่านผู้ดูแลระบบ การเปลี่ยนรหัสผ่านผู้ดูแลระบบมีขั้นตอนดังนี้

3.2.1) เข้าสู่ระบบผู้ดูแลระบบ

3.2.2) กดปุ่ม 8 ตามด้วยหมายเลขลำดับผู้ดูแลระบบ (1-3)

3.2.3) ป้อนรหัสผ่านใหม่ จำนวน 6 หลัก

3.2.4) ป้อนรหัสผ่านใหม่อีกครั้งเพื่อยืนยัน

หากการเปลี่ยนรหัสผ่านสำเร็จ ไฟแสดงสถานะสีเขียวจะติดสว่าง และเครื่องจะส่งเสียงสัญญาณจำนวน 1 ครั้ง หากการเปลี่ยนรหัสผ่านไม่สำเร็จ ไฟแสดงสถานะสีแดงจะติดสว่างและเครื่องจะส่งเสียงสัญญาณจำนวน 2 ครั้ง

หมายเหตุ: ระบบรองรับรหัสผ่านผู้ดูแลระบบได้สูงสุด 3 รหัส เพื่อรองรับการบริหารจัดการโดยผู้ดูแลหลายคน

3.3) การเพิ่มผู้ใช้งาน

การเพิ่มผู้ใช้งานสามารถทำได้ทั้งรูปแบบลายนิ้วมือและบัตร โดยมีขั้นตอนดังนี้

3.3.1) เข้าสู่ระบบผู้ดูแลระบบ

3.3.2) กดปุ่ม 1 เครื่องจะส่งเสียงสัญญาณ (beep) จำนวน 1 ครั้ง

3.3.3) กรณีเพิ่มผู้ใช้งานด้วยลายนิ้วมือ ให้วางนิ้วบนเซนเซอร์จำนวน 3 ครั้ง โดยทุกครั้งที่วางนิ้ว เครื่องจะส่งเสียงตอบรับ

3.3.4) กรณีเพิ่มผู้ใช้งานด้วยบัตร ให้ทาบบัตรที่เครื่องอ่านจำนวน 1 ครั้ง

3.3.5) หากเพิ่มผู้ใช้งานสำเร็จ ไฟแสดงสถานะสีเขียวจะติดสว่าง และเครื่องจะส่งเสียงสัญญาณจำนวน 1 ครั้ง

3.3.6) หากเพิ่มผู้ใช้งานไม่สำเร็จ ไฟแสดงสถานะสีแดงจะติดสว่าง และเครื่องจะส่งเสียงสัญญาณจำนวน 2 ครั้ง

3.3.7) หากต้องการเพิ่มผู้ใช้งานต่อเนื่อง สามารถวางนิ้วหรือทาบบัตรของผู้ใช้งานรายถัดไปได้ทันที

4. บันทึกผลการทดลองในตารางที่ 10.1, 10.2

ตารางที่ 10.1 การลงทะเบียนลายนิ้วมือ

ลำดับผู้ใช้	นิ้วที่ใช้	สแกนครั้งที่ 1	สแกนครั้งที่ 2	สแกนครั้งที่ 3	ผล
1					
2					
3					

ตารางที่ 10.2 ผลทดสอบการยืนยันตัวตน

ครั้งที่	วิธีทดสอบ	ผู้ใช้/อุปกรณ์	ผลที่คาดหวัง	รีเลย์	กลอน	เวลาปลดล็อก	ผล
1.	ลายนิ้วมือที่ลงทะเบียน	User 1	เปิด				
2.	ลายนิ้วมือที่ลงทะเบียน	User 2	เปิด				
3.	ลายนิ้วมือไม่ลงทะเบียน	–	ไม่เปิด				
4.	บัตรที่ลงทะเบียน	Card 1	เปิด				
5.	บัตรไม่ลงทะเบียน	Card 2	ไม่เปิด				
6.	รหัสผ่านถูกต้อง	PW 1	เปิด				
7.	รหัสผ่านผิด	–	ไม่เปิด				
8.	Exit Switch	–	เปิด				

สรุปผลการทดลอง

เอกสารอ้างอิง

เอชไอพี โกลบอล จำกัด. (2015). *คู่มือการใช้งาน CMG 280* [คู่มือผลิตภัณฑ์]. https://hip-servicecenter.com/newpro/download/คู่มือการใช้งาน%20Standalone%20Access%20Control%20CMG%20280.pdf.

HIP. (ม.ป.ป.). *คู่มือการใช้งาน Standalone Access Control CMG 280* [คู่มือการใช้งาน]. HIP Service Center. https://hip-servicecenter.com/newpro/download/คู่มือการใช้งาน%20Standalone%20Access%20Control%20CMG%20280.pdf.

P.CCTV Network Engineering Co., Ltd. (n.d.). *HIP access control—Manual*. https://www.pi-tech.biz/17131669/hip-access-control-manual.

	ใบงานที่ 11 เรื่อง ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ประยุกต์ใช้เทคโนโลยีจดจำใบหน้าในงานระบบรักษาความปลอดภัยได้

วัตถุประสงค์

1. ตรวจพบกล้องและเปิดภาพสดได้
2. เก็บภาพใบหน้าของผู้ใช้แต่ละคนได้อย่างเหมาะสม
3. ตรวจจับใบหน้าในภาพได้
4. แยกผู้ใช้ที่ลงทะเบียนกับบุคคลที่ไม่รู้จักได้
5. อ่านค่าอุณหภูมิจากเซนเซอร์อย่างน้อย 3 ครั้งต่อเหตุการณ์ได้
6. กำหนดสถานะ LED ตรงกับขั้นตอนการทำงานได้
7. สั่งรีเลย์ทำงานตามเวลาที่กำหนดได้
8. ป้องกันไม่ให้กลอนเปิดเมื่อระบบเริ่มต้นหรือโปรแกรมขัดข้องได้
9. ส่งข้อมูลเหตุการณ์ไปยัง Google Sheets ได้
10. ส่งข้อความแจ้งเตือนไปยัง LINE ได้

เครื่องมือและอุปกรณ์

1.	Raspberry Pi 3B+	1 บอร์ด
2.	MicroSD Card พร้อม Raspberry Pi OS	1 ใบ
3.	แหล่งจ่ายไฟสำหรับ Raspberry Pi ตามพิกัด	1 ชุด
4.	USB Webcam	1 ตัว
5.	เซนเซอร์ GY-906 หรือ MLX90614	1 โมดูล
6.	LCD 16×2 พร้อม I²C Module	1 ชุด
7.	โมดูลรีเลย์ที่รับลอจิก 3.3 V ได้	1 โมดูล
8.	กลอนประตูโซลินอยด์ DC	1 ตัว
9.	แหล่งจ่ายไฟสำหรับกลอนตามพิกัด	1 ชุด
10.	ฟิวส์และฐานฟิวส์	1 ชุด
11.	ไดโอดป้องกันแรงดันย้อน เช่น 1N4007	1 ตัว
12.	LED สีน้ำเงิน สีเหลือง สีเขียว และสีแดง สีละ	1 ดวง
13.	ตัวต้านทาน 220–330 Ω	4 ตัว
14.	เซนเซอร์ตรวจจับวัตถุหรือ Exit Sensor	1 ตัว
15.	Push Button สำหรับใช้แทนเซนเซอร์ทางออก	1 ตัว

16. Breadboard และสาย Jumper 1 ชุด
17. มัลติมิเตอร์ 1 เครื่อง
18. จอภาพ Keyboard และ Mouse หรือคอมพิวเตอร์สำหรับ SSH 1 ชุด
19. เราเตอร์ที่เชื่อมต่ออินเทอร์เน็ต 1 เครื่อง
20. ขาตั้งสำหรับ Webcam และ GY-906 1 ชุด
21. ซอฟต์แวร์ที่ใช้ Raspberry Pi OS, Python, OpenCV (OpenCV Contrib สำหรับฟังก์ชันจดจำใบหน้าบางวิธี), NumPy, ไลบรารีอ่านค่า MLX90614, ไลบรารี GPIO เช่น gpiozero, ไลบรารีควบคุม LCD, requests สำหรับส่ง HTTP/HTTPS, Google Apps Script,LINE Messaging API

ความรู้พื้นฐานในการปฏิบัติงาน

1. การตรวจจับและการจดจำใบหน้า

การตรวจจับใบหน้าและการจดจำใบหน้าเป็นคนละขั้นตอน

- Face Detection: ตรวจว่าภายในภาพมีใบหน้าอยู่บริเวณใด
- Face Recognition: เปรียบเทียบใบหน้าที่ตรวจพบกับข้อมูลที่ลงทะเบียนไว้

ระบบต้องตรวจจับใบหน้าก่อน จึงนำข้อมูลใบหน้าไปเปรียบเทียบกับฐานข้อมูล

2. เกณฑ์การจดจำ

ระบบจดจำใบหน้ามักให้ค่าความเหมือน ระยะห่าง หรือ Confidence โปรแกรมต้องกำหนด Threshold ที่เหมาะสม หากกำหนดเกณฑ์ง่ายเกินไป อาจเกิด False Acceptance คือยอมรับบุคคลที่ไม่ถูกต้อง หากกำหนดเข้มเกินไป อาจเกิด False Rejection คือปฏิเสธผู้ใช้ที่ถูกต้อง จึงต้องทดสอบหลายสภาพ เช่น

- ระยะห่างต่างกัน
- มุมใบหน้าต่างกัน
- แสงมากและแสงน้อย
- สวมแว่นตา
- มีบุคคลอื่นอยู่ในภาพ

3. Google Sheets

ระบบสามารถส่งข้อมูลไปยัง Google Apps Script Web App ผ่าน HTTPS แล้วให้สคริปต์เพิ่มข้อมูลใน Google Sheets ฟังก์ชันเว็บแอปโดยทั่วไปใช้ doPost(e) รับข้อมูลจาก Raspberry Pi ตามแนวทาง (https://developers.google.com/apps-script/guides/web) โดยข้อมูลที่บันทึกอาจประกอบด้วย วันที่, เวลา, ชื่อหรือรหัสผู้ใช้, อุณหภูมิ, สถานะ, วิธีเปิดประตู

4. LINE Messaging API

Raspberry Pi ส่ง Push message ไปยัง

https://api.line.me/v2/bot/message/push

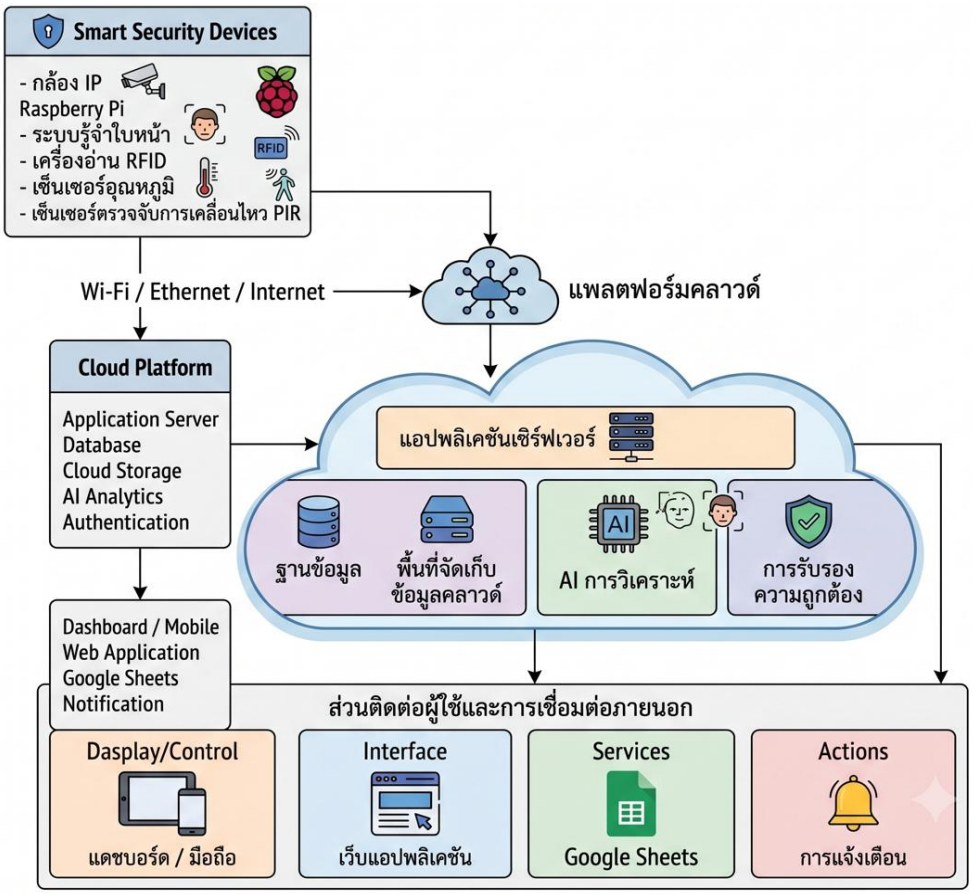
โดยใช้ Channel access token และ User ID หรือ Group ID ตามข้อกำหนดของ (https://developers.line.biz/en/docs/messaging-api/sending-messages/)

5. การทำงานของรีเลย์และกลอน

Raspberry Pi ไม่สามารถจ่ายกระแสให้กลอนหรือขดลวดรีเลย์เปล่าโดยตรง ต้องใช้โมดูลรีเลย์หรือวงจรขับที่รองรับลอจิก 3.3 V และใช้แหล่งจ่ายไฟแยกสำหรับกลอน

6. ระบบควบคุมการเข้า-ออกประตูด้วยเทคโนโลยีจดจำใบหน้า

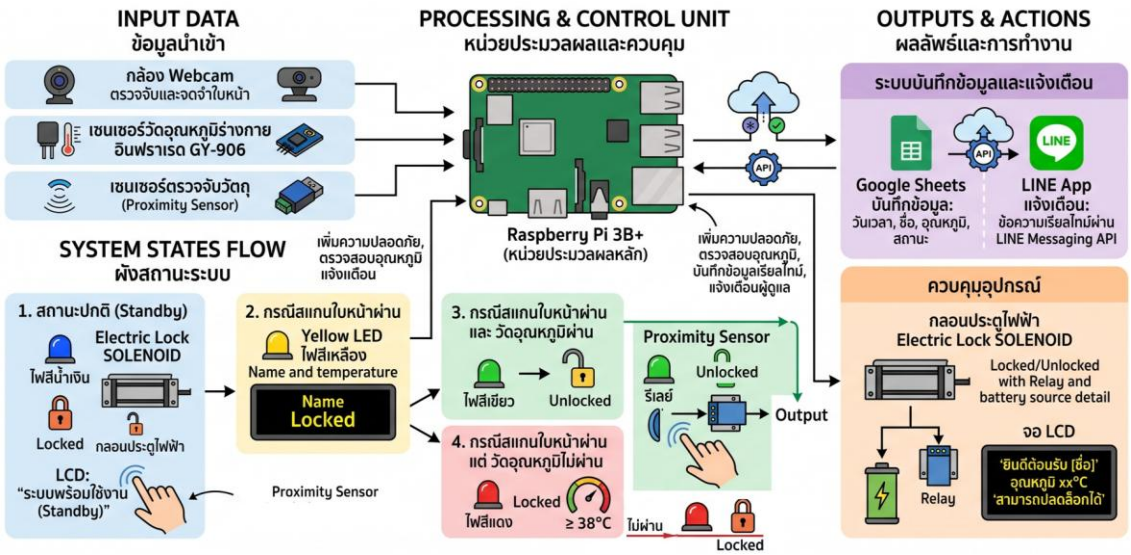
ระบบที่พัฒนาขึ้นประกอบด้วยอุปกรณ์รับข้อมูล ได้แก่ กล้อง webcam สำหรับตรวจจับและจดจำใบหน้า เซนเซอร์วัดอุณหภูมิ และเซนเซอร์ตรวจจับวัตถุ โดยมี Raspberry Pi 3B+ ทำหน้าที่เป็นหน่วยประมวลผลหลักของระบบ เมื่อได้รับข้อมูลจากอุปกรณ์ต่าง ๆ ระบบจะทำการวิเคราะห์และตัดสินใจควบคุมการทำงานของกลอนประตูไฟฟ้า พร้อมทั้งบันทึกข้อมูลและแจ้งเตือนไปยังผู้ดูแลระบบผ่าน Google Sheets และ LINE application แนวคิดการออกแบบระบบดังรูปที่ 11.1



รูปที่ 11.1 การออกแบบระบบควบคุมการเข้า-ออกประตูด้วยเทคโนโลยีจดจำใบหน้า

	ใบงานที่ 11 เรื่อง ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ระบบควบคุมการเข้าออกประตูอัจฉริยะที่พัฒนาขึ้นใช้ Raspberry Pi 3B+ เป็นศูนย์กลางในการประมวลผลข้อมูลจากกล้อง webcam เซนเซอร์วัดอุณหภูมิ และ และเซนเซอร์ตรวจจับวัตถุ โดยใช้การยืนยันตัวตนด้วยเทคโนโลยีจดจำใบหน้า (face recognition) ร่วมกับการคัดกรองอุณหภูมิร่างกาย เพื่อเพิ่มความปลอดภัยในการเข้าใช้งานพื้นที่ พร้อมทั้งรองรับการบันทึกข้อมูลบน Google Sheets และการแจ้งเตือนผ่าน LINE application แบบเรียลไทม์ ทำให้สามารถตรวจสอบและติดตามการเข้า ดังรูปที่ 11.2 มีรายละเอียดดังต่อไปนี้



รูปที่ 11.2 แนวคิดการออกแบบระบบจดจำใบหน้าในระบบรักษาความปลอดภัย

6.1) สถานะปกติ (Standby)

เมื่อระบบเริ่มทำงาน กลอนประตูไฟฟ้า (electric lock assembly solenoid) จะอยู่ในสถานะล็อก (locked) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และไฟแสดงสถานะสีน้ำเงิน (blue LED) จะติดสว่างเพื่อแสดงว่าระบบพร้อมใช้งาน นอกจากนี้จอ LCD จะแสดงข้อความ "ระบบพร้อมใช้งาน (standby)"

6.2) กรณีสแกนใบหน้าผ่าน

เมื่อผู้ใช้งานยืนอยู่หน้ากล้อง Webcam ระบบจะดำเนินการตรวจจับใบหน้า (face detection) และเปรียบเทียบข้อมูลใบหน้ากับฐานข้อมูลที่จัดเก็บไว้ หากพบว่าข้อมูลใบหน้าตรงกับข้อมูลในฐานข้อมูลตามเกณฑ์ที่กำหนด ระบบจะแสดงชื่อผู้ใช้งานบนจอ LCD

ในขั้นตอนนี้ ไฟสีน้ำเงินจะดับลง และไฟสีเหลือง (yellow LED) จะติดสว่าง เพื่อแสดงว่าระบบอยู่ในขั้นตอนการตรวจสอบข้อมูลเพิ่มเติมก่อนอนุญาตให้เข้าใช้งาน

6.3) กรณีสแกนใบหน้าผ่านและวัดอุณหภูมิผ่าน

หลังจากยืนยันตัวตนสำเร็จ ระบบจะทำการวัดอุณหภูมิร่างกายด้วยเซนเซอร์ GY-906 หากอุณหภูมิร่างกายมีค่าน้อยกว่า 38 องศาเซลเซียส ซึ่งอยู่ในเกณฑ์ที่กำหนด ระบบจะอนุญาตให้เข้าใช้งาน

จอ LCD จะแสดงชื่อผู้ใช้งาน ค่าอุณหภูมิ และข้อความ “สามารถปลดล็อกได้” พร้อมทั้งไฟสีเหลืองดับ ไฟสีเขียว (green LED) ติดสว่าง จากนั้น Raspberry Pi จะสั่งงาน Relay เพื่อปลดล็อกกลอนประตูไฟฟ้า

เมื่อการเข้าใช้งานสำเร็จ ระบบจะบันทึกข้อมูลผู้ใช้งาน วันที่ เวลา และค่าอุณหภูมิลงใน Google Sheets ผ่าน Google cloud และส่งข้อความแจ้งเตือนไปยัง LINE application ของผู้ดูแลระบบ

6.4) กรณีสแกนใบหน้าผ่านแต่วัดอุณหภูมิไม่ผ่าน

หากระบบสามารถยืนยันตัวตนจากใบหน้าได้ แต่ตรวจพบว่าอุณหภูมิร่างกายมีค่าตั้งแต่ 38 องศาเซลเซียสขึ้นไป ระบบจะไม่อนุญาตให้เข้าใช้งาน

จอ LCD จะแสดงชื่อผู้ใช้งาน ค่าอุณหภูมิ และข้อความ “ไม่สามารถปลดล็อกได้” พร้อมทั้งไฟสีน้ำเงินดับ และไฟสีแดง (red LED) ติดสว่าง เพื่อแจ้งเตือนว่าการตรวจสอบไม่ผ่าน

ในกรณีนี้ กลอนประตูจะยังคงอยู่ในสถานะล็อก และระบบจะบันทึกข้อมูลการตรวจสอบลงใน Google Sheets พร้อมทั้งส่งข้อความแจ้งเตือนไปยัง LINE application เพื่อให้ผู้ดูแลระบบทราบเหตุการณ์ดังกล่าว

6.5) กรณีปลดล็อกด้วยเซนเซอร์ตรวจจับวัตถุ

ระบบรองรับการปลดล็อกประตูผ่านเซนเซอร์ตรวจจับวัตถุ สำหรับการออกจากพื้นที่หรือการใช้งานในกรณีพิเศษ เมื่อเซนเซอร์ตรวจพบวัตถุภายในระยะที่กำหนด ระบบจะส่งสัญญาณไปยัง Raspberry Pi เพื่อประมวลผล

จอ LCD จะแสดงข้อความ “สามารถปลดล็อกได้” ไฟสีน้ำเงินจะดับ และไฟสีเขียวจะติดสว่าง จากนั้นระบบจะสั่งปลดล็อกกลอนประตูไฟฟ้า พร้อมทั้งบันทึกข้อมูลการใช้งานลงใน Google Sheets และส่งข้อความแจ้งเตือนไปยัง LINE application

6.6) การบันทึกข้อมูลและแจ้งเตือน

ทุกเหตุการณ์ที่เกิดขึ้นภายในระบบ ไม่ว่าจะเป็นการยืนยันตัวตนสำเร็จ การตรวจวัดอุณหภูมิไม่ผ่าน หรือการปลดล็อกผ่านเซนเซอร์ตรวจจับวัตถุ จะถูกบันทึกลงใน Google Sheets ประกอบด้วยข้อมูลสำคัญ ได้แก่ วันและเวลาที่ใช้งาน ชื่อผู้ใช้งาน ค่าอุณหภูมิร่างกาย สถานะการอนุญาตเข้าใช้งาน และวิธีการปลดล็อกประตู

นอกจากนี้ ระบบยังส่งข้อความแจ้งเตือนแบบเรียลไทม์ผ่าน LINE Messaging API เพื่อให้ผู้ดูแลระบบสามารถติดตามสถานะการเข้าออกของผู้ใช้งาน ได้อย่างมีประสิทธิภาพ

	ใบงานที่ 11 เรื่อง ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

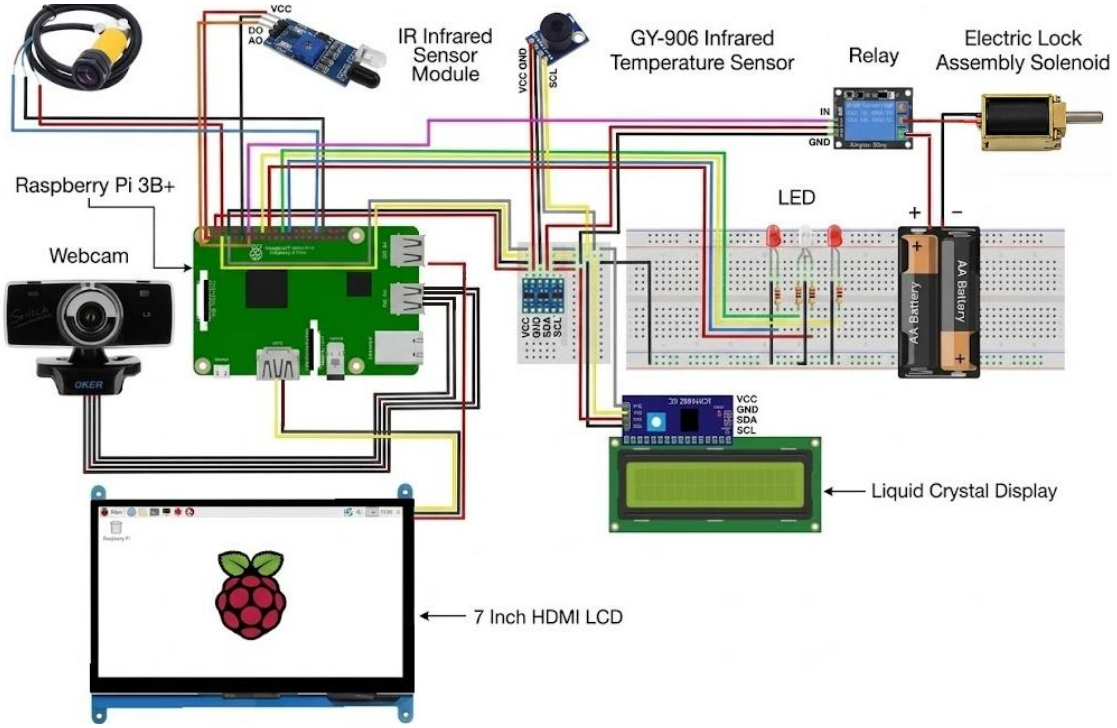
ขั้นตอนการปฏิบัติงาน

1. ต่อวงจรดังรูปที่ 11.3, 11.4 และตารางที่ 11.1

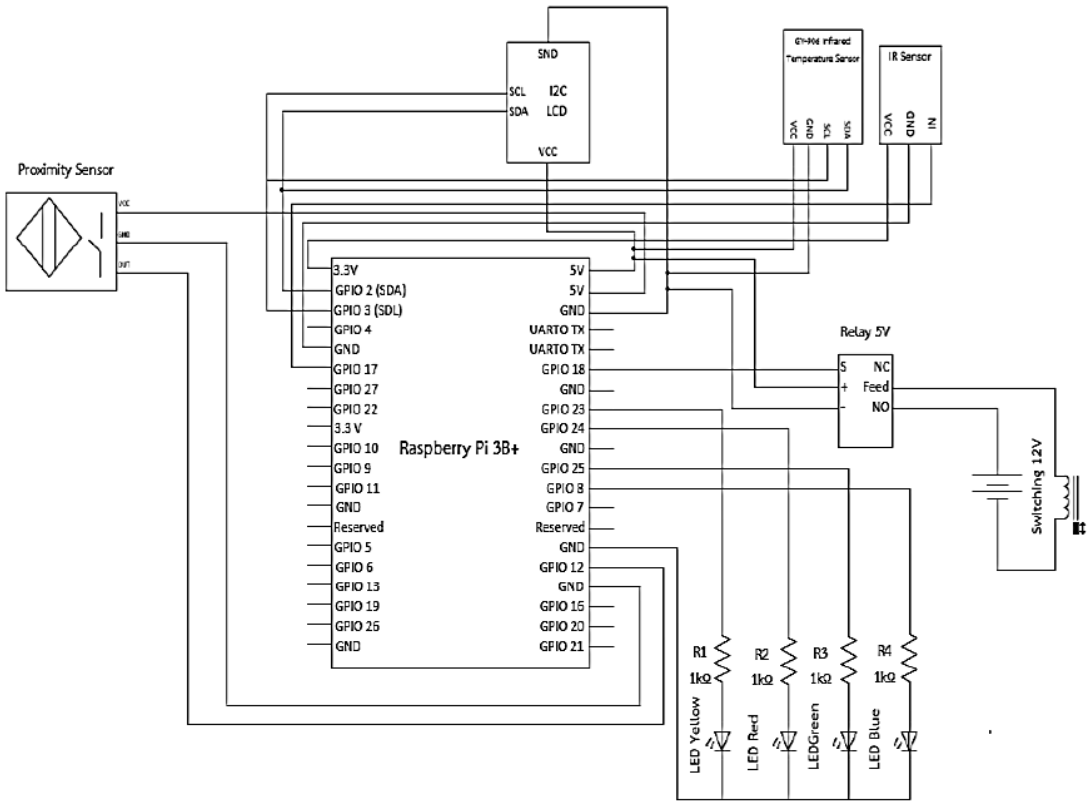
ตารางที่ 11.1 ตารางการต่อขาอุปกรณ์

ลำดับ	อุปกรณ์/สัญญาณ	ขาอุปกรณ์	Raspberry Pi/จุดต่อ
1	Webcam	USB	USB Port
2	HDMI Display	HDMI	HDMI Port
3	GY-906	SDA	GPIO2, Pin 3
4	GY-906	SCL	GPIO3, Pin 5
5	GY-906	VCC	3.3 V, Pin 1
6	GY-906	GND	GND, Pin 6
7	LCD I²C	SDA	GPIO2 ผ่าน Level Shifter
8	LCD I²C	SCL	GPIO3 ผ่าน Level Shifter
9	LCD I²C	VCC	5 V
10	LCD I²C	GND	GND
11	LED สีน้ำเงิน	Anode	GPIO17, Pin 11 ผ่าน R
12	LED สีเหลือง	Anode	GPIO27, Pin 13 ผ่าน R
13	LED สีเขียว	Anode	GPIO22, Pin 15 ผ่าน R
14	LED สีแดง	Anode	GPIO23, Pin 16 ผ่าน R
15	LED ทุกดวง	Cathode	GND
16	Exit Sensor	DO	GPIO25, Pin 22
17	Exit Sensor	AO	ไม่ต่อ
18	Relay	IN	GPIO24, Pin 18
19	Relay	VCC	5 V ตามพิกัด
20	Relay	GND	GND
21	แหล่งจ่ายกลอน	+12 V	ฟิวส์ > COM
22	Relay Contact	NO	ขั้วบวกกลอน
23	กลอน	ขั้วลบ	0 V ของแหล่งจ่าย 12 V
24	Flyback Diode	Cathode	ขั้วบวกกลอน
25	Flyback Diode	Anode	ขั้วลบกลอน

	ใบงานที่ 11 เรื่อง ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)



รูปที่ 11.3 แผนผังการเชื่อมต่อฮาร์ดแวร์ของระบบรักษาความปลอดภัยด้วยการจดจำใบหน้า



รูปที่ 11.4 วงจรระบบจดจำใบหน้าในระบบรักษาความปลอดภัย

	ใบงานที่ 11 เรื่อง ระบบควบคุมการเข้า–ออกประตูด้วยเทคโนโลยีจดจำใบหน้า	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ขั้นตอนการปฏิบัติงาน

1. ขั้นตอนที่ 1 ตรวจสอบอุปกรณ์ก่อนปฏิบัติงาน

1) ตรวจสอบรายการอุปกรณ์ให้ครบ ได้แก่ Raspberry Pi 3B+, MicroSD Card, USB Webcam, GY-906, LCD I²C, LED จำนวน 4 ดวง, IR Exit Sensor, Relay Module, กลอนประตู และแหล่งจ่ายไฟ

2) ตรวจสอบสภาพสายไฟและขั้วต่อว่าไม่มีรอยชำรุด

3) ตรวจสอบพิกัดอะแดปเตอร์ของ Raspberry Pi

4) ตรวจสอบแรงดันของกลอนประตู เช่น 12 VDC

5) ตรวจสอบว่าแหล่งจ่ายกลอนสามารถจ่ายกระแสได้เพียงพอ

6) ตรวจสอบว่า Relay Module รับสัญญาณควบคุมระดับ 3.3 V ได้

7) ตรวจสอบว่า GY-906 สามารถใช้ไฟเลี้ยง 3.3 V ได้

8) ตรวจสอบแรงดันเอาต์พุตของ IR Exit Sensor ว่าไม่เกิน 3.3 V

9) ตรวจสอบฟิวส์และไดโอดป้องกันแรงดันย้อน

10) ปิดแหล่งจ่ายไฟทั้งหมดก่อนต่อวงจร

ตารางที่ 1 การตรวจสอบอุปกรณ์

รายการ	**พิกัด/ค่าที่ตรวจพบ**	**ผล** (ผ่าน/ไม่ผ่าน)
อะแดปเตอร์ Raspberry Pi		
GY-906		
LCD I²C		
IR Exit Sensor		
Relay Module		
กลอนประตู		
แหล่งจ่ายกลอน		
ฟิวส์		
ไดโอด		

2. ขั้นตอนที่ 2 เตรียม Raspberry Pi และระบบปฏิบัติการ

1) ติดตั้ง Raspberry Pi OS ลงใน MicroSD Card

2) กำหนด Username และ Password

3) ใส่ MicroSD Card ลงใน Raspberry Pi

4) ต่อ Webcam, จอ HDMI, Keyboard และ Mouse

5) ต่อแหล่งจ่ายไฟให้ Raspberry Pi

6) รอจน Raspberry Pi OS เปิดใช้งานสำเร็จ

7) เชื่อมต่อ Raspberry Pi กับ Wi-Fi หรือ LAN

8) เปิด Terminal

9) ตรวจสอบ IP address ด้วยคำสั่ง

```
hostname -I
```

10) ตรวจสอบ Python ด้วยคำสั่ง

```
python3 –version
```

11) ตรวจสอบวันที่และเวลา หากวันที่หรือเขตเวลาผิด ให้แก้ไขก่อน เพราะจะทำให้ข้อมูลใน Google Sheets แสดงเวลาผิด

```
date
```

12) ทดสอบอินเทอร์เน็ต

```
ping -c 4 api.line.me
```

หากได้รับข้อความตอบกลับ แสดงว่า Raspberry Pi เชื่อมต่ออินเทอร์เน็ตได้

3. ขั้นตอนที่ 3 เปิดใช้งาน I²C

1) เปิด Terminal

2) พิมพ์คำสั่ง

```
sudo raspi-config
```

3) เลือก Interface Options

4) เลือก I2C

5) เลือก Yes เพื่อเปิดใช้งาน

6) เลือก Finish

7) Restart Raspberry Pi หากระบบแจ้งให้ดำเนินการ

8) ติดตั้งเครื่องมือตรวจสอบ I²C

```
sudo apt update
sudo apt install i2c-tools
```

9) ตรวจสอบอุปกรณ์บนบัส I²C

```
i2cdetect -y 1
```

10) ตรวจสอบ Address ที่ปรากฏบนหน้าจอ

11) ค่าที่คาดว่าจะพบ ได้แก่

```
GY-906  = 0x5A
```

LCD I²C = 0x27 หรือ 0x3F

12) บันทึก Address ที่ตรวจพบ

13) หากไม่พบ Address ให้ปิด Raspberry Pi แล้วตรวจ VCC, GND, SDA และ SCL

14) ห้ามสลับสายขณะ Raspberry Pi เปิดอยู่

4. ขั้นตอนที่ 4 เตรียมโฟลเดอร์และโปรแกรม Python

1) เปิด Terminal

2) สร้างโฟลเดอร์โครงการ

```
mkdir -p ~/smart-face-door
```

3) เข้าไปในโฟลเดอร์

```
cd ~/smart-face-door
```

4) สร้าง Python Virtual Environment

```
python3 -m venv --system-site-packages face-door-env
```

5) เปิดใช้งาน Virtual Environment

```
source face-door-env/bin/activate
```

6) เมื่อเปิดสำเร็จ จะเห็นชื่อ Environment ที่ด้านหน้าบรรทัดคำสั่ง เช่น

```
(face-door-env)
```

7) ติดตั้งไลบรารีพื้นฐาน

```
pip install numpy requests gpiozero
```

8) ติดตั้งไลบรารี GY-906 และ LCD ตามชนิดโมดูลที่ผู้สอนกำหนด

9) ตรวจสอบ OpenCV

```
python3 -c "import cv2; print(cv2.__version__)"
```

10) หากโปรแกรมแสดงหมายเลขเวอร์ชัน แสดงว่า OpenCV พร้อมใช้งาน

11) หากโปรแกรมใช้ cv2.face ให้ตรวจสอบด้วย

```
python3 -c "import cv2; print(hasattr(cv2, 'face'))"
```

12) หากแสดง False ให้ติดตั้ง OpenCV Contrib หรือนำ Environment ที่ผู้สอนเตรียมไว้มาใช้

13) สร้างโฟลเดอร์สำหรับข้อมูล

```
mkdir -p dataset
mkdir -p models
```

```
mkdir -p logs
mkdir -p config
```

โครงสร้างโฟลเดอร์ควรเป็นดังนี้

```
smart-face-door/
├── dataset/
├── models/
├── logs/
├── config/
├── capture_faces.py
├── train_faces.py
├── test_camera.py
├── test_temperature.py
├── test_gpio.py
├── test_cloud.py
└── main.py
```

5. ขั้นตอนที่ 5 กำหนดค่าของระบบ สร้างไฟล์สำหรับเก็บค่าตั้งต้น เช่น

```
config/settings.json
```

ค่าที่ต้องกำหนดประกอบด้วย

- หมายเลข GPIO ของ LED
- หมายเลข GPIO ของรีเลย์
- หมายเลข GPIO ของ Exit Sensor
- I²C Address ของ LCD
- I²C Address ของ GY-906
- Threshold ของการจดจำใบหน้า
- เกณฑ์อุณหภูมิสำหรับการทดลอง
- ระยะเวลาปลดล็อก
- Google Apps Script URL
- LINE User ID หรือ Group ID

ข้อมูลลับ เช่น Channel access token ไม่ควรเขียนไว้ในโปรแกรมหลัก ให้เก็บใน Environment Variable เช่น

```
export LINE_ACCESS_TOKEN="ใส่_TOKEN_จริง"
export LINE_TO_ID="ใส่_USER_ID_จริง"
```

ห้ามถ่ายภาพหรือเผยแพร่ค่าดังกล่าวในรายงานสู่สาธารณะ

5. ขั้นตอนที่ 5 เขียนและทดสอบโปรแกรม Webcam

1) เปิดไฟล์ test_camera.py
2) เขียนโปรแกรมเปิด Webcam ด้วย OpenCV

3) กำหนดหมายเลขกล้องเริ่มต้นเป็น 0
4) อ่านภาพทีละเฟรม
5) แสดงภาพในหน้าต่าง
6) กำหนดให้กดปุ่ม q เพื่อปิดโปรแกรม
7) บันทึกไฟล์
8) รันโปรแกรม

```
python3 test_camera.py
```

9) ตรวจสอบว่าภาพจาก Webcam ปรากฏ
10) ปรับตำแหน่งกล้องให้อยู่ระดับใบหน้า
11) ตรวจสอบแสงด้านหน้า
12) หลีกเลี่ยงแสงย้อน
13) บันทึกระยะที่เห็นใบหน้าชัดเจน
14) หากไม่พบกล้อง ให้ตรวจสอบ

```
ls -l /dev/video*
```

6. ขั้นตอนที่ 6 เก็บข้อมูลใบหน้า

1) ขอความยินยอมจากผู้ใช้ก่อนถ่ายภาพ
2) กำหนดรหัสผู้ใช้ เช่น USER001
3) สร้างโฟลเดอร์สำหรับผู้ใช้

```
mkdir -p dataset/USER001
```

4) เปิดโปรแกรม capture_faces.py
5) ให้ผู้ใช้ยืนในตำแหน่งที่กำหนด
6) ตรวจสอบว่าในภาพมีใบหน้าเพียงคนเดียว
7) เก็บภาพใบหน้าตรง
8) เก็บภาพหันซ้ายเล็กน้อย
9) เก็บภาพหันขวาเล็กน้อย
10) เก็บภาพก้มและเงยเล็กน้อย
11) เก็บภาพในสภาพแสงที่แตกต่างเล็กน้อย
12) ตรวจสอบภาพที่บันทึก
13) ลบภาพที่เบลอ มืด หรือมีใบหน้าหลายคน
14) ทำซ้ำกับผู้ใช้คนอื่น เช่น USER002
15) ห้ามใช้ชื่อ-นามสกุลเต็มเป็นชื่อไฟล์ หากไม่จำเป็น
16) จำกัดสิทธิ์เข้าถึงโฟลเดอร์ข้อมูล

7. ขั้นตอนที่ 7 สร้างฐานข้อมูลใบหน้า
   1) เปิดไฟล์ train_faces.py
   2) กำหนดให้โปรแกรมอ่านภาพจากโฟลเดอร์ dataset
   3) ตรวจจับใบหน้าในแต่ละภาพ
   4) ตัดเฉพาะบริเวณใบหน้า
   5) ปรับขนาดภาพให้เท่ากัน
   6) สร้างรหัสกำกับผู้ใช้
   7) ฝึกโมเดลหรือสร้าง Face Encoding
   8) บันทึกโมเดลไว้ในโฟลเดอร์ models
   9) บันทึกตารางจับคู่รหัสผู้ใช้กับชื่อที่ต้องการแสดง
   10) รันโปรแกรม

```
python3 train_faces.py
```

   11) ตรวจสอบว่ามีไฟล์โมเดลเกิดขึ้น
   12) ตรวจสอบว่าไม่มีข้อความผิดพลาด
   13) สำรองโมเดลตามที่ผู้สอนกำหนด
8. ขั้นตอนที่ 8 เขียนและทดสอบโปรแกรมจดจำใบหน้า
   1) เปิดโปรแกรมทดสอบการจดจำ
   2) โหลดโมเดลใบหน้าที่สร้างไว้
   3) เปิด Webcam
   4) ตรวจจับใบหน้าในภาพ
   5) เปรียบเทียบใบหน้ากับฐานข้อมูล
   6) แสดงรหัสหรือชื่อของผู้ใช้
   7) หากไม่ตรงกับฐานข้อมูล ให้แสดง UNKNOWN
   8) แสดงคะแนน Confidence หรือค่าระยะห่าง
   9) กำหนด Threshold ตามผลการทดลอง
   10) ทดสอบผู้ใช้ที่ลงทะเบียนอย่างน้อยคนละ 5 ครั้ง
   11) ทดสอบบุคคลที่ไม่ได้ลงทะเบียน
   12) บันทึกกรณีที่ระบบยอมรับผิด
   13) บันทึกกรณีที่ระบบปฏิเสธผู้ใช้ที่ถูกต้อง
   14) ปรับ Threshold และทดสอบซ้ำ
9. ขั้นตอนที่ 9 เขียนและทดสอบโปรแกรมอ่าน GY-906
   1) เปิดไฟล์ test_temperature.py

2) กำหนด I²C Address เป็นค่าที่ตรวจพบ เช่น 0x5A
3) อ่านค่าอุณหภูมิแวดล้อม
4) อ่านค่าอุณหภูมิวัตถุ
5) แสดงค่าบนหน้าจอ
6) รันโปรแกรม

```
python3 test_temperature.py
```

7) กำหนดระยะวัดให้คงที่
8) อ่านค่าอย่างน้อย 5 ครั้ง
9) เปรียบเทียบกับเครื่องมืออ้างอิง
10) คำนวณความคลาดเคลื่อน
11) กำหนด Offset เฉพาะเมื่อมีผลสอบเทียบ
12) ใช้ค่ามัธยฐานจากการอ่านหลายครั้ง
13) หากเซนเซอร์อ่านไม่ได้ ให้แสดง TEMP SENSOR ERROR
14) ห้ามแทนค่าที่อ่านไม่ได้ด้วย 0 แล้วอนุญาตให้เปิดประตู
15) กำหนดเกณฑ์ 38 °C เฉพาะการทดลอง

10. ขั้นตอนที่ 10 เขียนและทดสอบโปรแกรม GPIO

1) เปิดไฟล์ `test_gpio.py`
2) กำหนดหมายเลขขาแบบ BCM
3) กำหนด LED เป็น Output
4) กำหนดรีเลย์เป็น Output
5) กำหนด Exit Sensor เป็น Input
6) กำหนดรีเลย์ให้อยู่ในสถานะ OFF ก่อน
7) เปิด LED สีน้ำเงินแล้วปิด
8) เปิด LED สีเหลืองแล้วปิด
9) เปิด LED สีเขียวแล้วปิด
10) เปิด LED สีแดงแล้วปิด
11) อ่านค่าจาก Exit Sensor
12) สั่งรีเลย์ทำงานประมาณ 1 วินาที
13) สั่งรีเลย์หยุดทำงาน
14) ตรวจสอบว่ารีเลย์เป็น Active LOW หรือ Active HIGH
15) Restart Raspberry Pi
16) ตรวจสอบว่ารีเลย์ไม่ทำงานเองระหว่างบูต

17) หากรีเลย์ทำงานเอง ให้ตัดไฟกลอนและแก้วงจรก่อนดำเนินการต่อ

11. ขั้นตอนที่ 11 ต่อและทดสอบกลอนประตู

ดำเนินการเมื่อโปรแกรม GPIO ผ่านการทดสอบแล้วเท่านั้น

1) ปิด Raspberry Pi
2) ปิดแหล่งจ่ายกลอน
3) ใช้มัลติมิเตอร์ตรวจว่าไม่มีแรงดัน
4) ต่อขั้วบวกของแหล่งจ่าย 12 V ผ่านฟิวส์
5) ต่อจากฟิวส์ไปยัง COM ของรีเลย์
6) ต่อ NO ของรีเลย์ไปยังขั้วบวกของกลอน
7) ต่อขั้วลบของกลอนกลับ 0 V
8) ต่อไดโอดคร่อมกลอน
9) ต่อด้านที่มีแถบของไดโอดเข้าขั้วบวก
10) ต่ออีกด้านเข้าขั้วลบ
11) ตรวจสอบว่าไม่มีสายจาก NO ลง 0 V โดยตรง
12) ให้ผู้สอนตรวจวงจร
13) เปิด Raspberry Pi ก่อน
14) ตรวจสอบว่ารีเลย์ OFF
15) จ่ายไฟให้กลอน
16) ตรวจสอบว่ากลอนอยู่ในสถานะล็อก
17) สั่งรีเลย์ทำงาน 3–5 วินาที
18) ตรวจสอบว่ากลอนปลดล็อก
19) ตรวจสอบว่ากลอนกลับมาล็อก
20) ตรวจอุณหภูมิของกลอน รีเลย์ สายไฟ และแหล่งจ่าย

ตอนที่ 3

การเชื่อมต่อ Google Cloud และ Google Sheets

ระบบบันทึกการเข้าเรียนสามารถส่งข้อมูลจาก Raspberry Pi ไปจัดเก็บใน Google Sheets โดยใช้ Google Sheets API และบัญชีบริการ หรือ Service Account สำหรับยืนยันตัวตนของโปรแกรม บัญชีบริการเป็นบัญชีที่ใช้แทนแอปพลิเคชัน ไม่ใช่บัญชีผู้ใช้ทั่วไป การกำหนดสิทธิ์จึงควรยึดหลักสิทธิ์เท่าที่จำเป็น หรือ principle of least privilege โดยอนุญาตให้บัญชีบริการเข้าถึงเฉพาะไฟล์ที่ระบบต้องใช้งานเท่านั้น (Google for Developers, 2026)

1. การสร้างโปรเจกต์ใน Google Cloud

1.1 เข้าสู่ระบบ https://console.cloud.google.com/welcome/new?pli=1 ด้วยบัญชี Google ที่ต้องการใช้จัดการระบบ

1.2 เลือกตัวเลือกโปรเจกต์บริเวณส่วนบนของหน้าจอ แล้วเลือก **New Project** หรือไปที่ **IAM & Admin** > **Manage Resources**

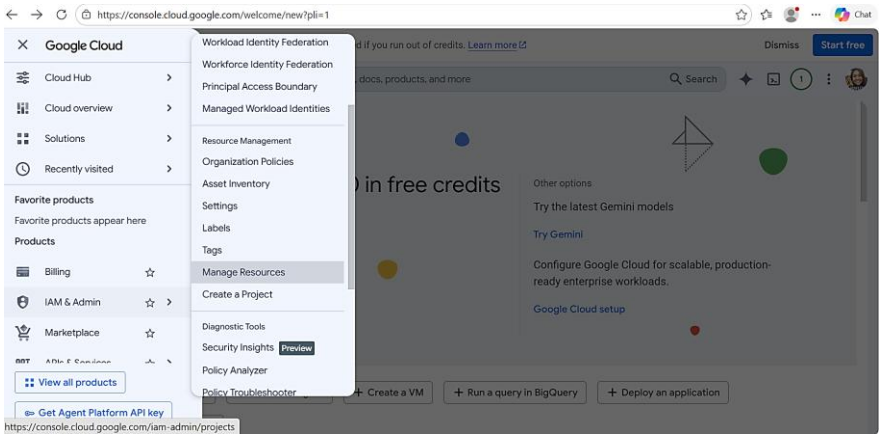
1.3 เลือก **Create Project**

1.4 กำหนดชื่อโปรเจกต์ เช่น face-attendance-system

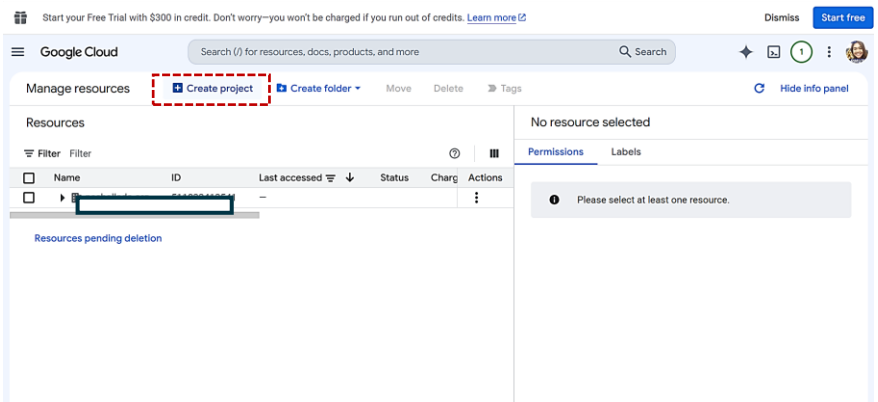
1.5 ตรวจสอบ Organization และ Location หากบัญชีดังกล่าวอยู่ภายใต้หน่วยงาน

1.6 คลิก **Create** และรอจนกระทั่งระบบสร้างโปรเจกต์เสร็จสมบูรณ์

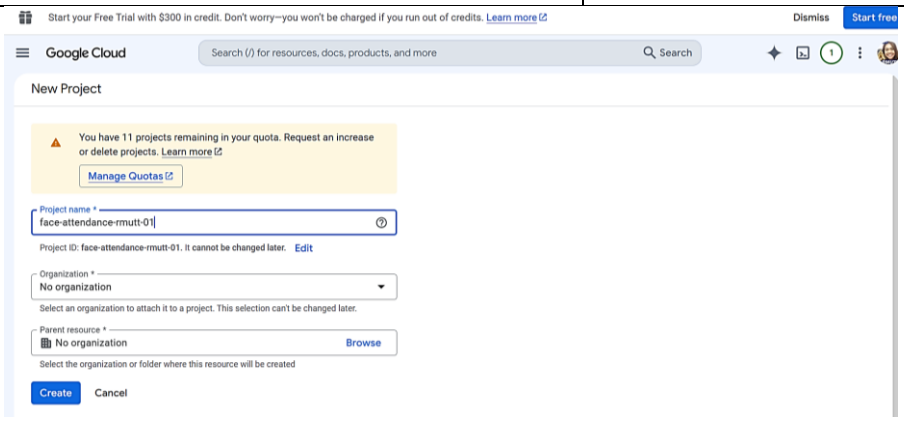
1.7 เลือกโปรเจกต์ที่สร้างขึ้นให้เป็นโปรเจกต์ปัจจุบันก่อนดำเนินการขั้นตอนต่อไป



รูปที่ 11.5 การเข้าสู่หน้าจัดการทรัพยากรเพื่อสร้างโปรเจกต์ใน Google Cloud



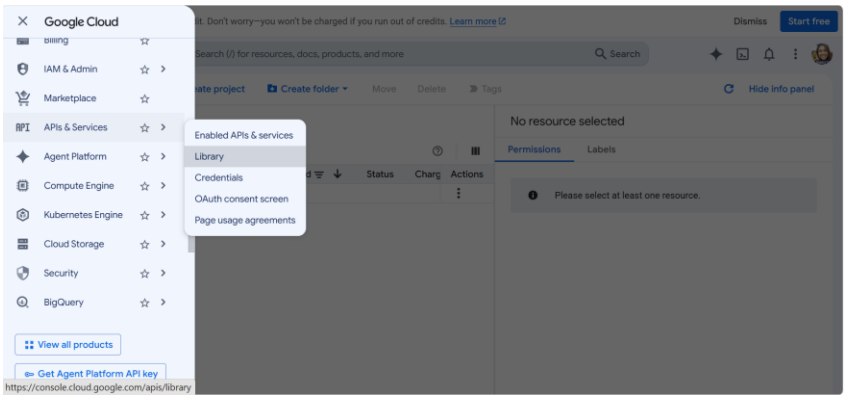
รูปที่ 11.6 การสร้างโปรเจกต์สำหรับระบบบันทึกข้อมูลลง Google Sheets



รูปที่ 11.7 การกำหนดชื่อและรายละเอียดของโปรเจกต์

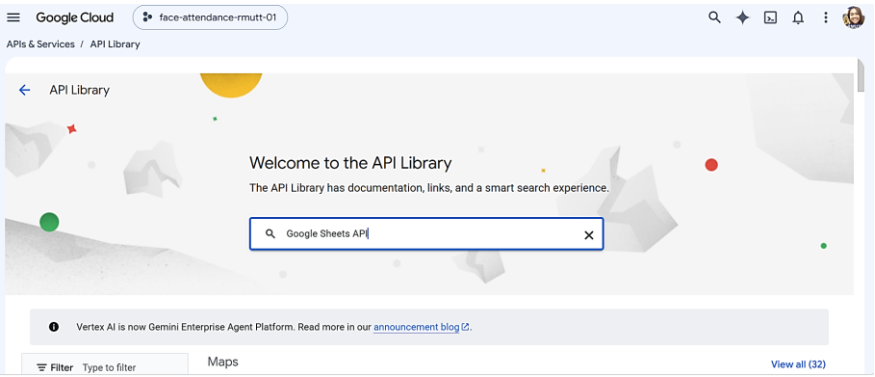
2. การเปิดใช้งาน Google Sheets API

2.1 ไปที่เมนู **APIs & Services** > **Library**



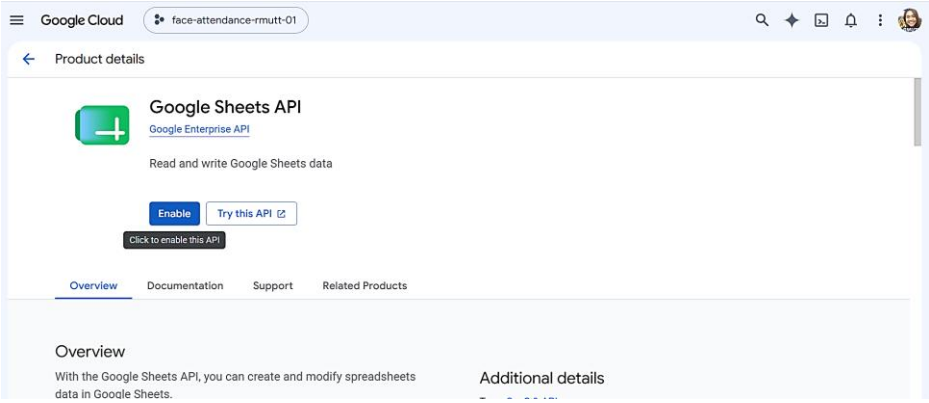
รูปที่ 11.8 หน้าแดชบอร์ดสำหรับตรวจสอบ API ของโปรเจกต์

2.2 ค้นหา **Google Sheets API**



รูปที่ 11.9 การค้นหาและเลือก Google Sheets API

2.3 เลือก **Google Sheets API** แล้วคลิก **Enable**

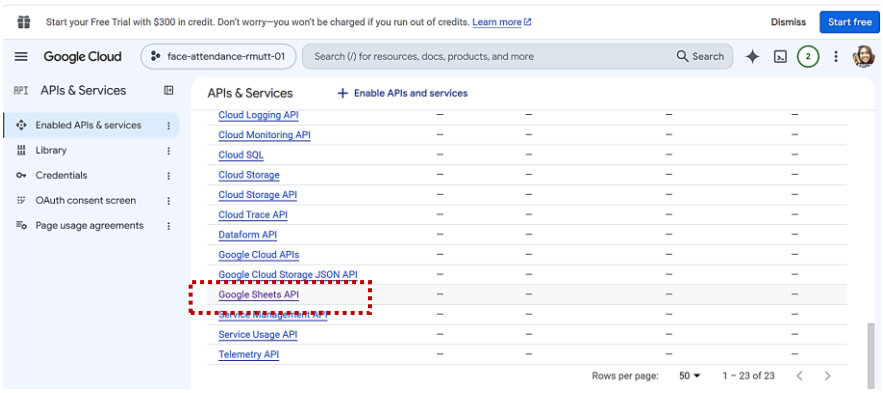


รูปที่ 11.10 การเปิดใช้งาน Google Sheets API

2.4 กลับไปที่หน้า **APIs & Services** > **Enabled APIs & services** เพื่อตรวจสอบว่า API อยู่ในสถานะเปิดใช้งานแล้ว

Google Sheets API เป็น API หลักที่จำเป็นสำหรับการอ่านและเขียนข้อมูลในเซลล์ ส่วน Google Drive API ไม่จำเป็นสำหรับการเขียนข้อมูลลงในสเปรดชีตที่ทราบรหัสไฟล์และแชร์สิทธิ์ให้บัญชีบริการแล้ว อย่างไรก็ตาม ควรเปิด Google Drive API เพิ่มเติมเมื่อโปรแกรมต้องค้นหา สร้าง คัดลอก ย้าย หรือจัดการสิทธิ์ของไฟล์ใน Google Drive หรือเมื่อไลบรารีที่เลือกใช้เรียกใช้ความสามารถดังกล่าว (Google for Developers, 2026)

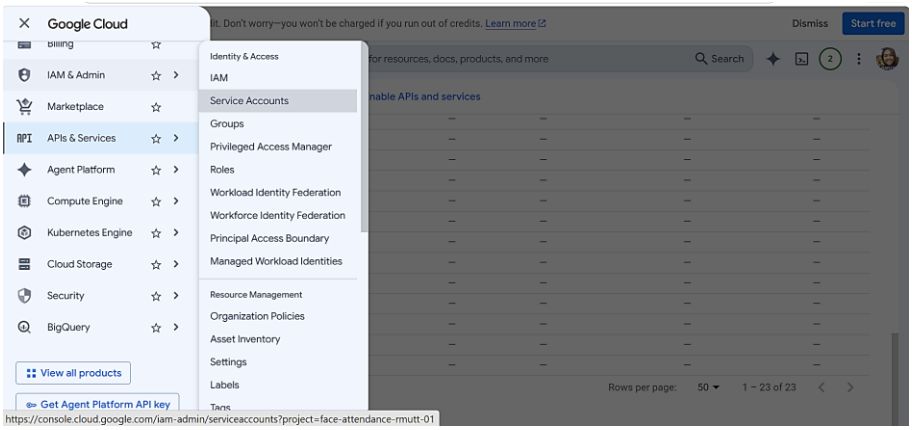
2.5 หากโปรแกรมจำเป็นต้องดำเนินการกับไฟล์ใน Google Drive ให้ค้นหา **Google Drive API** และคลิก **Enable**



รูปที่ 11.11 การตรวจสอบสถานะของ API ที่เปิดใช้งานแล้ว

3. การสร้างบัญชีบริการ

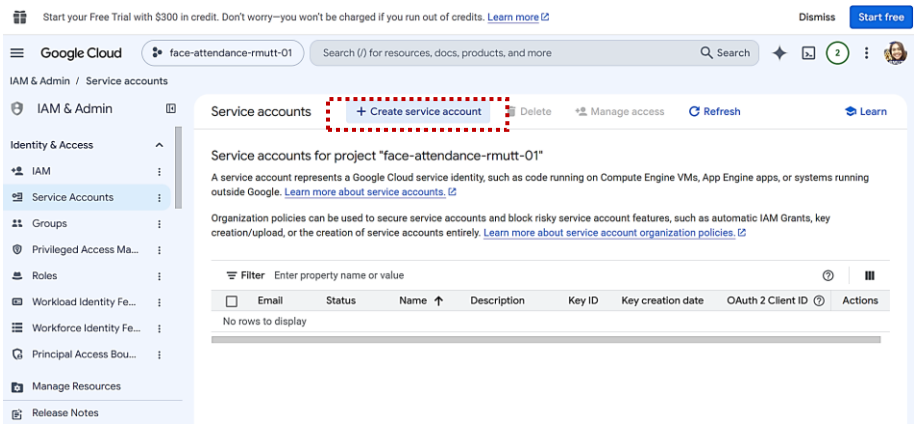
3.1 ไปที่เมนู **IAM & Admin** > **Service Accounts**



รูปที่ 11.12 การสร้างบัญชีบริการสำหรับแอปพลิเคชัน

3.2 เลือกโปรเจกต์ที่สร้างไว้

3.3 คลิก **Create Service Account**

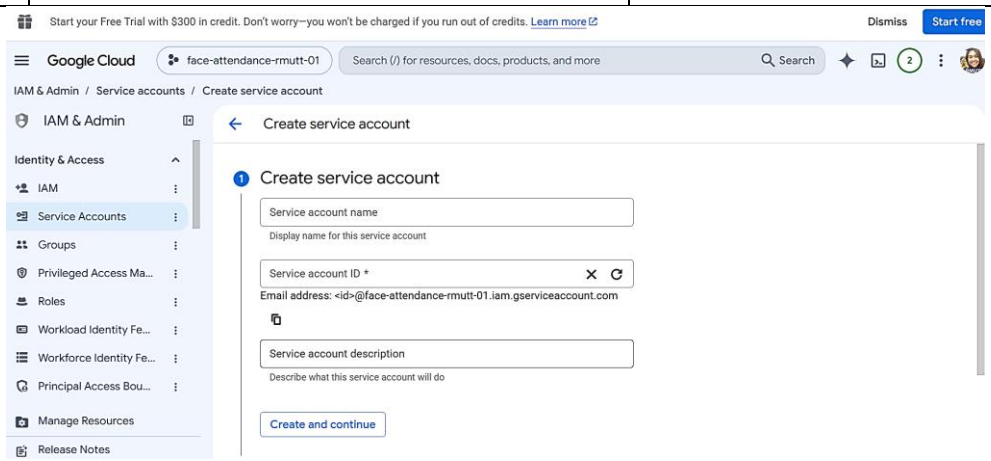


รูปที่ 11.13 ขั้นการ Create Service Account

3.4 กำหนดชื่อบัญชีบริการ เช่น face-attendance-service

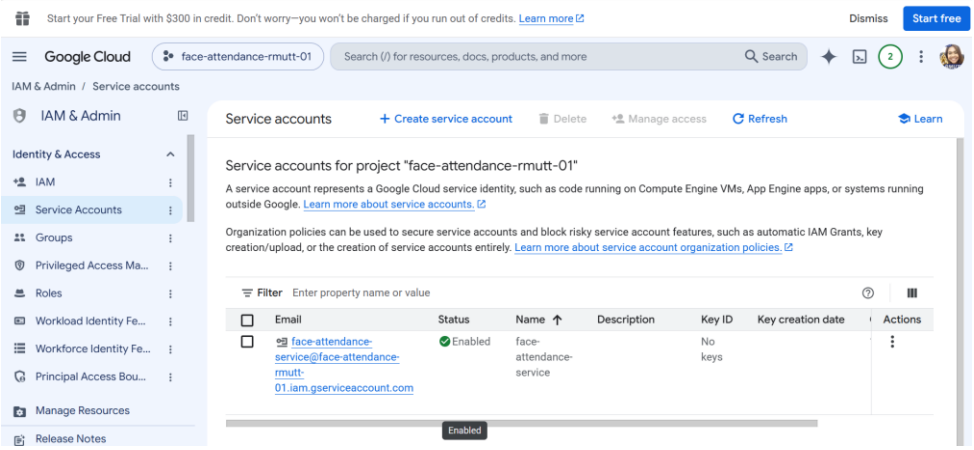
3.5 ตรวจสอบ Service Account ID ซึ่งระบบสร้างให้อัตโนมัติ

3.6 คลิก **Create and Continue**



รูปที่ 11.14 การกำหนดชื่อและรหัสของบัญชีบริการ

3.7 สำหรับระบบที่ต้องการอ่านและเขียนเฉพาะ Google Sheets ที่แชร์ให้โดยตรง ไม่จำเป็นต้องกำหนดบทบาท Editor ให้บัญชีบริการในระดับโปรเจกต์ จึงสามารถข้ามการกำหนดบทบาทและเลือก **Done** ได้



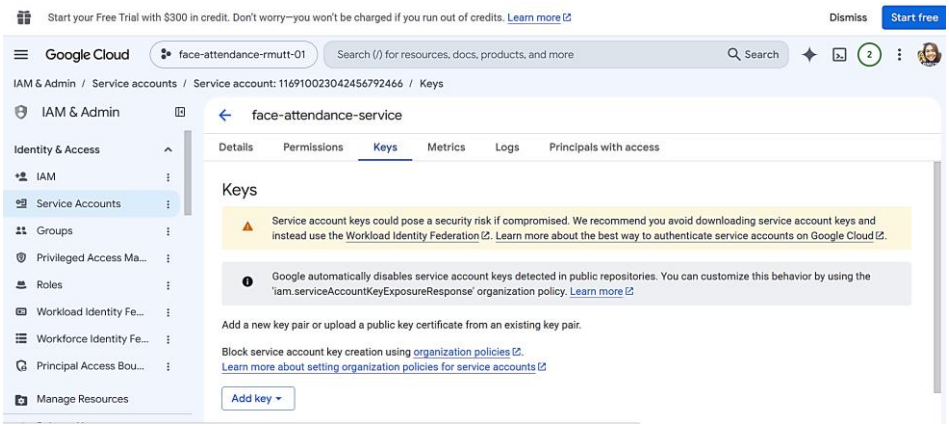
รูปที่ 11.15 เสร็จสิ้นการสร้างบัญชีบริการ

บทบาท IAM ของ Google Cloud ใช้ควบคุมทรัพยากรภายในโปรเจกต์ แต่ไม่ได้ให้สิทธิ์เข้าถึงไฟล์ Google Sheets โดยอัตโนมัติ การเข้าถึงสเปรดชีตต้องกำหนดผ่านเมนู Share ของไฟล์นั้นแยกต่างหาก (Google for Developers, 2026)

4. การสร้างไฟล์กุญแจของบัญชีบริการ

4.1 เปิดบัญชีบริการที่สร้างไว้

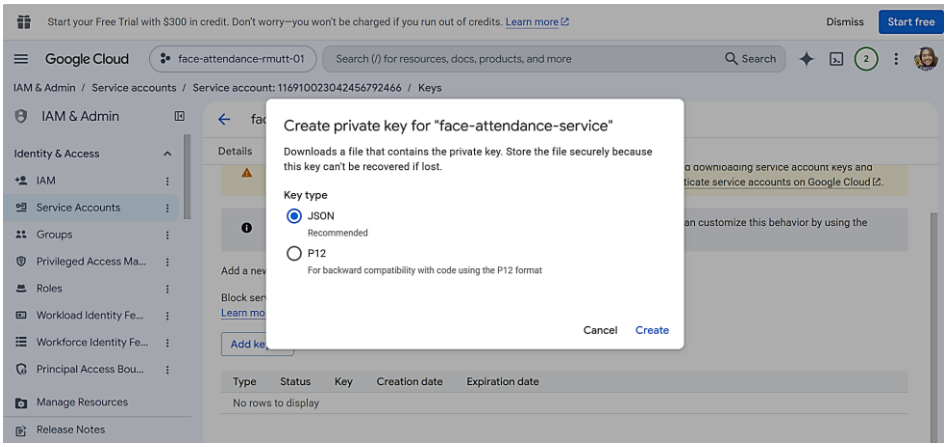
4.2 เลือกแท็บ **Keys**



รูปที่ 11.16 การเข้าสู่แท็บ Keys ของบัญชีบริการ

4.3 เลือก **Add Key** > **Create New Key**

4.4 เลือกประเภทกุญแจเป็น **JSON**



รูปที่ 11.17 การสร้างกุญแจของบัญชีบริการในรูปแบบ JSON

4.5 คลิก **Create** ระบบจะดาวน์โหลดไฟล์กุญแจลงในคอมพิวเตอร์โดยอัตโนมัติ

4.6 ย้ายไฟล์ดังกล่าวไปยัง Raspberry Pi ด้วยวิธีที่ปลอดภัย

อาจเปลี่ยนชื่อไฟล์เป็น credentials.json หรือ creds.json เพื่อให้เรียกใช้ในโปรแกรมได้สะดวก แต่การเปลี่ยนชื่อไม่ใช่ข้อกำหนดของ Google ไฟล์ JSON ดังกล่าวมี private key ซึ่งใช้ยืนยันตัวตนของแอปพลิเคชัน จึงห้ามเผยแพร่ผ่าน GitHub แนบไว้ในรายงาน ใส่ในภาพหน้าจอ

หรือส่งผ่านช่องทางสาธารณะ หากกุญแจรั่วไหลต้องยกเลิกหรือลบกุญแจเดิมและสร้างกุญแจใหม่ทันที (Google Cloud, 2026)

5. การกำหนดสิทธิ์เข้าถึง Google Sheets

5.1 เปิดไฟล์ JSON ด้วยโปรแกรมแก้ไขข้อความ

5.2 คัดลอกค่าในรายการ client_email ตัวอย่างเช่น

face-attendance-service@project-id.iam.gserviceaccount.com

5.3 สร้างหรือเปิด Google Sheets ที่ต้องการใช้จัดเก็บข้อมูล

5.4 คลิก **Share**

5.5 วางอีเมลของบัญชีบริการลงในช่องเพิ่มผู้ใช้งาน

5.6 กำหนดสิทธิ์เป็น **Editor** หากโปรแกรมต้องเขียนข้อมูล หรือกำหนดเป็น **Viewer** หากต้องการอ่านข้อมูลเพียงอย่างเดียว

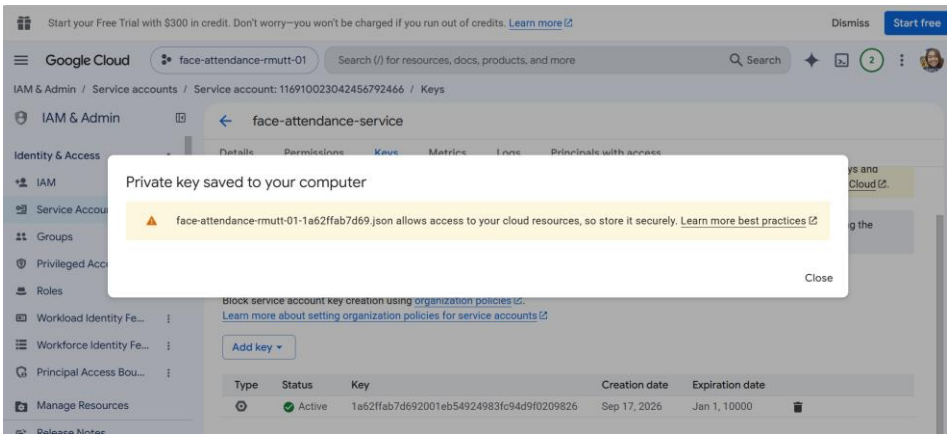
5.7 ปิดตัวเลือก **Notify people** เนื่องจากบัญชีบริการไม่มีกล่องรับอีเมล

5.8 คลิก **Share** เพื่อบันทึกการกำหนดสิทธิ์

5.9 คัดลอก Spreadsheet ID จาก URL ของ Google Sheets ตัวอย่างเช่น

https://docs.google.com/spreadsheets/d/SPREADSHEET_ID/edit

การแชร์ไฟล์โดยตรงให้อีเมลของบัญชีบริการเป็นวิธีที่เหมาะสมสำหรับระบบที่เข้าถึงเฉพาะสเปรดชีตที่กำหนด และไม่จำเป็นต้องเปิดใช้ Domain-wide Delegation (Google for Developers, 2026)



รูปที่ 11.18 การยืนยันการดาวน์โหลดกุญแจส่วนตัวของบัญชีบริการในรูปแบบ JSON

6. การจัดเก็บข้อมูลรับรองใน Raspberry Pi

6.1 จัดเก็บไฟล์ JSON ไว้ในไดเรกทอรีที่ผู้ใช้งานทั่วไปไม่สามารถเข้าถึงได้

6.2 ไม่ควรเขียน private key หรือเนื้อหาของไฟล์ JSON ลงในโปรแกรมโดยตรง

6.3 กำหนดตัวแปรสภาพแวดล้อมให้ชี้ไปยังไฟล์ข้อมูลรับรอง เช่น export GOOGLE_APPLICATION_CREDENTIALS="/home/pi/secure/credentials.json"

6.4 จำกัดสิทธิ์การเข้าถึงไฟล์ให้เฉพาะเจ้าของระบบ เช่น chmod 600 /home/pi/secure/credentials.json

6.5 ตรวจสอบว่าไฟล์ดังกล่าวไม่ถูกรวมอยู่ในระบบควบคุมเวอร์ชันหรือไฟล์รายงาน

Google แนะนำให้โปรแกรมค้นหาข้อมูลรับรองผ่าน Application Default Credentials และใช้ตัวแปร GOOGLE_APPLICATION_CREDENTIALS แทนการฝังตำแหน่งหรือข้อมูลลับไว้ในซอร์สโค้ด (Google Cloud Authentication, 2026)

7. การทดสอบการบันทึกข้อมูล

7.1 ติดตั้งไลบรารีภาษา Python ที่จำเป็น เช่น google-auth, google-api-python-client หรือ gspread ตามแนวทางการพัฒนาโปรแกรมที่เลือกใช้

7.2 ให้โปรแกรมเปิดสเปรดชีตด้วย Spreadsheet ID แทนการค้นหาจากชื่อไฟล์ เพื่อป้องกันความคลุมเครือเมื่อมีไฟล์ชื่อซ้ำกัน

7.3 ทดลองเพิ่มข้อมูลตัวอย่าง เช่น ชื่อ รหัสนักศึกษา วัน เวลา และอุณหภูมิ

7.4 ตรวจสอบว่าข้อมูลปรากฏในแถวและคอลัมน์ที่กำหนดอย่างถูกต้อง

7.5 ทดสอบกรณีอินเทอร์เน็ตขัดข้อง สิทธิ์ไม่ถูกต้อง และ Google API ตอบกลับข้อผิดพลาด

7.6 ออกแบบให้โปรแกรมบันทึกข้อมูลสำรองไว้ภายใน Raspberry Pi และส่งข้อมูลซ้ำเมื่อการเชื่อมต่อกลับสู่สภาวะปกติ

9.4.3 การเชื่อมต่อ LINE Messaging API

LINE Messaging API ใช้สำหรับส่งข้อความแจ้งเตือนจากระบบ Raspberry Pi ไปยังผู้ดูแล เช่น แจ้งผลการบันทึกการเข้าเรียน แจ้งอุณหภูมิสูงกว่าค่าที่กำหนด หรือแจ้งข้อผิดพลาดของระบบ ปัจจุบันไม่สามารถสร้าง Messaging API Channel โดยตรงจาก LINE Developers Console ได้ การเริ่มต้นต้องสร้างหรือเลือก LINE Official Account แล้วเปิดใช้งาน Messaging API ผ่าน LINE Official Account Manager จากนั้นระบบจึงสร้าง Messaging API Channel ให้โดยอัตโนมัติ (https://developers.line.biz/en/docs/messaging-api/getting-started/) (LINE Developers, n.d.)

1 การเตรียม LINE Official Account

1.1 สร้างหรือเลือก LINE Official Account สำหรับใช้ในการทดลอง

1.2 เข้าสู่ LINE Official Account Manager

1.3 เปิดใช้งาน **Messaging API**

1.4 เลือก Provider ที่ใช้จัดการระบบอย่างระมัดระวัง เนื่องจากเมื่อกำหนด Provider แล้วจะไม่สามารถเปลี่ยนหรือยกเลิกการเชื่อมโยงได้โดยง่าย

1.5 เข้าสู่ LINE Developers Console และตรวจสอบว่า Messaging API Channel ถูกสร้างขึ้นแล้ว

1.6 เพิ่ม LINE Official Account เป็นเพื่อน หรือเชิญบัญชีดังกล่าวเข้ากลุ่มที่ต้องการรับข้อความ

2 การออก Channel Access Token

2.1 เปิด Messaging API Channel ใน LINE Developers Console

2.2 ไปที่แท็บ **Messaging API**

2.3 ออก Channel Access Token ตามประเภทที่เหมาะสม

2.4 คัดลอก Token และจัดเก็บไว้ในระบบจัดการข้อมูลลับหรือตัวแปรสภาพแวดล้อม

2.5 ห้ามบันทึก Token ลงในซอร์สโค้ด รายงาน ภาคผนวก GitHub หรือภาพหน้าจอ

ตัวอย่างการกำหนดตัวแปรสภาพแวดล้อมบน Raspberry Pi คือ

export LINE_CHANNEL_ACCESS_TOKEN="ค่าของ Channel Access Token"

3 การกำหนดปลายทางของข้อความ

การส่ง Push Message ต้องระบุปลายทางด้วยรหัสที่ระบบ LINE กำหนด ได้แก่ userId, groupId หรือ roomId ตามประเภทของห้องสนทนา ไม่สามารถใช้ชื่อผู้ใช้ ชื่อที่แสดง หรือชื่อกลุ่มแทนรหัสดังกล่าวได้

หากต้องการส่งข้อความถึงผู้ใช้ ผู้ใช้ต้องเพิ่ม LINE Official Account เป็นเพื่อนหรือมีเงื่อนไขตรงตามข้อกำหนดของ Messaging API ส่วน groupId ต้องได้มาจาก Webhook Event เมื่อ LINE Official Account ถูกเพิ่มเข้าไปในกลุ่มและเกิดเหตุการณ์ในกลุ่มนั้น

4 การทดสอบส่งข้อความ

4.1 ทดสอบส่ง Push Message จากคอมพิวเตอร์ก่อนนำโปรแกรมไปทำงานบน Raspberry Pi

4.2 ตรวจสอบ HTTP status code และรายละเอียดข้อผิดพลาดที่ API ส่งกลับ

4.3 หากได้รับสถานะ 200 OK ให้ตรวจสอบว่าข้อความปรากฏใน LINE ของผู้รับ

4.4 ทดสอบข้อความภาษาไทย อักขระพิเศษ วัน เวลา และค่าตัวเลข

4.5 นำโปรแกรมไปทดสอบบน Raspberry Pi

4.6 ทดสอบกรณี Token ไม่ถูกต้อง ปลายทางไม่ถูกต้อง อินเทอร์เน็ตขัดข้อง และจำนวนข้อความเกินโควตาที่กำหนด

4.7 บันทึกเฉพาะผลการทดสอบและรหัสสถานะ โดยไม่แสดง Token หรือข้อมูลลับในรายงาน

โปรแกรมควบคุมการทำงานของระบบแสดงไว้ใน **ภาคผนวก ก Arduino Code 12** ทั้งนี้หากโปรแกรมส่วนที่เชื่อมต่อ Google Sheets และ LINE Messaging API พัฒนาด้วยภาษา Python บน Raspberry Pi ควรเปลี่ยนชื่อภาคผนวกเป็น **ภาคผนวก ก โปรแกรมภาษา Python สำหรับระบบบันทึกการเข้าเรียนและการแจ้งเตือน** เพื่อให้ตรงกับภาษาที่ใช้จริง

9.4.4 ลำดับการทำงานของระบบ

เมื่อระบบเริ่มทำงาน Raspberry Pi จะเตรียมกล้อง เซนเซอร์วัดอุณหภูมิ จอแสดงผล และอุปกรณ์แจ้งสถานะ จากนั้นโปรแกรมจะตรวจจับใบหน้าและเปรียบเทียบลักษณะใบหน้ากับฐานข้อมูล หากไม่สามารถระบุตัวบุคคลได้ ระบบจะแสดงข้อความปฏิเสธและไม่บันทึกการเข้าเรียน

หากระบบระบุตัวบุคคลได้สำเร็จ จะอ่านค่าอุณหภูมิจากเซนเซอร์ MLX90614 และเปรียบเทียบกับเกณฑ์ที่กำหนด เมื่อข้อมูลผ่านเงื่อนไข ระบบจะบันทึกชื่อ รหัสประจำตัว วันเวลา อุณหภูมิ และผลการตรวจสอบลงใน Google Sheets ผ่าน Google Sheets API พร้อมแสดงผลทางจอภาพและอุปกรณ์แจ้งสถานะ หากกำหนดให้มีการแจ้งเตือน ระบบจะส่ง Push Message ไปยังผู้ดูแลผ่าน LINE Messaging API

ในกรณีที่ไม่สามารถเชื่อมต่ออินเทอร์เน็ตหรือบริการภายนอกได้ ระบบควรบันทึกข้อมูลลงในหน่วยความจำภายในหรือฐานข้อมูลเฉพาะที่ก่อน แล้วจึงส่งข้อมูลไปยัง Google Sheets และ LINE เมื่อการเชื่อมต่อกลับสู่ภาวะปกติ แนวทางดังกล่าวช่วยลดความเสี่ยงของข้อมูลสูญหายและเพิ่มความน่าเชื่อถือของระบบ

เตรียม LINE Messaging API

1. สร้างหรือเลือก LINE Official Account สำหรับการทดลอง
2. เปิดใช้งาน Messaging API
3. เพิ่ม LINE Official Account เป็นเพื่อน
4. ออก Channel access token
5. คัดลอก User ID หรือ Group ID
6. ห้ามใช้ชื่อผู้ใช้แทน User ID
7. เก็บ token ไว้ใน Environment Variable
8. ทดสอบส่ง Push message จากคอมพิวเตอร์
9. ตรวจสอบ HTTP response code

10. หากได้ 200 ให้ตรวจสอบข้อความใน LINE
11. ทดสอบส่งจาก Raspberry Pi
12. ตรวจสอบว่าข้อความภาษาไทยแสดงถูกต้อง
13. ห้ามบันทึก token ลงในรายงานหรือภาพหน้าจอ

เมื่อระบบตรวจพบใบหน้า จะประมวลผลข้อมูลด้วยโปรแกรม Python จากนั้นอ่านค่าอุณหภูมิจากเซ็นเซอร์ผ่าน I²C หากผ่านเกณฑ์ที่กำหนด ระบบจะบันทึกข้อมูลผู้ใช้ลงใน Google Sheets ผ่าน Google Sheets API และสามารถส่งข้อความแจ้งเตือนไปยังผู้ดูแลผ่าน LINE Messaging API (โปรแกรมควบวบคุมการทำงาน ดังภาคผนวก ก Arduino Code: 12) ได้แบบอัตโนมัติ ทั้งนี้ GPIO ทำหน้าที่เป็นส่วนเชื่อมโยงระหว่าง Raspberry Pi กับอุปกรณ์ภาคสนาม ทำให้สามารถรับข้อมูลจากเซ็นเซอร์และควบคุมอุปกรณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ (Halvorsen, 2026; Mathe et al., 2024)

สรุปผลการทดลอง

เอกสารอ้างอิง

วัชรพงศ์ วิรัตน์ และ กิตติพัฒน์ ย้อยแสง. (2524). *การพัฒนาชุดฝึกปฏิบัติการระบบเข้าเรียนด้วยการสแกนใบหน้าร่วมกับการวัดอุณหภูมิ*. ปริญญานิพนธ์หลักสูตรครุศาสตร์อุตสาหกรรมบัณฑิต สาขาวิศวกรรมอิเล็กทรอนิกส์และโทรคมนาคม, ภาควิชาครุศาสตร์อุตสาหกรรม, คณะครุศาสตร์อุตสาหกรรม, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี. ปทุมธานี.

Google Cloud. (2026). *Set up Application Default Credentials*. https://docs.cloud.google.com/docs/authentication/provide-credentials-adc

Google for Developers. (2026). *Create access credentials*. https://developers.google.com/workspace/guides/create-credentials

Google for Developers. (2026). *Enable Google Workspace APIs*. https://developers.google.com/workspace/guides/enable-apis

Google Cloud. (2026). *Create and delete service account keys*. https://docs.cloud.google.com/iam/docs/keys-create-delete.

Hans-Petter Halvorsen Raspberry Pi Foundation. (2019). *The Official Raspberry Pi Projects Book, Volume 5*.

Halvorsen, H.-P. (2026). *Raspberry Pi and Python*. https://www.halvorsen.blog/documents/programming/python/.

LINE Developers. (2024). *Get started with the Messaging API*. https://developers.line.biz/en/docs/messaging-api/getting-started/

LINE Developers. (n.d.). *Messaging API reference*. https://developers.line.biz/en/reference/messaging-api/.

Mathe, S. E., Kondaveeti, H. K., Vappangi, S., Vanambathina, S. D., & Kumaravelu, N. K. (2024). A comprehensive review on applications of Raspberry Pi. *Computer Science Review, 52*, 100636.

	ใบงานที่ 12 เรื่อง งานตรวจจับก๊าซและควบคุมวาล์วแก๊ส อัตโนมัติด้วยเซนเซอร์ MQ-2	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความมุ่งหมาย

ออกแบบงานติดตั้ง และเขียนโปรแกรมควบคุมระบบตรวจจับก๊าซไวไฟด้วย MQ-2 ในงานระบบความปลอดภัยได้

วัตถุประสงค์

1. อธิบายหลักการทำงานของ MQ-2 และการเปลี่ยนแปลงของสัญญาณ AO ได้
2. อธิบายหน้าที่และการเชื่อมต่อของ NodeMCU รีเลย์ วาล์ว และปุ่มกดได้
3. ออกแบบลำดับควบคุมแบบตัดก๊าซและคงสถานะปิดได้อย่างปลอดภัย
4. ทดสอบ บันทึกผล และวิเคราะห์พฤติกรรมของระบบได้

เครื่องมือและอุปกรณ์

1. โมดูลเซนเซอร์ MQ-2	1 ชุด
2. NodeMCU ESP8266	1 บอร์ด
3. Relay module 2 channel	1 โมดูล
4. Motorized gas shut-off valve 12 VDC	1 ตัว
5. Switching power supply 12 VDC	1 ชุด
6. Push button	1 ตัว
7. วงจรแบ่งแรงดันและสายต่อ	ตามเหมาะสม
8. มัลติมิเตอร์และคอมพิวเตอร์	1 ชุด

ข้อกำหนดด้านความปลอดภัย

1. ใบงานนี้ใช้สำหรับการศึกษาและการทดสอบในสภาพแวดล้อมที่ควบคุม ห้ามปล่อย LPG หรือก๊าซไวไฟในห้องเรียนเพื่อทดสอบโดยตรง

2. ให้จำลองสัญญาณด้วยแหล่งสัญญาณที่ผู้สอนอนุมัติหรือทดสอบเซนเซอร์ด้วยวิธีที่ปลอดภัย และมีการระบายอากาศ

3. ตรวจสอบแรงดันสูงสุดที่ขา AO และใช้วงจรแบ่งแรงดันเมื่อเอาต์พุต MQ-2 สูงกว่าพิกัด ADC

4. ห้ามต่อมอเตอร์วาล์วเข้ากับ NodeMCU โดยตรง ต้องใช้ภาคขับ/รีเลย์และแหล่งจ่าย ตามพิกัด

5. งานใช้งานจริงควรใช้อุปกรณ์ตรวจจับและวาล์วที่ได้รับการรับรองตามมาตรฐาน พร้อมออกแบบแบบ fail-safe โดยผู้มีคุณสมบัติเหมาะสม

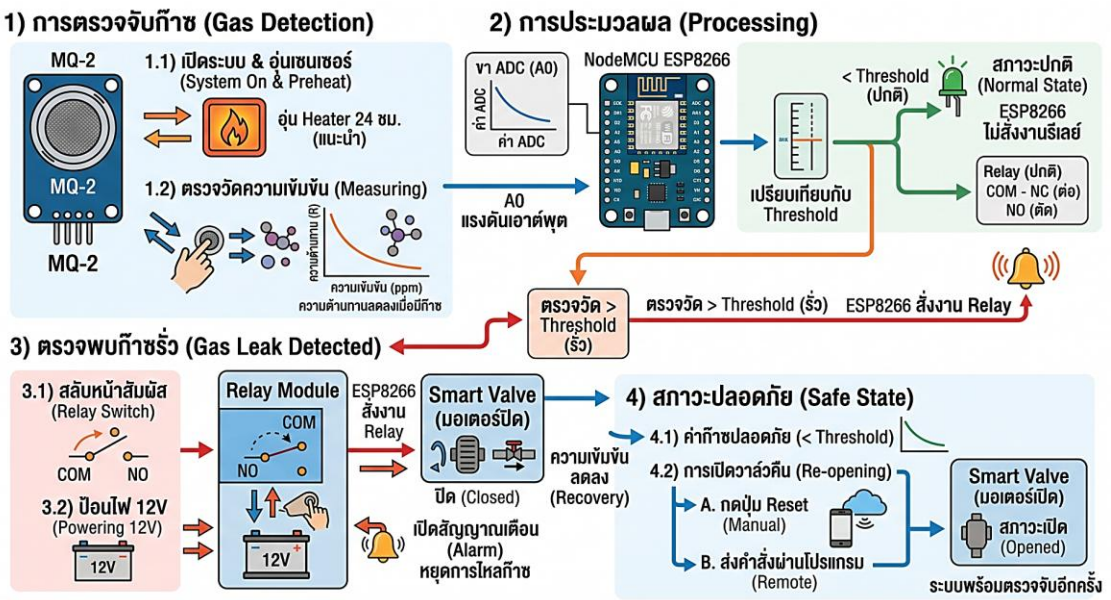
	ใบงานที่ 12 เรื่อง งานตรวจจับก๊าซและควบคุมวาล์วแก๊ส อัตโนมัติด้วยเซนเซอร์ MQ-2	รหัสวิชา 02242308 ระบบรักษาความปลอดภัยอัจฉริยะ (Smart Security System)

ความรู้พื้นฐานในการปฏิบัติงาน

ระบบตรวจจับก๊าซรั่วไหลเป็นองค์ประกอบสำคัญของระบบรักษาความปลอดภัยอัจฉริยะ โดยเฉพาะในอาคารที่มีการใช้ก๊าซหุงต้ม (Liquefied Petroleum Gas: LPG) หรือก๊าซธรรมชาติ (natural gas) หากเกิดการรั่วไหลของก๊าซโดยไม่ได้รับการตรวจพบ อาจก่อให้เกิดเพลิงไหม้หรือการระเบิด ส่งผลกระทบต่อชีวิตและทรัพย์สินได้

วงจรประกอบด้วยอุปกรณ์หลัก ได้แก่ เซนเซอร์ตรวจจับก๊าซ MQ-2, บอร์ด ESP8266 NodeMCU, Relay module 2 channel, smart valve (motorized gas shut-off valve), switching power supply 12 VDC, และ push button สำหรับรีเซตหรือทดสอบระบบ โดยเซนเซอร์ MQ-2 ทำหน้าที่ตรวจวัดความเข้มข้นของก๊าซไวไฟ เช่น LPG, โพรเพน (propane), บิวเทน (butane), มีเทน (CH_4) ไฮโดรเจน (H_2) และควัน (Smoke) ส่งสัญญาณแอนะล็อกไปยังบอร์ด ESP8266 ผ่านขา A0 เพื่อประมวลผลค่าความเข้มข้นของก๊าซ

1. หลักการจับก๊าซและควบคุมวาล์วแก๊สอัตโนมัติด้วยเซนเซอร์ MQ-2 และ NodeMCU ESP8266



รูปที่ 12.1 แนวคิดการออกแบบระบบการจับก๊าซและควบคุมวาล์วแก๊สอัตโนมัติด้วยเซนเซอร์ MQ-2 และ NodeMCU ESP8266

การทำงานของระบบสามารถอธิบายเป็นลำดับขั้นตอน ดังนี้

1.1 ขั้นตอนที่ 1 การตรวจจับก๊าซ เมื่อเปิดระบบ เซนเซอร์ MQ-2 จะได้รับไฟเลี้ยงและเริ่มอุ่นไส้ทำความร้อน (heater element) ภายในเซนเซอร์ หลังจากอุณหภูมิคงที่ เซนเซอร์จะ

ตรวจวัดความเข้มข้นของก๊าซในบรรยากาศอย่างต่อเนื่อง หากความเข้มข้นของก๊าซเพิ่มขึ้น ความต้านทานของวัสดุไวต่อก๊าซภายในเซนเซอร์จะลดลง ส่งผลให้แรงดันเอาต์พุตที่ขา A0 เปลี่ยนแปลงตามความเข้มข้นของก๊าซ

1.2 ขั้นตอนที่ 2 การประมวลผลเริ่มจาก ESP8266 อ่านค่าแรงดันจากขา A0 ผ่านตัวแปลง ADC แล้วนำค่าที่ได้ไปเปรียบเทียบกับค่าที่ตั้งไว้ กรณี ค่าที่วัดได้ < Threshold แสดงว่าอยู่ในสภาวะปกติ บอร์ด ESP8266 จะไม่สั่งงานRelay

1.3 ขั้นตอนที่ 3 ตรวจพบก๊าซรั่ว เมื่อความเข้มข้นของก๊าซสูงกว่าค่าที่กำหนด โดย ESP8266 จะ เปิดสัญญาณเตือน (ถ้ามี) และ ส่งคำสั่งไปยัง Relay module Relayทั้งสองจะสลับหน้าสัมผัส ทำให้แรงดันไฟฟ้า 12 V ถูกป้อนเข้าสู่มอเตอร์ของ smart valve ในทิศทางที่ทำให้วาล์วปิดทันที เพื่อหยุดการไหลของก๊าซ

1.4 ขั้นตอนที่ 4 ระบบเข้าสู่สภาวะปลอดภัย หลังจากวาล์วปิด ก๊าซจะหยุดไหล ค่าความเข้มข้นของก๊าซค่อย ๆ ลดลง เมื่อค่ากลับเข้าสู่ระดับปลอดภัย ผู้ใช้งานสามารถกดปุ่ม Reset หรือส่งคำสั่งผ่านโปรแกรมเพื่อเปิดวาล์วอีกครั้ง

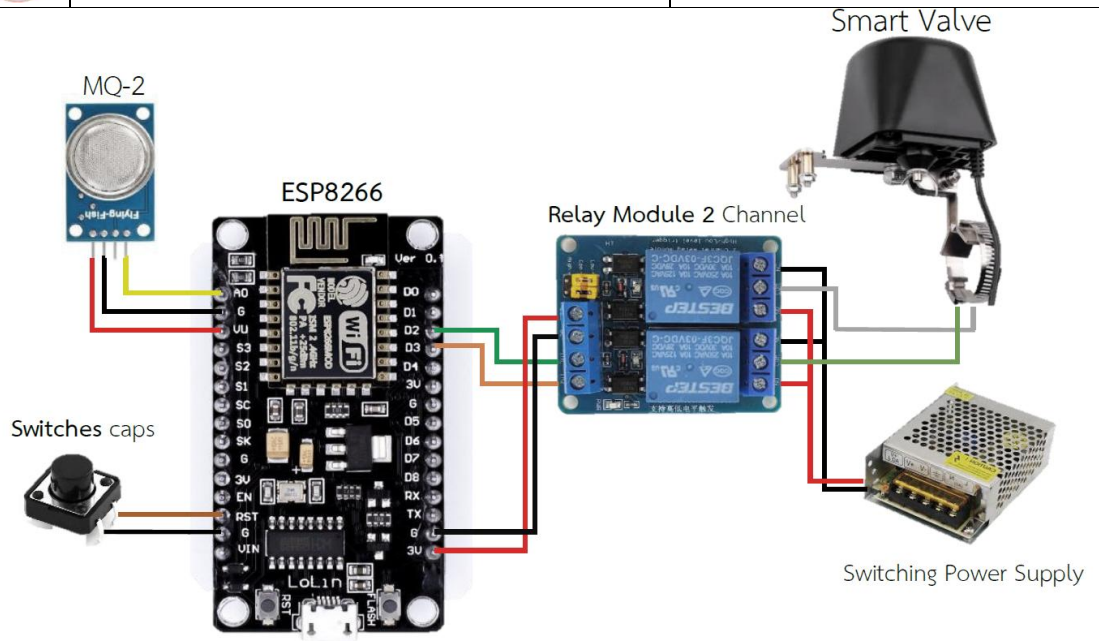
ขั้นตอนการปฏิบัติงาน

1. ต่อวงจรตรวจจับก๊าซและควบคุมวาล์วแก๊สอัตโนมัติด้วยเซนเซอร์ MQ-2 ดังรูปที่ 12.2

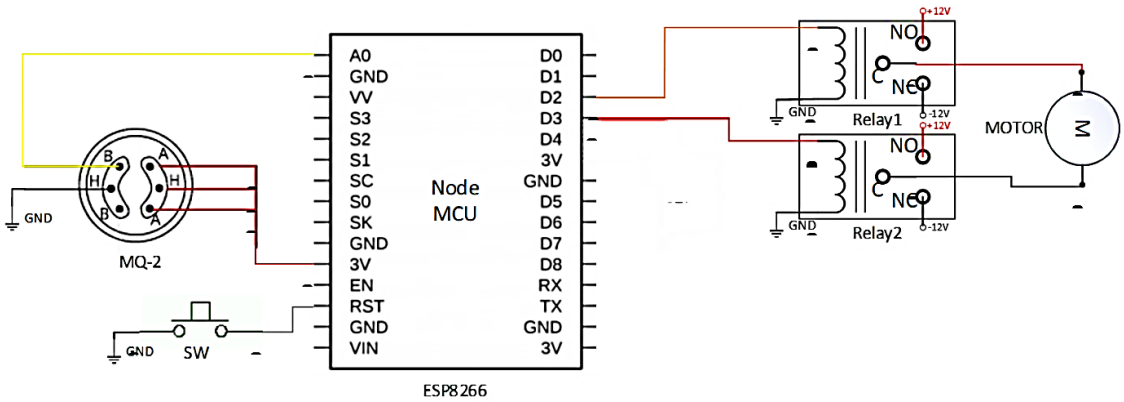
วงจรประกอบด้วยเซนเซอร์ตรวจจับก๊าซ MQ-2 ทำหน้าที่ตรวจจับก๊าซและส่งสัญญาณให้บอร์ด NodeMCU ESP8266 ประมวลผล จากนั้น NodeMCU จะส่งสัญญาณควบคุมไปยัง โมดูล Relay 2 ช่อง เพื่อควบคุมการจ่ายไฟให้มอเตอร์ของ smart valve สำหรับสั่งปิดวาล์วแก๊สเมื่อเกิดการรั่วไหล โดยมีสวิตช์กดสำหรับสั่งรีเซตหรือควบคุมการกลับสู่สภาวะปกติ

1.1 การเชื่อมต่อเซนเซอร์ MQ-2

จากรูปที่ 12.2 ขาเอาต์พุตแอนะล็อกของโมดูล MQ-2 เชื่อมต่อเข้ากับขา A0 ของ NodeMCU ESP8266 เพื่อให้ไมโครคอนโทรลเลอร์อ่านค่าระดับสัญญาณจากเซนเซอร์ ส่วนขาไฟเลี้ยงของโมดูลเชื่อมต่อกับแหล่งจ่ายไฟตามพิกัดของโมดูล และขา GND เชื่อมต่อกับกราวด์ของวงจร โดยเมื่อ MQ-2 สัมผัสก๊าซที่เซนเซอร์มีความไว ค่าความต้านทานของส่วนตรวจจับจะเปลี่ยนแปลง ส่งผลให้แรงดันเอาต์พุตเปลี่ยนตามไปด้วย NodeMCU จึงสามารถอ่านค่าแรงดันดังกล่าวผ่าน ADC ที่ขา A0 และนำไปประมวลผลได้ ข้อควรระวัง ต้องตรวจสอบพิกัดแรงดันอินพุตสูงสุดของขา A0 ของบอร์ด NodeMCU รุ่นที่ใช้จริง กับช่วงแรงดันเอาต์พุตของ MQ-2 หากแรงดันจาก MQ-2 สูงกว่าที่ ADC รองรับ จำเป็นต้องใช้วงจรแบ่งแรงดันก่อนต่อเข้าขา A0 เพื่อป้องกันความเสียหายต่อ ESP8266



(ก) แผนภาพการเชื่อมต่อวงจร (wiring diagram)



(ข) แผนผังวงจรไฟฟ้า (circuit schematic)

รูปที่ 12.2 วงจรตรวจจับก๊าซและควบคุมวาล์วแก๊สอัตโนมัติด้วยเซนเซอร์ MQ-2 และ NodeMCU ESP8266

1.2 การเชื่อมต่อโมดูลRelay 2 ช่อง

จากรูปที่ 12.2 สัญญาณควบคุมRelayต่อจากขาดิจิทัลของ NodeMCU โดยใช้ D2 และ D3 เป็นสัญญาณควบคุมRelayแต่ละช่อง Relayทำหน้าที่เป็นสวิตช์ไฟฟ้าสำหรับควบคุมวงจรกำลังของ smart valve โดยไม่ให้ NodeMCU ขับมอเตอร์โดยตรง การใช้ Relay 2 ช่อง ในวงจรนี้สัมพันธ์กับการควบคุมมอเตอร์ของ smart valve ในสองทิศทาง กล่าวคือ Relayทำหน้าที่จัด

เส้นทางแรงดันให้มอเตอร์เพื่อให้กลไกสามารถเคลื่อนที่ไปยังตำแหน่ง ปิด หรือกลับไปยังตำแหน่ง เปิด ตามคำสั่งของระบบ

1.3 การเชื่อมต่อ smart valve และแหล่งจ่ายไฟ

Smart valve ในรูปที่ 12.2 เป็นอุปกรณ์ขับเคลื่อนด้วยมอเตอร์ จึงต้องใช้แหล่งจ่ายไฟภายนอกที่มีแรงดันและกระแสเหมาะสมกับพิกัดของอุปกรณ์ โดยแหล่งจ่ายไฟเชื่อมต่อผ่านหน้าสัมผัส COM, NO, หรือ NC ของ Relay ตามรูปแบบการควบคุมที่ออกแบบไว้ ซึ่งเมื่อ NodeMCU ตรวจพบค่าจาก MQ-2 สูงกว่าเกณฑ์ที่กำหนด โปรแกรมจะเปลี่ยนสถานะขาเอาต์พุตเพื่อสั่ง Relay จากนั้นหน้าสัมผัสของRelayจะเปลี่ยนตำแหน่งและทำให้มอเตอร์ของ smart valve ได้รับแรงดันในลักษณะที่ทำให้กลไกหมุนไป ปิดวาล์วแก๊ส จึงเป็นการตัดการจ่ายก๊าซในกรณีที่ตรวจพบความผิดปกติ

1.4 การเชื่อมต่อสวิตช์กด

สวิตช์กดเชื่อมต่อกับขาอินพุตดิจิทัลของ NodeMCU และ GND โดยสามารถกำหนดขาดังกล่าวเป็น INPUT_PULLUP ในโปรแกรม เพื่อใช้ตัวต้านทาน pull-up ภายในไมโครคอนโทรลเลอร์ ในสภาวะปกติขาอินพุตจะมีสถานะลอจิก HIGH และเมื่อกดสวิตช์จะเปลี่ยนเป็น LOW สวิตช์นี้สามารถกำหนดให้ทำหน้าที่เป็น reset/manual re-open กล่าวคือ หลังจากระบบตรวจพบก๊าซและสั่งปิดวาล์วแล้ว ผู้ใช้งานต้องตรวจสอบและแก้ไขสาเหตุของการรั่วไหลก่อน เมื่อค่าก๊าซกลับสู่ระดับที่กำหนดให้ปลอดภัย จึงกดสวิตช์เพื่ออนุญาตให้ระบบสั่ง smart valve กลับสู่ตำแหน่งเปิด

2. ปิดแหล่งจ่ายไฟทั้งหมดก่อนต่อวงจร และให้ผู้สอนตรวจสอบ wiring diagram
3. ตรวจสอบพิกัดไฟเลี้ยง MQ-2 พิกัด AO ลอจิกของรีเลย์ และพิกัดวาล์ว
4. ต่อวงจรควบคุมและทดสอบอ่านค่า ADC โดยยังไม่ต่อโหลดวาล์ว
5. ทดสอบสัญญาณ D2 และ D3 ให้แน่ใจว่าไม่ทำงานพร้อมกัน
6. ต่อแหล่งจ่าย 12 VDC และวาล์วผ่านหน้าสัมผัสรีเลย์ตามแบบที่ตรวจสอบแล้ว
7. จำลองค่าเกิน Threshold ระบบต้องสั่งปิดวาล์วและล็อกสถานะ alarm
8. ทำให้ค่า ADC กลับสู่ระดับปลอดภัย วาล์วต้องยังคงปิด
9. กด Reset เมื่อปลอดภัย ระบบจึงอนุญาตให้เปิดวาล์ว
10. เขียนโปรแกรมควบคุมการทำงาน ดังภาคผนวก ข (Arduino Code: 13)

สรุปผลการทดลอง

เอกสารอ้างอิง

อิทธพัฒน์ อ่อนด้วง, วรดาธิษย์ อุทัยศรี, จิราพรรณ แผ้วไพรินทร์. (2565). *ระบบตรวจจับแก๊สแอลพีจีภายในบ้านและแจ้งเตือนอัตโนมัติผ่านแอปพลิเคชันไลน์*. ปริญญานิพนธ์หลักสูตรครุศาสตร์อุตสาหกรรมบัณฑิต สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์และระบบอัตโนมัติ, คณะครุศาสตร์อุตสาหกรรม, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี. ปทุมธานี.

Nagpal, R., Ababii, N., & Lupan, O. (2025). *Comprehensive advances in gas sensing: Mechanisms, material innovations, and applications in environmental and health monitoring. Materials Today Electronics, 15*, 100192. https://doi.org/10.1016/j.mtelec.2025.100192.

Wu, Q., Ding, Z., & Zhang, W. (2025). *Research progress on electrochemical gas sensors for fire detection. International Journal of Electrochemical Science, 20*, 101043. https://doi.org/10.1016/j.ijoes.2025.101043

Yunusa, Z., Hamidon, M. N., Kaiser, A., & Awang, Z. (2014). *Gas sensors: A review. Sensors & Transducers, 168*(4), 61–75.

ภาคผนวก ข
โปรแกรมควบวบคุมการทำงาน

```
//****************************************************
*Arduino Code: 1_Reading RFID Tag
//****************************************************
* Typical pin layout used:
 * -----------------------------------------------------------------------------------------
 *             MFRC522      Arduino    Arduino    Arduino   Arduino          Arduino
 *             Reader/PCD   Uno/101    Mega       Nano v3   Leonardo/Micro   Pro Micro
 *             Signal       Pin        Pin        Pin       Pin              Pin
 * -----------------------------------------------------------------------------------------
 * RST/Reset   RST            9             5       D9         RESET/ICSP-5     RST
 * SPI SS      SDA(SS)        10            53      D10        10               10
 * SPI MOSI    MOSI           11 / ICSP-4   51      D11        ICSP-4           16
 * SPI MISO    MISO           12 / ICSP-1   50      D12        ICSP-1           14
 * SPI SCK     SCK            13 / ICSP-3   52      D13        ICSP-3           15
 */
#include <SPI.h>
#include <MFRC522.h>
#define RST_PIN         9             // Configurable, see typical pin layout above
#define SS_PIN          10            // Configurable, see typical pin layout above
MFRC522 mfrc522(SS_PIN, RST_PIN);     // Create MFRC522 instance

void setup() {
        Serial.begin(9600);           // Initialize serial communications with the PC
        while (!Serial);              // Do nothing if no serial port is opened (added for
Arduinos based on ATMEGA32U4)
        SPI.begin();                  // Init SPI bus
        mfrc522.PCD_Init();           // Init MFRC522
        delay(4);                     // Optional delay. Some board do need more time after
init to be ready, see Readme
        mfrc522.PCD_DumpVersionToSerial();  // Show details of PCD - MFRC522 Card Reader
details
        Serial.println(F("Scan PICC to see UID, SAK, type, and data blocks…"));
}
void loop() {
        // Reset the loop if no new card present on the sensor/reader. This saves the entire
process when idle.
        If ( ! mfrc522.PICC_IsNewCardPresent()) {
                return;
        }

        // Select one of the cards
        if ( ! mfrc522.PICC_ReadCardSerial()) {
                return;
        }

        // Dump debug info about the card; PICC_HaltA() is automatically called
        mfrc522.PICC_DumpToSerial(&(mfrc522.uid));
}
```

```
//****************************************************
*Arduino Code: 2_RFID Circuit Controlling LED
//****************************************************
        #include "SPI.h"
        #include "MFRC522.h"
        #define SS_PIN 10
        #define RST_PIN 9
        #define LED_PIN A0

        MFRC522 rfid(SS_PIN, RST_PIN);

        MFRC522::MIFARE_Key key;
        void setup() {
            Serial.begin(9600);
            SPI.begin();
            rfid.PCD_Init();
            pinMode(LED_PIN, OUTPUT);
        }
        void loop() {
          if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())
            return;
```

```
  // Serial.print(F("PICC type: "));
  MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
  // Serial.println(rfid.PICC_GetTypeName(piccType));

  // Check is the PICC of Classic MIFARE type
  if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&
    piccType != MFRC522::PICC_TYPE_MIFARE_1K &&
    piccType != MFRC522::PICC_TYPE_MIFARE_4K) {
    Serial.println(F("Your tag is not of type MIFARE Classic."));
    return;
  }

  String strID = "";
  for (byte i = 0; i < 4; i++) {
    strID +=
    (rfid.uid.uidByte[i] < 0x10 ? "0" : "") +
    String(rfid.uid.uidByte[i], HEX) +
    (i!=3 ? ":" : "");
  }
  strID.toUpperCase();
  Serial.print("2A:3D:EE:81");
  Serial.println(strID);
  // โค้ดส่วนควบคุมหลอด LED โดยเอาค่าจากตัวแปร strID มาเทียบ
  if (strID.indexOf("2A:3D:EE:81") >= 0) {
    digitalWrite(LED_PIN, HIGH);
  } else {
    digitalWrite(LED_PIN, LOW);
  }

  rfid.PICC_HaltA();
  rfid.PCD_StopCrypto1();
}
#include "SPI.h"
#include "MFRC522.h"

#define SS_PIN 10
#define RST_PIN 9
#define LED_PIN A0

MFRC522 rfid(SS_PIN, RST_PIN);

MFRC522::MIFARE_Key key;

void setup() {
    Serial.begin(9600);
    SPI.begin();
    rfid.PCD_Init();
    pinMode(LED_PIN, OUTPUT);
}

void loop() {
  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())
    return;

  // Serial.print(F("PICC type: "));
  MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
  // Serial.println(rfid.PICC_GetTypeName(piccType));

  // Check is the PICC of Classic MIFARE type
  if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&
    piccType != MFRC522::PICC_TYPE_MIFARE_1K &&
    piccType != MFRC522::PICC_TYPE_MIFARE_4K) {
    Serial.println(F("Your tag is not of type MIFARE Classic."));
    return;
  }

  String strID = "";
  for (byte i = 0; i < 4; i++) {
    strID +=
    (rfid.uid.uidByte[i] < 0x10 ? "0" : "") +
    String(rfid.uid.uidByte[i], HEX) +
    (i!=3 ? ":" : "");
  }
  strID.toUpperCase();
```

```
          Serial.print("Tap card key: ");
          Serial.println(strID);

          // โค้ดส่วนควบคุมหลอด LED โดยเอาค่าจากตัวแปร strID มาเทียบ
          if (strID.indexOf("2A:3D:EE:81") >= 0) {
              digitalWrite(LED_PIN, HIGH);
              delay(2000);                    // wait for 2 second
              digitalWrite(LED_PIN, LOW);    // turn the LED off by making the voltage LOW

          } else {
         //   digitalWrite(LED_PIN, LOW);
          }
          // Look for new cards
              if (strID.indexOf("9E:73:55:88") >= 0)
              digitalWrite(LED_PIN, HIGH);
              delay(2000);                    // wait for 2 second
              digitalWrite(LED_PIN, LOW);    // turn the LED off by making the voltage LOW
               return;
         rfid.PICC_HaltA();
          rfid.PCD_StopCrypto1();
        }




//****************************************************
*Arduino Code: 4_RFID with ESP8266 Basic
//****************************************************
#include "SPI.h"                      //For RFID

#include <MFRC522.h>                  //For RFID

#define SS_PIN D3                     //SDA Pin D3        >>>   RFID

#define RST_PIN D8                    //Reset Pin D8      >>>   RFID

                                      //SCK Pin 5 Only

                                      //MISO Pin D6 Only

                                      //MOSI Pin D7 Only

MFRC522 rfid(SS_PIN, RST_PIN); //For RFID  Reader

MFRC522::MIFARE_Key key;              //For RFID  Tag

void setup()

{                                     //Start setup loop

     Serial.begin(115200);            //Serial Mornitor baud rate 115200

     SPI.begin();                     //For  SPI(RFID)

     rfid.PCD_Init();                 //For  RFID

}                                     //END setup loop

void loop()

{                                     //Start void loop

       if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())

          {

              return;

          }

        Serial.print(F("PICC type: "));

        MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);

        Serial.println(rfid.PICC_GetTypeName(piccType));      // Read Type RFID Tag like 1K
4K
```

```
        //Check is the PICC of Classic MIFARE type
        if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI && piccType !=
        MFRC522::PICC_TYPE_MIFARE_1K && piccType != MFRC522::PICC_TYPE_MIFARE_4K)
          {
              Serial.println(F("Your tag is not of type MIFARE Classic."));
              return;
          }
     String strID = "";
     for (byte i = 0; i <= 4; i++)
          {
              strID += (rfid.uid.uidByte[i] < 0x10 ? "0" : "") + String(rfid.uid.uidByte[i],
HEX) + (i!=3 ?    ":" : "");
          }
    strID.toUpperCase();              //ตัวแปร strID เก็บค่า UID ของแท็กไว้...สามารถนำไปใช้งานได้
    Serial.print("Tap card key: ");   //"Tap card key: "
    Serial.println(strID);            //Print Tag Number
    Serial.println();
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
}                                     //End void loop


//****************************************************
*Arduino Code: 4_RFID with ESP8266 and LED
//****************************************************
#include "SPI.h"                      //For RFID
#include <Wire.h>                     //For I2C 1602LCD such as  SDA - CLK
#include <MFRC522.h>                  //For RFID
#include "Adafruit_MCP23017.h"        //For IC MCP23017
#define SS_PIN D3                     //SDA Pin D3           >>>   RFID
#define RST_PIN D8                    //Reset Pin D8         >>>   RFID
#define LED_R 7                       //LED RED              >>>   MCP23017 Pin 28
#define LED_Y 6                       //LED YELLOW           >>>   MCP23017 Pin 27
#define LED_G 5                       //LED GREEN            >>>   MCP23017 Pin 26
                                      //SCK Pin 5 Only
                                      //MISO Pin D6 Only
                                      //MOSI Pin D7 Only
MFRC522 rfid(SS_PIN, RST_PIN);        //For RFID  Reader
MFRC522::MIFARE_Key key;              //For RFID  Tag
Adafruit_MCP23017 mcp;                //For IC MCP23017
void setup() {                        //Start setup loop
      Serial.begin(115200);           //Serial Mornitor baud rate 115200
```

```
      SPI.begin();                    //For  SPI (RFID)
      rfid.PCD_Init();                //For  RFID
      mcp.begin();                    //For  MCP23017
      mcp.pinMode(7,OUTPUT);          //LED_RED       is    OUTPUT
      mcp.pinMode(6,OUTPUT);          //LED_YELLOW    is    OUTPUT
      mcp.pinMode(5,OUTPUT);   /      /LED_GREEN     is    OUTPUT
      mcp.digitalWrite(6,1);           //LED_YELLOW    >>    High
}                                     //END setup loop
void loop() {                         //Start void loop
     if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())
          {
              return;
          }
      Serial.print(F("PICC type: "));
      MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
      Serial.println(rfid.PICC_GetTypeName(piccType));
     //Check is the PICC of Classic MIFARE type
     if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI && piccType !=
     MFRC522::PICC_TYPE_MIFARE_1K && piccType != MFRC522::PICC_TYPE_MIFARE_4K)
          {
              Serial.println(F("Your tag is not of type MIFARE Classic."));
              return;
          }
     String strID = "";
     for (byte i = 0; i <= 4; i++)
          {
              strID += (rfid.uid.uidByte[i] < 0x10 ? "0" : "") + String(rfid.uid.uidByte[i],
HEX) + (i!=3 ?
              ":" : "");
          }
    strID.toUpperCase();
    Serial.print("Tap card key: ");
    Serial.println(strID);
    Serial.println();
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
    if (strID.indexOf("DA:03:B1:19")>= 0)     //TRUE
          {
        mcp.digitalWrite(6,0);                //LED_YELLOW OFF
        mcp.digitalWrite(5,1);                //LED_GREEN  ON
        delay(3000);                          //Delay 3 s
```

```
        mcp.digitalWrite(7,0);                //LED_RED OFF
        mcp.digitalWrite(6,1);                //LED_YELLOW ON
        mcp.digitalWrite(5,0);                //LED_GREEN OFF
          }
        else
        {
        mcp.digitalWrite(6,0);                //LED_YELLOW OFF
        mcp.digitalWrite(7,1);                //LED_RED ON
        delay(3000);                          //Delay 3 s
        mcp.digitalWrite(7,0);                //LED_RED OFF
        mcp.digitalWrite(6,1);                //LED_YELLOW ON
        }
}                                             //End void loop


//*************************************************
*Arduino Code: 5_ESP8266 Web Server
//*************************************************
// เรียกใช้ไลบรารีสำหรับเชื่อมต่อ Wi-Fi
#include <ESP8266WiFi.h>

// กำหนดชื่อเครือข่ายและรหัสผ่าน Wi-Fi
const char* ssid = "REPLACE_WITH_YOUR_SSID";
const char* password = "REPLACE_WITH_YOUR_PASSWORD";

// สร้างเว็บเซิร์ฟเวอร์ที่พอร์ต 80
WiFiServer server(80);

// ตัวแปรสำหรับเก็บข้อมูลส่วนหัวของ HTTP Request
String header;

// ตัวแปรสำหรับเก็บสถานะปัจจุบันของเอาต์พุต
String output5State = "off";
String output4State = "off";

// กำหนดหมายเลข GPIO ที่ใช้เป็นเอาต์พุต
const int output5 = 5;
const int output4 = 4;

void setup() {
  Serial.begin(115200);

  // กำหนด GPIO เป็นเอาต์พุต
  pinMode(output5, OUTPUT);
  pinMode(output4, OUTPUT);

  // กำหนดสถานะเริ่มต้นของเอาต์พุตเป็น LOW
  digitalWrite(output5, LOW);
  digitalWrite(output4, LOW);

  // เชื่อมต่อเครือข่าย Wi-Fi ด้วย SSID และรหัสผ่าน
  Serial.print("Connecting to ");
  Serial.println(ssid);

  WiFi.begin(ssid, password);
```

```
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }

  // แสดง IP Address และเริ่มต้นเว็บเซิร์ฟเวอร์
  Serial.println("");
  Serial.println("WiFi connected.");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());

  server.begin();
}

void loop() {
  // ตรวจสอบว่ามีไคลเอนต์เชื่อมต่อเข้ามาหรือไม่
  WiFiClient client = server.available();

  if (client) {
    Serial.println("New Client.");

    // ตัวแปรสำหรับเก็บข้อมูลของบรรทัดปัจจุบัน
    String currentLine = "";

    // ทำงานตราบเท่าที่ไคลเอนต์ยังคงเชื่อมต่อ
    while (client.connected()) {
      if (client.available()) {
        char c = client.read();

        // แสดงข้อมูลที่รับได้ทาง Serial Monitor
        Serial.write(c);

        // เก็บข้อมูลทั้งหมดไว้ในตัวแปร header
        header += c;

        if (c == '\n') {
          /*
            หาก currentLine มีความยาวเป็นศูนย์ หมายความว่าได้รับ
            อักขระขึ้นบรรทัดใหม่สองครั้งต่อเนื่องกัน ซึ่งเป็นจุดสิ้นสุด
            ของ HTTP Request Header
          */
          if (currentLine.length() == 0) {

            // ส่ง HTTP Response Header กลับไปยังไคลเอนต์
            client.println("HTTP/1.1 200 OK");
            client.println("Content-type:text/html");
            client.println("Connection: close");
            client.println();

            // ตรวจสอบ URL และควบคุม GPIO ตามคำสั่ง
            if (header.indexOf("GET /5/on") >= 0) {
              Serial.println("GPIO 5 on");
              output5State = "on";
              digitalWrite(output5, HIGH);

            } else if (header.indexOf("GET /5/off") >= 0) {
              Serial.println("GPIO 5 off");
              output5State = "off";
              digitalWrite(output5, LOW);

            } else if (header.indexOf("GET /4/on") >= 0) {
              Serial.println("GPIO 4 on");
              output4State = "on";
              digitalWrite(output4, HIGH);
```

```
} else if (header.indexOf("GET /4/off") >= 0) {
  Serial.println("GPIO 4 off");
  output4State = "off";
  digitalWrite(output4, LOW);
}

// เริ่มสร้างหน้าเว็บ HTML
client.println("<!DOCTYPE html><html>");

client.println(
  "<head><meta name=\"viewport\" "
  "content=\"width=device-width, initial-scale=1\">"
);

/*
  ป้องกันไม่ให้เว็บเบราว์เซอร์ส่งคำขอไฟล์ favicon เพิ่มเติม
*/
client.println("<link rel=\"icon\" href=\"data:,\">");

// กำหนดรูปแบบการแสดงผลด้วย CSS
client.println(
  "<style>html { font-family: Helvetica; "
  "display: inline-block; margin: 0px auto; "
  "text-align: center;}"
);

client.println(
  ".button { background-color: #195B6A; "
  "border: none; color: white; padding: 16px 40px;"
);

client.println(
  "text-decoration: none; font-size: 30px; "
  "margin: 2px; cursor: pointer;}"
);

client.println(
  ".button2 {background-color: #77878A;}"
  "</style></head>"
);

// หัวเรื่องของหน้าเว็บ
client.println("<body><h1>ESP8266 Web Server</h1>");

// แสดงสถานะและปุ่มควบคุม GPIO5
client.println(
  "<p>GPIO 5 - State " + output5State + "</p>"
);

if (output5State == "off") {
  client.println(
    "<p><a href=\"/5/on\">"
    "<button class=\"button\">ON</button>"
    "</a></p>"
  );
} else {
  client.println(
    "<p><a href=\"/5/off\">"
    "<button class=\"button button2\">OFF</button>"
    "</a></p>"
  );
}

// แสดงสถานะและปุ่มควบคุม GPIO4
client.println(
```

```
            "<p>GPIO 4 - State " + output4State + "</p>"
          );

          if (output4State == "off") {
            client.println(
              "<p><a href=\"/4/on\">"
              "<button class=\"button\">ON</button>"
              "</a></p>"
            );
          } else {
            client.println(
              "<p><a href=\"/4/off\">"
              "<button class=\"button button2\">OFF</button>"
              "</a></p>"
            );
          }

          client.println("</body></html>");

          // ปิดท้าย HTTP Response ด้วยบรรทัดว่าง
          client.println();

          // ออกจากลูป while
          break;

        } else {
          // เมื่อขึ้นบรรทัดใหม่ ให้ล้างข้อมูลบรรทัดปัจจุบัน
          currentLine = "";
        }

      } else if (c != '\r') {
        /*
          หากอักขระที่รับมาไม่ใช่ Carriage Return
          ให้เพิ่มอักขระลงใน currentLine
        */
        currentLine += c;
      }
    }
  }

  // ล้างข้อมูล HTTP Header
  header = "";

  // ยุติการเชื่อมต่อกับไคลเอนต์
  client.stop();

  Serial.println("Client disconnected.");
  Serial.println("");
 }
}
```

```
//**************************************************
*Arduino Code: 6_RFID Security System with Keypad, Servo, and Buzzer
//**************************************************
// Include required libraries
#include <MFRC522.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#include <Servo.h>
#include <SPI.h>

// Create instances
LiquidCrystal_I2C lcd(0x27, 16, 2);
```

```
MFRC522 mfrc522(10, 9); // MFRC522 mfrc522(SS_PIN, RST_PIN)
Servo sg90;

// Initialize Pins for led's, servo and buzzer
// Set Pins for led's, servo, buzzer and wipe button
constexpr uint8_t greenLed = 7;
constexpr uint8_t blueLed = 6;
constexpr uint8_t redLed = 5;
constexpr uint8_t servoPin = 8;
constexpr uint8_t buzzerPin = 4;
constexpr uint8_t wipeB = 3;                        // Button pin for WipeMode

char initial_password[4] = {'1', '2', '3', '4'};      // Variable to store initial password
String tagUID = "2A 3D EE 81";  // String to store UID of tag. Change it with your tag's UID
//String tagUID2 = "AA 1A A3 19";  // String to store UID2 of tag. Change it with your tag's
UID2
char password[4];                                   // Variable to store users password
boolean RFIDMode = true;                            // boolean to change modes
char key_pressed = 0;                               // Variable to store incoming keys
uint8_t i = 0;  // Variable used for counter

// defining how many rows and columns our keypad have
const byte rows = 4;
const byte columns = 4;

// Keypad pin map
char hexaKeys[rows][columns] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};

// Initializing pins for keypad
byte row_pins[rows] = {A0, A1, A2, A3};
byte column_pins[columns] = {2, 1, 0};

// Create instance for keypad
Keypad keypad_key = Keypad( makeKeymap(hexaKeys), row_pins, column_pins, rows, columns);

void setup() {
  // Arduino Pin configuration
  pinMode(buzzerPin, OUTPUT);
  pinMode(redLed, OUTPUT);
  pinMode(greenLed, OUTPUT);
  sg90.attach(servoPin);  //Declare pin 8 for servo
  sg90.write(0); // Set initial position at 90 degrees

  lcd.begin();   // LCD screen
  lcd.backlight();
  SPI.begin();      // Init SPI bus
  mfrc522.PCD_Init();   // Init MFRC522

  lcd.clear(); // Clear LCD screen
}

void loop() {
  // System will first look for mode
  if (RFIDMode == true) {
  digitalWrite(blueLed, HIGH);
    lcd.setCursor(0, 0);
    lcd.print(" RFID Door Lock");
    lcd.setCursor(0, 1);
    lcd.print(" Scan Your Card ");

 // Look for new cards
    if ( ! mfrc522.PICC_IsNewCardPresent()) {
      return;
    }

    // Select one of the cards
    if ( ! mfrc522.PICC_ReadCardSerial()) {
      return;
    }
```

```
  //Reading from the card
  String tag = "";
  for (byte j = 0; j < mfrc522.uid.size; j++)
  {
    tag.concat(String(mfrc522.uid.uidByte[j] < 0x10 ? " 0" : " "));
    tag.concat(String(mfrc522.uid.uidByte[j], HEX));
  }
  tag.toUpperCase();
  //Checking the card
  if (tag.substring(1) == tagUID)
 //if (tag.substring(2) == tagUID2)
   {
    // If UID of tag is matched.
    lcd.clear();
    lcd.print("Tag Matched");
    digitalWrite(greenLed, HIGH);
    digitalWrite(blueLed, LOW);
    delay(5000);
    digitalWrite(greenLed, LOW);
    digitalWrite(blueLed, HIGH);

    lcd.clear();
    lcd.print("Enter Password:");
    lcd.setCursor(0, 1);
    RFIDMode = false; // Make RFID mode false
  }

  else
  {
    // If UID of tag is not matched.
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Wrong Tag Shown");
    lcd.setCursor(0, 1);
    lcd.print("Access Denied");
    digitalWrite(buzzerPin, HIGH);
    digitalWrite(redLed, HIGH);
    digitalWrite(blueLed, LOW);
    delay(3000);
    digitalWrite(buzzerPin, LOW);
    digitalWrite(redLed, LOW);
    lcd.clear();
  }
}

// If RFID mode is false, it will look for keys from keypad
   if (RFIDMode == false) {
   key_pressed = keypad_key.getKey(); // Storing keys
   if (key_pressed)
  {
    password[i++] = key_pressed; // Storing in password variable
    lcd.print("*");
  }
     if (i == 4) // If 4 keys are completed
   {
    delay(200);
    if (!(strncmp(password, initial_password, 4))) // If password is matched
    {
      lcd.clear();
      lcd.print("Pass Accepted");
      digitalWrite(greenLed, HIGH);
       delay(2000);
      sg90.write(90); // Door Opened
       delay(5000);
      sg90.write(0); // Door Closed
      digitalWrite(greenLed, LOW);
      digitalWrite(blueLed, HIGH);

      lcd.clear();
      i = 0;
      RFIDMode = true; // Make RFID mode true
    }
    else    // If password is not matched
    {
```

```
        lcd.clear();
        lcd.print("Wrong Password");
        digitalWrite(buzzerPin, HIGH);
        digitalWrite(redLed, HIGH);
        digitalWrite(blueLed, LOW);
        delay(3000);
        digitalWrite(buzzerPin, LOW);
        digitalWrite(redLed, LOW);

        lcd.clear();
        i = 0;
        RFIDMode = true;  // Make RFID mode true
      }
    }
  }
}
```

```
//**************************************************
*Arduino Code: 7_RFID with ESP8266, LED, and LCD
//**************************************************
#include "SPI.h"                                //For RFID

#include <Wire.h>                               //For I2C 1602LCD such as  SDA - CLK

#include <MFRC522.h>                            //For RFID

#include <LiquidCrystal_I2C.h>                  //For I2C 1602LCD

#include "Adafruit_MCP23017.h"                  //For IC MCP23017

#define SS_PIN D3                               //SDA Pin D3       >>>   RFID

#define RST_PIN D8                              //Reset Pin D8     >>>   RFID

#define LED_R 7                                 //LED RED          >>>   MCP23017 Pin 28

#define LED_Y 6                                 //LED YELLOW       >>>   MCP23017 Pin 27

#define LED_G 5                                 //LED GREEN        >>>   MCP23017 Pin 26

#define SW D0                                   //Switch Pin D0

                                                //SCK Pin 5 Only

                                                //MISO Pin D6 Only

                                                //MOSI Pin D7 Only

MFRC522 rfid(SS_PIN, RST_PIN);                  //For RFID  Reader

MFRC522::MIFARE_Key key;                        //For RFID  Tag

LiquidCrystal_I2C lcd(0x27, 16, 2);             //For I²C   LCD Change 0x3F or 0x27

Adafruit_MCP23017 mcp;                          //For IC    MCP23017

void setup()

{                                               //Start setup loop

      Serial.begin(115200);                     //Serial Mornitor baud rate 115200

      SPI.begin();                                      //For  SPI (RFID)

      lcd.backlight();                                  //FOR LCD Screen

      rfid.PCD_Init();                                  //For  RFID

      lcd.begin();                                      //For  LCD

      mcp.begin();                                      //For  MCP23017

      lcd.backlight();                                  //LCD  Open  Light
```

```
      lcd.setCursor(1,0);                              //SetCursor Column 1 - Low 1
      lcd.print("RFID Door Lock");                     //LCD  print "RFID Door Lock"
      lcd.setCursor(3,1);                              //SetCursor Column 3 - Low 2
      lcd.print("PRESS TAG!");                         //LCD  print "PRESS TAG!"
      mcp.pinMode(7,OUTPUT);                           //LED_RED is OUTPUT
      mcp.pinMode(6,OUTPUT);                           //LED_YELLOW is OUTPUT
      mcp.pinMode(5,OUTPUT);                           //LED_GREEN is OUTPUT
      mcp.digitalWrite(6,1);                           //LED_YELLOW >> High
}                                                      //END setup loop


void loop()
{                                                      //Start void loop
     if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())
          {
              return;
          }
      Serial.print(F("PICC type: "));
      MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
      Serial.println(rfid.PICC_GetTypeName(piccType));
     //Check is the PICC of Classic MIFARE type
     if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI && piccType !=
MFRC522::PICC_TYPE_MIFARE_1K && piccType != MFRC522::PICC_TYPE_MIFARE_4K)
          {
              Serial.println(F("Your tag is not of type MIFARE Classic."));
              return;
          }
     String strID = "";
     for (byte i = 0; i <= 4; i++)
          {
              strID += (rfid.uid.uidByte[i] < 0x10 ? "0" : "") + String(rfid.uid.uidByte[i],
HEX) + (i!=3 ?
              ":" : "");
          }
    strID.toUpperCase();
    Serial.print("Tap card key: ");
    Serial.println(strID);
    Serial.println();
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
    if (strID.indexOf("DA:03:B1:19")>= 0)
          {
```

```
            RFID_Tag_TRUE();                        //Call RFID_Tag_TRUE() Function
        }
                                                    //RFID Tag is FALSE
    else
        {
            RFID_Tag_FALSE();                       //Call RFID_Tag_FALSE() Function
        }
}                                                   //End void loop
void OriginalDisplay()                              //OriginalDisplay Function
{
       lcd.clear();                                 //Clear LCD    Display
       lcd.setCursor(1,0);                          //SetCursor    Column 1 - Low 1
       lcd.print("RFID Door Lock");                 //LCD  print   "RFID Door Lock"
       lcd.setCursor(3,1);                          //SetCursor    Column 3 - Low 2
       lcd.print("PRESS TAG!");                     //LCD  print   "PRESS TAG!"
       mcp.digitalWrite(7,0);                       //LED_RED OFF
       mcp.digitalWrite(6,1);                       //LED_YELLOW ON
       mcp.digitalWrite(5,0);                       //LED_GREEN OFF
}
void RFID_Tag_TRUE()                                //RFID_Tag_TRUE Function
{
      lcd.clear();                                  //Clear LCD Display
      lcd.setCursor(4,0);                           //SetCursor  Column 4 - Low 1
      lcd.print("WELCOME!");                        //LCD print  "Welcome"
      lcd.setCursor(4,1);                           //SetCursor  Column 4 - Low 2
      lcd.print("THANKYOU");                        //LCD print  "Thank you"
      mcp.digitalWrite(6,0);                        //LED_YELLOW OFF
      mcp.digitalWrite(5,1);                        //LED_GREEN  ON
      delay(3000);                                  //Delay 3s
      OriginalDisplay();                            //Call OriginalDisplay() Function
}
void RFID_Tag_FALSE()                               //RFID_Tag_FALSE Function
{
      lcd.clear();                                  //Clear LCD Display
      lcd.setCursor(4,0);                           //SetCursor   Column 4 - Low 1
      lcd.print("SORRY!!");                         //LCD print   "WRONG!!"
      lcd.setCursor(2,1);                           //SetCursor   Column 3 - Low 2
      lcd.print("NOT ACCESS");                      //LCD print   "TRY AGAIN"
      mcp.digitalWrite(7,1);                        //LED_RED     ON
      mcp.digitalWrite(6,0);                        //LED_YELLOW  OFF
      delay(3000);
      OriginalDisplay();                            //Call OriginalDisplay() Function
}
```

```
//****************************************************
*Arduino Code: 8_RFID with ESP8266, LED, LCD, and Solenoid Door Lock
//****************************************************
#include "SPI.h"                                //For RFID

#include <Wire.h>                               //For I2C 1602LCD such as  SDA - CLK

#include <MFRC522.h>                            //For RFID

#include <LiquidCrystal_I2C.h>                  //For I2C 1602LCD

#include "Adafruit_MCP23017.h"                  //For IC MCP23017

#define SS_PIN D3                               //SDA Pin D3        >>>   RFID

#define RST_PIN D8                              //Reset Pin D8      >>>   RFID

#define LED_R 7                                 //LED RED           >>>   MCP23017 Pin 28

#define LED_Y 6                                 //LED YELLOW        >>>   MCP23017 Pin 27

#define LED_G 5                                 //LED GREEN         >>>   MCP23017 Pin 26

#define RELAY 4                                 //Relay_Module      >>>   MSP23017 Pin 25

#define SW D0                                   //Switch Pin D0

                                                //SCK Pin 5 Only

                                                //MISO Pin D6 Only

                                                //MOSI Pin D7 Only

MFRC522 rfid(SS_PIN, RST_PIN);                  //For RFID  Reader

MFRC522::MIFARE_Key key;                        //For RFID  Tag

LiquidCrystal_I2C lcd(0x27, 16, 2);             //For I2C   LCD Change 0x3F or 0x27

Adafruit_MCP23017 mcp;                          //For IC    MCP23017

void setup()

  {                                             //Start setup loop

      Serial.begin(115200);                     //Serial Mornitor baud rate 115200

      SPI.begin();                              //For  SPI (RFID)

      lcd.backlight();

      rfid.PCD_Init();                          //For  RFID

      lcd.begin();                              //For  LCD

      mcp.begin();                              //For  MCP23017

      lcd.backlight();                          //LCD  Open    Light

      lcd.setCursor(1,0);                       //SetCursor    Column 1 - Low 1

      lcd.print("RFID Door Lock");              //LCD  print   "RFID Door Lock"

      lcd.setCursor(3,1);                       //SetCursor    Column 3 - Low 2

      lcd.print("PRESS TAG!");                  //LCD  print   "PRESS TAG!"

          pinMode(D0,INPUT);                    //Switch        is    INPUT

      mcp.pinMode(7,OUTPUT);                    //LED_RED       is    OUTPUT

      mcp.pinMode(6,OUTPUT);                    //LED_YELLOW    is    OUTPUT

      mcp.pinMode(5,OUTPUT);                    //LED_GREEN     is    OUTPUT

      mcp.pinMode(4,OUTPUT);                    //Relay         is    OUTPUT

      mcp.digitalWrite(6,1);                    //LED_YELLOW   >>    High

      mcp.digitalWrite(4,1);                    //Relay >>    High ( Relay Active Low(0) )
```

```
}                                                   //END setup loop
void loop()
{                                                   //Start void loop
    if(digitalRead(D0)==0)                          //If Press the switch
          {
              Switch();                             //Call Switch() Function
          }
     if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())
          {
              return;
          }
      Serial.print(F("PICC type: "));
      MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
      Serial.println(rfid.PICC_GetTypeName(piccType));
     //Check is the PICC of Classic MIFARE type
     if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI && piccType !=
     MFRC522::PICC_TYPE_MIFARE_1K && piccType != MFRC522::PICC_TYPE_MIFARE_4K)
          {
              Serial.println(F("Your tag is not of type MIFARE Classic."));
              return;
          }
     String strID = "";
     for (byte i = 0; i <= 4; i++)
          {
              strID += (rfid.uid.uidByte[i] < 0x10 ? "0" : "") + String(rfid.uid.uidByte[i],
HEX) + (i!=3 ?
              ":" : "");
          }
    strID.toUpperCase();
    Serial.print("Tap card key: ");
    Serial.println(strID);
    Serial.println();
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
    if (strID.indexOf("DA:03:B1:19")>= 0)
          {
              RFID_Tag_TRUE();                          //Call RFID_Tag_TRUE() Function
          }
    //RFID Tag is FALSE
    else
          {
              RFID_Tag_FALSE();                         //Call RFID_Tag_FALSE() Function
          }
}                                                   //End void loop
```

```
void OriginalDisplay()                          //OriginalDisplay Function
{
       lcd.clear();                             //Clear LCD      Display
       lcd.setCursor(1,0);                      //SetCursor    Column 1 - Low 1
       lcd.print("RFID Door Lock");            //LCD  print   "RFID Door Lock"
       lcd.setCursor(3,1);                      //SetCursor    Column 3 - Low 2
       lcd.print("PRESS TAG!");                //LCD  print   "PRESS TAG!"
       mcp.digitalWrite(7,0);                   //LED_RED OFF
       mcp.digitalWrite(6,1);                   //LED_YELLOW ON
       mcp.digitalWrite(5,0);                   //LED_GREEN OFF
}
void Switch()                                   //Switch Function
{
       lcd.clear();                             //Clear LCD      Display
       lcd.setCursor(3,0);                      //SetCursor      Column 3 - Low 1
       lcd.print("SWITCHMODE");                //LCD print      "SwitchMode"
       mcp.digitalWrite(6,0);                   //LED_YELLOW     OFF
       mcp.digitalWrite(5,1);                   //LED_GREEN      ON
       mcp.digitalWrite(4,0);                   //Relay = 0      >>>  Working
       delay(5000);                             //Delay 5s
       mcp.digitalWrite(4,1);                   //Relay = 1      >>>  Stop Working
       OriginalDisplay();                       //Call OriginalDisplay() Function
}
void RFID_Tag_TRUE()                            //RFID_Tag_TRUE Function
{
      lcd.clear();                              //Clear LCD Display
      lcd.setCursor(4,0);                       //SetCursor  Column 4 - Low 1
      lcd.print("WELCOME!");                    //LCD print  "Welcome"
      lcd.setCursor(4,1);                       //SetCursor  Column 4 - Low 2
      lcd.print("THANKYOU");                    //LCD print  "Thank you"
      mcp.digitalWrite(6,0);                    //LED_YELLOW OFF
      mcp.digitalWrite(5,1);                    //LED_GREEN  ON
      mcp.digitalWrite(4,0);                    //Relay Working
      delay(5000);                              //Delay 5s
      mcp.digitalWrite(4,1);                    //Relay Stop Working
      OriginalDisplay();                        //Call OriginalDisplay() Function
}
void RFID_Tag_FALSE()                           //RFID_Tag_FALSE Function
{
      lcd.clear();                              //Clear LCD Display
```

```
      lcd.setCursor(4,0);                           //SetCursor   Column 4 - Low 1
      lcd.print("SORRY!!");                         //LCD print   "WRONG!!"
      lcd.setCursor(2,1);                           //SetCursor   Column 3 - Low 2
      lcd.print("NOT ACCESS");                      //LCD print   "TRY AGAIN"
      mcp.digitalWrite(7,1);                        //LED_RED     ON
      mcp.digitalWrite(6,0);                        //LED_YELLOW  OFF
      delay(3000);
      OriginalDisplay();                            //Call OriginalDisplay() Function
}
```

```
//****************************************************
*Arduino Code: 9_RFID, ESP8266, with LINE Messaging API
//****************************************************
#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <ESP8266HTTPClient.h>
#include "SPI.h"
#include <Wire.h>
#include <MFRC522.h>
#include <LiquidCrystal_I2C.h>
#include "Adafruit_MCP23017.h"

#define SS_PIN D3
#define RST_PIN D8
#define LED_R 7
#define LED_Y 6
#define LED_G 5
#define RELAY 4
#define SW D0

const char* ssid = "YOUR_WIFI_NAME";
const char* pass = "YOUR_WIFI_PASSWORD";

// LINE Messaging API
String LINE_ACCESS_TOKEN = "YOUR_CHANNEL_ACCESS_TOKEN";
String LINE_USER_ID = "YOUR_USER_ID_OR_GROUP_ID";

MFRC522 rfid(SS_PIN, RST_PIN);
MFRC522::MIFARE_Key key;
LiquidCrystal_I2C lcd(0x27, 16, 2);
Adafruit_MCP23017 mcp;

void sendLineMessage(String message) {
  WiFiClientSecure client;
  HTTPClient https;

  client.setInsecure();

  if (https.begin(client, "https://api.line.me/v2/bot/message/push")) {
    https.addHeader("Content-Type", "application/json");
    https.addHeader("Authorization", "Bearer " + LINE_ACCESS_TOKEN);

    String payload = "{";
    payload += "\"to\":\"" + LINE_USER_ID + "\",";
    payload += "\"messages\":[{";
    payload += "\"type\":\"text\",";
    payload += "\"text\":\"" + message + "\"";
    payload += "}]";
    payload += "}";
    int httpCode = https.POST(payload);
    Serial.print("LINE Response Code: ");
    Serial.println(httpCode);

    https.end();
```

```
  }
}

void setup() {
  Serial.begin(115200);
  SPI.begin();

  lcd.begin();
  lcd.backlight();

  rfid.PCD_Init();
  mcp.begin();

  WiFi.begin(ssid, pass);
  while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(500);
  }

  Serial.println();
  Serial.println("WiFi connected");
  Serial.print("IP Address: ");
  Serial.println(WiFi.localIP());

  sendLineMessage("RFID Door Lock Connected");

  lcd.setCursor(1, 0);
  lcd.print("RFID Door Lock");
  lcd.setCursor(3, 1);
  lcd.print("PRESS TAG!");

  pinMode(SW, INPUT);

  mcp.pinMode(LED_R, OUTPUT);
  mcp.pinMode(LED_Y, OUTPUT);
  mcp.pinMode(LED_G, OUTPUT);
  mcp.pinMode(RELAY, OUTPUT);

  mcp.digitalWrite(LED_Y, 1);
  mcp.digitalWrite(RELAY, 1);   // Relay Active LOW
}
void loop() {
  if (digitalRead(SW) == 0) {
    Switch();
  }

  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial()) {
    return;
  }

  String strID = "";

  for (byte i = 0; i < rfid.uid.size; i++) {
    strID += (rfid.uid.uidByte[i] < 0x10 ? "0" : "");
    strID += String(rfid.uid.uidByte[i], HEX);
    if (i < rfid.uid.size - 1) strID += ":";
  }

  strID.toUpperCase();

  Serial.print("Tap card key: ");
  Serial.println(strID);

  rfid.PICC_HaltA();
  rfid.PCD_StopCrypto1();

  if (strID == "DA:03:B1:19") {
    RFID_Tag_TRUE();
  } else {
    RFID_Tag_FALSE();
  }
}

void OriginalDisplay() {
```

```
  lcd.clear();
  lcd.setCursor(1, 0);
  lcd.print("RFID Door Lock");
  lcd.setCursor(3, 1);
  lcd.print("PRESS TAG!");

  mcp.digitalWrite(LED_R, 0);
  mcp.digitalWrite(LED_Y, 1);
  mcp.digitalWrite(LED_G, 0);
}

void Switch() {
  sendLineMessage("Door opened by switch");
  lcd.clear();
  lcd.setCursor(3, 0);
  lcd.print("SWITCHMODE");

  mcp.digitalWrite(LED_Y, 0);
  mcp.digitalWrite(LED_G, 1);
  mcp.digitalWrite(RELAY, 0);

  delay(5000);

  mcp.digitalWrite(RELAY, 1);
  OriginalDisplay();
}

void RFID_Tag_TRUE() {
  sendLineMessage("Access granted: Door opened");

  lcd.clear();
  lcd.setCursor(4, 0);
  lcd.print("WELCOME!");
  lcd.setCursor(4, 1);
  lcd.print("THANKYOU");

  mcp.digitalWrite(LED_Y, 0);
  mcp.digitalWrite(LED_G, 1);
  mcp.digitalWrite(RELAY, 0);

  delay(5000);

  mcp.digitalWrite(RELAY, 1);
  OriginalDisplay();
}

void RFID_Tag_FALSE() {
  sendLineMessage("Access denied: Unknown RFID tag");

  lcd.clear();
  lcd.setCursor(4, 0);
  lcd.print("SORRY!!");
  lcd.setCursor(2, 1);
  lcd.print("NOT ACCESS");

  mcp.digitalWrite(LED_R, 1);
  mcp.digitalWrite(LED_Y, 0);

  delay(2000);
  OriginalDisplay();
}



//**************************************************
*Arduino Code: 10_RFID, ESP8266, IP camera, with LINE Messaging API
//**************************************************

/*
*RFID + ESP8266 + IP Camera Link + LINE Messaging API
*
*Board: NodeMCU 1.0 (ESP-12E Module)
*
```

```
*RFID-RC522
* SDA/SS -> D3 (GPIO0)
* RST    -> D8 (GPIO15)
* SCK    -> D5 (GPIO14)
* MISO   -> D6 (GPIO12)
* MOSI   -> D7 (GPIO13)
* VCC    -> 3.3V
* GND    -> GND
*
*I2C
* SDA -> D2 (GPIO4)
* SCL -> D1 (GPIO5)
*
*MCP23017
* GPA7 -> LED red
* GPA6 -> LED yellow
* GPA5 -> LED green
* GPA4 -> relay IN (active LOW)
*
*Exit switch
* D0 (GPIO16) -> switch -> GND
* Install an external 10 kΩ pull-up resistor from D0 to 3.3V
*/

#include <ESP8266WiFi.h>
#include <WiFiClientSecureBearSSL.h>
#include <ESP8266HTTPClient.h>

#include <SPI.h>
#include <Wire.h>
#include <MFRC522.h>
#include <LiquidCrystal_I2C.h>
#include <Adafruit_MCP23X17.h>

//-----------------------------------------------
//Pin configuration
//-----------------------------------------------
constexpr uint8_t RFID_SS_PIN  = D3;
constexpr uint8_t RFID_RST_PIN = D8;
constexpr uint8_t EXIT_SWITCH_PIN = D0;

//MCP23017 logical pin numbers
constexpr uint8_t LED_RED_PIN    = 7;  // GPA7, DIP pin 28
constexpr uint8_t LED_YELLOW_PIN = 6;  // GPA6, DIP pin 27
constexpr uint8_t LED_GREEN_PIN  = 5;  // GPA5, DIP pin 26
constexpr uint8_t RELAY_PIN      = 4;  // GPA4, DIP pin 25

//Relay module is active LOW
constexpr uint8_t RELAY_ON  = LOW;
constexpr uint8_t RELAY_OFF = HIGH;

//-----------------------------------------------
//Time configuration
//-----------------------------------------------
constexpr unsigned long DOOR_OPEN_TIME_MS = 5000;
constexpr unsigned long DENIED_TIME_MS    = 3000;
constexpr unsigned long RFID_DEBOUNCE_MS  = 2000;
constexpr unsigned long SWITCH_DEBOUNCE_MS = 80;
constexpr unsigned long WIFI_TIMEOUT_MS   = 20000;
constexpr unsigned long HTTP_TIMEOUT_MS   = 10000;

//-----------------------------------------------
//Network configuration
//Do not publish real credentials.
//-----------------------------------------------
const char WIFI_SSID[]     = "YOUR_WIFI_NAME";
```

```
const char WIFI_PASSWORD[] = "YOUR_WIFI_PASSWORD";

//-----------------------------------------
// LINE Messaging API
//-----------------------------------------
const char LINE_PUSH_ENDPOINT[] =
  "https://api.line.me/v2/bot/message/push";

const char LINE_CHANNEL_ACCESS_TOKEN[] =
  "YOUR_CHANNEL_ACCESS_TOKEN";

const char LINE_RECIPIENT_ID[] =
  "YOUR_USER_ID_GROUP_ID_OR_ROOM_ID";

//-----------------------------------------
// Camera link
//
// This must not contain the camera username/password.
// A local URL can only be opened from the same LAN or VPN.
//-----------------------------------------
const char CAMERA_VIEW_URL[] =
  "http://192.168.43.2:8475/";

//-----------------------------------------
// Authorized RFID UID
//-----------------------------------------
const char MASTER_UID[] = "DA:03:B1:19";

//-----------------------------------------
// I2C configuration
//-----------------------------------------
constexpr uint8_t LCD_ADDRESS = 0x27;
constexpr uint8_t MCP_ADDRESS = 0x20;

//-----------------------------------------
// Objects
//-----------------------------------------
MFRC522 rfid(RFID_SS_PIN, RFID_RST_PIN);
LiquidCrystal_I2C lcd(LCD_ADDRESS, 16, 2);
Adafruit_MCP23X17 mcp;

//-----------------------------------------
// State variables
//-----------------------------------------
unsigned long lastRFIDTime = 0;
unsigned long lastSwitchChangeTime = 0;

bool previousSwitchReading = HIGH;
bool stableSwitchState = HIGH;

//-----------------------------------------
// Function declarations
//-----------------------------------------
void showReadyScreen();
void showNetworkError();

bool connectWiFi();
bool sendLineText(const String &message);

String readRFIDUID();
String maskUID(const String &uid);
String jsonEscape(const String &text);

void openDoorFor(unsigned long durationMs);
void openBySwitch();
void accessGranted(const String &uid);
void accessDenied(const String &uid);

void processExitSwitch();
```

```
void finishRFIDCommunication();

//==========================================
// SETUP
//==========================================
void setup()
{
    Serial.begin(115200);
    delay(100);

 /*
 * GPIO16/D0 does not provide the usual INPUT_PULLUP
 * behavior on ESP8266. Use INPUT and install an
 * external 10 kΩ pull-up resistor to 3.3V.
 */
    pinMode(EXIT_SWITCH_PIN, INPUT);

 // I2C: SDA = D2, SCL = D1
    Wire.begin(D2, D1);

 // Initialize LCD
    lcd.init();
    lcd.backlight();

 // Initialize MCP23017
    if (!mcp.begin_I2C(MCP_ADDRESS, &Wire)) {
        Serial.println(F("ERROR: MCP23017 not detected"));

        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print(F("MCP23017 ERROR"));
        lcd.setCursor(0, 1);
        lcd.print(F("Check wiring"));

  // Stop because relay and LEDs cannot be controlled safely.
        while (true) {
            delay(1000);
        }
    }

    mcp.pinMode(LED_RED_PIN, OUTPUT);
    mcp.pinMode(LED_YELLOW_PIN, OUTPUT);
    mcp.pinMode(LED_GREEN_PIN, OUTPUT);
    mcp.pinMode(RELAY_PIN, OUTPUT);

 /*
 * Set the relay OFF immediately after MCP23017 starts.
 * A hardware pull-up on relay IN is also recommended
 * to prevent a brief unlock during startup.
 */
    mcp.digitalWrite(RELAY_PIN, RELAY_OFF);
    mcp.digitalWrite(LED_RED_PIN, LOW);
    mcp.digitalWrite(LED_YELLOW_PIN, HIGH);
    mcp.digitalWrite(LED_GREEN_PIN, LOW);

 // Initialize SPI and RFID
    SPI.begin();
    rfid.PCD_Init();

    showReadyScreen();

    if (connectWiFi()) {
        Serial.print(F("ESP8266 IP address: "));
        Serial.println(WiFi.localIP());

        sendLineText(
            F("RFID Door Lock พร้อมใช้งาน\n"
    "สถานะประตู: ล็อก")
  );
```

```
    } else {
        showNetworkError();
        delay(1500);
        showReadyScreen();
    }

    Serial.println(F("System initialization complete"));
}

//=====================================
//MAIN LOOP
//=====================================
void loop()
{
    processExitSwitch();

    if (!rfid.PICC_IsNewCardPresent()) {
        delay(5);
        return;
    }

    if (!rfid.PICC_ReadCardSerial()) {
        delay(5);
        return;
    }

    const unsigned long now = millis();

    if (now - lastRFIDTime < RFID_DEBOUNCE_MS) {
        finishRFIDCommunication();
        return;
    }

    lastRFIDTime = now;

    const String uid = readRFIDUID();

    Serial.print(F("RFID UID: "));
    Serial.println(uid);

    finishRFIDCommunication();

    if (uid.equalsIgnoreCase(MASTER_UID)) {
        accessGranted(uid);
    } else {
        accessDenied(uid);
    }
}

//=====================================
//WI-FI
//=====================================
bool connectWiFi()
{
    if (WiFi.status() == WL_CONNECTED) {
        return true;
    }

    WiFi.mode(WIFI_STA);
    WiFi.persistent(false);
    WiFi.setAutoReconnect(true);

    WiFi.begin(WIFI_SSID, WIFI_PASSWORD);

    Serial.print(F("Connecting to Wi-Fi"));

    const unsigned long startTime = millis();

    while (WiFi.status() != WL_CONNECTED &&
           millis() - startTime < WIFI_TIMEOUT_MS) {
        Serial.print('.');
        delay(500);
    }
```

```
    Serial.println();

    if (WiFi.status() == WL_CONNECTED) {
        Serial.println(F("Wi-Fi connected"));
        return true;
    }

    Serial.println(F("Wi-Fi connection failed"));
    return false;
}

//=========================================
//EXIT SWITCH
//=========================================
void processExitSwitch()
{
    const bool currentReading = digitalRead(EXIT_SWITCH_PIN);

    if (currentReading != previousSwitchReading) {
        lastSwitchChangeTime = millis();
        previousSwitchReading = currentReading;
    }

    if (millis() - lastSwitchChangeTime >= SWITCH_DEBOUNCE_MS) {
        if (currentReading != stableSwitchState) {
            stableSwitchState = currentReading;

   //Falling edge: switch has just been pressed.
            if (stableSwitchState == LOW) {
                openBySwitch();
            }
        }
    }
}

//=========================================
//RFID
//=========================================
String readRFIDUID()
{
    String uid;
    uid.reserve((rfid.uid.size * 3) - 1);

    for (byte i = 0; i < rfid.uid.size; i++) {
        if (rfid.uid.uidByte[i] < 0x10) {
            uid += '0';
        }

        uid += String(rfid.uid.uidByte[i], HEX);

        if (i < rfid.uid.size - 1) {
            uid += ':';
        }
    }

    uid.toUpperCase();
    return uid;
}

void finishRFIDCommunication()
{
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
}

String maskUID(const String &uid)
{
 /*
 *Example:
 *DA:03:B1:19 -> DA:03:**:**
 */
```

```
    const int secondSeparator = uid.indexOf(
        ':',
        uid.indexOf(':') + 1
);

    if (secondSeparator < 0){
        return F("Hidden");
    }

    return uid.substring(0, secondSeparator) + F(":**:**");
}

//=====================================
//DOOR CONTROL
//=====================================
void openDoorFor(unsigned long durationMs)
{
 //Unlock
    mcp.digitalWrite(RELAY_PIN, RELAY_ON);

    const unsigned long unlockStart = millis();

    while (millis() - unlockStart < durationMs) {
        delay(10);
    }

 //Lock before performing any network communication.
    mcp.digitalWrite(RELAY_PIN, RELAY_OFF);
}

void openBySwitch()
{
    Serial.println(F("Door requested by exit switch"));

    lcd.clear();
    lcd.setCursor(2, 0);
    lcd.print(F("SWITCH MODE"));
    lcd.setCursor(3, 1);
    lcd.print(F("DOOR OPEN"));

    mcp.digitalWrite(LED_RED_PIN, LOW);
    mcp.digitalWrite(LED_YELLOW_PIN, LOW);
    mcp.digitalWrite(LED_GREEN_PIN, HIGH);

 //Unlock for exactly the configured interval.
    openDoorFor(DOOR_OPEN_TIME_MS);

 //The door is locked again before sending LINE.
    showReadyScreen();

    String message;
    message.reserve(200);

    message += F("มีการกดสวิตช์ปิดประตูจากด้านใน\n");
    message += F("สถานะ: เปิดชั่วคราว 5 วินาทีและล็อกกลับแล้ว\n");
    message += F("ภาพจากกล้อง: ");
    message += CAMERA_VIEW_URL;

    sendLineText(message);
}

void accessGranted(const String &uid)
{
    Serial.println(F("Access granted"));

    lcd.clear();
    lcd.setCursor(4, 0);
    lcd.print(F("WELCOME!"));
    lcd.setCursor(3, 1);
    lcd.print(F("DOOR OPEN"));
```

```
    mcp.digitalWrite(LED_RED_PIN, LOW);
    mcp.digitalWrite(LED_YELLOW_PIN, LOW);
    mcp.digitalWrite(LED_GREEN_PIN, HIGH);

 //Unlock first, then lock before calling LINE API.
    openDoorFor(DOOR_OPEN_TIME_MS);

    showReadyScreen();

    String message;
    message.reserve(220);

    message += F("อนุญาตให้เข้าใช้งาน\n");
    message += F("UID: ");
    message += maskUID(uid);
    message += F("\nสถานะ: เปิด 5 วินาทีและล็อกกลับแล้ว\n");
    message += F("ภาพจากกล้อง: ");
    message += CAMERA_VIEW_URL;

    sendLineText(message);
}

void accessDenied(const String &uid)
{
    Serial.println(F("Access denied"));

 //Explicitly keep the relay OFF.
    mcp.digitalWrite(RELAY_PIN, RELAY_OFF);

    lcd.clear();
    lcd.setCursor(4, 0);
    lcd.print(F("SORRY!!"));
    lcd.setCursor(2, 1);
    lcd.print(F("ACCESS DENIED"));

    mcp.digitalWrite(LED_RED_PIN, HIGH);
    mcp.digitalWrite(LED_YELLOW_PIN, LOW);
    mcp.digitalWrite(LED_GREEN_PIN, LOW);

    delay(DENIED_TIME_MS);

    showReadyScreen();

    String message;
    message.reserve(220);

    message += F("แจ้งเตือน: ปฏิเสธการเข้าใช้งาน\n");
    message += F("UID: ");
    message += maskUID(uid);
    message += F("\nสถานะประตู: ล็อก\n");
    message += F("ภาพจากกล้อง: ");
    message += CAMERA_VIEW_URL;

    sendLineText(message);
}

//==========================================
//DISPLAY
//==========================================
void showReadyScreen()
{
 //Fail-secure state: relay OFF and door locked.
    mcp.digitalWrite(RELAY_PIN, RELAY_OFF);

    mcp.digitalWrite(LED_RED_PIN, LOW);
    mcp.digitalWrite(LED_YELLOW_PIN, HIGH);
    mcp.digitalWrite(LED_GREEN_PIN, LOW);

    lcd.clear();
    lcd.setCursor(1, 0);
    lcd.print(F("RFID Door Lock"));
    lcd.setCursor(3, 1);
```

```
    lcd.print(F("PRESS TAG!"));
}

void showNetworkError()
{
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print(F("NETWORK ERROR"));
    lcd.setCursor(0, 1);
    lcd.print(F("Door remains lock"));
}

//=========================================
//JSON
//=========================================
String jsonEscape(const String &text)
{
    String escaped;
    escaped.reserve(text.length() + 32);

    for (size_t i = 0; i < text.length(); i++) {
        const char c = text.charAt(i);

        switch (c) {
            case '\\':
                escaped += F("\\\\");
                break;

            case '"':
                escaped += F("\\\"");
                break;

            case '\n':
                escaped += F("\\n");
                break;

            case '\r':
                break;

            case '\t':
                escaped += F("\\t");
                break;

            default:
     /*
     *UTF-8 Thai bytes are preserved.
     *Other control characters are omitted.
     */
                if (static_cast<uint8_t>(c) >= 0x20) {
                    escaped += c;
                }
                break;
        }
    }

    return escaped;
}

//=========================================
//LINE MESSAGING API
//=========================================
bool sendLineText(const String &message)
{
    if (WiFi.status() != WL_CONNECTED && !connectWiFi()) {
        Serial.println(F("LINE not sent: Wi-Fi unavailable"));
        return false;
    }

    if (String(LINE_CHANNEL_ACCESS_TOKEN).startsWith("YOUR_") ||
        String(LINE_RECIPIENT_ID).startsWith("YOUR_")) {
        Serial.println(F("LINE credentials are not configured"));
        return false;
```

```
    }

    BearSSL::WiFiClientSecure secureClient;

 /*
 *IMPORTANT:
 *This setting is acceptable only for a controlled classroom
 *demonstration. It encrypts traffic but does not authenticate
 *the LINE server.
 *
 *For deployment, remove setInsecure() and configure the current
 *trusted Root CA with BearSSL::X509List and setTrustAnchors().
 */
    secureClient.setInsecure();
    secureClient.setTimeout(HTTP_TIMEOUT_MS / 1000);

    HTTPClient https;
    https.setTimeout(HTTP_TIMEOUT_MS);

    if (!https.begin(secureClient, LINE_PUSH_ENDPOINT)) {
        Serial.println(F("Unable to initialize LINE HTTPS connection"));
        return false;
    }

    https.addHeader(F("Content-Type"), F("application/json"));
    https.addHeader(
        F("Authorization"),
        String(F("Bearer ")) + LINE_CHANNEL_ACCESS_TOKEN
);

    String payload;
    payload.reserve(message.length() + 160);

    payload += F("{\"to\":\"");
    payload += jsonEscape(LINE_RECIPIENT_ID);
    payload += F("\",\"messages\":[{\"type\":\"text\",\"text\":\"");
    payload += jsonEscape(message);
    payload += F("\"}]}");

    const int httpCode = https.POST(payload);
    const String response = https.getString();

    Serial.print(F("LINE HTTP status: "));
    Serial.println(httpCode);

    if (response.length() > 0) {
        Serial.print(F("LINE response: "));
        Serial.println(response);
    }

    https.end();

    const bool success =
        httpCode >= 200 && httpCode < 300;

    if (!success) {
        Serial.println(F("LINE message delivery failed"));
    }

    return success;
}
```

```
//*****************************************************
*Arduino Code: 11_ Fingerprint Basic
//*****************************************************

//โปรแกรมเก็บลายนิ้วมือ
        #include <Adafruit_Fingerprint.h>

        // On Leonardo/Micro or others with hardware serial, use those! #0 is green wire, #1
        is white
        // uncomment this line:
        // #define mySerial Serial1

        // For UNO and others without hardware serial, we must use software serial...
        // pin #2 is IN from sensor (GREEN wire)
        // pin #3 is OUT from arduino  (WHITE wire)
        // comment these two lines if using hardware serial
        #include <SoftwareSerial.h>
        SoftwareSerial mySerial(2, 3);

        Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

        uint8_t id;

        void setup()
        {
          Serial.begin(9600);
          while (!Serial);  // For Yun/Leo/Micro/Zero/...
          delay(100);
          Serial.println("\n\nAdafruit Fingerprint sensor enrollment");

          // set the data rate for the sensor serial port
          finger.begin(57600);

          if (finger.verifyPassword()) {
            Serial.println("Found fingerprint sensor!");
          } else {
            Serial.println("Did not find fingerprint sensor :(");
            while (1) { delay(1); }
          }
        }

        uint8_t readnumber(void) {
          uint8_t num = 0;

          while (num == 0) {
            while (! Serial.available());
            num = Serial.parseInt();
          }
          return num;
        }

        void loop()                     // run over and over again
        {
          Serial.println("Ready to enroll a fingerprint!");
          Serial.println("Please type in the ID # (from 1 to 127) you want to save this
        finger as...");
          id = readnumber();
          if (id == 0) {// ID #0 not allowed, try again!
             return;
          }
          Serial.print("Enrolling ID #");
          Serial.println(id);

          while (!  getFingerprintEnroll() );
        }

        uint8_t getFingerprintEnroll() {

          int p = -1;
          Serial.print("Waiting for valid finger to enroll as #"); Serial.println(id);
          while (p != FINGERPRINT_OK) {
            p = finger.getImage();
            switch (p) {
            case FINGERPRINT_OK:
```

```
    Serial.println("Image taken");
    break;
  case FINGERPRINT_NOFINGER:
    Serial.println(".");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    break;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Imaging error");
    break;
  default:
    Serial.println("Unknown error");
    break;
  }
}

// OK success!

p = finger.image2Tz(1);
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image converted");
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
    return p;
}

Serial.println("Remove finger");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}
Serial.print("ID "); Serial.println(id);
p = -1;
Serial.println("Place same finger again");
while (p != FINGERPRINT_OK) {
  p = finger.getImage();
  switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image taken");
    break;
  case FINGERPRINT_NOFINGER:
    Serial.print(".");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    break;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Imaging error");
    break;
  default:
    Serial.println("Unknown error");
    break;
  }
}

// OK success!

p = finger.image2Tz(2);
```

```
          switch (p) {
            case FINGERPRINT_OK:
              Serial.println("Image converted");
              break;
            case FINGERPRINT_IMAGEMESS:
              Serial.println("Image too messy");
              return p;
            case FINGERPRINT_PACKETRECIEVEERR:
              Serial.println("Communication error");
              return p;
            case FINGERPRINT_FEATUREFAIL:
              Serial.println("Could not find fingerprint features");
              return p;
            case FINGERPRINT_INVALIDIMAGE:
              Serial.println("Could not find fingerprint features");
              return p;
            default:
              Serial.println("Unknown error");
              return p;
          }

          // OK converted!
          Serial.print("Creating model for #");  Serial.println(id);

          p = finger.createModel();
          if (p == FINGERPRINT_OK) {
            Serial.println("Prints matched!");
          } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
            Serial.println("Communication error");
            return p;
          } else if (p == FINGERPRINT_ENROLLMISMATCH) {
            Serial.println("Fingerprints did not match");
            return p;
          } else {
            Serial.println("Unknown error");
            return p;
          }

          Serial.print("ID "); Serial.println(id);
          p = finger.storeModel(id);
          if (p == FINGERPRINT_OK) {
            Serial.println("Stored!");
          } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
            Serial.println("Communication error");
            return p;
          } else if (p == FINGERPRINT_BADLOCATION) {
            Serial.println("Could not store in that location");
            return p;
          } else if (p == FINGERPRINT_FLASHERR) {
            Serial.println("Error writing to flash");
            return p;
          } else {
            Serial.println("Unknown error");
            return p;
          }
}


//ควบคุมการเปิด-ปิด LED
#include <Adafruit_Fingerprint.h>

//On Leonardo/Micro or others with hardware serial, use those! #0 is green wire, #1 is white
//uncomment this line:
//#define mySerial Serial1

//For UNO and others without hardware serial, we must use software serial...
//pin #2 is IN from sensor (GREEN wire)
//pin #3 is OUT from arduino  (WHITE wire)
//comment these two lines if using hardware serial
#include <SoftwareSerial.h>
SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
```

```
void setup()
{
  pinMode(13, OUTPUT);
  digitalWrite(13, LOW);
  Serial.begin(9600);
  while (!Serial);  // For Yun/Leo/Micro/Zero/...
  delay(100);
  Serial.println("\n\nAdafruit finger detect test");

//set the data rate for the sensor serial port
  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1){ delay(1); }
  }

  finger.getTemplateCount();
  Serial.print("Sensor contains "); Serial.print(finger.templateCount); Serial.println(" 
templates");
  Serial.println("Waiting for valid finger...");
}

void loop()                     // run over and over again
{
  getFingerprintIDez();
  delay(50);            //don't ned to run this at full speed.
}

uint8_t getFingerprintID() {
  uint8_t p = finger.getImage();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println("No finger detected");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return p;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      return p;
    default:
      Serial.println("Unknown error");
      return p;
  }

//OK success!

  p = finger.image2Tz();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image converted");
      break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("Image too messy");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return p;
    case FINGERPRINT_FEATUREFAIL:
      Serial.println("Could not find fingerprint features");
      return p;
    case FINGERPRINT_INVALIDIMAGE:
      Serial.println("Could not find fingerprint features");
      return p;
    default:
      Serial.println("Unknown error");
```

```
      return p;
  }

//OK converted!
  p = finger.fingerFastSearch();
  if (p == FINGERPRINT_OK) {
    Serial.println("Found a print match!");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return p;
  } else if (p == FINGERPRINT_NOTFOUND) {
    Serial.println("Did not find a match");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }

//found a match!
  Serial.print("Found ID #"); Serial.print(finger.fingerID);
  Serial.print(" with confidence of "); Serial.println(finger.confidence);

  return finger.fingerID;
}

//returns -1 if failed, otherwise returns ID #
int getFingerprintIDez() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK)  return -1;

  p = finger.image2Tz();
  if (p != FINGERPRINT_OK)  return -1;

  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK)  return -1;

//found a match!
  Serial.print("Found ID #"); Serial.print(finger.fingerID);
  Serial.print(" with confidence of "); Serial.println(finger.confidence);
  if(finger.fingerID == 1){
    digitalWrite(13, HIGH);
    Serial.println("LED ON");
  }
    if(finger.fingerID == 2){
    digitalWrite(13, LOW);
    Serial.println("LED OFF");
  }

  return finger.fingerID;
}



//****************************************************
*Arduino Code: 12_ Real Time Face Recognition
//****************************************************
==> Each face stored on dataset/ dir, should have a unique numeric integer ID as 1, 2, 3,
etc
==> LBPH computed model (trained faces) should be on trainer/ dir
Based on original code by Anirban Kar: https://github.com/thecodacus/Face-Recognition
Developed by Marcelo Rovai - MJRoBot.org @ 21Feb18
'''
from signal import signal, SIGTERM, SIGHUP, pause
from rpi_lcd import LCD
lcd = LCD()
def safe_exit(signum, frame):
exit(1)
import RPi.GPIO as GPIO
GPIO.setwarnings(False)
GPIO.setmode(GPIO.BCM)
button = 12
```

```
stemp= 17
relay = 18
yellow = 23
red = 24
green = 25
blue = 8

step=0
GPIO.setup(button, GPIO.IN)
GPIO.setup(stemp, GPIO.IN)
GPIO.setup(relay, GPIO.OUT)
GPIO.setup(yellow, GPIO.OUT)
GPIO.setup(red, GPIO.OUT)
GPIO.setup(green, GPIO.OUT)
GPIO.setup(blue, GPIO.OUT)
GPIO.output(relay, 0)
GPIO.output(yellow, 0)
GPIO.output(red, 0)
GPIO.output(green, 0)
GPIO.output(blue, 1)
import pygame
import time
pygame.mixer.init()
c1=0
import cv2
import numpy as np
import os
import gspread
from oauth2client.service_account import ServiceAccountCredentials
import pprint
import datetime

import time
from smbus2 import SMBus
from mlx90614 import MLX90614
import requests
bus = SMBus(1)
sensor = MLX90614(bus, address=0x5A)
tt=0.00
i=0
enable=0
scope = ['https://spreadsheets.google.com/feeds', 'https://www.googleapis.com/auth/drive']
creds = ServiceAccountCredentials.from_json_keyfile_name('creds.json',scope)
client = gspread.authorize(creds)
sheet = client.open('database').sheet1
pp = pprint.PrettyPrinter()
recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read('/home/pi/Desktop/trainer.yml') #load trained model
cascadePath = "haarcascade_frontalface_default.xml"
faceCascade = cv2.CascadeClassifier(cascadePath);
font = cv2.FONT_HERSHEY_SIMPLEX
#iniciate id counter, the number of persons you want to include
id = 3 #two persons (e.g. Jacob, Jack)

names = ['','watcharapong','kittipat','cholthicha']
#names = ['','watcharapong','kittipat'] #key in names, start from the second place, leave
first empty
#names = ['',''] #key in names, start from the second place, leave first empty
# Initialize and start realtime video capture
cam = cv2.VideoCapture(0)
cam.set(3, 360) # set video widht 640
cam.set(4, 280) # set video height 480
# Define min window size to be recognized as a face
minW = 0.1*cam.get(3) #3
minH = 0.1*cam.get(4) #4
global count
per=0
i+=1
sheet.update_cell(i,1,"Datetime")
sheet.update_cell(i,2,'Name')
sheet.update_cell(i,3,'Temperature(C)')
count1=0
count2=0
while True:
```

```
#global step
timer = datetime.datetime.now()
ret, img =cam.read()
bus = SMBus(1)
sensor = MLX90614(bus, address=0x5A)
print('enable =',enable)
#print('sensor = ',str(GPIO.input(stemp)))
#print(' button = ',str(GPIO.input(button)))
#print('step =',step)
print()
try:
#print ("Ambient Temperature :", sensor.get_ambient())
#print ("Object Temperature :", sensor.get_object_1())
print()
tt=float(sensor.get_object_1())
#print("{0:.2f}".format(tt))
temp="{0:.2f}".format(tt)
if(step == 1):
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text("Temp :"+str(temp)+'C*', 2)
#print ("Ambient Temperature :", sensor.get_ambient())
print ("Object Temperature :", sensor.get_object_1())
if(step == 0):
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" Standby ", 1)
if (GPIO.input(button) == False and step == 0 ):
GPIO.output(blue, 0)
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" Open Door ", 1)

print(' Exit -------------------------- ')
GPIO.output(relay, 1)
GPIO.output(green, 1)
time.sleep(5)
GPIO.output(relay, 0)
GPIO.output(green, 0)
GPIO.output(blue, 1)
lcd.clear()
enable=0
if (enable == 1 and GPIO.input(stemp) == False ):
print('>>>ok',temp)
if(float(temp) >= 28.00 and float(temp) <= 37.5 ):
arr=temp
box=list(arr)
#print(box)
count1+=1
count2=0
print(' count1 = ',count1)
time.sleep(1)
if(count1 == 2 ):
step=2
GPIO.output(red, 0)
GPIO.output(green, 1)

GPIO.output(relay, 1)
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" Open Door ", 1)
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" ", 2)
print(' ooooooooooooooooooooooo ')
tt = str(timer)+",t="+str(temp)+'c'
url = "https://notify-api.line.me/api/notify"
token = "9nJ3yjPcnNDzBcMNGcDPIdQS77jP1RFP35WM591vDbZ"
headers = {'Authorization': 'Bearer ' + token}
ssm = str(id)+",temp="+str(temp)+'C* Open Door'
msg = {
"message": (None, ssm),
"imageFile": open('/home/pi/Desktop/picture.jpg', "r+b")
}
res = requests.post(url, headers=headers, files=msg)
```

```
print(res.text)

i+=1
sheet.update_cell(i,1,str(timer))
sheet.update_cell(i,2,str(id))
sheet.update_cell(i,3,temp)
time.sleep(3)
GPIO.output(relay, 0)
lcd.clear()
step=0
enable=0
GPIO.output(yellow, 0)
GPIO.output(blue, 1)
GPIO.output(red, 0)
GPIO.output(green, 0)
count1=0
if(float(temp) >= 37.5 ):
#print('****************************************')
arr=temp
box=list(arr)
#print(box)
count2+=1
count1=0
print(' count2 = ',count2)
time.sleep(1)
if(count2 == 2 ):

GPIO.output(red, 1)
GPIO.output(green, 0)
step=3
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" Temp Over! ", 1)
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" ", 2)
print(' xxxxxxxxxxxxxxxxxxxxxxxx ')
tt = str(timer)+",t="+str(temp)+'c'
url = "https://notify-api.line.me/api/notify"
token = "9nJ3yjPcnNDzBcMNGcDPIdQS77jP1RFP35WM591vDbZ"
headers = {'Authorization': 'Bearer ' + token}
ssm = str(id)+",temp="+str(temp)+'C* Temp Over'
msg = {
"message": (None, ssm),
"imageFile": open('/home/pi/Desktop/picture.jpg', "r+b")
}
res = requests.post(url, headers=headers, files=msg)
print(res.text)

i+=1
sheet.update_cell(i,1,str(timer))
sheet.update_cell(i,2,str(id))
sheet.update_cell(i,3,temp)
time.sleep(3)
lcd.clear()
step=0
GPIO.output(yellow, 0)
GPIO.output(blue, 1)
GPIO.output(red, 0)
GPIO.output(green, 0)
count2=0
enable=0
except:
print('...')
gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)
faces = faceCascade.detectMultiScale(
gray,
scaleFactor = 2.0, #3.0
minNeighbors = 5, #5
minSize = (int(minW), int(minH)),
)

for(x,y,w,h) in faces:
cv2.rectangle(img, (x,y), (x+w,y+h), (0,255,0), 2)
```

```
id, confidence = recognizer.predict(gray[y:y+h,x:x+w])
# Check if confidence is less them 100 ==> "0" is perfect match
if (confidence < 100):
#i+=1
id = names[id]
confidence = " {0}%".format(round(100 -confidence))
#per=100-int(confidence)
print('confidence = ',confidence)
ppp = list(confidence)
#print('ppp=',ppp,len(ppp))
if ( len(ppp) == 5 ):
ten=int(ppp[2])
one=int(ppp[3])
per = ten*10 + one*1;
print(' percent = ',per)
if ( int(per) >= 25 ):
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(" ", 1)
signal(SIGTERM, safe_exit)
signal(SIGHUP, safe_exit)
lcd.text(str(id), 1)

step=1
GPIO.output(yellow, 1)
out=cv2.imwrite('/home/pi/Desktop/picture.jpg',img)
time.sleep(1)
print('ok')
enable=1
GPIO.output(blue, 0)
else:
enable=0
id = "unknown"
confidence = " {0}%".format(round(100 -confidence))
c1=0
cv2.putText(img, str(id), (x+5,y-5), font, 1, (255,255,255), 2)
cv2.putText(img, str(confidence), (x+5,y+h-5), font, 1, (0,0,255), 3)
#print('CF=== ',type(confidence))
#print('CF int === ',per)
#if ( per >= 30 ):
# enable=1
cv2.imshow('camera',img)
k = cv2.waitKey(10) & 0xff # Press 'ESC' for exiting video 97

if k == 27:
break
# Do a bit of cleanup
print("\n [INFO] Exiting Program and cleanup stuff")
cam.release()
bus.close()
cv2.destroyAllWindows()


//**************************************************
*Arduino Code: 13_ MQ-2 Gas Control
//**************************************************
/*
ระบบตรวจจับก๊าซและควบคุมวาล์วอัตโนมัติ
  Hardware:
    MQ-2 AO        -> A0
    Relay CLOSE    -> D2 (GPIO4)
    Relay OPEN     -> D3 (GPIO0)
    Reset button   -> D5 (GPIO14) , อีกขาต่อ GND

หลักความปลอดภัย:
 - ตรวจพบก๊าซแล้วล็อกสถานะ Alarm และสั่งปิดวาล์ว
 - ค่าก๊าซลดลงแล้วจะไม่เปิดวาล์วเอง
 - เปิดวาล์วได้เมื่อค่าปลอดภัยต่อเนื่องและผู้ใช้กด Reset เท่านั้น
 - ไม่ให้รีเลย์ OPEN และ CLOSE ทำงานพร้อมกัน

คำเตือน: D3 คือ GPIO0 ซึ่งมีผลต่อโหมดบูตของ ESP8266
อินพุตของรีเลย์ต้องไม่ดึงขานี้เป็น LOW ตอนเปิดเครื่อง หากบอร์ดบูตไม่ได้
```

```
 ให้ย้าย Relay OPEN ไป D1 แล้วแก้ PIN_RELAY_OPEN เป็น D1
*/

#include <Arduino.h>

// ---------------- กำหนดขา ----------------
const uint8_t PIN_MQ2   = A0;
const uint8_t PIN_RELAY_CLOSE = D2;
const uint8_t PIN_RELAY_OPEN  = D3;
const uint8_t PIN_RESET       = D5;

// โมดูลรีเลย์ส่วนมากเป็น Active LOW
// หากรีเลย์ของจริงเป็น Active HIGH ให้สลับสองค่านี้
const uint8_t RELAY_ON  = LOW;
const uint8_t RELAY_OFF = HIGH;

// ---------------- ค่าที่ต้องปรับจากการทดลอง ----------------
const int GAS_THRESHOLD = 600;   // ค่า ADC ที่ถือว่าอันตราย (0-1023)
const int GAS_HYSTERESIS = 50;   // ต้องต่ำกว่า Threshold อย่างน้อยค่านี้จึงถือว่าปลอดภัย

const unsigned long SENSOR_WARMUP_MS = 60000UL; // ตัวอย่าง 60 วินาที
const unsigned long SAMPLE_INTERVAL_MS = 200UL;
const unsigned long VALVE_DRIVE_MS = 3000UL;     // เวลาจ่ายไฟให้มอเตอร์วาล์ว
const unsigned long SAFE_HOLD_MS = 3000UL;       // ต้องปลอดภัยต่อเนื่องก่อนรับ Reset
const unsigned long DEBOUNCE_MS = 40UL;
const uint8_t ALARM_CONFIRM_SAMPLES = 5;

enum ValveMotion {
  VALVE_STOPPED,
  VALVE_OPENING,
  VALVE_CLOSING
};

ValveMotion valveMotion = VALVE_STOPPED;
bool alarmLatched = true;        // เริ่มระบบแบบปลอดภัย: ไม่เปิดวาล์วอัตโนมัติ
bool warmupFinished = false;
int gasAdc = 0;
uint8_t highGasCount = 0;

unsigned long bootTime = 0;
unsigned long lastSampleTime = 0;
unsigned long motionStartTime = 0;
unsigned long safeSince = 0;

bool lastButtonReading = HIGH;
bool stableButtonState = HIGH;
unsigned long buttonChangedTime = 0;

void allRelaysOff() {
  digitalWrite(PIN_RELAY_CLOSE, RELAY_OFF);
  digitalWrite(PIN_RELAY_OPEN, RELAY_OFF);
}

void stopValve() {
  allRelaysOff();
  valveMotion = VALVE_STOPPED;
}

void startClosingValve() {
 // Interlock: ปิดรีเลย์ทั้งสองก่อนเปลี่ยนทิศทาง
  allRelaysOff();
  delay(20);
  digitalWrite(PIN_RELAY_CLOSE, RELAY_ON);
  valveMotion = VALVE_CLOSING;
  motionStartTime = millis();
  Serial.println(F("ACTION: CLOSE valve"));
}

void startOpeningValve() {
```

```
// เปิดได้เฉพาะเมื่อ Alarm ถูกยกเลิกแล้ว
  if (alarmLatched) return;

  allRelaysOff();
  delay(20);
  digitalWrite(PIN_RELAY_OPEN, RELAY_ON);
  valveMotion = VALVE_OPENING;
  motionStartTime = millis();
  Serial.println(F("ACTION: OPEN valve"));
}

void updateValveMotor() {
  if (valveMotion != VALVE_STOPPED &&
      millis() - motionStartTime >= VALVE_DRIVE_MS) {
    stopValve();
    Serial.println(F("ACTION: valve motor stopped"));
  }
}

bool resetButtonPressed() {
  bool reading = digitalRead(PIN_RESET);

  if (reading != lastButtonReading) {
    lastButtonReading = reading;
    buttonChangedTime = millis();
  }

  if (millis() - buttonChangedTime >= DEBOUNCE_MS &&
      reading != stableButtonState) {
    stableButtonState = reading;
    if (stableButtonState == LOW) return true;
  }

  return false;
}

bool gasIsSafe() {
  return gasAdc <= (GAS_THRESHOLD - GAS_HYSTERESIS);
}

void sampleGas() {
  if (millis() - lastSampleTime < SAMPLE_INTERVAL_MS) return;
  lastSampleTime = millis();
  gasAdc = analogRead(PIN_MQ2);

  Serial.print(F("ADC="));
  Serial.print(gasAdc);
  Serial.print(F("  Alarm="));
  Serial.print(alarmLatched ? F("LATCHED") : F("NORMAL"));
  Serial.print(F("  Warmup="));
  Serial.println(warmupFinished ? F("DONE") : F("WAIT"));

  if (!warmupFinished) return;

// ยืนยันหลายตัวอย่างเพื่อลดการเตือนผิดพลาดจากสัญญาณกระชาก
  if (gasAdc >= GAS_THRESHOLD) {
    if (highGasCount < ALARM_CONFIRM_SAMPLES) highGasCount++;
  } else {
    highGasCount = 0;
  }

  if (highGasCount >= ALARM_CONFIRM_SAMPLES && !alarmLatched) {
    alarmLatched = true;
    safeSince = 0;
    startClosingValve();
    Serial.println(F("ALARM: gas level is above threshold"));
  }

// จับเวลาที่ค่าก๊าซอยู่ในระดับปลอดภัยอย่างต่อเนื่อง
  if (gasIsSafe()) {
    if (safeSince == 0) safeSince = millis();
  } else {
    safeSince = 0;
```

```
  }
}

void setup() {
  Serial.begin(115200);

// เขียนสถานะ OFF ไว้ก่อนตั้งเป็น OUTPUT เพื่อลดรีเลย์กระตุกตอนเริ่มระบบ
  digitalWrite(PIN_RELAY_CLOSE, RELAY_OFF);
  digitalWrite(PIN_RELAY_OPEN, RELAY_OFF);
  pinMode(PIN_RELAY_CLOSE, OUTPUT);
  pinMode(PIN_RELAY_OPEN, OUTPUT);
  allRelaysOff();

  pinMode(PIN_RESET, INPUT_PULLUP);

  bootTime = millis();
  Serial.println();
  Serial.println(F("Gas leak safety controller started"));
// เริ่มต้นแบบ fail-safe: สั่งปิดวาล์วหนึ่งครั้งเสมอ
  startClosingValve();
  Serial.println(F("Valve closes at startup and remains locked until warmup, safe gas level,
and manual Reset"));
}

void loop() {
  updateValveMotor();

  if (!warmupFinished && millis() - bootTime >= SENSOR_WARMUP_MS) {
    warmupFinished = true;
    Serial.println(F("MQ-2 warmup finished"));
  }

  sampleGas();

  if (resetButtonPressed()) {
    bool safeLongEnough = safeSince != 0 &&
                          millis() - safeSince >= SAFE_HOLD_MS;

    if (!warmupFinished) {
      Serial.println(F("RESET DENIED: sensor is warming up"));
    } else if (!gasIsSafe() || !safeLongEnough) {
      Serial.println(F("RESET DENIED: gas level is not safely stable"));
    } else if (valveMotion != VALVE_STOPPED) {
      Serial.println(F("RESET DENIED: valve motor is running"));
    } else {
      alarmLatched = false;
      highGasCount = 0;
      startOpeningValve();
      Serial.println(F("RESET ACCEPTED: valve opening"));
    }
  }
}
```

ดัชนีค้นคำ

เนื้อหาระบบรักษาความปลอดภัยอัจฉริยะและการประยุกต์ใช้

ก

กล้องโทรทัศน์วงจรปิด 1-4, 6-8, 10, 15-16, 25, 37, 103-196, 310, 324, 518-522

กล้องวงจรปิดแบบแอนะล็อก 304, 466

กล้องวงจรปิดแบบไอพี 3, 8, 111, 118-119, 127, 131, 168, 185-187, 282, 310-311, 315-323, 329-331, 334-335, 345, 347, 367-369, 371-377, 380-385, 387-389, 392, 395, 398, 435, 460, 463, 466-467, 518, 522-523, 528-529

กล้องอินฟราเรด 107, 118-119, 185, 284

กล้องไอพี 3, 8, 111, 118-119, 127, 131, 168, 185-187, 282, 310-311, 315-323, 329-331, 334-335, 345, 347, 367-369, 371-377, 380-385, 387-389, 392, 395, 398, 435, 460, 463, 466-467, 518, 522-523, 528-529

กลอนประตูไฟฟ้า 531-533

การควบคุมการเข้า–ออก 1-3, 8-10, 14, 37, 202, 221, 226, 231, 282, 284, 286-287, 298, 437-441, 461, 463, 467, 518, 523-534, 537

การควบคุมจากระยะไกล 36, 397, 442, 466

การแจ้งเตือน 1-8, 11-13, 15-16, 36-40, 48, 52-53, 56, 61-62, 64-68, 70, 75, 77, 79-81, 83-87, 89-92, 96-97, 99, 132, 182, 188, 208, 232, 253, 285, 306, 310-311, 313, 329, 335, 366-369, 371, 373-374, 380-382, 384, 395-398, 419, 431-433, 436, 438, 440-442, 444-445, 449-450, 460-463, 466-467, 470-473, 475, 478-479, 483-484, 486-489, 498, 502-504, 509-511, 513-514, 524-529, 531-538

การตรวจจับก๊าซ 43, 66, 69-75, 77, 97, 100, 312, 398, 518, 537-538

การตรวจจับควัน 2, 4-5, 13, 37, 40, 43, 61-69, 81, 97, 99-101, 257, 261, 310, 312, 356, 366, 382, 395, 398, 460, 473, 476

การตรวจจับความเคลื่อนไหว 2, 4, 357, 361, 435, 440, 460, 463, 466-467, 522

การตรวจจับใบหน้า 3, 117, 264, 282-288, 304, 431-432, 435, 463, 470-471, 479, 484-486, 489-491, 493, 502, 504, 506, 509, 514-515, 517, 534-535

การตรวจจับผู้บุกรุก 513

การตรวจจับเปลวไฟ 13, 44, 81-92, 97, 99, 262, 312

การตรวจจับวัตถุ 3, 46, 286, 289, 432, 472-474, 482, 484-485, 489, 497, 509, 533-534

การตรวจสอบสิทธิ์ 8, 198, 201, 230, 235, 240-245, 251, 258, 263, 466, 523, 526-529

การป้องกันการบุกรุก 2, 15, 96, 311

การพิสูจน์ตัวตน 201-202, 234-235, 240, 251, 253, 261, 263, 265-266,

291, 294-295, 300, 311, 313, 322, 332, 367, 369, 371, 374, 380, 382-383
การเรียนรู้ของเครื่อง 48, 75, 282, 470, 476
การเรียนรู้เชิงลึก 282, 292-293, 299
การรู้จำใบหน้า 431-432, 440-441, 472-473, 475, 479, 489, 510, 535-536
การวิเคราะห์ข้อมูล 3, 5, 47-48, 299, 313, 395-397, 432, 440, 442, 460, 463, 466, 472-473, 475-478, 509
การสแกนลายนิ้วมือ 15-16, 201, 264, 266-269, 275-280, 298, 301-302, 306, 312, 518, 531-532
การสื่อสารข้อมูล 11, 75, 109, 112, 168, 204, 221-222, 233, 253, 278, 280, 311, 319, 325, 329-330, 335, 339, 347, 354, 357, 361, 403, 431, 434
การสื่อสารแบบไร้สาย 331, 335, 348
การเข้ารหัสข้อมูล 113, 210-211, 234-236, 240, 243-244, 247, 253-254, 304, 311, 313, 355, 357, 359, 366, 373-374, 436, 442, 475, 506
การเชื่อมต่อเครือข่าย 109-111, 131, 148, 188, 254, 307, 314, 330-331, 333, 337, 339, 342, 344, 348, 365, 380, 412, 429, 431-433, 462, 466, 522, 526, 529-530
การแบ่งส่วนเครือข่าย 367
การแยกเครือข่าย 332, 350, 382, 386
เกตเวย์ 330, 334, 362
ข
ข้อมูลชีวมิติ 282, 290-291, 298, 301, 303, 475, 487, 506, 510, 517, 529
ข้อมูลจากเซนเซอร์ 5, 36, 38, 47, 278-280, 316, 351, 353, 356, 362, 396, 398, 403, 412, 430-431, 438, 462, 474, 479
ข้อมูลภาพ 8, 107, 117, 165-166, 188, 268, 274, 282, 316, 428, 430, 442, 473, 475, 481, 495, 498, 511, 522, 529
ข้อมูลวิดีโอ 107, 290, 323, 333-334, 371, 502, 522
ข้อมูลส่วนบุคคล 226, 247, 290, 303, 475, 480, 489, 504, 510
ขั้วทำงาน 74, 76
ขั้วอ้างอิง 74, 76
ขาแอนะล็อก 79-80
ขาดิจิทัล 52-53, 406-407, 430, 525
ขาอินพุตและเอาต์พุต 398-399, 433, 461-462, 465
ค
คลาวด์ 3, 183, 202, 310, 313-314, 333, 350, 380-381, 394-395, 428, 431-433, 435-442, 466, 539
คลาวด์แพลตฟอร์ม 313, 362, 364, 394, 435-436, 439-442, 463, 466-468, 537
คลื่นความถี่วิทยุ 202-203, 205, 208-209, 248, 259, 523
คลื่นไมโครเวฟ 98, 261, 331
คลื่นแม่เหล็กไฟฟ้า 44, 82-83, 112, 139, 141-142, 144, 203, 208, 213, 216-217, 220-221, 225, 260, 319, 335
คลื่นอัลตราไวโอเลต 71, 81-86, 99-101, 378, 413, 462
คลื่นอินฟราเรด 84, 86, 112, 261, 331

ความปลอดภัยของข้อมูล 142, 226, 276, 278, 364, 475, 510
ความปลอดภัยของเครือข่าย 356
ความไวของเซนเซอร์ 48, 50-51, 64
ค่าความเชื่อมั่น 479, 485, 489, 499
ค่าความแม่นยำ 495
คุณลักษณะของใบหน้า 282, 489
เครื่องบันทึกวิดีโอเครือข่าย 7-8, 40, 106-107, 110, 117-118, 130-131, 135-136, 145, 147, 149, 153, 157-158, 168, 183-185, 187-188, 313, 315, 317-318, 320, 322-323, 332, 334, 345, 347, 350, 368-369, 371-372, 381-382, 385-386, 388-389, 522
เครื่องอ่านบัตร RFID 312, 376
เครือข่ายเฉพาะที่ 108-112, 338
เครือข่ายบริเวณกว้าง 308, 330, 333, 381, 383
เครือข่ายแบบดาว 110
เครือข่ายแบบเมช 261, 315-316, 351, 354-355, 357, 362, 364, 380, 382, 384, 386, 388, 391
เครือข่ายไร้สาย 112, 312, 332, 338, 348-350, 354, 526
โครงข่ายประสาทเทียม 282, 293-295, 299, 473
โครงสร้างเครือข่าย 308, 311, 338, 354-355, 364, 392, 522
ง
งานรักษาความปลอดภัย 2, 7, 37, 290, 513
งานอัตโนมัติ 4, 12, 122, 205, 460
จ
จุดกระจายสัญญาณไร้สาย 377
จุดเชื่อมต่อ 179, 331-332, 334, 414
จุดเชื่อมต่อไร้สาย 331-332
จุดติดตั้งกล้อง 193
ฉ
ฉนวนไฟฟ้า 23, 31
ช
ช่องทางการสื่อสาร 445-446
ช่องสัญญาณ 132, 145, 179, 209, 335, 339, 344, 350-352, 354, 358-359, 382, 520
ชุดควบคุม 15, 66, 200-201, 242, 251, 263, 284
ชุดควบคุมประตู 201
ชุดข้อมูล 227, 244, 283, 290, 298, 470, 476, 478-481, 484, 487-489, 491-493, 495, 509, 511, 516
ชุดข้อมูลทดสอบ 476
ชุดตรวจจับ 85, 270
ซีวมิติ 15-16, 282, 284, 290-291, 293-294, 298, 301, 303, 330, 376, 440, 475, 480, 487, 506, 510, 517, 529
ซ
ซับเน็ต 326-327, 329
ซิกบี 75, 262, 304, 308, 310, 312-313, 315-316, 348, 351-357, 362, 364, 378, 382, 386, 391, 396, 460
เซนเซอร์ 2-6, 12, 15, 36, 38, 43-101, 103, 120, 122, 124, 126-129, 160-165, 207, 239, 245, 258, 264, 266-271, 274-282, 284, 298, 301-302, 310-312, 316, 332, 351-353, 355-357, 361-363, 366, 371, 376, 380, 382-383, 386, 395-398, 400-403, 405, 412-415, 429-438, 440-

443, 460-463, 466-467, 472-474, 476, 479, 487-488, 509, 518, 529-531, 533-534, 537-538
เซนเซอร์ก๊าซ 75-76, 537
เซนเซอร์ควัน 357, 361, 435, 440, 463
เซนเซอร์ตรวจจับความเคลื่อนไหว 2, 4, 357, 361, 435, 440, 460, 463, 467
เซนเซอร์ตรวจจับเปลวไฟ 44, 81-92, 97, 99, 312
เซนเซอร์ประตูและหน้าต่าง 43, 53, 56, 312, 382
เซนเซอร์แม่เหล็ก 15
เซนเซอร์ลายนิ้วมือ 264, 266-271, 277, 279-280, 298, 530
เซนเซอร์อัลตราโซนิก 48
เซนเซอร์อินฟราเรด 15, 48, 86, 88, 96, 533
เซนเซอร์ฮอลล์ 55, 58-59
เซอร์โวมอเตอร์ 242-243, 245-246, 252, 258, 434, 461, 524-525
เซิร์ฟเวอร์ 111, 200, 241-243, 247, 254, 310, 312, 321, 330, 345, 347-348, 362, 366-367, 371, 373-374, 380-381, 386, 393, 412, 420-426, 432, 435, 442-445, 462, 529

ฐ

ฐานข้อมูล 10, 53, 98, 111-112, 200, 206, 240, 242-247, 251-252, 254-255, 258, 263, 265-266, 268-270, 272-273, 275, 278, 281, 283-284, 286, 290, 292-294, 298-299, 301, 303, 321, 346, 371-372, 397, 419, 431-432, 435, 437, 439-442, 463, 468, 475-476, 479, 489, 495, 529
ฐานข้อมูลผู้ใช้งาน 292
ฐานข้อมูลลายนิ้วมือ 273, 278

ด

ดิจิทัลอินพุต 79, 414-415
ดิจิทัลเอาต์พุต 80-81, 91

ต

ตัวควบคุม 67, 122, 124, 242, 279, 315, 359-360, 401, 429, 462
ตัวตรวจจับ 45, 62, 69-70, 86-87
ตัวตรวจจับควัน 62, 69
ตัวรับส่งสัญญาณ 203
ตัวเก็บประจุ 67, 79, 90-91, 209, 214, 223, 225-226, 258, 279
ตัวต้านทาน 51, 67, 70, 78-81, 90-91, 214, 258, 279, 281, 411-412, 414, 419, 424
ตัวต้านทานโหลด 78
ตำแหน่งขา 233, 259, 413

ถ

แถบความถี่ 206

ท

โทโพโลยีทางกายภาพ 314
โทโพโลยีทางตรรกะ 314
โทโพโลยีเครือข่าย 314, 380
ทรานซิสเตอร์ 51-52, 65-67, 214, 242, 279
ที่อยู่แมค 256, 319-320, 322, 324-325, 330-331, 338-341, 345-346, 369, 374, 381-382, 384, 389
ที่อยู่ไอพี 148-149, 187, 256, 307, 319-320, 322, 324-325, 327, 331, 369, 371, 374, 380-381, 384-385, 389, 425-426, 465
เทคโนโลยีเครือข่าย 308, 337-339, 348, 381-382
เทคโนโลยีไร้สาย 75, 233, 382

เทคโนโลยี RFID 202, 233, 252-253, 518, 523, 526
น
นโยบายควบคุมการเข้าถึง 367
บ
บริการคลาวด์ 310, 428, 431-433, 435-438, 440, 466
บอร์ดไมโครคอนโทรลเลอร์ 398, 401, 418, 460
บอร์ด Arduino 52, 232, 399-401, 404, 406, 412, 524
บอร์ด ESP 412, 416, 418, 421-424, 450
บอร์ด NodeMCU 413-414, 416, 424, 450, 462, 537
บอร์ด Raspberry Pi 433
บัซเซอร์ 52-53, 67-68, 420, 434
บัตรประจำตัว 15, 211, 221, 265, 272, 531
แบบจำลองตรวจจับใบหน้า 515
แบบจำลอง 47, 148, 198, 243, 269, 283-284, 292-294, 299-300, 318-319, 321, 330-331, 339, 470, 472-491, 493-496, 502, 505, 509-511, 514-516, 520-522
ป
ประตูอัจฉริยะ 282, 298, 306, 357, 382, 518, 523, 525, 529, 533
ประสิทธิภาพของแบบจำลอง 476, 481, 483, 487-488
ปัญญาประดิษฐ์ 2-3, 47-48, 75, 84-86, 202, 251, 281, 286, 291-292, 299, 395, 428, 430, 432, 437, 440, 460, 470-517, 533
ปุ่มกด 414, 434, 531
โปรโตคอล 211-212, 236, 307-308, 315-318, 320-322, 330, 336-337, 340-341, 353, 358, 361-362, 364, 380, 383, 385, 396-397, 403, 407, 412, 430, 432-434, 440, 442, 444, 460, 462, 465-466
โปรโตคอลการสื่อสาร 211-212, 361, 396, 403, 433-434, 442
โปรโตคอลเครือข่าย 383, 432
โปรโตคอล MQTT 442
โปรโตคอล ONVIF 318, 322, 380, 523
โปรโตคอล RTSP 71, 318, 322, 380
โปรโตคอล TCP/IP 307, 316, 318, 380, 412, 462
โปรแกรมควบคุม 35, 301, 406, 410, 412, 420-421, 530
ผ
ผู้ดูแลระบบ 177, 200, 242, 313, 332, 365, 367-369, 371, 381, 398, 435, 438-439, 528, 533-535
ผู้บุกรุก 4, 6, 467, 513, 515
ผู้ใช้งาน 3-4, 6, 8, 12-13, 16, 29-30, 65, 67, 77-78, 80, 91-92, 107, 111, 142, 145, 156-157, 168-170, 185, 199-202, 234, 240-242, 244-247, 251, 254, 259, 261-263, 267, 274, 277, 280, 284, 292-293, 299, 304-305, 311, 313-314, 330, 333, 335, 354, 364-365, 367-369, 371, 373-374, 380, 396-397, 403, 414-415, 429-430, 436, 438-440, 442-446, 448, 450, 457, 472-475, 478, 504, 522-523, 525-529, 532-535
ผู้ใช้งานที่ได้รับอนุญาต 5, 8, 11, 16, 37, 199-200, 230, 240, 242-244, 251, 258, 294, 313, 332, 334, 355, 367,

371-372, 380, 419, 440-441, 444, 462, 468, 477-480, 487, 506, 516, 523-524, 527-529, 532
ผู้ให้บริการคลาวด์ 435-437
แผงควบคุม 53, 56, 66, 97
แผนผังการเชื่อมต่อ 280
แผนผังวงจร 68-69, 78, 91, 281, 418, 420, 423
พ
พอร์ตอนุกรม 281, 422
พื้นที่เฝ้าระวัง 156, 509, 520
แพลตฟอร์มคลาวด์ 394, 435-436
ฟ
เฟิร์มแวร์ 132, 189, 196, 278, 382
ไฟร์วอลล์ 8, 170, 332, 334, 437
เฟรมข้อมูล 330, 342, 344-346, 352, 354, 358
ภ
ภาพจากกล้องวงจรปิด 3, 311, 313, 436, 440
ภาพดิจิทัล 120, 170, 268, 274, 282, 520
ภาพใบหน้า 282-283, 299, 442, 487, 491, 504, 533
ภาพวิดีโอ 84, 135, 290, 381, 428, 463, 473
ภัยคุกคาม 2, 13, 199, 313, 383, 398, 460, 472, 483, 503, 505, 509-510
ภัยคุกคามทางไซเบอร์ 510
ม
มาตรฐานการสื่อสาร 310, 313, 380
มาตรฐานความปลอดภัย 240
มาตรฐาน IEEE 112, 309, 331-332, 338-341, 344-345, 348-349, 351-352, 354, 356, 370, 374-377, 381-382, 387
ไมโครคอนโทรลเลอร์ 45, 52-53, 56, 69, 75, 77, 79, 86-87, 90-92, 96, 203, 232-233, 238-243, 245-246, 252, 259, 264, 276, 278-281, 298, 353, 393, 398-399, 401-404, 406-407, 412-415, 418-420, 428, 437, 460-461, 464, 466, 523, 525-527, 538
โมดูลกล้อง 241
โมดูลตรวจจับ 90
โมดูลสื่อสาร 312, 395, 398, 402-403, 405, 429-430, 433, 461
โมดูลตรวจสอบลายนิ้วมือ 296
โมดูล 51-52, 55, 69, 79-80, 90-92, 197, 205, 231-233, 240-241, 252, 256-257, 277-279, 293-294, 312, 319, 393, 395, 398, 402-413, 415-416, 418-420, 423-425, 429-430, 432-433, 461-462, 465-466, 497, 524-528, 530
โมดูล MQ-2 66, 69-70, 79-80, 99-101, 518, 537-538
โมเดลตรวจจับใบหน้า 486
ย
ย่านความถี่ 208, 212-213, 216, 308, 335, 349, 351-353, 357, 363, 382, 524
ร
รหัสผ่าน 173, 200, 238, 241, 247, 251, 262, 265, 267, 272, 290, 301-304, 350, 382, 386, 403, 425, 450, 461, 467, 523-525, 531-532
รหัสประจำตัว 210, 242, 263, 529, 535

รหัสผู้ใช้งาน 242
ระบบกล้องวงจรปิด 3, 103, 192, 199, 251, 281, 290-291, 304, 311-313, 332, 337, 348, 371, 376, 386-387, 390, 395, 436, 438, 440, 466, 472-473, 476, 478, 509, 511, 522-523, 539
ระบบควบคุมการเข้า–ออก 1-3, 8-10, 14, 37, 202, 221, 226, 231, 282, 284, 286-287, 298, 437-441, 461, 463, 467, 518, 523-534, 537
ระบบควบคุมประตู 16, 39, 201, 252-253, 258, 282, 304, 311, 371, 398, 419-420, 460, 467, 479, 518, 523, 529-530, 532-533, 537
ระบบคลาวด์ 3, 183, 202, 310, 313-314, 333, 350, 380-381, 394-395, 428, 431-433, 435-442, 466, 539
ระบบเครือข่าย 2-3, 6-8, 10-12, 36, 53, 103, 105-112, 117-119, 130-131, 134, 139-142, 144, 147-150, 155-156, 158, 166, 168-170, 183, 185, 187-188, 193, 195-196, 238-240, 247, 253-256, 258, 307-392, 395-398, 401-402, 412, 421, 425-426, 429, 431-433, 435-437, 439-442, 450, 460, 462-464, 466, 474-475, 512, 519, 522-523, 525-526, 528-530, 536
ระบบเครือข่ายเฉพาะที่ 108-112, 338
ระบบตรวจจับก๊าซ 43, 66, 69-75, 77, 97, 100, 312, 398, 518, 537-538
ระบบตรวจจับควัน 2, 4-5, 13, 37, 40, 43, 61-69, 81, 97, 99-101, 257, 261, 310, 312, 356, 366, 382, 395, 398, 460, 473, 476
ระบบตรวจจับความเคลื่อนไหว 2, 4, 357, 361, 435, 440, 460, 463, 466-467, 522
ระบบตรวจจับใบหน้า 3, 117, 264, 282-288, 304, 431-432, 435, 463, 470-471, 479, 484-486, 489-491, 493, 502, 504, 506, 509, 514-515, 517, 534-535
ระบบตรวจจับเปลวไฟ 13, 44, 81-92, 97, 99, 262, 312
ระบบบันทึกภาพ 4, 6-8, 15, 38-39, 103, 105-107, 116, 118, 127, 130-131, 133, 135-136, 145-147, 156-158, 160, 165-170, 179, 181-182, 185, 188, 191-192, 194-196, 285, 301-302, 312, 367, 466, 471-472, 486, 495, 501-503, 511, 520, 522, 528-529
ระบบประตูอัจฉริยะ 282, 298, 306, 357, 382, 518, 523, 525, 529, 533
ระบบรักษาความปลอดภัย 1-101, 105, 108, 118, 183, 185, 199, 207, 226, 236, 245, 251-252, 264-265, 267, 269, 276, 279-282, 284, 290-291, 298-299, 302, 307-540
ระบบรักษาความปลอดภัยอัจฉริยะ 1-42, 45, 47-48, 75, 96-97, 252, 284, 299, 309-310, 313-316, 319-322, 330-335, 337, 339, 345, 347, 366-367, 371-373, 376, 380, 383-384, 387, 393, 395, 398, 412, 428, 433, 435, 460, 470, 472-476, 478-479, 489, 509, 511-512, 518-540
ระบบรู้จำใบหน้า 431-432, 440-441, 472-473, 475, 479, 489, 510, 535-536

ระบบสมองกลฝังตัว 279, 395, 398, 401, 405, 412, 427, 429, 433, 460, 462
ระบบสัญญาณเตือนภัย 3, 15
ระบบอัตโนมัติ 2-4, 6, 10, 12, 15, 27, 30, 35, 39, 45, 48, 51, 59, 75, 91, 96, 99, 119, 122-124, 129, 153, 188, 200, 202, 205, 208, 212, 215, 220, 234, 236, 238, 243, 251, 253-254, 276, 292, 294-295, 298-299, 302, 310, 313, 315, 322, 329, 337, 346, 351, 354-355, 357, 369, 374, 395, 397-398, 404, 420, 428, 431, 441, 446-447, 450, 454-456, 460-461, 472-473, 475, 477, 495, 509, 518, 537-538
รีดสวิตซ์ 55, 57
รีเลย์ 51-52, 68, 70, 87, 89, 91, 96, 98, 234, 242-243, 245-246, 252, 257-258, 284, 302, 352, 398, 412, 419-420, 430, 432, 434, 461-462, 466, 527
เราเตอร์ 8, 108, 148, 166, 318, 320, 322-323, 325, 331-334, 336-337, 386, 425, 523
ล
ลายนิ้วมือ 3, 15-16, 200-201, 247, 251, 264-280, 285, 298-299, 301-302, 306, 312, 518, 529-532
เลเยอร์กายภาพ 310, 319-320, 322-324, 330, 338-341, 358, 381
เลเยอร์การนำเสนอ 318, 321, 386
เลเยอร์การประยุกต์ 310-311, 318-319, 321-324, 351, 353, 380, 386, 388, 396, 460
เลเยอร์การเชื่อมโยงข้อมูล 310, 320, 322-324, 330, 338-341, 367-368, 381, 383-384, 386
เลเยอร์เครือข่าย 148, 310-311, 319-320, 322-325, 331, 340, 351, 353, 367-368, 385
เลเยอร์เซสชัน 318, 321
เลเยอร์ขนส่ง 310, 320, 323-324, 384
ว
วงจรขยายสัญญาณ 65, 74, 85-87
วงจรควบคุม 52, 65, 67-68, 77, 213, 236, 279, 402, 413, 422, 462, 538
วงจรควบคุมกลอนประตู 467, 527
วงจรตรวจจับก๊าซ 69
วงจรตรวจจับควัน 66-67
วาล์วแก๊ส 518, 537-538
วิดีโออัจฉริยะ 473
ไวไฟ 62, 65, 67, 69-70, 83, 99, 348, 382, 537
ศ
ศูนย์ควบคุม 2, 4-6, 311, 331, 334, 348, 398, 460
ศูนย์ข้อมูล 333, 337, 339, 341, 435, 437-438
ศูนย์รักษาความปลอดภัย 183
ส
สถาปัตยกรรมเครือข่าย 309, 347, 357-358, 363-364, 386
สวิตซ์เครือข่าย 8, 166, 168, 329-331, 338-339
สวิตซ์แม่เหล็ก 53-58, 96, 100
สวิตซ์ PoE 312, 315-316, 319, 375-376, 380, 383-384, 387
สัญญาณดิจิทัล 78, 80, 90, 117, 131, 187, 299, 395, 434

สัญญาณเตือน 2-6, 15-16, 62, 64, 68, 385, 441, 483, 502-503, 512
สัญญาณเตือนภัย 3, 15
สัญญาณแอนะล็อก 45, 56, 70, 78-79, 89, 92, 116, 131, 147, 414
สัญญาณไร้สาย 108, 377
สายคู่บิดเกลียว 112, 139-140, 142, 147, 150, 319, 331, 340, 374, 382
สายใยแก้วนำแสง 112, 142-143, 316-317, 331, 333, 335, 338, 340, 348, 385
สื่อสารแบบไร้สาย 331, 335, 348
เสาอากาศ 20, 41, 208, 235, 252, 255, 257, 335, 363, 412-413, 418-419, 462
ห
โหนด 309, 354-356, 359-362, 380, 382, 391
โหนดเซ็นเซอร์ 362
โหนดปลายทาง 360
หมายเลขประจำอุปกรณ์ 330, 403
หมายเลขพอร์ต 319, 346, 369, 384
หมายเลขไอพี 148-149, 187, 256, 307, 319-320, 322, 324-325, 327, 331, 369, 371, 374, 380-381, 384-385, 389, 425-426, 465
หน่วยความจำ 170, 205, 207-208, 210-211, 230, 238-239, 242, 304, 356, 398-403, 410, 412-413, 415, 429-431, 436-437, 440-441, 461-465, 482, 488, 490, 495, 529
หน่วยประมวลผลกลาง 401, 429-430, 433
หน่วยประมวลผลกราฟิก 286, 482, 488, 490, 493-496, 505
อ
อัลกอริทึม 47, 75, 81, 84, 89, 148, 244, 254, 262, 281, 285-286, 290, 402, 430, 432, 476, 479, 489
อัลตราไวโอเลต 81-84, 100
อัตราการยอมรับผิด 273
อัตราการปฏิเสธผิด 486
อัตราการส่งข้อมูล 134, 142, 166, 215
อินเทอร์เน็ต 3-4, 6, 8, 12, 40, 47-48, 51, 106, 108, 117, 119, 131, 134, 168-169, 185, 187, 192, 253, 255, 257-258, 302-304, 306, 310, 313, 318, 330-333, 336, 360, 365, 371-372, 380, 393-469, 472, 479, 486, 511
อินเทอร์เฟซ 132, 148, 239, 277, 322, 325, 330, 340-341, 381, 398, 461
อินฟราเรด 5, 12, 15, 48-51, 53, 62, 65, 81-84, 86, 88-90, 92, 96-98, 100, 107, 112, 115, 118-119, 130, 181, 185, 255, 261, 284, 301, 331, 414, 522, 533
อีเทอร์เน็ต 8, 131, 140, 148, 150, 168, 308-310, 312, 314-315, 319-320, 322, 324, 330-332, 334, 337-348, 350, 364, 370, 374-376, 378, 381-384, 386, 390, 396, 429, 431-432, 460, 522-523, 540
อีเทอร์เน็ตสวิตช์ 308, 338-339, 342-343, 345-347
อุปกรณ์ควบคุม 1, 5, 8, 11, 15, 200-201, 251, 310, 331, 351, 380, 382, 429, 432-433, 435, 440, 473, 526, 538

อุปกรณ์ตรวจจับ 1, 3-5, 12-13, 36, 38, 40, 61-62, 64-66, 81, 311, 382, 401, 440
อุปกรณ์ปลายทาง 136, 238, 310, 316, 329-331, 341, 345-348, 350, 355-356, 361-364, 369, 373-375, 377, 380-383, 385-386, 392, 402, 441, 460, 475
อุปกรณ์รักษาความปลอดภัย 13, 35, 310-311, 315, 361, 371, 380, 382, 440
อุปกรณ์รับ–ส่งสัญญาณ 353
อุปกรณ์เครือข่าย 108, 134, 144, 148, 158, 166, 309-310, 312-313, 321-322, 324, 331-332, 335, 338-339, 345, 347-348, 361, 367, 370, 376, 380, 522
แอปพลิเคชัน 4, 6, 12, 36, 53, 117, 157, 169-170, 203, 206, 238, 254, 262, 311, 313-314, 316-318, 320-323, 353, 362, 364, 380, 435, 437-438, 441-443, 445, 450, 454, 456, 460, 463, 466, 472, 486, 523
แอปพลิเคชันบนคลาวด์ 442
แอนะล็อกอินพุต 79-80
แอนะล็อกเอาต์พุต 80, 92
ไอโอที 3-4, 35, 47-48, 70, 72, 75, 94-97, 199, 202, 220, 234-235, 239, 247-248, 251-253, 294, 296, 299, 302, 310, 312, 322, 332, 345, 347-348, 351-353, 361-363, 365, 368, 371-372, 375-379, 381-383, 393, 395-401, 404, 412-413, 415, 419, 428-433, 435, 437, 439-440, 442, 444-445, 449, 458-464, 466, 472-476, 507, 509, 526-527
ฮ
ฮอลล์เอฟเฟกต์ 55, 58-59
ฮอลล์เซนเซอร์ 55
ฮาร์ดแวร์ 111, 170, 194, 360, 398, 405, 432, 434, 438, 461, 490, 495, 497
ฮับ 342

www.rmutt.ac.th ราชมงคลธัญบุรี

ภาควิชาครุศาสตร์อุตสาหกรรม คณะครุศาสตร์อุตสาหกรรม

มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี