

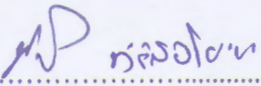
**ระบบไร้สายโดยใช้ Zigbee เพื่อควบคุมและติดตามสถานะเครื่องจักร
และเซ็นเซอร์ในโรงงานผ่านเครือข่ายอินเทอร์เน็ต**

พูนศักดิ์ ปรเพิ่มพูน

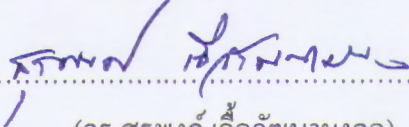
**วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์และระบบสารสนเทศ)
คณะสถิติประยุกต์
สถาบันบัณฑิตพัฒนบริหารศาสตร์**

2556

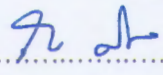
ระบบไร้สายโดยใช้ Zigbee เพื่อควบคุมและติดตามสถานะเครื่องจักร
และเซ็นเซอร์ในโรงงานผ่านเครือข่ายอินเทอร์เน็ต
พูนศักดิ์ ปรเพิ่มพูน
คณะสถิติประยุกต์

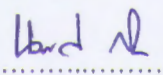
รองศาสตราจารย์..........อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ดร.พิพัฒน์ หิรัญวณิชชากร)

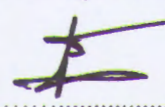
คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของ
การศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์และระบบสารสนเทศ)

รองศาสตราจารย์..........ประธานกรรมการ
(ดร.สุรพงศ์ เอื้อวัฒนามงคล)

รองศาสตราจารย์..........กรรมการ
(ดร.พิพัฒน์ หิรัญวณิชชากร)

ผู้ช่วยศาสตราจารย์..........กรรมการ
(ดร. โออม สรนิล)

อาจารย์..........กรรมการ
(ดร.นรณัฐ สงวนศักดิ์โยธิน)

ศาสตราจารย์..........รักษาราชการแทนคณบดี
(ดร. ตำรวม จงเจริญ)

บทคัดย่อ

ชื่อวิทยานิพนธ์	ระบบไร้สายโดยใช้ Zigbee เพื่อควบคุมและติดตามสถานะเครื่องจักร และเซ็นเซอร์ในโรงงานผ่านเครือข่ายอินเทอร์เน็ต
ชื่อผู้เขียน	นายพูนศักดิ์ พรเพิ่มพูน
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์และระบบสารสนเทศ)
ปีการศึกษา	2556

ระบบการผลิตอัตโนมัติในโรงงาน สามารถเพิ่มประสิทธิภาพในการผลิตในโรงงานให้เพิ่มมากขึ้น อย่างไรก็ตาม การควบคุมการทำงานของเครื่องจักรอัตโนมัติ ยังจำกัดอยู่ที่ระยะทางของสายเคเบิลที่เชื่อมต่อเครื่องควบคุมเข้ากับเครื่องจักรอัตโนมัติ งานวิจัยชิ้นนี้จึงมุ่งนำเสนอแนวคิดการพัฒนาระบบแบบระบบฝังตัว (Embedded System) เพื่อควบคุมเครื่องจักรอัตโนมัติจากระยะไกลผ่านเครือข่ายอินเทอร์เน็ต และตรวจสอบสถานะภายในโรงงานจากเซ็นเซอร์ที่ติดตั้งภายในโรงงาน โดยมุ่งนำเสนอแนวคิดของระบบที่สามารถทำงานได้อย่างมีประสิทธิภาพ มีการคำนึงถึงความปลอดภัยของข้อมูลที่ส่งผ่านระบบอินเทอร์เน็ต และความสะดวกในการควบคุมอุปกรณ์ในโรงงานด้วยระบบไร้สาย Zigbee

ABSTRACT

Title of Thesis	Zigbee based Remote System for controlling and Monitoring Machine and Sensor in Factory through Internet
Author	Poonsuk Ponpurmpoon
Degree	Master of Science (Computer Science and Information Systems)
Year	2013

Factory Automation can significantly increase the productivity of the production systems. However, range of control system is limited by the length of the cable cords that connect the Automatic Machines with control system, This paper proposes an embedded system for controlling machines and monitoring sensors in Factory by using Zigbee Technology. Because its objective is to control the machines through internet, performance and security issues are concerned

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จขึ้นได้ด้วยความอนุเคราะห์ของบุคคลผู้สนับสนุนหลายท่าน โดยได้รับคำแนะนำ ปรับปรุงในทุกขั้นตอน จนสำเร็จวิทยานิพนธ์ฉบับนี้ได้

ขอกราบขอบพระคุณ รองศาสตราจารย์ ดร. พัทธน์ หิรัณย์วิชชากร เป็นอย่างสูง ที่ได้กรุณาเสียสละเวลาอันมีค่าเพื่ออ่านและให้คำปรึกษารวมถึงแนะนำแนวทางที่ควรในการจัดทำวิทยานิพนธ์แก่ผู้เขียนเสมอมาตลอดมาในทุกขั้นตอนการจัดทำวิทยานิพนธ์ฉบับนี้เป็นอย่างดีที่สุด

ขอกราบขอบพระคุณ รองศาสตราจารย์ ดร. สุรพงศ์ เอื้อวัฒนามงคล ที่ให้ความกรุณาตั้งสอนให้ความรู้ และติดตามสอบถามความก้าวหน้าพร้อมแนะนำแนวทางในการพัฒนางานวิจัยให้สมบูรณ์ยิ่งขึ้นไปอีกในอนาคต

ขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. โอม ศรีนิล ที่กรุณาให้การสนับสนุนให้คำแนะนำด้วยการให้มุมมองที่แปลกใหม่จากการชี้จุดดีของวิทยานิพนธ์ในมุมซึ่งผู้เขียนคาดไม่ถึง

ขอกราบขอบพระคุณ อาจารย์ ดร. นรณัฐ สงวนศักดิ์โยธิน ที่ตั้งสอนให้ความรู้ รวมถึงอำนวยความสะดวกให้อย่างสะดวกที่สุด ทำให้วิทยานิพนธ์ฉบับนี้สำเร็จได้อย่างรวดเร็ว

ขอขอบคุณสถาบันบัณฑิตพัฒนบริหารศาสตร์ ที่รวบรวมอาจารย์ผู้มีความสามารถเอาไว้ให้เป็นแหล่งค้นคว้าความรู้เท่าที่ผู้เรียนจะเรียนได้ ขอขอบคุณมหาวิทยาลัยรามคำแหงที่หล่อหลอมให้ผู้เขียนมีความอดทน ไม่ท้อถอยในการทำงาน

ขอขอบคุณเจ้าหน้าที่คณะสถิติประยุกต์ทุกท่านที่ให้คำแนะนำที่มีประโยชน์และอำนวยความสะดวกในขั้นตอนการติดต่อต่างๆกับมหาลัยตลอดเวลาที่ผู้เขียนได้ศึกษาที่ สถาบันบัณฑิตพัฒนบริหารศาสตร์

ขอขอบคุณเจ้าหน้าที่ห้องสมุด คลินิกวิทยานิพนธ์ ที่ให้คำแนะนำทางด้านรูปแบบการจัดทำวิทยานิพนธ์ รวมถึงให้วิธีแก้ปัญหาโปรแกรมที่ใช้งาน ทำให้สามารถแก้ปัญหาที่เกิดขึ้นได้อย่างตรงจุด โดยใช้เวลาไปน้อยที่สุด

สุดท้ายนี้ ขอกราบขอบพระคุณบิดา มารดา ที่เคารพรักอย่างสูงยิ่ง ที่ได้สนับสนุนทางด้านการศึกษาของผู้เขียนตลอดมาด้วยความเชื่อมั่นและอดทนเป็นอย่างยิ่งตลอดมา

พูนศักดิ์ พรเพิ่มพูน

สิงหาคม 2556

สารบัญ

หน้า

บทคัดย่อ	(5)
ABSTRACT	(6)
กิตติกรรมประกาศ	(7)
สารบัญ	(8)
สารบัญตาราง	(10)
สารบัญภาพ	(11)
บทที่ 1 บทนำ	1
1.1 ปัญหาและความเป็นมา	1
1.2 วัตถุประสงค์การวิจัย	3
1.3 ขอบเขตการวิจัย	3
1.4 วิธีดำเนินการวิจัย	4
1.5 ประโยชน์ที่คาดว่าจะได้รับ	4
บทที่ 2 แนวคิดทฤษฎี และทบทวนวรรณกรรมที่เกี่ยวข้อง	5
2.1 งานวิจัยที่เกี่ยวข้อง	5
2.2 ทฤษฎีที่เกี่ยวข้อง	13
บทที่ 3 ระบบไร้สายเพื่อควบคุมการทำงานของเครื่องจักรและตรวจสอบสถานะ แวดล้อมภายในโรงงานจากระยะไกล	42
3.1 แนวคิดในการออกแบบระบบ	42
3.2 Remote Site ระบบควบคุมจากระยะไกล	43
3.3 Factory Site ระบบควบคุมในโรงงาน	44
3.4 ความมั่นคงของข้อมูล	48
3.5 การจัดการอุปกรณ์ปลายทางในโรงงาน	49

บทที่ 4 การ Implement ระบบไร้สายเพื่อควบคุมการทำงานของเครื่องจักร และตรวจสอบสถานะแวดล้อมภายในโรงงานจากระยะไกล	51
4.1 ฝั่ง Remote Site	51
4.2 ฝั่ง Factory Site	57
4.3 ระบบที่ได้พัฒนาในการทดลอง	67
บทที่ 5 ผลการทดลองการใช้งาน	69
5.1 ผลการทดลองจากเครื่องคอมพิวเตอร์ PC	69
5.2 ผลการทดลองจากโทรศัพท์เคลื่อนที่	71
บทที่ 6 สรุปผลการวิจัยและข้อเสนอแนะ	75
6.1 สรุปผลการวิจัย	75
6.2 ข้อเสนอแนะ	76
บรรณานุกรม	77
ประวัติผู้เขียน	79

สารบัญตาราง

ตารางที่	หน้า
2.1 แสดงรายละเอียดของฟังก์ชัน F G H I ที่ใช้ใน Compression Function	27
2.2 แสดงรายละเอียดของ Android OS ที่เผยแพร่จนปัจจุบัน	36
4.1 แสดงข้อมูลจำเพาะของเครื่องคอมพิวเตอร์ที่ใช้	52
4.2 แสดงข้อมูลจำเพาะของโทรศัพท์เคลื่อนที่ที่ใช้	54
4.3 แสดงข้อมูลจำเพาะของ Microcontroller Arduino ADK 2560 R3	59
5.1 แสดงเวลาเฉลี่ยที่ดำเนินไปของการทำงานในแต่ละชั้น	74

สารบัญภาพ

ภาพที่	หน้า
2.1 แสดงแนวคิดของระบบ Bluetooth Based Telemetry/PLC System	5
2.2 แสดงแนวคิดของระบบในการใช้ Zigbee เพื่อควบคุม PLC	7
2.3 VCI ซึ่งใช้ควบคุม PLC ในรูปแบบ GUI	8
2.4 แสดงโครงสร้างของระบบ “Study on remote PLC experiment system based on web”	9
2.5 แสดงแนวคิดของ ZigBee-Based Home Automation System	11
2.6 แสดงองค์ประกอบของ Zigbee Protocol Stack	14
2.7 แสดงการเปรียบเทียบ Zigbee กับระบบเครือข่ายไร้สายประเภทอื่นๆ	15
2.8 แสดงรายละเอียดของ Physical Layer ตามมาตรฐาน IEEE 802.15.4	16
2.9 แสดงภาพ Topology ในการใช้งาน Zigbee Network	18
2.10 แสดงการเชื่อมต่อแบบไร้สายโดยใช้ระบบ Zigbee	19
2.11 แสดงการเชื่อมต่อ Microcontroller 2 ตัว โดยใช้ Zigbee Module	20
2.12 แสดง UART Data Packet	20
2.13 แสดงรูปแบบของ AT Command	21
2.14 แสดงรูปแบบของ API Frame	22
2.15 แสดง Message Digest generation Using MD5	24
2.16 แสดง Initialize MD Buffer	25
2.17 แสดง Initialize MD Buffer ในรูปแบบ Little-endian Format	25
2.18 แสดงการประมวลผลแบบ MD5 ของบล็อก q	26
2.19 แสดงการประมวล Buffer A B C D หนึ่งรอบในแบบ Diagram	28
2.20 แสดงการทำ Message Digest ด้วยการ Hash	29
2.21 แสดงกระบวนการสร้างและตรวจสอบ Integrity โดยวิธีการ Message Digest	30
2.22 แสดงกระบวนการทำ Message Authentication Code	30

2.23	แสดงกระบวนการสร้าง HMAC	31
2.24	แสดงยืนยันตัวตนด้วย Digital Signature	31
2.25	แสดงการ Challenge-Response แบบ Symmetric Key	32
2.26	แสดงการ Challenge-Response แบบ Symmetric Key โดยเพิ่ม Time Stamp	33
2.27	แสดงการ Challenge-Response แบบ Asymmetric Key	33
2.28	แสดงการ Challenge-Response แบบ Symmetric Key โดย Digital Signature	34
2.29	แสดง Android Low-Level System Architecture	37
2.30	แสดงขั้นตอนการคอมไพล์โค้ดโปรแกรมสำหรับ Android	40
2.31	แสดงส่วนประกอบของไฟล์ Android Package	41
3.1	แสดงแนวคิดของระบบ	43
3.2	แสดงแนวคิด Multi User และ Multi Device	44
3.3	แสดงการเข้ารหัสข้อมูลและสร้าง HMAC	48
3.4	แสดงการติดต่อขณะกำลัง Authentication	49
4.1	แสดง Software Architecture ที่ใช้บน Notebook PC	53
4.2	แสดง Software Architecture ของ software บนโทรศัพท์เคลื่อนที่	55
4.3	แสดงลำดับขั้นตอนการทำงานของโปรแกรมบนโทรศัพท์เคลื่อนที่	56
4.4	แสดงภาพด้านบนของ Microcontroller Arduino ADK 2560 R3	58
4.5	แสดงภาพด้านล่างของ Microcontroller Arduino ADK 2560 R3	58
4.6	แสดง Software Architecture ซึ่งทำงานบน Microcontroller	60
4.7	แสดงลำดับขั้นตอนการทำงานของ GATEWAY	61
4.8	แสดงลำดับขั้นตอนการทำงานของ BACK OFFICE	62
4.9	แสดงการเชื่อมต่อ Device Node เข้ากับ PLC ในการ ทำงาน Transparent Mode	64
4.10	แสดง Device Node ซึ่งมีอุปกรณ์เป็น Sensor โดยมีการ ทำงานแบบ API Mode	65
4.11	แสดงภาพด้านล่างของ Sensor Board ที่ทำงานแบบ API Mode	65

4.12 แสดง Coordinator Node ซึ่งมีการทำงานทั้ง Transparent Mode และ API Mode	66
4.13 แสดงระบบที่ได้พัฒนาขึ้นในการทดสอบการควบคุม	67
5.1 แสดงหน้าจอขณะ Login เข้าสู่ระบบ บนเครื่องคอมพิวเตอร์ Notebook	69
5.2 แสดงหน้าจอผลลัพธ์การเข้าสู่ระบบ เมื่อทำการ Login ได้สำเร็จ	69
5.3 แสดงการทดสอบการอ่านข้อมูลจาก PLC ด้วยโปรแกรม GX Developer	70
5.4 แสดงหน้าจอผลของค่าที่ได้จาก Sensor Board	71
5.5 แสดงขั้นตอนการ Login จากโปรแกรมที่พัฒนาขึ้นบน Android	72
5.6 แสดงส่วนการตรวจสอบสถานะของ PLC หลังจากที่ทำ Login เรียบร้อยแล้ว	72
5.7 ผลแสดงผลการตรวจสอบสถานะของ PLC ซึ่งกำลังทำงานอยู่ใน โหมด STOP	73
5.8 แสดงผลลัพธ์การตรวจสอบสถานะของ PLC ซึ่งกำลังทำงานอยู่ใน โหมด RUN	73

บทที่ 1

บทนำ

1.1 ปัญหาและความเป็นมา

การควบคุมการทำงานของเครื่องจักรกลในสมัยแรก ออกแบบการควบคุมโดยใช้รีเลย์ ร่วมกับอุปกรณ์อื่นๆ เช่น ปุ่มกด คอนแทกเตอร์ เป็นต้น เพื่อให้สามารถควบคุมเครื่องจักรกลได้ตามความต้องการ แต่การออกแบบส่วนควบคุมนั้น ก็ทำได้ยาก เพราะต้องใช้วิธี Hardwire โดยตรง และส่วนควบคุมนั้นก็มีขนาดใหญ่ ซ่อมบำรุงได้ยากเพราะมีความซับซ้อน อีกทั้งเมื่อลักษณะงานที่ต้องการควบคุมเปลี่ยนไป วงจรเดิมก็ไม่สามารถใช้ได้อีก ต้องมีการแก้ไข ซึ่งเป็นเรื่องยาก ดังนั้น จึงมีการออกแบบวงจรควบคุมอัตโนมัติแบบโปรแกรมได้ขึ้นมาเพื่อแทนวงจรการควบคุมแบบเดิม ซึ่งระบบวงจรควบคุมอัตโนมัติแบบโปรแกรมได้ คือ Programmable Logic Control (PLC) ซึ่งมีข้อดีกว่าระบบเดิม คือ มีขนาดเล็ก กะทัดรัด เมื่อเทียบกับวงจรการควบคุมแบบเดิม แก้ไขลำดับการทำงานได้ง่ายด้วยการเขียนโปรแกรม ไม่จำเป็นต้องมีการแก้ไขตัววงจรจริงๆ ด้วยข้อดีของระบบการควบคุมอัตโนมัตินี้ ทำให้มีการใช้งานกันอย่างกว้างขวางออกไปทั้งในบ้านเรือนและโรงงานอุตสาหกรรม เช่น ใช้ควบคุมลิฟต์ บันไดเลื่อน เครื่องจักรต่างๆ ในโรงงานอุตสาหกรรม เป็นต้น

การนำระบบอัตโนมัติมาใช้ในโรงงานอุตสาหกรรม สามารถเพิ่มผลผลิตและลดความผิดพลาดในการผลิตได้อย่างมาก โดยเฉพาะในอุตสาหกรรมที่มีอันตรายในการผลิต เช่น โรงกลั่นน้ำมัน แร่แยกก๊าซ โรงงานผลิตสารเคมี เป็นต้น การใช้เซ็นเซอร์ตรวจวัดร่วมกับระบบอัตโนมัติในการผลิต เช่น แชนกัล หุ่นยนต์ ระบบควบคุมอัตโนมัติ เป็นต้น สามารถช่วยลดทั้งความผิดพลาดที่เกิดจากการทำงาน และความสูญเสียต่อชีวิตมนุษย์เมื่อเกิดอุบัติเหตุขึ้นได้

แม้ว่าการใช้ระบบควบคุมอัตโนมัติจะมีประโยชน์ต่อการผลิตในโรงงานอุตสาหกรรมอย่างมาก แต่ในการสั่งงานควบคุมระบบอัตโนมัตินี้ กลับถูกจำกัดไว้ด้วยระยะทางของสายเคเบิลที่ทำการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ใช้ควบคุม กับระบบควบคุมอัตโนมัตินี้เอง แม้ว่าจะมีผู้ผลิต PLC บางยี่ห้อที่ออกแบบให้สามารถเชื่อมต่อกันเป็นเครือข่ายได้ แต่ก็จำกัดอยู่ภายใต้

เครือข่ายของตนเท่านั้น ไม่สามารถควบคุมจากระยะไกลได้ จึงมีความพยายามที่จะพัฒนาระบบการผลิตอัตโนมัติในด้านต่างๆ อย่างต่อเนื่อง สำหรับการควบคุมระบบอัตโนมัติโดยใช้ระบบไร้สายก็เป็นด้านหนึ่งที่มีงานวิจัยเพื่อการพัฒนาอย่างต่อเนื่องจากการควบคุมในแบบปกติ เช่น งานวิจัย Abou El-Ela and Alkanhel (2007) ซึ่งเสนอแนวคิดนำ Bluetooth Module มาใช้แทนสายเคเบิลในการเชื่อมต่อระหว่าง Programmable Logic Controller (PLC) เข้ากับเครื่องที่ใช้ควบคุม ข้อจำกัดของระบบนี้ คือ การทำงานของ Bluetooth อาจมีการรบกวนกับการทำงานของ WIFI ซึ่งอยู่ภายในบริเวณเดียวกันได้ และยังไม่สามารถจัดการอุปกรณ์หลายๆ ชิ้นในรูปแบบของเครือข่าย นอกจากนี้งานวิจัยนี้ยังไม่ได้คำนึงถึงการควบคุมผ่านเครือข่ายอินเทอร์เน็ต งานวิจัย (Li and Li, 2009: 533–536) นำเสนอแนวคิดการนำ Zigbee มาใช้แทนสายเคเบิลในการเชื่อมต่อส่วนคอมพิวเตอร์ที่ใช้ควบคุมเข้ากับ PLC แบบไร้สายในระยะใกล้ โดยมีการใช้ Zigbee ในรูปแบบเครือข่ายทำให้สามารถเชื่อมต่อ PLC เข้าในระบบได้หลายตัว ข้อจำกัดของงานวิจัยนี้คือเป็นระบบการสื่อสารระยะใกล้เท่านั้น ยังไม่ได้คำนึงถึงการส่งผ่านเครือข่ายอินเทอร์เน็ต ซึ่งจำเป็นต้องมีการพัฒนาระบบสนับสนุนที่จำเป็นเพิ่มเติมอีกด้วย เช่น ระบบการจัดการผู้ใช้แบบหลายผู้ใช้ ระบบการแปลงรูปแบบคำสั่งที่ใช้ติดต่อกับ PLC ในแบบ Serial ให้สามารถส่งผ่านอินเทอร์เน็ตได้ ระบบการจัดการด้านความปลอดภัยขณะที่ส่งข้อมูลผ่านอินเทอร์เน็ต งานวิจัย (Hui and Jing, 2011: 1683–1686) นำเสนอแนวคิดของการแสดงสถานะของ PLC ในรูปแบบ GUI เรียกว่า Virtual Control Interface (VCI) โดยมีจุดมุ่งหมายเพื่อนำไปใช้ในการเรียนการสอนแบบระยะไกล ซึ่ง VCI นี้พัฒนาขึ้นในรูปแบบเว็บเพจเพื่อให้ผู้เรียนจากระยะไกล สามารถทดลองใช้ PLC จากระยะไกล ข้อจำกัดของการแสดงสถานะด้วย VCI คือ การนำแนวคิดประยุกต์ใช้งานจริงจะขาดความยืดหยุ่น โดย VCI ที่สร้างขึ้นใช้ได้เฉพาะกับ PLC ที่จำลองออกมาเท่านั้นแม้จะทำการเชื่อมต่อแบบ Serial เหมือนกันก็ตาม การที่จะต้องแก้ไข VCI เพื่อให้ใช้กับ PLC ตัวอื่นทำได้ยากและอาจต้องเสียทรัพยากรมาก งานวิจัย (Gill, Shuang-Hua, Fang and Xin, 2009: 422–430) นำเสนอแนวคิดการควบคุมการทำงานของอุปกรณ์เครื่องใช้ไฟฟ้าภายในบ้านจากระยะไกลผ่านเครือข่ายอินเทอร์เน็ต และระยะใกล้ภายในบ้าน โดยนำเสนอหลักการจัดการอุปกรณ์ภายในบ้านซึ่งประกอบด้วย 2 ส่วน คือ Home Gateway และ Virtual Home โดย Home Gateway ทำหน้าที่ดูแลการรับคำสั่งทั้งที่ส่งมาจากภายในบ้านและที่ส่งจากระยะไกลผ่านอินเทอร์เน็ต Virtual Home เป็นส่วนที่ใช้ตรวจสอบความถูกต้องของคำสั่งที่ได้รับมา ก่อนที่จะส่งให้อุปกรณ์ปลายทางทำงาน ระบบนี้ใช้ควบคุมอุปกรณ์ที่ใช้ภายในบ้านซึ่งมักมีสถานะที่ไม่ซับซ้อน เช่น การเปิดปิด สวิตช์ไฟ การควบคุมอุณหภูมิของเครื่องปรับอากาศ ดังนั้นระบบนี้จึงเป็นการยากที่จะนำไปใช้ควบคุมอุปกรณ์

ที่มีการควบคุมซับซ้อนและต้องอาศัยส่วนควบคุมและมีการเชื่อมต่ออุปกรณ์ที่ถูกรวบรวมมาเฉพาะ เช่น ในโรงงานที่มักใช้อุปกรณ์ที่ต้องใช้โปรแกรมควบคุมเฉพาะตามที่คุณผลิตกำหนดมา และมักใช้การส่งข้อมูลด้วย Serial Port

เพื่อเป็นการเพิ่มประสิทธิภาพในการใช้งาน PLC ในโรงงาน บทความวิจัยนี้จึงประยุกต์ใช้แนวคิดการควบคุมระยะไกลมาใช้ โดยได้นำเสนอแนวคิด การแปลงรูปแบบคำสั่งให้สามารถส่งผ่านอินเทอร์เน็ต ซึ่งจะทำให้สามารถใช้โปรแกรมเดิมจากผู้ผลิตได้ และสามารถเพิ่มอุปกรณ์เข้าไปในระบบโดยไม่ต้องแก้ไขระบบที่ได้พัฒนาไว้แล้ว รวมถึงแนวคิดการจัดการระบบเพื่อสนับสนุนผู้ใช้แบบหลายคน (Multi User) ซึ่งจะทำให้สามารถจัดการอุปกรณ์ภายในโรงงานได้อย่างถูกต้องและเหมาะสม เสนอแนวคิดในการจัดการด้านความมั่นคงปลอดภัยของระบบในการทำงานเพื่อความปลอดภัยและปลอดภัย นอกจากนี้การใช้ระบบไร้สายในการควบคุมยังลดความเสี่ยงในการเกิดอุบัติเหตุในการทำงานโดยไม่ได้นำเครื่องควบคุมเข้าไปยังพื้นที่ซึ่งมีเครื่องจักรอันตรายทำงานอยู่

1.2 วัตถุประสงค์การวิจัย

เพื่อศึกษาวิจัยระบบฝังตัวแบบไร้สายเพื่อควบคุมและตรวจสอบการสั่งงานในโรงงานผ่านเครือข่ายอินเทอร์เน็ต

1.3 ขอบเขตการวิจัย

1.3.1 เป็นระบบ EMBEDDED SYSTEM ที่สามารถให้บริการในการควบคุม PLC และตรวจสอบสถานะของ Sensor ภายในโรงงานจากระยะไกลผ่านอินเทอร์เน็ตได้ โดยมีการรักษาความปลอดภัยของระบบ EMBEDDED SYSTEM ให้ทนทานต่อการโจมตีผ่านอินเทอร์เน็ตในรูปแบบต่างๆ อย่างเหมาะสม

1.3.2 การสื่อสารระยะไกลในโรงงาน ใช้เครือข่ายการสื่อสารแบบ Zigbee เชื่อมโยงภายในโรงงาน

1.3.3 ใช้โปรแกรมควบคุมเดิมซึ่งถูกกำหนดจากผู้ผลิต PLC ได้เต็มประสิทธิภาพ

1.3.4 ใช้โทรศัพท์เคลื่อนที่ในการควบคุมผ่านโปรแกรมที่พัฒนาขึ้นเองได้

1.4 วิธีดำเนินการวิจัย

1.4.1 ศึกษาคุณสมบัติของ Protocol TCP/IP เพื่อนำไปใช้อำนวยความสะดวกและรักษาความถูกต้องในการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต

1.4.2 ศึกษาหลักการทำงานของ Zigbee เพื่อเลือกใช้งานให้เหมาะสมในการนำไปใช้ควบคุมในระยะใกล้ภายในโรงงาน

1.4.3 ศึกษาการพัฒนาโปรแกรมบน Android OS

1.4.7 ออกแบบระบบการเชื่อมต่อ Remote PC เข้ากับ PLC จากระยะไกล ผ่านโปรแกรมแปลง Packet

1.4.8 พัฒนาโปรแกรมประยุกต์ที่ส่งคำสั่งแบบ API ให้อ่านค่า Sensor ผ่าน Zigbee จากระยะไกล

1.4.9 ทดสอบการทำงานของโปรแกรมทั้งระบบ

1.4.10 สรุปผลการวิจัย และข้อเสนอแนะ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 สามารถเข้าใจและสั่งงาน PLC จากระยะไกลได้

1.5.2 สามารถพัฒนาโปรแกรมประยุกต์บน Notebook ให้อ่านค่าสถานะจาก Sensor จากระยะไกลได้

1.5.3 ทำให้เข้าใจโปรแกรมประยุกต์ประเภทแปลง UART Packet เป็น TCP/IP Packet และเลือกใช้งานได้ตามเหมาะสม

1.5.4 สามารถเข้าใจการทำงานของ Zigbee พร้อมทั้งเลือกใช้งานโหมดการทำงานที่มีได้อย่างเหมาะสม

1.5.5 สามารถพัฒนาโปรแกรมบนระบบโทรศัพท์เคลื่อนที่ Android เพื่อให้ส่งคำสั่งไปยัง PLC และรับผลลัพธ์การประมวลผลจาก PLC จากระยะไกลผ่านระบบอินเทอร์เน็ตได้

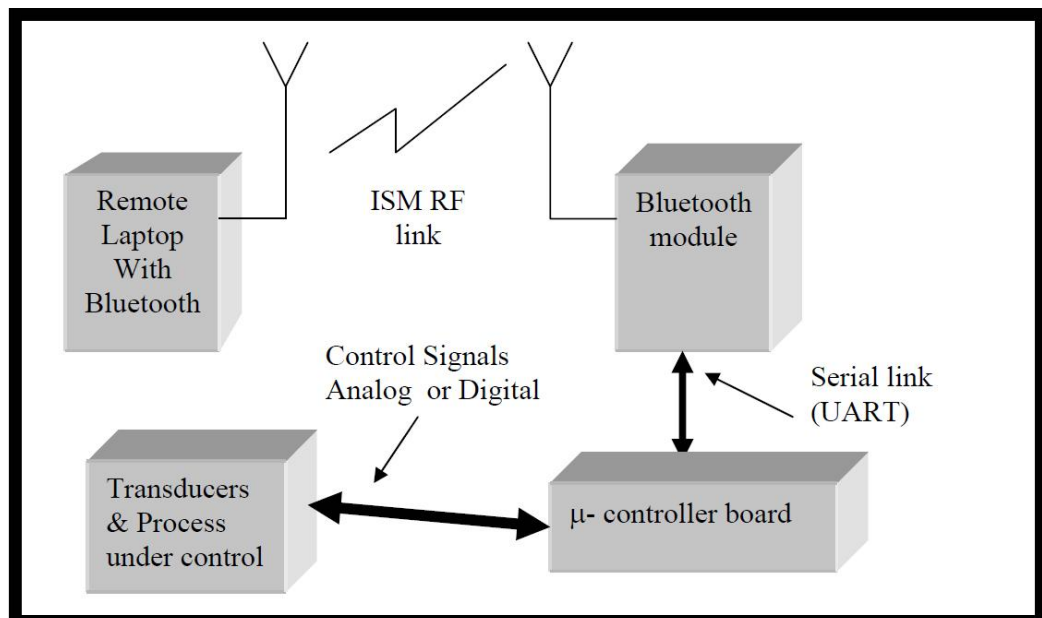
บทที่ 2

แนวคิดทฤษฎีและทบทวนวรรณกรรมที่เกี่ยวข้อง

2.1 งานวิจัยที่เกี่ยวข้อง

2.1.1 Bluetooth Based Telemetry/PLC System

งานวิจัยนี้ Abou El-Ela and Alkanhel (2007) เสนอแนวคิดนำ Bluetooth Module มาใช้แทนสายเคเบิลในการเชื่อมต่อระหว่าง Programmable Logic Controller (PLC) เข้ากับเครื่องที่ใช้ควบคุม ซึ่งทำให้สามารถขยายความสามารถในการสั่งงาน PLC ให้สะดวกมากขึ้น เนื่องจากไม่ถูกจำกัดด้วยระยะทางของสายเคเบิลอีกต่อไป ซึ่งข้อดีของการเลือกใช้ Bluetooth ก็คือ เป็นระบบการสื่อสารที่เสถียร ทนทานต่อสภาวะแวดล้อมที่มี Noise มาก มีความเร็วในการทำงานเพียงพอ ใช้พลังงานน้อย นอกจากนี้ การใช้เครือข่ายไร้สาย Bluetooth ทำให้ไม่ต้องนำเครื่องที่ใช้ควบคุมเข้าไปยังพื้นที่ซึ่งอาจมีอันตรายจากการทำงานของเครื่องจักรได้



ภาพที่ 2.1 แสดงแนวคิดของระบบ Bluetooth Based Telemetry/PLC System

แหล่งที่มา: Abou El-Ela and Alkanhel, 2007.

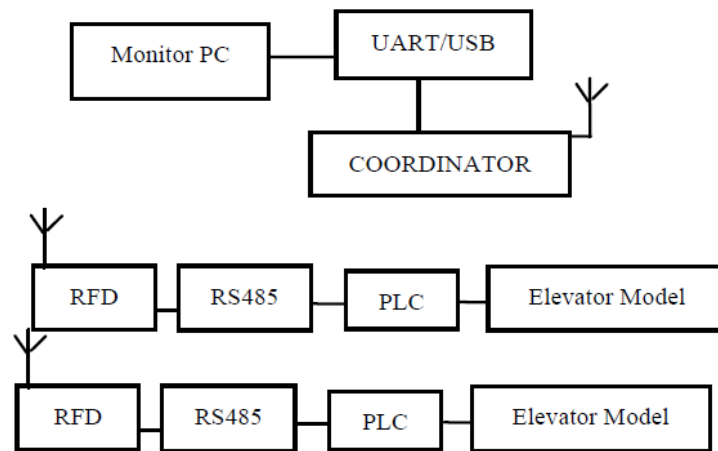
จากภาพ 2.1 แสดงแนวคิดการทำงานของระบบ โดย Remote Laptop ที่ใช้สั่งงาน จะส่งคำสั่งควบคุมผ่านไปยัง Microcontroller Board โดยอาศัยการเชื่อมต่อระหว่าง Bluetooth Module ภายในเครื่อง Laptop กับ Bluetooth Module ซึ่งเชื่อมต่อกับ Microcontroller Board ในแบบ Serial Link โดยเมื่อ Microcontroller Board ได้รับคำสั่งจาก Remote Laptop แล้ว ก็จะส่งสัญญาณควบคุมออกไปยัง PLC ตามที่ได้โปรแกรมลำดับการทำงานไว้ล่วงหน้าแล้ว

ข้อจำกัดของระบบนี้ คือ การทำงานของ Bluetooth อาจมีการรบกวนกับการทำงานของ WIFI ซึ่งอยู่ภายในบริเวณเดียวกันได้ รวมถึงการที่ยังไม่สามารถจัดการอุปกรณ์หลายๆ ชิ้นในรูปแบบของเครือข่ายได้ เนื่องจากรูปแบบการเชื่อมโยงของ Bluetooth เป็นลักษณะของการส่งข้อมูลแบบ Master และ Slave (จุดต่อจุด) นั่นเอง นอกจากนี้งานวิจัยนี้ยังไม่ได้คำนึงถึงการควบคุมผ่านเครือข่ายอินเทอร์เน็ต ทำให้ระบบนี้ยังจำกัดระยะทางการควบคุมอยู่ในระยะการทำงานของ Bluetooth Module นั่นเอง

2.1.2 Application of Communication and Remote Control in PLC Based on ZigBee Technology

งานวิจัยนี้ (Li and Li, 2009: 533–536) เสนอแนวคิดและผลการทดลองของการนำเอา Zigbee มาใช้ในการสื่อสารข้อมูลในระยะใกล้ เพื่อเชื่อมต่อระหว่าง PLC เข้ากับเครื่องควบคุม ซึ่งข้อดีของ Zigbee เมื่อเปรียบเทียบกับ Bluetooth ก็คือ Zigbee สามารถรับส่งข้อมูลในแบบเครือข่ายซึ่งใช้ Topology ได้ทั้ง Ad-hoc, Peer to Peer, Star, Mesh ทำให้สามารถเลือกรูปแบบของ Topology ที่จะใช้ได้ตามการวางแผนผังสายการผลิตของเครื่องจักรในโรงงานได้อย่างลงตัว ซึ่งเหนือกว่า Bluetooth ซึ่งใช้การรับส่งข้อมูลในแบบ Peer to Peer ซึ่งอาจกลายเป็นข้อจำกัดเมื่อแผนผังสายการผลิตของเครื่องจักรในโรงงานนั้นไม่อำนวยให้จัดเรียงตามลักษณะการรับส่งข้อมูลแบบจุดต่อจุดของ Bluetooth

โดยการเปลี่ยนมาใช้ระบบเครือข่ายไร้สาย ทำให้ไม่ต้องถูกจำกัดด้วยสายเคเบิลแบบในระบบเดิม โดยนำเสนอระบบที่ใช้ในการทดลองดังรูป



ภาพที่ 2.2 แสดงแนวคิดของระบบในการใช้ Zigbee เพื่อควบคุม PLC

แหล่งที่มา: Li and Li, 2009: 533.

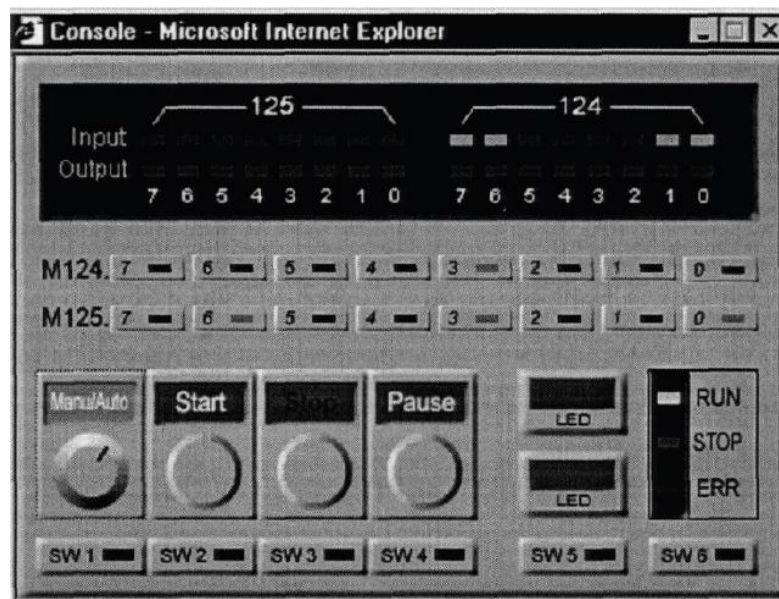
จากภาพ 2.2 Monitor PC คือ เครื่อง PC ที่ใช้ทำการควบคุม PLC ของระบบนี้ โดย Monitor PC จะต่อกับ ZIGBEE ที่เชื่อมต่อให้เป็น COORDINATOR NODE ด้วย Serial Port หรือ USB Port ก็ได้ สำหรับ RFD Node นั้นถูก Implement ด้วย Chip CC2430 ซึ่งเป็น Chip ที่มีองค์ประกอบหลายส่วนรวมกัน คือ 1) Zigbee Module ที่ตั้งให้ทำงานในแบบ End Device Mode ของระบบ จะคอยรับคำสั่งจาก COORDINATOR MODE 2) Microcontroller ที่ Compatible กับ Microcontroller ตระกูล 8051 เป็นหน่วยประมวลผลกลาง ทำหน้าที่คำนวณและจัดการการทำงานทั้งหมดของ Chip CC2430 ซึ่งทำงานคล้ายกับที่ CPU ทำหน้าที่ประมวลผลในเครื่องคอมพิวเตอร์ นอกจากนี้ ส่วน RFD นี้จะต้องมีการใส่วงจรแปลง OUTPUT ของ CHIP CC2430 ให้เป็น RS485 เนื่องจาก OUTPUT ของ CC2430 นั้นเป็น Serial Port แต่ Input ของ PLC มี Interface เป็นแบบ RS485 จึงต้องมีการแปลงทั้งการส่งจาก RFD ไปยัง PLC และแปลงผลลัพธ์จาก PLC กลับมายัง RFD สำหรับงานวิจัยนี้ Monitor PC จะทำการ Monitor สถานะการทำงานของ PLC ซึ่งทำการควบคุมการทำงานของลิฟต์

ข้อจำกัดของงานวิจัยนี้คือเป็นระบบการสื่อสารระยะใกล้เท่านั้น ยังไม่ได้คำนึงถึงการส่งผ่านเครือข่ายอินเทอร์เน็ต ซึ่งต้องมีการพัฒนาระบบเพิ่มเติม เช่น การจัดการผู้ใช้ รูปแบบของ Protocol ได้ตอบที่จะใช้ในการสื่อสารของโปรแกรมควบคุมกับ PLC เมื่อควบคุมผ่านอินเทอร์เน็ต รวมถึงการจัดการด้านความปลอดภัยของระบบขณะที่ส่งข้อมูลผ่านอินเทอร์เน็ตอีกด้วย

งานวิจัยนี้สรุปผลการวิจัยโดยชี้ให้เห็นว่า Zigbee สามารถส่งข้อมูลเพื่อใช้ควบคุมและ Monitor PLC ได้โดยมีความถูกต้องแม่นยำสูง เหมาะกับการใช้งานควบคุมภายในโรงงานได้เป็นอย่างดี

2.1.3 Study on remote PLC experiment system based on web

งานวิจัยนี้ (Hui and Jing, 2011: 1683–1686) นำเสนอแนวคิดของการแสดงสถานะของ PLC ในรูปแบบ GUI เรียกว่า Virtual Control Interface (VCI) โดยมีจุดมุ่งหมายเพื่อนำไปใช้ในการเรียนการสอนแบบระยะไกล ซึ่ง VCI นี้พัฒนาขึ้นในรูปแบบเว็บเพจเพื่อให้ผู้เรียนจากระยะไกล สามารถทดลองควบคุมการทำงานของ PLC จากระยะไกล โดยตัวอย่างของ VCI ที่ระบบนี้สร้างขึ้น แสดงไว้ในภาพ 2.3 ดังนี้

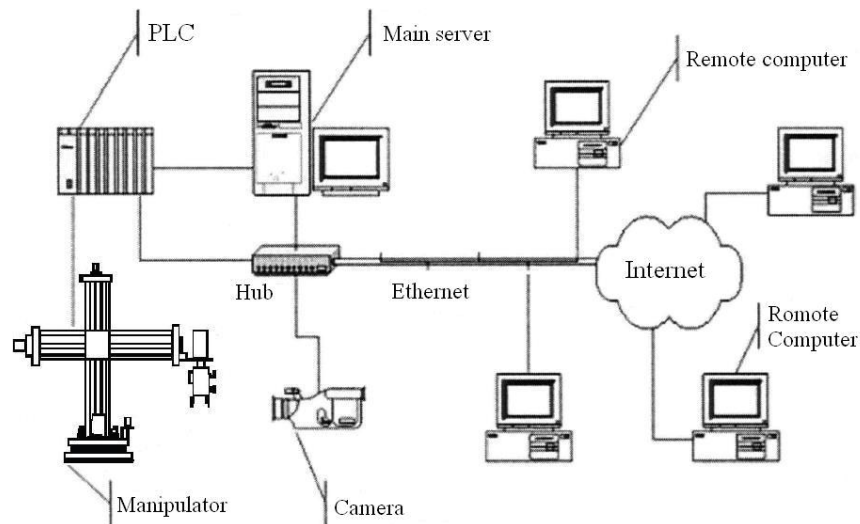


ภาพที่ 2.3 แสดง VCI ซึ่งใช้ควบคุม PLC ในรูปแบบ GUI

แหล่งที่มา: Hui and Jing, 2011: 1685.

สำหรับโครงสร้างของระบบนี้ PLC จะเชื่อมต่อด้วยเครือข่ายแบบมีสายแบบ Ethernet LAN โดยที่ PLC จะรับคำสั่งจากส่วนติดต่อกับผู้ใช้ คือ VCI ซึ่งเก็บอยู่ใน Web Server ที่

ประมวลผลอยู่ภายใน Main Server หลังจากที่ได้รับคำสั่งผ่านทาง VCI แล้ว จากนั้น PLC ก็ทำงานตามคำสั่งโดยการไปสั่งงานแขนกลตามคำสั่งที่ได้รับมา โดยจะแสดงสถานะปัจจุบันของ PLC กลับไปให้ผู้ใช้งานทราบผ่านทาง VCI ดังภาพที่ 2.4



ภาพที่ 2.4 แสดงโครงสร้างของระบบ “Study on Remote PLC Experiment System Based on Web”

แหล่งที่มา: Hui and Jing, 2011: 1683.

ระบบนี้ออกแบบเพื่อให้ นักเรียนสามารถสั่งงาน PLC จากระยะไกล การทำงานเริ่มต้นโดยผู้ใช้งาน ซึ่งเป็นนักเรียน ทำการใช้ Web Browser เข้าไปยัง Web Server ซึ่งมีการพัฒนา VCI ดังภาพ 2.4 ไว้ในรูปแบบของ Java Applet และ Java Script จากนั้นนักเรียนก็จะสามารถทดสอบการสั่งงาน PLC ได้ด้วยการ กดปุ่มต่างๆ บน VCI ซึ่งเมื่อ VCI ได้รับคำสั่งจากนักเรียนแล้ว ก็จะส่งสัญญาณควบคุมไปยัง PLC ตัวจริงที่เชื่อมต่ออยู่ จากนั้น VCI ก็จะอ่านผลลัพธ์จากการสั่งงานครั้งนั้นจาก PLC ตัวจริงกลับมาอัปเดตสถานะที่แสดงอยู่บน VCI ให้นักเรียนได้เห็นผลลัพธ์การทำงานได้ คล้ายกับฝึกหัดกับ PLC โดยตรง

ข้อจำกัดของระบบเมื่อนำไปประยุกต์ใช้ควบคุมภายในโรงงานคือ ในโรงงานมักจะมีเครื่องจักรทำงานอยู่พร้อมๆ กันเป็นจำนวนมาก ซึ่งทำให้ต้องมี PLC หลายหน่วย ดังนั้นการใช้การเชื่อมต่อแบบมีสาย จึงไม่อำนวยความสะดวกเมื่อมีการเพิ่มหรือลดจำนวนของ PLC รวมถึงการเคลื่อนย้ายเครื่องจักรตามผังโรงงานที่ปรับปรุงไป โดยจะต้องมีค่าใช้จ่ายเพิ่มเติมในการติดตั้งและแก้ไขสาย LAN และอุปกรณ์ เครือข่ายที่เกี่ยวข้องเช่น Hub หรือ Switch นอกจากนี้ Main Server

ที่ใช้ในการทำงานเป็น Web Server นั้นต้องใช้เครื่องที่มีประสิทธิภาพสูงเพื่อสร้าง VCI ติดต่อกับผู้ใช้ โดยเฉพาะการทำงานในโรงงานที่จะมีผู้ใช้หลายคน และมี PLC หลายหน่วย ซึ่งต้องการการจัดการแบบ Multi User – Multi Device ทำให้ต้องใช้ Main Server ที่มีประสิทธิภาพสูงตามไปด้วย ซึ่งหมายถึงค่าใช้จ่ายที่เพิ่มขึ้นตามจำนวน User นั้นเอง

ข้อจำกัดของการควบคุมและแสดงสถานะด้วย VCI คือ การนำแนวคิดประยุกต์ใช้งานจริงจะขาดความยืดหยุ่น โดย VCI ที่สร้างขึ้นใช้ได้เฉพาะกับ PLC ที่จำลองออกมาเท่านั้นแม้จะทำการเชื่อมต่อแบบ Serial เหมือนกันก็ตาม การที่จะต้องแก้ไข VCI เพื่อให้ใช้กับ PLC ตัวอื่นทำได้ยากและอาจต้องเสียทรัพยากรมาก

เมื่อจะประยุกต์ระบบนี้มาใช้งานควบคุมจริงภายในโรงงาน ควรเปลี่ยนเครือข่ายภายในโรงงานเป็นแบบไร้สายระยะไกลเพื่อให้สามารถปรับเปลี่ยน Topology ของเครือข่ายภายในโรงงานได้สะดวก ตามการจัดวางเครื่องจักรภายในโรงงานตามผังโรงงานที่จะเปลี่ยนแปลงไปในอนาคต รวมถึงต้องมีการออกแบบระบบการจัดการ Multi User และ Multi Device เพื่อให้เหมาะสมกับลักษณะการทำงานของโรงงาน ซึ่งจะมีผู้ควบคุมหลายคน และมีอุปกรณ์ PLC หลายหน่วย นอกจากนี้ยังควรออกแบบรูปแบบการติดต่อสื่อสารและการรักษาความปลอดภัยของระบบเมื่อส่งผ่านเครือข่ายอินเทอร์เน็ตให้มีความถูกต้อง ปลอดภัย และรัดกุม

2.1.4 A ZigBee-Based Home Automation System

งานวิจัยนี้ (Gill, Shuang-Hua, Fang and Xin, 2009: 422-430) นำเสนอแนวคิดของการควบคุมอุปกรณ์ เครื่องใช้ไฟฟ้าต่างๆ ภายในบ้าน จากระยะไกลผ่านเครือข่าย Internet โดยมีการกล่าวถึงระบบ Home Automation แบบเดิมที่รูปแบบพร้อมระบุปัญหาของระบบไว้ คือ

ระบบที่หนึ่ง Java Based Home Automation เป็นแบบพัฒนาส่วนควบคุมของเครื่องใช้ไฟฟ้าต่างๆ ด้วยระบบที่เป็น Java Embedded Base แล้วทำการควบคุมจากระยะไกลด้วย Web Server แบบนี้มีปัญหาคือ Controller ที่ใช้ มีราคาแพง และต้องใช้ PC ประสิทธิภาพสูงเป็น Server

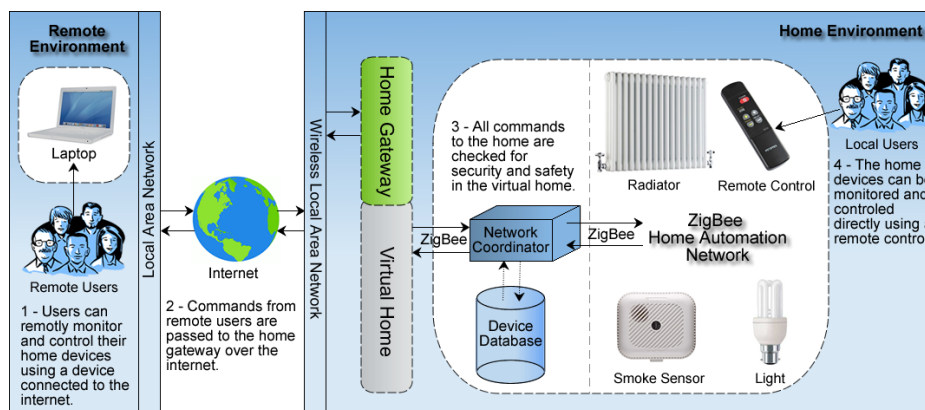
ระบบที่สอง แบบ Bluetooth Based Home Automation เป็นแบบที่ใช้ Bluetooth ในการติดต่อสั่งงานอุปกรณ์ โดยจะกำหนดโครงสร้างการควบคุมออกเป็นสองส่วนคือ Primary Controller ที่เชื่อมต่ออยู่กับฝั่งที่ใช้ควบคุม และ Sub-controller ที่เชื่อมต่ออยู่กับอุปกรณ์ที่จะถูกควบคุม โดยอุปกรณ์เครื่องใช้ไฟฟ้าต่างๆ จะเชื่อมต่อเข้ากับ Sub-controller แบบมีสาย ซึ่ง Sub-controller จะรับคำสั่งการควบคุมแบบไร้สายจาก Primary Controller แบบนี้มีข้อเสียคือ ถ้า

ใช้ Sub-controller หนึ่งตัวต่ออุปกรณ์หนึ่งชิ้น จะทำให้ต้องใช้ Sub-controller หลายตัวเพื่อควบคุมอุปกรณ์หลายชิ้น ทำให้มีราคาแพง หรือถ้าใช้ Sub-controller หนึ่งตัวควบคุมอุปกรณ์หลายชิ้น จะทำให้เกิด Access Delay ได้

ระบบที่สาม แบบใช้โทรศัพท์ในการควบคุมอุปกรณ์ระยะไกล เป็นแบบที่ใช้การโทรศัพท์เข้าไปยังศูนย์ควบคุมอุปกรณ์ปลายทาง แล้วส่งงานด้วยการกดปุ่มบนโทรศัพท์ โดยศูนย์ควบคุมอุปกรณ์ปลายทางจะแปลงรหัสหมายเลขที่ส่งงานเป็นการควบคุมอุปกรณ์ แบบนี้มีข้อเสียคือ ไม่มีส่วนติดต่อกับผู้ใช้ ต้องจำรหัสเลขหมายเพื่อส่งงานอุปกรณ์แต่ละชิ้นให้ได้

ระบบที่สี่ แบบใช้การสั่งงานระบบ Home Automation ด้วยการเคลื่อนที่ของมือ แบบนี้จะใช้การจดจำรูปแบบของการเคลื่อนที่ของมือในรูปแบบต่างๆ ในการควบคุมอุปกรณ์ ซึ่งจะมีปัญหาคือ ความไม่คงที่ของมนุษย์ในการออกท่าทางการเคลื่อนที่ของมือ และความเมื่อยล้าในการควบคุม

จากปัญหาของระบบ Home Automation แบบเดิม งานวิจัยชิ้นนี้จึงนำเสนอแนวคิดระบบ Home Automation แบบใหม่ที่เชื่อมต่อกับ Zigbee เพื่อที่จะสามารถควบคุมและสั่งงานอุปกรณ์หลายๆ ชนิด ได้จากระยะไกลโดยผ่าน Internet และ ระยะใกล้ ด้วย Zigbee Remote Control มีรูปแบบดังนี้



ภาพที่ 2.5 แสดงแนวคิดของ ZigBee-Based Home Automation System

แหล่งที่มา: Gill, Shuang-Hua, Fang and Xin, 2009: 424.

จากภาพ 2.5 การทำงานของ ZigBee-Based Home Automation System ประกอบด้วยสองส่วนใหญ่ๆ คือ ส่วน Remote Environment คือส่วนที่ให้ Remote User ทำการสั่งให้ Home Automation System ทำงาน และ ส่วน Home Environment เป็นส่วนที่รับคำสั่งและทำงานจริง

โดยส่วน Home Environment นี้มีองค์ประกอบที่สำคัญคือ Home Gateway ซึ่งจะทำหน้าที่ Interface กับ ผู้ใช้ในการสั่งงานอุปกรณ์ภายใน Home Environment ทั้งจากทาง ระยะไกล เช่น ผ่าน Internet และระยะใกล้ เช่น ผ่าน Zigbee Remote control นอกจากนี้ Home Gateway ยังทำหน้าที่เชื่อมโยงระบบควบคุมภายในบ้านที่เป็นส่วนของเครือข่าย Zigbee กับระบบที่จะใช้เป็นเส้นทางออกสู่เครือข่ายอินเทอร์เน็ตผ่านระบบ Wi-Fi ให้สามารถรับคำสั่งได้

นอกจาก Home Gateway แล้ว ยังมี Virtual Home ที่ทำหน้าที่ตรวจสอบความถูกต้องของคำสั่ง รวมถึงสิทธิของผู้สั่งอีกด้วย โดยหลังจากที่ตรวจสอบแล้วว่าคำสั่งถูกต้อง และมีสิทธิในการสั่งนี้ คำสั่งก็จะถูกส่งออกไปยัง Zigbee ที่ถูกกำหนดเป็น Coordinator Mode เพื่อส่งไปยัง Zigbee ที่เป็น End Device ซึ่งผูกติดอยู่กับอุปกรณ์ต่อไป ในการ Implement จริงนั้น Virtual Home จะถูก Implement ด้วยภาษา C และถูกรวมอยู่กับส่วนที่เป็น Home Gateway ในลักษณะ Embedded System

งานวิจัยนี้ทำการทดลองตามแนวคิดแล้วสรุปผลการวิจัยว่า การสั่งงานอุปกรณ์ให้ทำงาน เปิด/ปิด สามารถทำงานได้ถูกต้อง 100% สำหรับการประยุกต์แนวคิดของระบบ Home Automation นี้ไปใช้ในการควบคุมภายในโรงงานนั้น ต้องมีการปรับเปลี่ยนเล็กน้อยเพื่อให้เหมาะกับการใช้งานในโรงงาน โดยควรเพิ่มระบบจัดการ Multi User – Multi Device เพื่อให้เหมาะกับการใช้งานภายในโรงงาน ซึ่งมักจะมีผู้ใช้เข้าสั่งงาน PLC จำนวนมากพร้อมๆ กัน จึงต้องมีระบบจัดการ PLC ที่เหมาะสมเพื่อให้ทำงานได้อย่างถูกต้อง

นอกจากนี้การที่ PLC มีคำสั่งที่ใช้ควบคุมซับซ้อนกว่าอุปกรณ์เครื่องใช้ภายในบ้าน ซึ่งมีสถานะการทำงานไม่มากนัก เช่น หลอดไฟ หรือเครื่องปรับอากาศ ซึ่งใช้รูปแบบของคำสั่งไม่ซับซ้อน ทำให้การควบคุม PLC ให้เต็มประสิทธิภาพควรจะใช้โปรแกรมควบคุมที่ถูกกำหนดจากผู้ผลิต ซึ่งมักใช้ช่องทางเชื่อมต่อแบบ Serial เป็นหลัก ดังนั้นจึงต้องพัฒนาส่วนการแปลงข้อมูลที่ได้รับจาก Serial Port ให้สามารถติดต่อสั่งงานผ่านเครือข่ายอินเทอร์เน็ตได้

2.2 ทฤษฎีที่เกี่ยวข้อง

2.2.1 คุณสมบัติของ Zigbee

Zigbee เป็นมาตรฐานของอุปกรณ์ไร้สาย ถูกกำหนดโดยกลุ่ม Zigbee Alliance ซึ่งเริ่มก่อตั้งขึ้นเมื่อปี 2002 เพื่อใช้ควบคุมอุปกรณ์ต่างๆ รอบตัวที่ใช้ในชีวิตประจำวันในแบบไร้สายซึ่งไม่ต้องการความเร็วสูงมากนัก เช่น สวิตช์เปิดปิดแสงสว่าง ระบบควบคุมอุณหภูมิห้อง เป็นต้น รวมไปถึงใช้ในการรับค่าจาก Sensor ต่างๆ โดย Zigbee ถูกออกแบบโดยมุ่งให้มีคุณลักษณะดังนี้

2.2.1.1 เป็นเครือข่ายไร้สายในระยะใกล้

2.2.1.2 ราคาไม่แพง

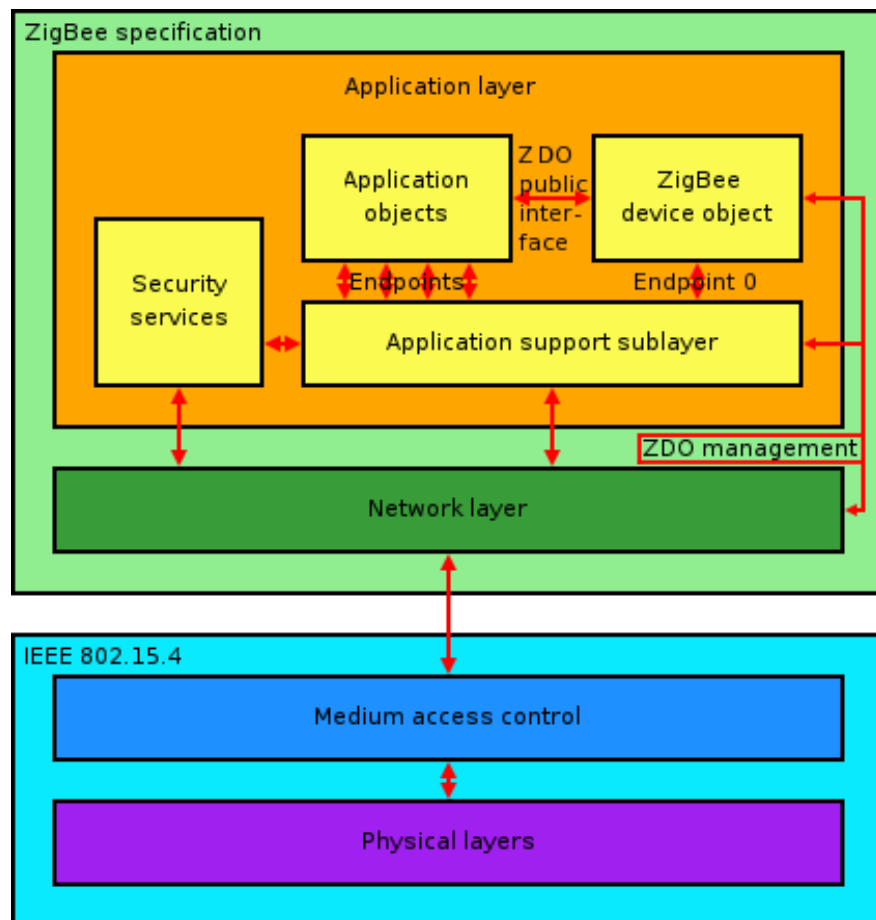
2.2.1.3 ติดตั้งง่าย สามารถประยุกต์ใช้งานได้หลากหลาย

2.2.1.4 สามารถรับส่งข้อมูลได้โดยเชื่อมั่นในความถูกต้องได้

2.2.1.5 ใช้พลังงานในการทำงานต่ำ

2.2.2 Zigbee Protocol Stack

Zigbee Protocol Stack นั้น ถูกออกแบบขึ้นให้ทำงานตาม Zigbee Specification ซึ่งถูกกำหนดจาก Zigbee Alliance โดย Zigbee Specification ฉบับแรก ถูกกำหนดขึ้นเมื่อปี 2004 และได้รับการปรับปรุงเรื่อยมา สำหรับรูปแบบของ Zigbee Protocol Stack นั้น มีรูปแบบดังนี้



ภาพที่ 2.6 แสดงองค์ประกอบของ Zigbee Protocol Stack

แหล่งที่มา: Wikipedia, 2013.

จากภาพ 2.6 แสดงองค์ประกอบของ Zigbee Protocol Stack โดยประกอบด้วย Application Layer และ Zigbee Network Layer ซึ่งสร้างขึ้นตาม Zigbee Specification และ MAC Layer กับ Physical Layer ซึ่งเป็นมาตรฐานเดียวกันกับ IEEE 802.15.4

ความเร็วในการรับส่งข้อมูลของ Zigbee คือประมาณ 250 KB/s ซึ่งเพียงพอสำหรับการส่งสัญญาณควบคุม หรือรับส่งผลลัพธ์จากอุปกรณ์ Sensor ต่างๆ ได้ดี โดยเมื่อเปรียบเทียบ Zigbee กับ ระบบ Cellular และ Wi-Fi 802.11b และ Bluetooth Version 4 ในด้าน พลังงานที่ใช้ จำนวนโหนดที่สามารถมีได้ในเครือข่าย อัตราการรับส่งข้อมูล ระยะทางที่สามารถติดต่อได้ สรุปได้ดังนี้

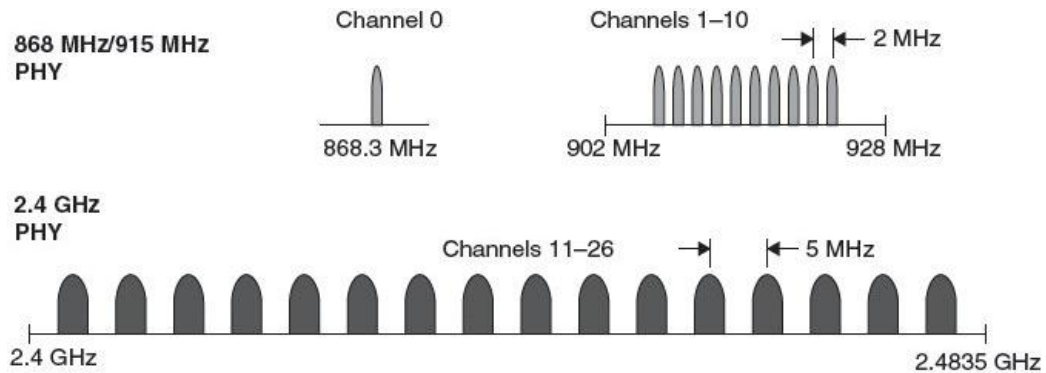
Market Name	ZigBee®	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA/1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2 ⁶⁴)	1	32	7
Maximum Data Rate (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

ภาพ 2.7 แสดงการเปรียบเทียบ Zigbee กับระบบเครือข่ายไร้สายประเภทอื่นๆ

แหล่งที่มา: Zigbee Alliance, 2013.

2.2.3 Zigbee Protocol Stack : Physical Layer

ในระดับ Physical Layer ของ Zigbee นั้น เป็นมาตรฐานเดียวกันกับ IEEE 802.15.4 ซึ่งมีรายละเอียดดังนี้



ภาพที่ 2.8 แสดงรายละเอียดของ Physical Layer ตามมาตรฐาน IEEE 802.15.4

จากภาพ 2.8 แสดงคลื่นความถี่ที่ Zigbee ใช้ นั้น เป็นคลื่นความถี่ในช่วง ISM Band 3 ช่วงคลื่น คือ 868MHz, 915MHz, 2.4GHz ด้วยวิธีการส่งแบบ Direct Spread Spectrum (DSSS) ทำให้มีคุณสมบัติทนทานต่อ Noise เหมาะจะใช้ในพื้นที่ซึ่งมี Noise เช่นภายในโรงงาน สำหรับความถี่แต่ละช่วงจะได้อัตราเร็วในการรับส่งข้อมูล ดังนี้

ความถี่ 868 MHz	Modulation แบบ Binary Phase-shift Keying	อัตรารับส่งข้อมูล 20 kb/s
ความถี่ 915 MHz	Modulation แบบ Binary Phase-shift Keying	อัตรารับส่งข้อมูล 40 kb/s
ความถี่ 2.4 GHz	Modulation แบบ Quadrature Phase-shift Keying	อัตรารับส่งข้อมูล 250 kb/s

2.2.4 Zigbee Protocol Stack : MAC Layer

2.2.4.1 Device Class อุปกรณ์ Zigbee แบ่ง Device Class ไว้เป็น 2 ประเภท ได้แก่

1) Full Function Device (FFD) ซึ่งมีคุณสมบัติ คือ

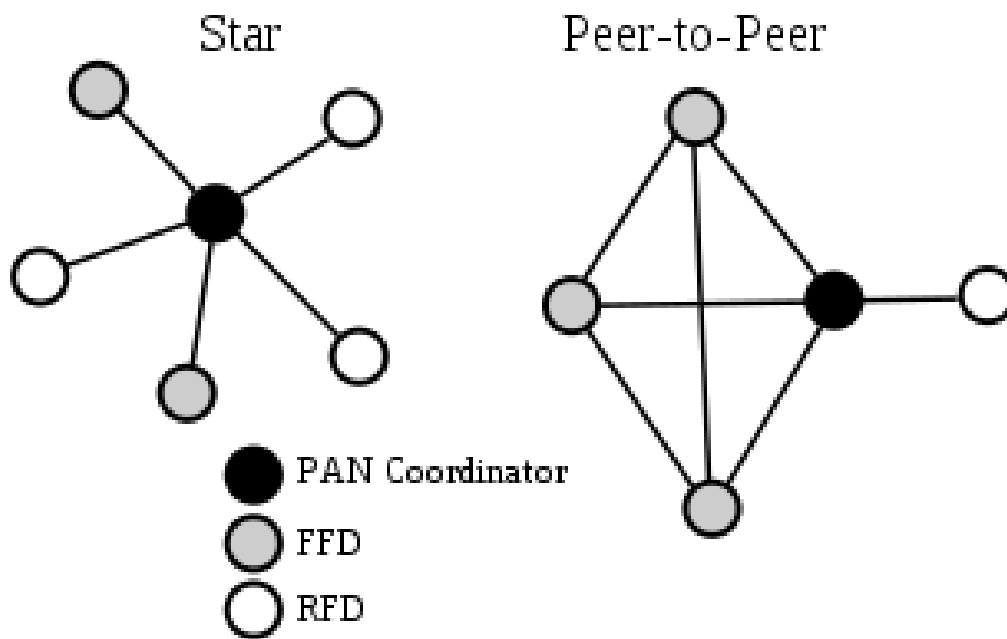
- (1) สามารถทำการ Routing เพื่อหาเส้นทางสำหรับส่งข้อมูลได้
- (2) ใช้งานได้ในทุกรูปแบบ Topology
- (3) ติดต่อกับอุปกรณ์ Zigbee โหนดอื่นได้ทั้งประเภท FFD และ RFD
- (4) สามารถเป็น PAN Coordinator ซึ่งจะเป็นศูนย์กลางของเครือข่ายไร้สาย Zigbee โดยจะทำหน้าที่จัดตั้ง Zigbee Network ขึ้นมา พร้อมทั้งเก็บสารสนเทศของ Zigbee Network นั้น เช่น Key ที่ใช้ในการเข้ารหัสข้อมูลภายใน Zigbee Network นี้เป็นต้น โดยในหนึ่ง Zigbee Network จะมี Coordinator นี้เพียงหนึ่งโหนดเท่านั้น

2) Reduced Function Device (RFD)

- (1) ไม่สามารถหาเส้นทางให้ Zigbee Packet ได้ จึงใช้งานได้เฉพาะ Peer-to-Peer Topology เท่านั้น
- (2) เป็น PAN Coordinator ไม่ได้
- (3) เป็นได้เฉพาะ End Node ใน Zigbee Network

2.2.4.2 Topology ในการทำงานแบบเครือข่ายของ Zigbee

รูปแบบของ Topology ที่เป็นมาตรฐานในการใช้งาน Zigbee Network ตามมาตรฐาน 802.15.4 คือ Star Topology และ Peer-to-Peer Topology แสดงได้ดังภาพ



ภาพที่ 2.9 แสดงภาพ Topology ในการใช้งาน Zigbee Network

แหล่งที่มา: Wikipedia, 2013.

จากการที่ Zigbee รองรับ Topology ที่หลากหลายนี้เองทำให้เหมาะสมในการเลือกใช้ เป็นเครือข่ายระยะใกล้ภายในโรงงาน เนื่องจาก Topology ที่หลากหลาย ทำให้มีความยืดหยุ่นใน การนำไปใช้ในโรงงาน โดยสามารถเลือก Topology ที่เหมาะสมกับรูปแบบการวางผังเครื่องจักรใน สายการผลิตภายในโรงงานได้ดีกว่าระบบไร้สายระยะใกล้แบบอื่นๆ เช่น Bluetooth นอกจากนี้การ ที่ Zigbee เป็นเครือข่ายไร้สายที่สามารถเลือก Topology ได้อย่างยืดหยุ่น ทำให้ไม่ต้องมีค่าใช้จ่าย เพิ่มเติมในการเปลี่ยนแปลงรูปแบบของ Network หรือ Topology เมื่อมีการเปลี่ยนรูปแบบการวาง ผังเครื่องจักรในสายการผลิตตามหลักการจัดการผังโรงงานในอนาคต

2.2.5 Zigbee Security

การรักษาความปลอดภัยของ Zigbee นั้นจะใช้การเข้ารหัสแบบ 128-bit AES เป็นหลัก โดยจะมีศูนย์กลางในการรักษาความปลอดภัยของ Zigbee Network อยู่ที่ Coordinator Node โดยเป็น Trust Center ซึ่งทำหน้าที่จัดการด้านความปลอดภัยในด้านต่างๆ ดังนี้

Trust Manager คือตรวจสอบว่าอุปกรณ์ที่ร้องขอเข้าใน Zigbee Network นั้นมีสิทธิในการเข้าใช้เครือข่ายหรือไม่

Network Manager คือ แจกจ่าย Network Key ให้สมาชิกใน Zigbee Network เพื่อให้ทุก Node มี Key ร่วมกัน ซึ่งทำให้การเข้ารหัสเป็นแบบ Group Encryption คือ ทุก Node ใน Zigbee Network จะเห็นข้อมูลเหมือนกันหมด

Configuration Manager คือการสร้างความปลอดภัยในการส่งข้อมูลในรูปแบบระหว่าง Node ต่อ Node ใน Network โดยการใช้ Link Key

สำหรับ Key ที่ใช้ในระบบ Zigbee นั้น มี 3 ประเภทได้แก่ Master Key Network Key และ Link Key ซึ่งมีวิธีใช้แตกต่างกันออกไป ดังนี้

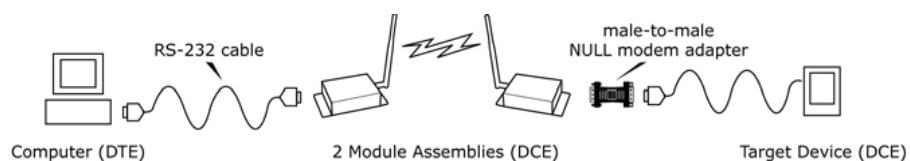
Master Keys เป็น Key ร่วมเพื่อใช้สร้าง Link Keys ที่จะใช้เข้ารหัสระหว่าง Zigbee 2 Nodes

Network Keys เป็น Key ที่ใช้เข้ารหัสข้อมูลในระดับ Network Layer ของ Zigbee Network โดย Zigbee ทุก Node จะใช้ Key เดียวกัน จุดประสงค์ของ Network Keys เพื่อใช้ปกป้องความลับของ Zigbee Network จากภายนอก

Link Keys เป็น key ที่ใช้ในการเข้ารหัสเพื่อส่งข้อมูล โดยจะใช้ในการรักษาความลับของการส่งข้อมูลระหว่าง Node 2 Node ซึ่งอยู่ภายในเครือข่าย Zigbee Network เดียวกัน

2.2.6 การส่งข้อมูลแบบ Serial ด้วย Zigbee Module

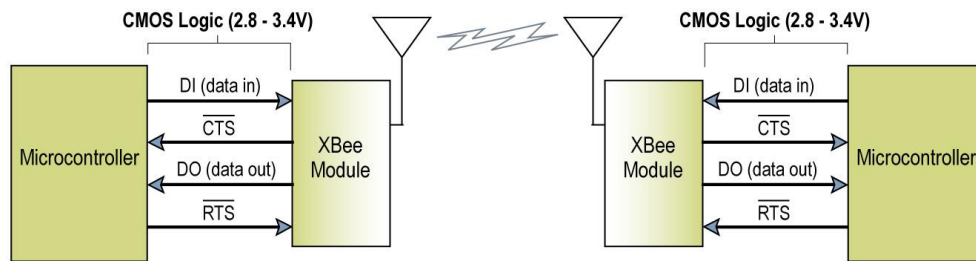
Zigbee Module ที่เลือกใช้นี้สามารถทำหน้าที่เป็น DCE เพื่อให้ DTE ทั้งสองฝั่งสามารถติดต่อกันได้ เสมือนกับว่า DTE ทั้งสองฝั่งติดต่อกันด้วยสาย Serial โดยตรงนั่นเอง ดังภาพ 2.10



ภาพที่ 2.10 แสดงการเชื่อมต่อแบบไร้สายโดยใช้ระบบ Zigbee

แหล่งที่มา: Digi International, 2007.

Zigbee Module ที่เลือกใช้นี้ถูกออกแบบให้สามารถติดต่อกับอุปกรณ์ที่มี UART Interface ได้โดยเชื่อมต่อเข้ากับ PIN ของ Zigbee Module ให้ถูกต้อง ดังรูป

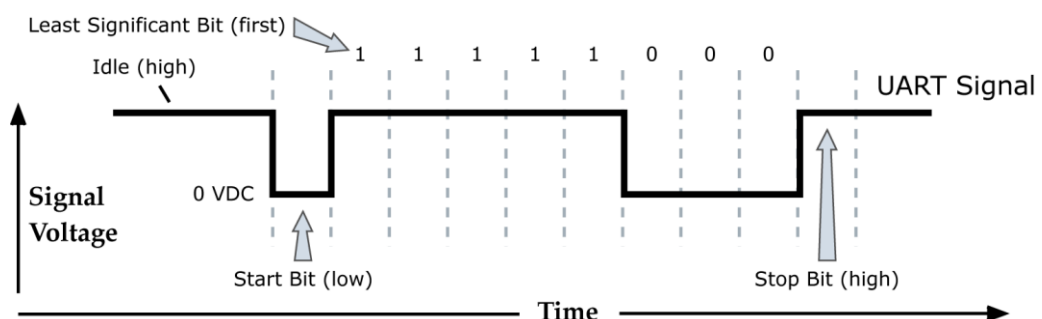


ภาพที่ 2.11 แสดงการเชื่อมต่อ Microcontroller 2 ตัว โดยใช้ Zigbee Module

แหล่งที่มา: Digi International, 2008.

จากภาพ 2.11 แสดงการเชื่อมต่อ Microcontroller 2 ตัวเพื่อส่งข้อมูลถึงกัน โดยใช้ Zigbee Module ในการส่งผ่านข้อมูลไปยังปลายทางแบบไร้สาย ในการเชื่อมต่ออย่างง่ายที่สุดนั้น เพียงเชื่อมต่อ PIN Data In, Data Out, Clear To Send, Request To Send จาก Microcontroller เข้ากับ Zigbee Module ฟังก์ชันเอง ก็พร้อมที่ส่งข้อมูลผ่าน Zigbee Module ได้แล้ว อย่างไรก็ตาม ควรตรวจสอบให้แน่ใจว่า Microcontroller รุ่นที่ใช้ นั้น ส่งสัญญาณ Data ออกมาในระดับเดียวกับที่ Zigbee รับได้ เพื่อป้องกันความเสียหายที่จะเกิดกับ Zigbee Module

UART Signal ใน Zigbee Module นั้นมีระดับสัญญาณเมื่อ Idle เป็น High เมื่อมีข้อมูลเข้ามายัง UART ทาง PIN 3 (DI) ของ Zigbee module ข้อมูลจะอยู่ในรูปแบบสัญญาณ Asynchronous Serial ซึ่งเป็น Packet ดังภาพ



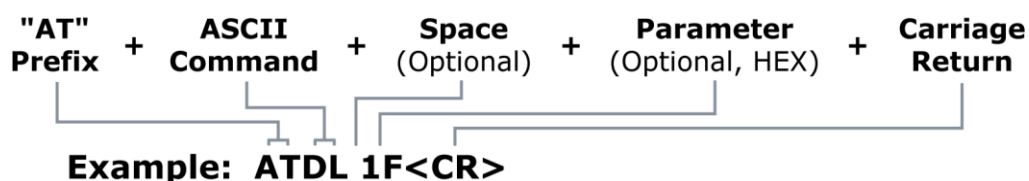
ภาพที่ 2.12 แสดง UART Data Packet ของข้อมูล 0x1F (Decimal Number “31”)

แหล่งที่มา: Digi International, 2008.

จากภาพ 2.12 แสดง UART Data Packet ที่ถูกส่งเข้ามายัง UART Module เริ่มต้นที่สัญญาณ Idle มีค่าเป็น High จากนั้นจะเป็น Start Bit จำนวน 1 Bit ตามด้วยข้อมูล จำนวน 8 Bit ปิดท้ายด้วย Stop Bit จำนวน 1 Bit ซึ่งเป็นรูปแบบที่ได้กำหนดไว้ในการส่งข้อมูลคือ 8-N-1 คือ 8 Bit Data – Non Parity Bit – 1 Stop Bit ข้อมูลที่แสดงในตัวอย่าง เป็นข้อมูลที่ถูกส่งเข้ามาใน UART Module โดยมีค่าในระบบเลขฐานสิบคือ 31 เมื่อเขียนในระบบเลขฐานสอง คือ 0001 1111 ซึ่งตรงตามรูปแบบที่แสดงในตัวอย่างที่ส่งแบบ Least Significant Bit ขึ้นต้นก่อนนั่นเอง

Zigbee Module ที่ใช้ในงานวิจัยนี้ มีโหมดการทำงานสองโหมด คือ Transparent Mode และ API Mode ซึ่งสองโหมดนั้นจะมีรูปแบบการส่งข้อมูลและคำสั่งที่ใช้ติดต่อกับ Zigbee Module ต่างกันออกไป

ใน Transparent Mode นั้น Zigbee Module จะทำหน้าที่เป็น Serial Line Replacement นั่นคือ มีรูปแบบการใช้งานเหมือนกับการเชื่อมต่อด้วยสาย Serial ธรรมดา นั่นเอง โดยใน Transparent Mode นี้เราสามารถสั่งงาน Zigbee Module ด้วย AT Command ผ่านทางโปรแกรม Terminal ต่างๆ ได้ ซึ่ง AT Command มีรูปแบบดังนี้



ภาพที่ 2.13 แสดงรูปแบบของ AT Command

แหล่งที่มา: Digi International, 2008.

จากภาพ 2.13 เป็นตัวอย่างการใช้งาน AT Command ซึ่งเป็นการตั้งค่าของ Address ของ Zigbee Module ปลายทางที่ต้องการติดต่อกับ ในส่วน Low Address เป็น 1F นั่นเอง

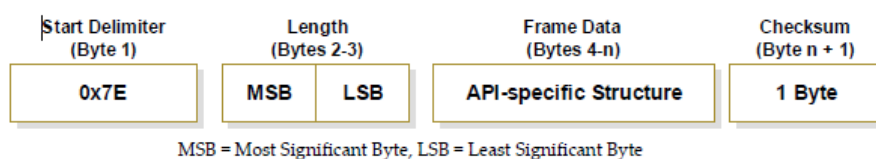
ตัวอย่างของ AT Command อื่นที่สามารถเลือกใช้ได้ เช่น

ATRR X โดย X เป็นมีค่าได้ตั้งแต่ 0 ถึง 6 ซึ่งคำสั่งนี้จะเป็นการกำหนดจำนวนครั้งของ Xbee Retry ที่ต้องการให้ทำการลองส่งใหม่เมื่อเกิดการส่งผิดพลาดขึ้นที่ชั้น MAC Layer โดย Xbee Retry 1 ครั้งนั้น จะสั่งให้ทำการส่งข้อมูลใหม่ในชั้น MAC Layer 3 ครั้ง

ATND เป็นการสั่งให้ทำการค้นหา Zigbee Module ซึ่งอยู่ภายในระยะที่สามารถรับส่งข้อมูลกันได้ โดยจะแสดงรายละเอียดเช่น Address แบบ 16Bits เลข Serial Number ของ Zigbee Module นั้น ระดับของสัญญาณที่ติดต่อกับ Node นั้นได้ เป็นต้น

ATAP X โดย X มีค่าได้ตั้งแต่ 0 ถึง 2 คำสั่งนี้จะเป็นการสั่งให้ Zigbee ทำการเปิด/ปิดการใช้ API Mode

สำหรับ API Mode (Application Programming Interface Mode) ทั้งข้อมูลและคำสั่งจะอยู่ในรูปแบบ Frame-Based ทั้งหมด โดย API Frame จะมีรูปแบบดังนี้



ภาพที่ 2.14 แสดงรูปแบบของ API Frame

แหล่งที่มา: Digi International, 2008.

Byte 1 เป็น Start Delimiter บอกการเริ่มต้น Frame มีค่าเป็น 0x7E เสมอ

Byte 2 ถึง 3 เป็นจำนวน Byte ของส่วน Frame Data

Byte 4 ถึง n เป็นส่วนคำสั่งและพารามิเตอร์ หรือเป็นข้อมูล

Byte n+1 ใช้เป็น checksum

ตัวอย่างของ API Frame

คำสั่ง ATND สำหรับค้นหาโหนดซึ่งอยู่ในรัศมี เมื่ออยู่ในรูปแบบ API Command จะมีรูปแบบ

7E 00 04 08 01 4E 44 64

โดยมีความหมายคือ

7E	เป็น Start Delimiter
00 04	เป็น Length
08	เป็นการระบุว่า เป็น AT Command
01	เป็นการระบุว่า เป็นคำสั่งชนิดที่จะมีผลการทำงานตอบกลับมา
4E 44	เป็นคำสั่ง ND ในรูปแบบ Hexadecimal
64	เป็น Checksum

2.2.7 การ Hash

การ Hash เป็นกระบวนการที่กระทำกับข้อมูล เช่น แบ่งข้อมูลเป็นส่วนย่อยๆ แล้วดำเนินการผสมกลับเข้ากันใหม่ด้วยวิธีการที่กำหนด โดยมีจุดประสงค์ในการทำเช่นนั้นเพื่อให้ได้ผลลัพธ์ซึ่งเป็น Finger Print อันเป็นเอกลักษณ์เฉพาะของข้อมูลชุดนั้นๆ ในวิทยานิพนธ์ฉบับนี้มีการใช้การ Hash ในการรักษาความปลอดภัยในหลายส่วน เช่น ใช้ในการการเข้ารหัสข้อมูล การยืนยันตนเองเพื่อเข้าสู่ระบบ การตรวจสอบความถูกต้องของข้อมูลที่ส่งผ่านอินเทอร์เน็ต ซึ่งจะได้กล่าวรายละเอียดไว้ในบทที่ 3

คุณสมบัติหลักของ Hash Function ที่ดีนั้น มี 3 ประการ ดังนี้

2.2.7.1 One-wayness คือ มีลักษณะที่สามารถกระทำได้ทางเดียวเท่านั้น ไม่สามารถย้อนกระบวนการกลับมาได้ กล่าวคือ สามารถกระทำกับข้อมูลตั้งต้น ให้ได้ผลลัพธ์ออกมาได้ทางเดียว ไม่สามารถนำผลลัพธ์ที่ได้นี้ไปผ่านกระบวนการใดๆ เพื่อได้ข้อมูลตั้งต้นกลับมาได้

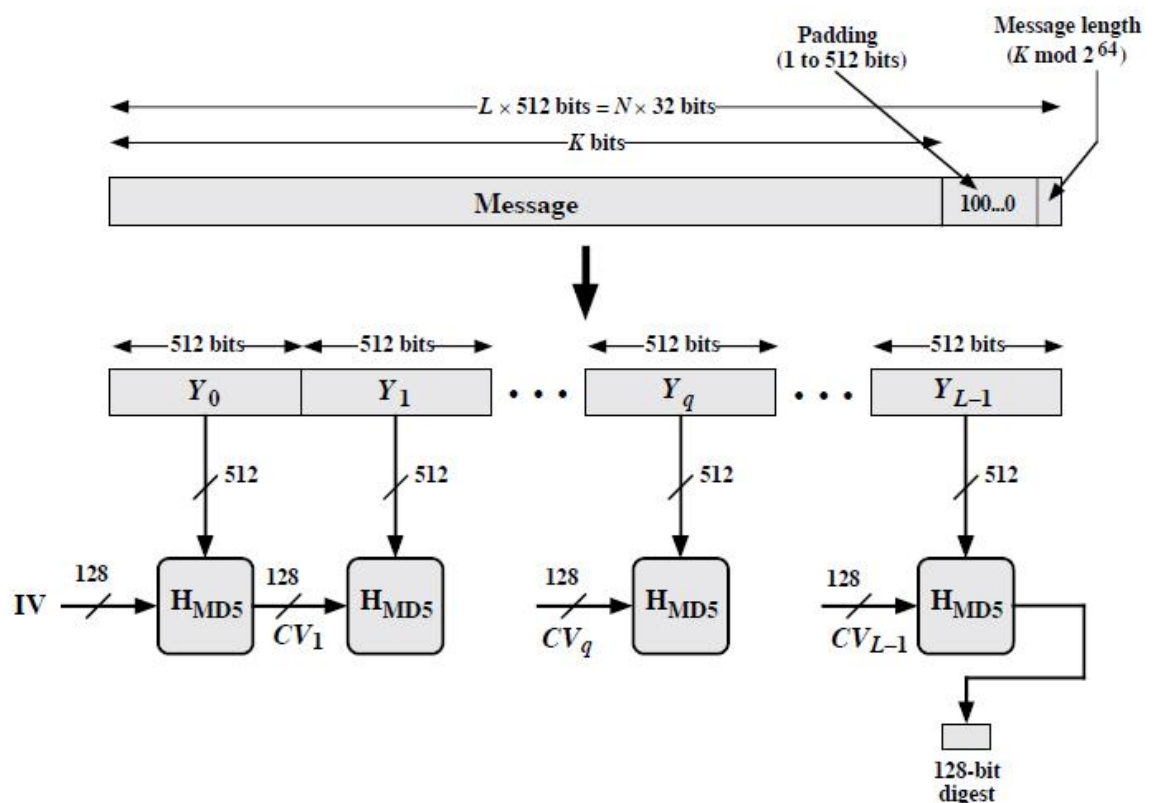
2.2.7.2 Weak Collision Resistance คือ Hash Function ที่ดีนั้น แม้จะรู้ข้อมูลตั้งต้นและผล hash ของข้อมูลชุดแรก ก็ไม่ควรจะสร้างผลการ hash เดียวกันจากข้อมูลชุดอื่นได้

2.2.7.3 Strong Collision Resistance คือ ต้องไม่สร้างผลการ Hash ออกมาซ้ำกัน

กระบวนการ Hash นั้นเป็นกระบวนการหลักในการทำ Message Digest ในรูปแบบต่างๆ ซึ่งมีประโยชน์ในด้านการรักษาความปลอดภัยของการส่งข้อมูลผ่านเครือข่ายต่างๆ ตัวอย่าง Message Digest ที่ใช้ในวิทยานิพนธ์นี้ คือ MD5 ซึ่งมีรายละเอียด ดังนี้

2.2.8 MD5 หรือ Message-Digest Algorithm (RFC 1321)

เป็นกระบวนการทำ Message Digest ซึ่งคิดค้นโดย Ron Rivest จาก MIT (เป็นหนึ่งในผู้ร่วมคิดค้นการเข้ารหัสแบบ RSA ด้วย) โดยการทำงาน จะรับข้อมูลตั้งต้นที่ขนาดเท่าใดก็ได้ แล้วจะทำการประมวลผลจนได้ผลลัพธ์สุดท้ายออกมาเป็น Message ขนาด 128-bit ซึ่งกระบวนการทำ MD5 นั้นแสดงได้ดังภาพ 2.15



ภาพที่ 2.15 แสดง Message Digest generation ชนิด MD5

แหล่งที่มา: Stallings, 2003: 349.

จากภาพแสดงกระบวนการการทำ Message Digest ด้วยวิธี MD5 โดยกระบวนการจะเริ่มที่

ขั้น 1. ใส่ Padding Bit เพิ่มเข้าไป โดยจะเพิ่มบิตต่อท้ายจนกว่าข้อมูลเริ่มต้นจะมีขนาดเป็น จำนวนบิตเป็น $(512 \times X) + 448$ สำหรับ X ที่เป็นศูนย์ขึ้นไป โดยจะต้องมีการเติม Padding Bit ต่อท้ายเสมอ แม้กรณีที่ข้อมูลเริ่มต้นมีขนาดเป็น $(512 \times X) + 448$ แล้วก็ตาม โดยจะเพิ่ม Padding

bit เข้าไปอีก 512 Bit เช่น ข้อมูลเริ่มต้น 448 ดังนั้นต้องเติม Padding Bit เข้าไปอีกจนเป็น 960 Bits นั่นคือจำนวนของ Padding Bits ที่เติมเข้าไปจะมีขนาดระหว่าง 1 ถึง 512 Bits นั่นเอง

ขั้น 2. ขยาย Length ของ Message ที่เป็นผลลัพธ์จากข้อ 1 ให้มีขนาดของ Length เป็น 2^{64} แต่ถ้าขนาด Length ของ Message เดิมเกิน 2^{64} อยู่แล้วก็จะใช้เฉพาะ Low-order 64 Bits เท่านั้น

หลังจากเติม Padding Bits และ Message Length แล้ว ก็จะมีการแบ่งออกเป็น Block โดยให้แต่ละ Block มีขนาด 512 Bits เป็นจำนวน L บล็อกนั่นเอง

ขั้น 3. กำหนด MD Buffer เริ่มต้น โดยใช้ Buffer ขนาด 128 Bits เพื่อเป็นพื้นที่เก็บผลลัพธ์สะสมในระหว่างการทำ Message Digest และเก็บผลลัพธ์เมื่อกระบวนการ Message Digest สิ้นสุด โดย Buffer ขนาด 128 bits นี้จะแบ่งออกเป็น 4 ส่วน ส่วนละ 32 Bits โดยค่าที่เก็บจะอยู่ในรูปแบบ Hexadecimal ดังภาพ 2.16

```
A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
```

ภาพที่ 2.16 แสดง Initialize MD Buffer

แหล่งที่มา: Stallings, 2003: 350.

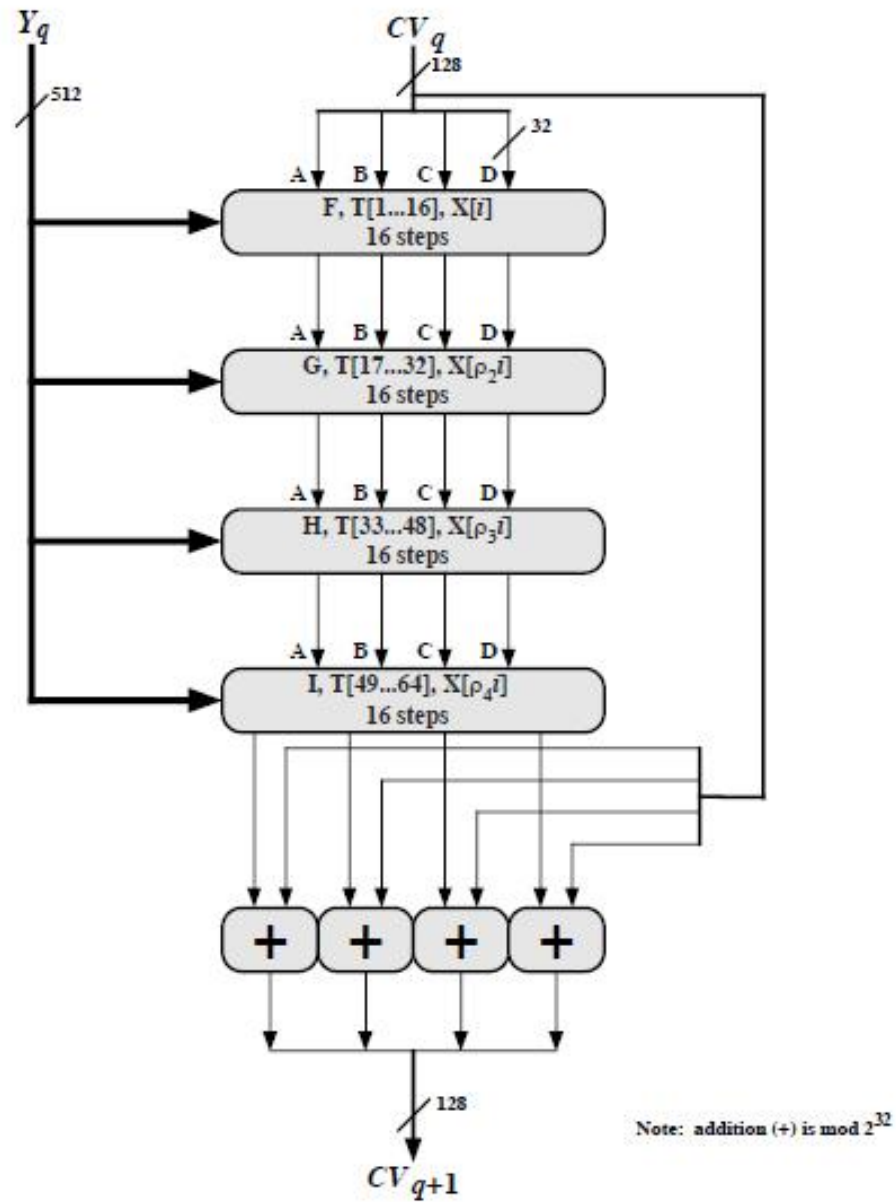
โดยเมื่อจัดเก็บ Initialize MD Buffer นี้ในรูปแบบ Little-endian Format คือ Least Significant Byte ของ Word จะอยู่ใน Low-address Byte Position ดังภาพ 2.17

```
Word A: 01 23 45 67
Word B: 89 AB CD EF
Word C: FE DC BA 98
Word D: 76 54 32 10
```

ภาพที่ 2.17 แสดง Initialize MD Buffer ในรูปแบบ Little-endian Format

แหล่งที่มา: Stallings, 2003: 350.

ขั้นที่ 4. ทำการประมวลผล Message ขั้นตอนนี้จะเป็นการประมวลผลจริง โดยจะเริ่มต้นกระบวนการที่ Message Y_0 ซึ่งแบ่งไว้ขนาด 512 Bits และ Initialize MD Buffer ขนาด 128 Bits โดยมีกระบวนการทำงานดังภาพ



ภาพที่ 2.18 แสดงการประมวลผลแบบ MD5 ของบล็อก q

แหล่งที่มา: Stallings, 2003: 351.

จากภาพ 2.18 เป็นการประมวลผลของส่วน Block Diagram ซึ่ง Label ว่า H_{MD5} ซึ่งแสดงไว้ในภาพที่ 2.15 โดยมี Message ขนาด 1 บล็อก (จากตัวอย่างคือ Y_q) และ MD Buffer (จากตัวอย่างคือ CV_q) เป็น Input โดยนำไปผ่านกระบวนการซึ่งเรียกว่า Compression Function 4 รอบ ดังที่ได้แสดงในภาพที่ 2.19 แล้วก็จะได้ Output ออกมาเป็น CV_{q+1} ซึ่งนำไปเป็น Input ให้กับการประมวลผลในรอบถัดไปได้

สำหรับฟังก์ชันที่ใช้ในการประมวลผล Compression Function ทั้ง 4 รอบนั้น ก็จะใช้ฟังก์ชันที่ดำเนินการแตกต่างกันในแต่ละรอบ โดย ฟังก์ชัน F G H I ที่แสดงในภาพ 2.18 นั้น มีรายละเอียดแต่ละฟังก์ชันดังนี้

ตาราง 2.1 แสดงรายละเอียดของฟังก์ชัน F G H I ที่ใช้ใน Compression Function

Round	Primitive function g	$g(b,c,d)$
1	$F(b,c,d)$	$(b \wedge c) \vee (\bar{b} \wedge d)$
2	$G(b,c,d)$	$(b \wedge d) \vee (c \wedge \bar{b})$
3	$H(b,c,d)$	$b \oplus c \oplus d$
4	$I(b,c,d)$	$c \oplus (b \vee \bar{d})$

นั่นคือในการประมวลผล MD5 Compression Functions แต่ละรอบของการประมวลผลทั้ง 4 รอบของ H_{MD5} ขนาด 512 Bit Block นั้น จะประมวลผล Buffer A B C D แต่ละชั้นในรูปแบบ ดังนี้

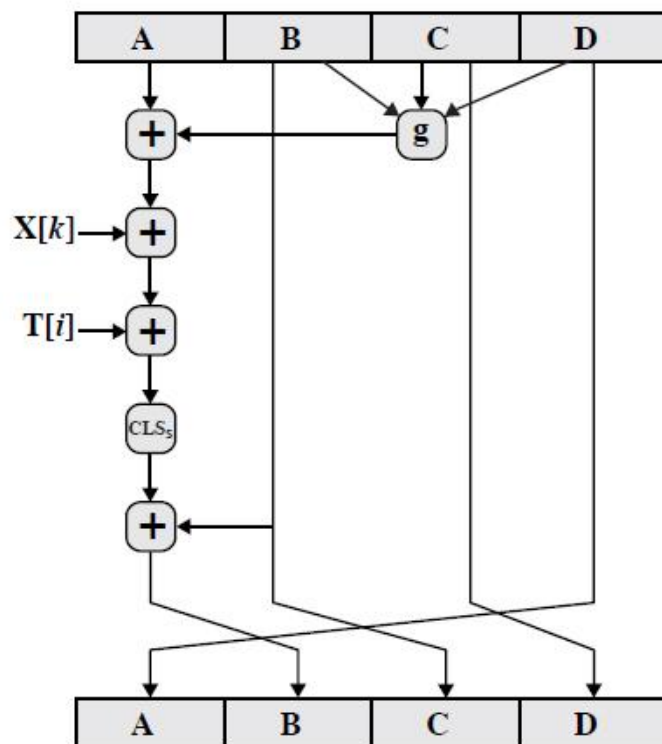
$$a \leftarrow b + ((a + g(b,c,d) + X[k] + T[i]) \lll s)$$

โดย

- a,b,c,d คือ 4 Word Buffer ซึ่งเป็น input
- g คือ ฟังก์ชัน F G H I ในแต่ละรอบ
- $\lll s$ คือ การทำ Rotation ด้วยการ Circular Left Shift ที่ละ s Bits
- $X[k]$ คือ ลำดับที่ k ใน 32 Bit Word เทียบกับลำดับที่ q ใน 512 Bit Block ของข้อมูล คำนวณได้ด้วยสมการ $M[q \times 16 + k]$

$T[i]$ คือ ลำดับที่ i ในแบบ 32 Bit Word ใน Matrix T
 $+$ คือ การบวกแบบ Modulo 2^{32}

โดยสามารถใช้ภาพ 2.19 เพื่อแสดงการทำงานของสมการ โดยแสดงในรูปแบบ Diagram ได้ ดังนี้



ภาพที่ 2.19 แสดงการประมวล Buffer A B C D หนึ่งรอบในรูปแบบ Diagram

แหล่งที่มา: Stallings, 2003: 353.

ขั้น 5. ทำซ้ำจนได้ผลลัพธ์ ทำซ้ำกระบวนการในขั้น 4 ตั้งแต่บล็อก Y_0 จนถึงบล็อก Y_{L-1} ก็จะได้ผลลัพธ์เป็นเลข Hexadecimal ขนาด 128-Bit ซึ่งอยู่ในรูปแบบ MD5 แล้ว

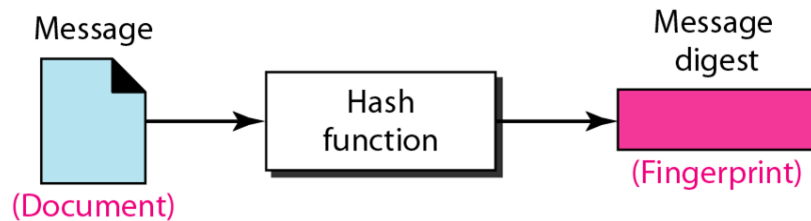
2.2.9 Network Security

กระบวนการที่เกี่ยวข้องในการรักษาความปลอดภัยในการส่งข้อมูลข่าวสารผ่านเครือข่ายสามารถแบ่งออกเป็นด้านต่างๆ ได้ดังนี้

2.2.9.1 ระบบความปลอดภัยสำหรับตัว Message ที่ส่ง มี 4 ด้าน ดังนี้

1) Confidentiality คือ การรักษาความลับของข้อมูลข่าวสารที่ส่ง โดยใช้การเข้ารหัสข้อมูล ซึ่งมีสองแบบคือ การเข้ารหัสแบบ Symmetric-key ซึ่งจะใช้ Key เดียวกันทั้งผู้เข้ารหัสและผู้ถอดรหัสข้อความข่าวสาร และ Asymmetric-key ซึ่งผู้ส่งจะใช้ Public Key ของเครื่องปลายทางในการเข้ารหัส ซึ่งจะถูกลดรหัสได้เฉพาะจาก Private Key ของเครื่องปลายทางเท่านั้น

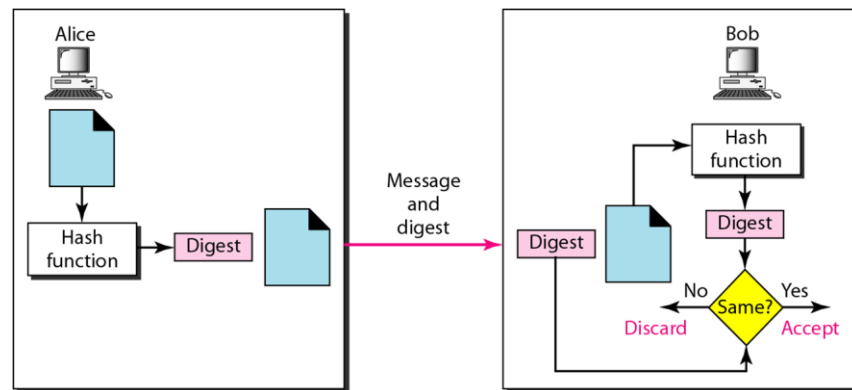
2) Integrity คือ การรักษาเนื้อความของข้อมูลข่าวสารที่ส่งให้เหมือนเดิมจากผู้ส่งไปยังผู้รับ ไม่ถูกแก้ไขเปลี่ยนแปลงระหว่างทาง ซึ่งการจะทำเช่นนี้ได้ ต้องอาศัยหลักการทำ Message Digest ซึ่งใช้หลักการ hash ดังที่ได้กล่าวมา โดยกระบวนการนั้น แสดงได้ดังภาพที่ 2.20



ภาพที่ 2.20 แสดงการทำ message digest ด้วยการ hash

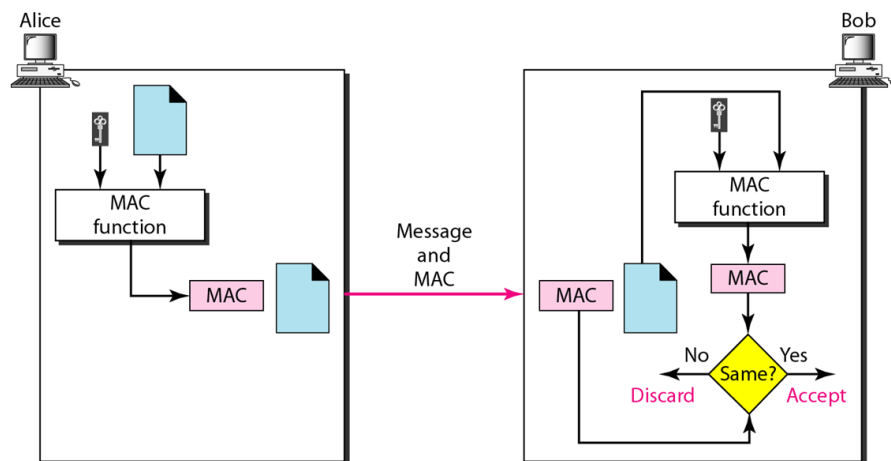
แหล่งที่มา: Forouzan, 2007: 965.

สำหรับการตรวจสอบความถูกต้องของข่าวสารที่ได้รับมาที่ฝั่งผู้รับ ก็จะทำการนำข่าวสารที่ได้รับมานั้น ไปผ่าน Hash Function เช่นเดียวกัน เพื่อนำผลการทำ Message Digest มาเปรียบเทียบกับ Message Digest ที่ได้รับมาพร้อมกับส่วนข้อมูลข่าวสาร ซึ่งถ้า Message Digest ทั้งสองตรงกัน ก็จะแสดงว่า ข้อมูลข่าวสารที่ได้รับมานั้น ถูกต้อง ไม่ได้ถูกแก้ไขระหว่างทาง โดยกระบวนการเปรียบเทียบ แสดงได้ดังภาพที่ 2.21 โดยการส่งตามภาพ 2.21 นั้นข้อมูลที่ถูกลงส่ง ต้องส่งผ่าน Secure Channel แล้วจึงจะเกิด Integrity ขึ้นได้



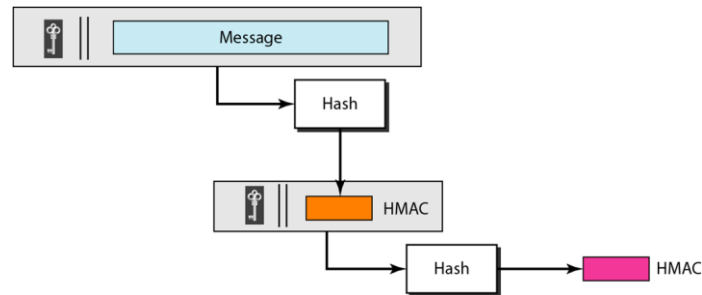
ภาพที่ 2.21 แสดงกระบวนการสร้างและตรวจสอบ Integrity โดยวิธีการ message digest
แหล่งที่มา: Forouzan, 2007: 966.

3) Authentication คือการยืนยันว่าข้อมูลข่าวสารที่ส่งมานั้น ถูกส่งมาจากผู้ส่งที่รู้จักกัน สำหรับวิธีที่จะยืนยันข้อมูลข่าวสารนั้นก็จะใช้หลักการที่เรียกว่า Message Authentication Code หรือ MAC ซึ่งจะนำ Symmetric Key ไป Concatenate กับ ข้อมูลข่าวสาร แล้วจึงไปผ่าน Hash Function ได้ผลลัพธ์ออกมาเป็น MAC ซึ่งสามารถใช้ยืนยันข้อมูลข่าวสารได้ เนื่องจาก Key นั้นจะรู้กันเพียงผู้ส่งและผู้รับเท่านั้น โดยมีกระบวนการวิธีดังภาพ 2.22



ภาพที่ 2.22 แสดงกระบวนการทำ Message Authentication Code
แหล่งที่มา: Forouzan, 2007: 970.

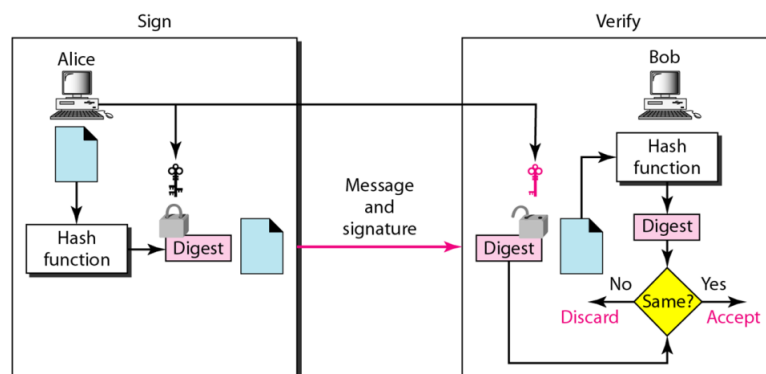
HMAC หรือ Hash MAC เป็นกระบวนการซึ่งประยุกต์หลักการของ MAC ไปใช้ โดยจะทำการสร้าง MAC ขึ้นกันสองชั้น โดยใช้ Symmetric Key เดียวกัน Hash Function เดียวกัน ดังภาพที่ 2.23



ภาพที่ 2.23 แสดงกระบวนการสร้าง HMAC

แหล่งที่มา: Forouzan, 2007: 971.

4) Nonrepudiation คือ คุณสมบัติที่ผู้ส่ง/ผู้รับ จะไม่สามารถปฏิเสธได้ว่า ไม่ได้ส่ง/รับ ข้อความนี้ วิธีหนึ่งในการทำก็คือ Digital Signature หรือ ลายเซ็นอิเล็กทรอนิกส์ ซึ่งก็ใช้คุณสมบัติของ Asymmetric Key เป็นสำคัญ เนื่องจาก Key ที่ใช้ในระบบ Asymmetric Key ซึ่งได้แก่ Private Key และ Public Key นั้นมีคุณสมบัติเฉพาะ คือ Private Key นั้นมีเฉพาะผู้ส่งเท่านั้น ผู้รับจะมีเฉพาะ Public Key และเมื่อเข้ารหัสด้วย Private Key แล้ว จะถอดรหัสได้ด้วย Public Key เท่านั้น แต่ถ้าเข้ารหัสด้วย Public Key แล้ว ก็จะสามารถถอดรหัสได้ด้วย Private Key เท่านั้น ดังนั้นจึงใช้หลักการของ Asymmetric Key ในการทำลายเซ็นดิจิทัล ดังภาพที่ 2.24



ภาพที่ 2.24 แสดงยืนยันตัวตนด้วย Digital Signature

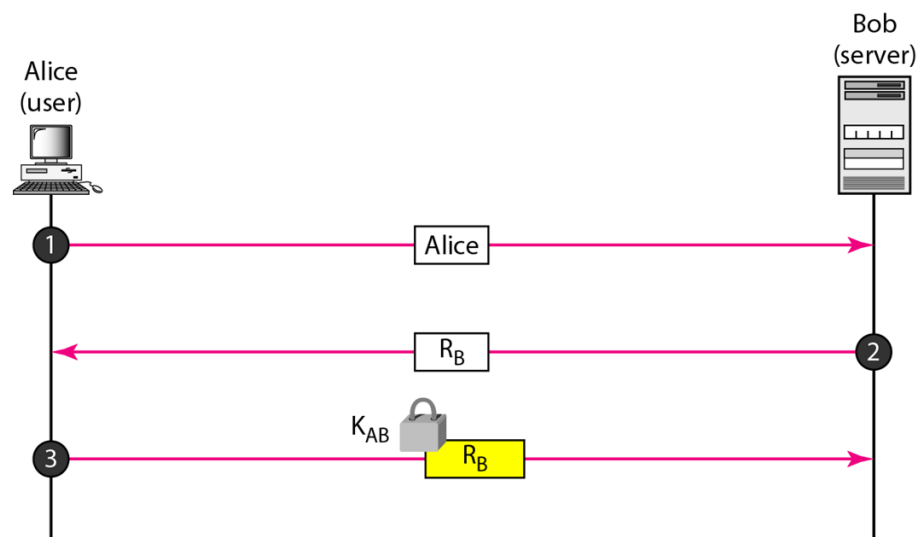
แหล่งที่มา: Forouzan, 2007: 974.

กระบวนการทำ Digital Signature เริ่มต้นโดย ผู้ส่งจะทำ Message Digest ด้วยการนำ ข้อมูลข่าวสารที่จะส่ง ไปผ่าน Hash Function จากนั้น จะนำ Message Digest ที่ได้นี้ ไปเข้ารหัส ด้วย Private Key ของผู้ส่ง ได้ผลลัพธ์เป็น Digital Signature นั้นเอง แล้วจึงส่ง Digital Signature พร้อมข่าวสารข้อมูลออกไป ที่ฝั่งผู้รับ ก็จะตรวจสอบ Digital Signature ด้วยการนำ Message Digest กับข่าวสารข้อมูลที่ได้รับมา แล้วนำไปเทียบกับ Message Digest ที่ได้จากการนำ Digital Signature ไปถอดรหัสด้วย Public Key ที่ตนเองมี ผลลัพธ์คือ ถ้า Message Digest ทั้งสอง เหมือนกัน แสดงว่าผู้ส่งนั้นคือผู้ที่มี Private Key เพียงผู้เดียวนั่นเอง

2.2.9.2 ระบบความปลอดภัยสำหรับ Entity Authentication เป็นการตรวจสอบผู้ ที่จะเข้าใช้ระบบว่ามีสิทธิในการเข้าใช้หรือไม่ โดยวิธีที่นิยมใช้ก็คือ

1) Password เป็นการเข้ารหัสผ่านลับในการตรวจสอบสิทธิการเข้าใช้ ระบบ ข้อดีคือใช้งานง่าย ข้อเสียคือ อาจถูกขโมย หรือ ถูกเดาได้โดยง่ายในบางกรณี

2) Challenge-Response เป็นกระบวนการที่จะตอบโต้กันระหว่างผู้เข้า ใช้และผู้ตรวจสอบสิทธิ โดยสามารถเลือกใช้ได้ทั้งแบบ Symmetric Key และ Asymmetric Key ดังภาพ

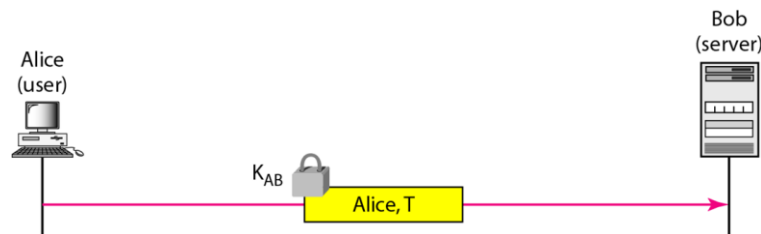


ภาพที่ 2.25 แสดงการ Challenge-Response แบบ Symmetric key

แหล่งที่มา: Forouzan, 2007: 979.

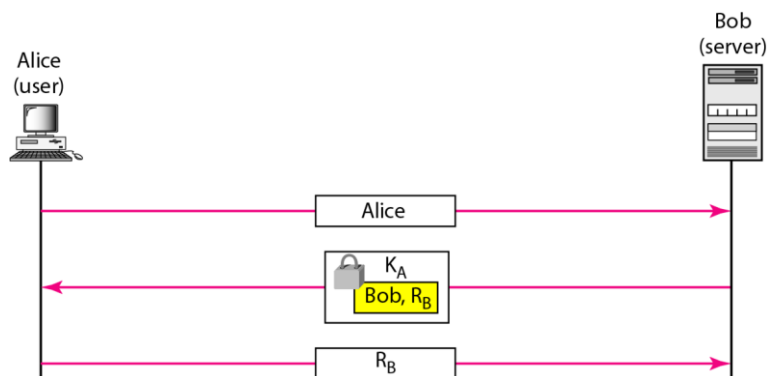
จากภาพ 2.24 แสดงการ Challenge-Response เริ่มต้นด้วยผู้เข้าใช้ระบบส่งคำร้องขอไปยังผู้ตรวจสอบสิทธิ์ จากนั้นผู้ตรวจสอบสิทธิ์ก็จะสุ่มเลขขึ้นมาชุดหนึ่งแล้วส่งไปให้ผู้ร้องขอ ซึ่งผู้ร้องขอก็ต้องแสดงสิทธิ์ตัวเองด้วยการเข้ารหัสเลขสุ่มนั้นแล้วส่งกลับไปยังผู้ตรวจสอบสิทธิ์ ซึ่งถ้าผู้ร้องขอรู้ Key ที่ถูกต้อง ผู้ตรวจสอบสิทธิ์ก็จะสามารถถอดรหัสเลขสุ่มนั้นกลับมาได้อย่างถูกต้องเช่นเดียวกัน

อย่างไรก็ตาม การ Challenge Response แบบนี้ยังมีจุดอ่อนที่เปิดโอกาสให้เกิด Replay Attack ได้โดยการสำเนาชุดเลขสุ่มที่เข้ารหัสอย่างถูกต้องไว้แล้ว แล้วนำไปใช้ในภายหลังได้ ดังนั้นจึงมีการพัฒนาเล็กน้อยเพื่อแก้ปัญหาในจุดนี้ โดยการเพิ่ม Time Stamp เข้าไปในชุดเลขสุ่มที่เข้ารหัสกลับไป ดังภาพที่ 2.26



ภาพที่ 2.26 แสดงการ Challenge-Response แบบ Symmetric Key โดยเพิ่ม Time Stamp
แหล่งที่มา: Forouzan, 2007: 979.

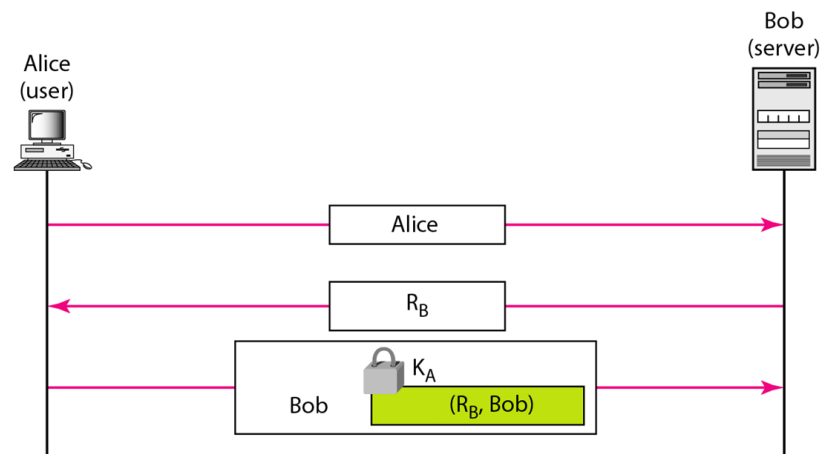
นอกจากการใช้ Symmetric Key แล้ว ก็ยังมีการ Challenge Response โดยใช้หลักการของ Asymmetric Key ซึ่งแสดงได้ดังภาพ 2.27



ภาพที่ 2.27 แสดงการ Challenge-Response แบบ Asymmetric Key
แหล่งที่มา: Forouzan, 2007: 980.

กระบวนการเริ่มต้นเมื่อมีผู้ร้องขอเข้าระบบ ผู้ตรวจสอบสิทธิ์ก็จะสุ่มเลขขึ้นมาแล้วเข้ารหัสด้วย Public Key ของผู้ร้องขอ จากนั้นก็จะส่งออกไปให้ผู้ร้องขอ ถ้าผู้ร้องขอสามารถถอดรหัสเลขสุ่มนั้นกลับมาได้อย่างถูกต้อง ก็แสดงว่าผู้ร้องขอนั้นมี Private Key ที่ถูกต้อง เป็นผู้ร้องขอเข้าระบบตัวจริง

นอกจากนี้ยังมีการ Challenge Response ซึ่งใช้หลักการของ Asymmetric Key อีกแบบหนึ่ง คือ ใช้หลักการของการสร้างและตรวจสอบ Digital Signature นั่นเอง ดังภาพ 2.28



ภาพที่ 2.28 แสดงการ Challenge-Response แบบ symmetric Key โดย Digital Signature
แหล่งที่มา: Forouzan, 2007: 981.

กระบวนการเริ่มต้นเมื่อมีผู้ร้องขอเข้าระบบ ผู้ตรวจสอบสิทธิ์ก็จะสุ่มเลขขึ้นมาแล้วส่งไปให้ผู้ร้องขอ ซึ่งผู้ร้องขอก็ต้องทำการ Sign เลขสุ่มนั้นด้วย Digital Signature แล้วส่งกลับมายังผู้ตรวจสอบสิทธิ์ ซึ่งผู้ตรวจสอบสิทธิ์ ก็จะทำการตรวจสอบว่าเป็น Digital Signature จากผู้ร้องขอจริงหรือไม่ ถ้าถูกต้องก็จะอนุญาตให้เข้าใช้งานระบบได้

2.2.10 Android OS

ความสามารถของโทรศัพท์เคลื่อนที่นั้นมีการพัฒนาอย่างต่อเนื่อง เช่นในโทรศัพท์ในยุคปัจจุบันนั้น ได้พัฒนาความสามารถจนสามารถใช้งานได้หลากหลายมากกว่าเดิมที่ใช้แค่ติดต่อกันด้วยเสียงพูด โดยในปัจจุบันโทรศัพท์เคลื่อนที่นั้นถูกเรียกว่า Smart Phone หรือ โทรศัพท์อัจฉริยะ ซึ่งนอกจากจะสามารถใช้ติดต่อสื่อสารในรูปแบบเสียงพูดแบบเดิมแล้ว ยังสามารถเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ต เพื่อพูดคุยแบบเห็นหน้าตาได้ทันที สามารถใช้ Web Browser เพื่อติดตามข่าวสาร เช็คเมลล์ รวมไปถึงแบ่งปันสิ่งที่ได้พบในชีวิตประจำวันผ่านสังคมแบบออนไลน์ได้อย่างสะดวกผ่านเครือข่ายแบบไร้สาย เปรียบเสมือนกับเป็นคอมพิวเตอร์พกพาเครื่องหนึ่งได้เลยทีเดียว ดังนั้นจึงไม่น่าแปลกใจว่า Smart Phone จึงเป็นทิศทางที่ผู้ผลิตโทรศัพท์เคลื่อนที่จะมุ่งเน้นพัฒนาออกมาแข่งขันกันเป็นจำนวนมาก

ระบบปฏิบัติการบน Smart Phone ก็เป็นส่วนหนึ่งที่มีความสำคัญต่อตัว Smart Phone ในแง่ของประสิทธิภาพ ความสวยงาม ความสะดวกในการใช้งาน และความปลอดภัย รวมไปถึงจำนวน application ที่จะมีสนับสนุนการใช้งาน โดย OS ของ Smart Phone ที่ได้รับความนิยมในปัจจุบันนั้นได้แก่ IOS จาก Apple Computer Android OS จาก Google Inc. และ Windows Phone จาก Microsoft

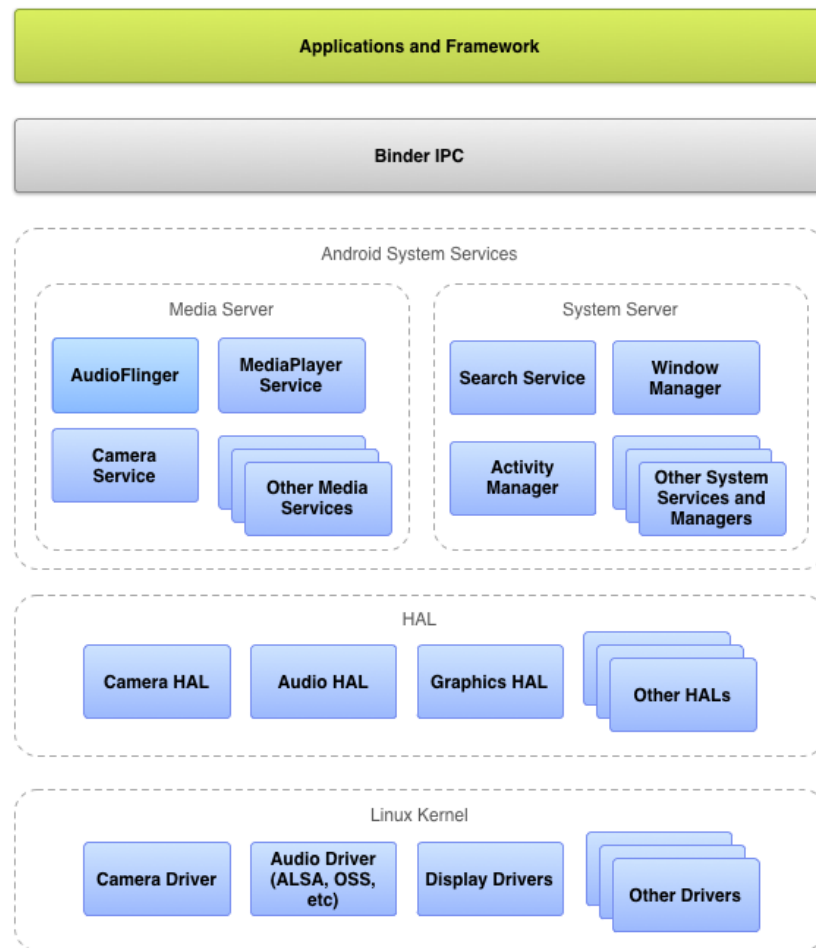
Android OS เป็นระบบปฏิบัติการจาก Google ถูกออกแบบมาให้เป็นระบบปฏิบัติการสำหรับโทรศัพท์สมาร์ทโฟนและแท็บเล็ต โดยแจกจ่ายในรูปแบบซอฟต์แวร์ Open-source Stack โดยมี Google เป็นผู้นำในการให้การสนับสนุนกลุ่มผู้พัฒนา ทำให้เหล่าบรรดาผู้ผลิตนำไปใช้กันอย่างกว้างขวาง เนื่องจากการทำงานที่ยืดหยุ่น มีผู้ผลิตโปรแกรมให้ Android จำนวนมาก และที่สำคัญคือ ไม่มีค่าใช้จ่ายในการเลือกใช้ Android OS

สำหรับ Android OS รุ่นต่างๆ ที่ Google ได้เคยปล่อยออกมาให้ผู้ใช้งานได้ใช้งานนั้น มีรายละเอียดแสดงเลขที่รุ่น โค้ดเนมที่ใช้เรียกแต่ละรุ่น และวันที่แต่ละรุ่นประกาศเผยแพร่ดังตาราง

ตารางที่ 2.2 แสดงรายละเอียดของ Android OS ที่เผยแพร่จนปัจจุบัน

Version	Code name	Release date
4.2.x	Jelly Bean	November 13, 2012
4.1.x	Jelly Bean	July 9, 2012
4.0.x	Ice Cream Sandwich	December 16, 2011
3.2	Honeycomb	July 15, 2011
3.1	Honeycomb	May 10, 2011
2.3.3–2.3.7	Gingerbread	February 9, 2011
2.3–2.3.2	Gingerbread	December 6, 2010
2.2	Froyo	May 20, 2010
2.0–2.1	Eclair	October 26, 2009
1.6	Donut	September 15, 2009
1.5	Cupcake	April 30, 2009

ในด้านการทำงานของ Android OS นั้น แสดงได้ด้วย System Architecture แบบ Low-Level ของ Android OS ดังภาพที่ 2.29



ภาพที่ 2.29 แสดง Android Low-Level System Architecture

แหล่งที่มา: Android Open Source Project, 2013.

จากภาพ 2.29 แสดงให้เห็น System Architecture ของ Android OS ในแบบ Low-Level ซึ่งจะพบว่า Android OS นั้นถูกออกแบบมาให้ผู้ใช้และผู้พัฒนาโปรแกรมสามารถใช้งานและพัฒนาโปรแกรมได้อย่างสะดวก ผ่านบริการต่างๆ ที่ออกแบบไว้เป็นลำดับชั้น โดยมีรายละเอียดในแต่ละ Layer ดังนี้

Applications and Framework นั้นเป็น Layer ที่ใช้พัฒนาโปรแกรมผ่านคอมไพเลอร์ต่างๆ บน API ซึ่ง Google ได้เตรียมไว้ให้แล้ว ทำให้การพัฒนาโปรแกรมบน Android OS นั้นสะดวกยิ่งขึ้น

Binder IPC เป็นส่วนเชื่อมระหว่าง Application Framework กับระบบการทำงานในส่วน Low Level โดยผ่านทาง Call Service Code ของ Android System ได้จาก Framework ของ API

Android System Services เป็นส่วนที่ให้บริการ System Service ในแต่ละด้าน เช่น Service เกี่ยวกับกล้องถ่ายรูป Service เกี่ยวกับการจัดการหน้าต่างการทำงานที่มีในปัจจุบัน เป็นต้น เพื่ออำนวยความสะดวกในการเรียกใช้จาก framework API

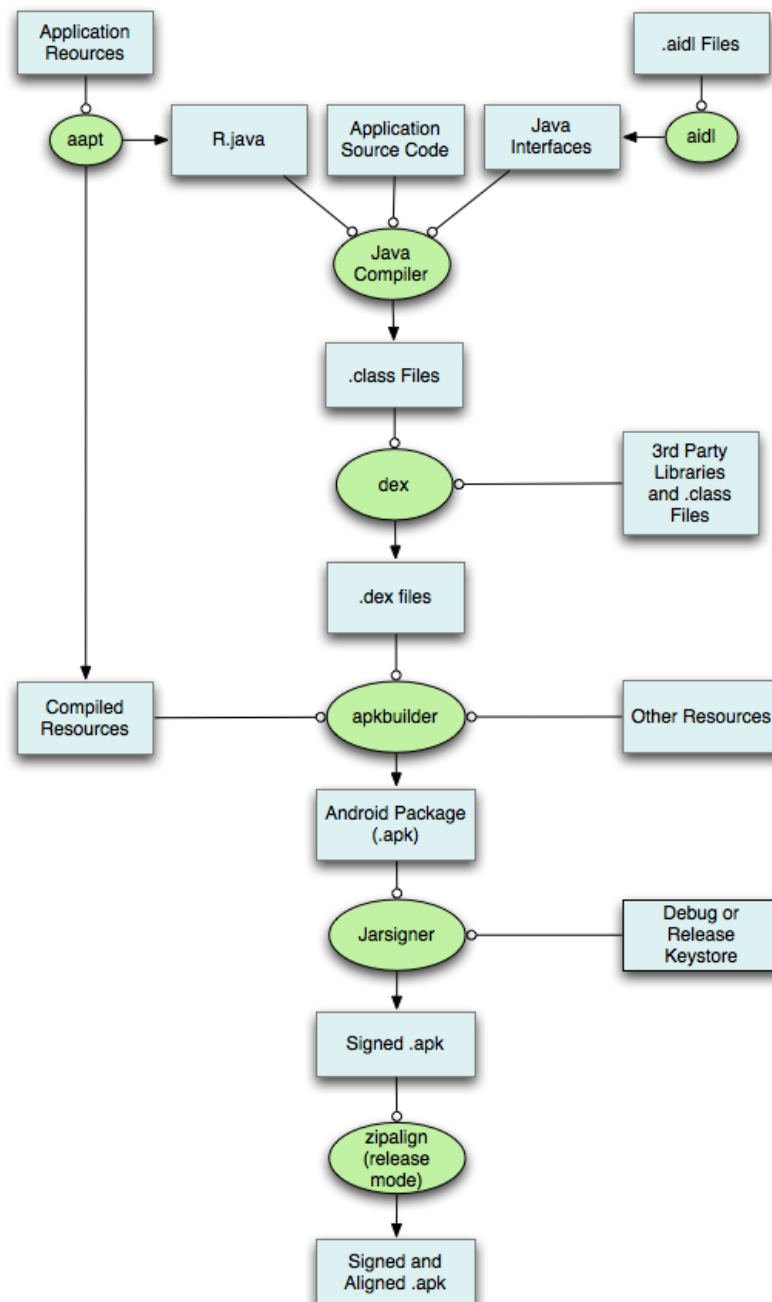
HAL ทำหน้าที่เป็น Standard Interface เพื่อให้การติดต่อ Device จริงๆ ผ่านทาง Driver นั้นมีมาตรฐานที่เป็นอันหนึ่งอันเดียว โดยทั้ง Device Driver และ HAL นี้จะต้องถูกพัฒนาขึ้นมาเฉพาะให้เหมาะกับอุปกรณ์เฉพาะรุ่นที่ต้องการใช้งาน

Linux Kernel เป็นส่วนที่เป็นหัวใจของระบบ ซึ่งจะควบคุมให้ระบบต่างๆ นั้นทำงานจริง เช่น ระบบการจัดการ Thread การทำ CPU Scheduling การทำ Process Synchronization รวมถึงการจัดการ Main Memory และ Storage การจัดการ File-system การจัดการอุปกรณ์ I/O ผ่านทาง Device Driver ที่สร้างขึ้น ซึ่ง Linux Kernel นี้ก็จะให้บริการ HAL โดยจะรอรับคำสั่งที่ HAL จะสั่งมาโดยการเรียกใช้ Device Driver แล้ว Linux Kernel ก็จะไปสั่งให้ hardware ปฏิบัติงานจริง

2.2.11 ความแตกต่างของ Java API และ Android API

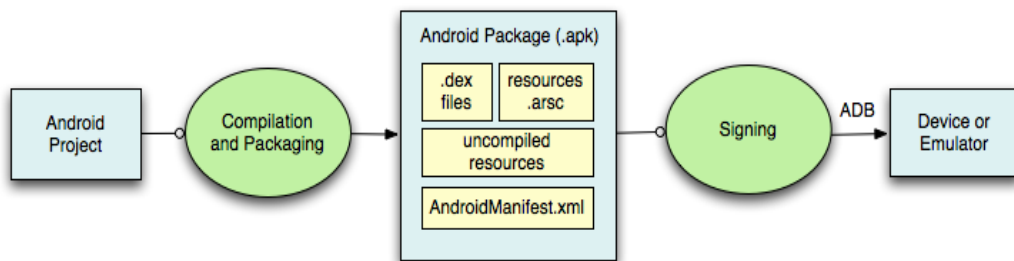
แม้ว่าโปรแกรมบน Android OS นั้นจะใช้ภาษา Java ในการพัฒนา แต่ก็มี ความแตกต่างกันระหว่าง Java API ที่ทำงานบนเครื่องคอมพิวเตอร์ และ Android API อยู่บ้าง นั่นก็มาสาเหตุมาจากการที่รูปแบบการทำงานของ Java Virtual Machine ที่ใช้สำหรับทำงานตามคำสั่งใน Java Bytecode บนเครื่องคอมพิวเตอร์นั้น มีสถาปัตยกรรมเป็นแบบ Stack-Based ซึ่งจะทำงานตาม Instruction เพื่อโหลดข้อมูลลงไป Stack แล้วจึงประมวลผล ซึ่งมีข้อดีคือ Instruction จะไม่ซับซ้อน แต่มีข้อเสียคือ ต้องใช้หลายๆ Instruction ในการทำงานใดงานหนึ่ง ซึ่งทำให้ต้องใช้หน่วยความจำมากตามไปด้วย ด้วยเหตุผลนี้เองทำให้ Java Virtual Machine ไม่เหมาะกับการทำงานบนอุปกรณ์ประเภทพกพาซึ่งมักมี หน่วยประมวลผลที่ความเร็วไม่สูงมาก หน่วยความจำที่จำกัด ไม่มีพื้นที่สำหรับสลับโปรแกรมออกจากหน่วยความจำหลัก และต้องใช้แบตเตอรี่เป็นแหล่งพลังงานหลัก ดังนั้น Android OS จึงได้พัฒนา Virtual Machine ซึ่งเหมาะกับการทำงานของอุปกรณ์พกพาขึ้นมา นั่นก็คือ Dalvik Virtual Machine ซึ่ง Dalvik VM นี้มีสถาปัตยกรรมเป็นแบบ Register-Based ซึ่งเน้นการใช้ Register ในการทำงาน โดยพยายามให้ Instruction ใช้ Register ในการเก็บข้อมูลเพื่อประมวลผลแทนการใช้ Stack ซึ่งต้องใช้พื้นที่บนหน่วยความจำหลัก ซึ่งการใช้ Register นั้นมีข้อดีคือ Register นั้นมีความเร็วในการทำงานมากกว่าหน่วยความจำหลัก ทำให้เพิ่มประสิทธิภาพในการประมวลผลได้ดี และมีจำนวนของ Instruction ที่ต้องประมวลผลน้อยกว่าแบบ Stack-Based ในเมื่อเทียบกับการทำงานเดียวกันจากโค้ดโปรแกรมชั้น High Level Language สำหรับข้อจำกัดของ Register-Based ก็คือ Instruction จะมีความซับซ้อนและมีความยาวมากกว่า Instruction ในแบบ Stack-Based เนื่องจากต้องระบุ Source และ Destination Register ลงใน Instruction ด้วย

อย่างไรก็ตาม ข้อดีและข้อเสียของสถาปัตยกรรมแบบ Stack-Based และ Register-Based นั้นยังเป็นหัวข้อที่ยังมีหยาบยกมาพูดคุยเพื่อเปรียบเทียบประสิทธิภาพอยู่เสมอๆ โดยยังไม่มีข้อสรุปที่แน่นอนว่าสถาปัตยกรรมแบบใดนั้นมีข้อดีกว่า



ภาพที่ 2.30 แสดงขั้นตอนการคอมไพล์โค้ดโปรแกรมสำหรับ Android
แหล่งที่มา: Android Developers, 2013.

โปรแกรมที่เราพัฒนาขึ้นด้วยภาษา Java บน Eclipse IDE นั้นจะแทนด้วย “Application Source Code” ซึ่งแสดงในภาพ 2.30 โดย Application Source Code นั้นจะอยู่ในรูปของไฟล์นามสกุล .java จากนั้นจะถูก Java Compiler แปลงเป็น .class ซึ่งสามารถทำงานได้บน Java VM ได้ แต่บนระบบปฏิบัติการ Android นั้นใช้ Dalvik VM จึงต้องมีการแปลงจาก .class ให้เป็น .dex เพื่อให้ทำงานกับ Dalvik VM ได้ เมื่อได้แอปพลิเคชันที่ถูกแปลงในรูปแบบ .dex แล้ว ก็จะนำไปรวมกับ Resource ส่วนอื่นๆ ของแอปพลิเคชัน เช่น ภาพ เป็นต้น เพื่อรวมเป็นไฟล์ติดตั้งนามสกุล .apk เพื่อใช้ติดตั้งบนระบบ Android ต่อไป โดยส่วนประกอบของไฟล์ .apk นั้นแสดงไว้ดังภาพ 2.31



ภาพที่ 2.31 แสดงส่วนประกอบของไฟล์ Android Package

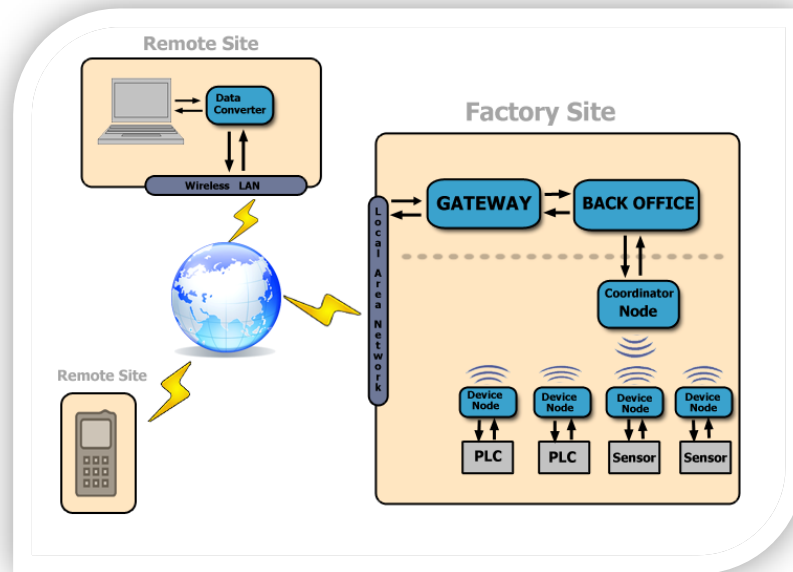
แหล่งที่มา: Android Developers, 2013.

บทที่ 3

ระบบไร้สายโดยใช้ ZigBee เพื่อควบคุมและติดตามสถานะเครื่องจักร และเซ็นเซอร์ในโรงงานผ่านเครือข่ายอินเทอร์เน็ต

3.1 แนวคิดในการออกแบบระบบ

จากการทำงานระบบเดิมที่การควบคุม PLC ต้องกระทำโดยการใส่โปรแกรมเฉพาะในการควบคุมสั่งงาน PLC โดยตรง โดยโปรแกรมเฉพาะนี้จะทำงานอยู่บนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับ PLC โดยตรงผ่านสาย Serial Port เมื่อเราต้องการระบบที่สามารถควบคุม PLC ผ่านทางเครือข่ายอินเทอร์เน็ตได้ จึงต้องมีการออกแบบระบบที่สามารถแปลงข้อมูลในรูปแบบของ Serial Data เป็น TCP/IP Packet ได้ และในทางกลับกัน ก็ต้องสามารถแปลงข้อมูลจาก TCP/IP Packet ที่ได้รับ ให้อยู่ในรูปแบบ Serial Data ได้เช่นกัน นอกจากนี้ รูปแบบของการทำงานในโรงงานมักมีเครื่องจักรจำนวนมาก รวมถึงผู้ปฏิบัติงานจำนวนมากด้วย ดังนั้น จึงควรคำนึงถึงระบบจัดการผู้ใช้แบบหลายคนและระบบจัดการอุปกรณ์แบบหลายหน่วยเพื่อให้สามารถบริการผู้ใช้หลายๆ คน พร้อมกันด้วยอุปกรณ์ที่มีได้อย่างถูกต้อง และมีประสิทธิภาพ นอกจากนี้ระบบที่พัฒนาขึ้นสามารถเข้าถึงได้ทุกที่ภายในเครือข่ายอินเทอร์เน็ต ดังนั้นระบบการรักษาความปลอดภัยของข้อมูลจึงมีความสำคัญเป็นอย่างยิ่งอีกด้วย จากความต้องการของระบบใหม่นี้ ทำให้สามารถออกแบบระบบซึ่งมีรายละเอียดดังนี้



ภาพที่ 3.1 แสดงแนวคิดของระบบ

จากภาพ 3.1 แสดงแนวคิดการทำงานของระบบนี้ ซึ่งแบ่งส่วนการทำงานของระบบเป็น Remote Site และ Factory Site โดย Remote Site จะทำหน้าที่ติดต่อกับผู้ใช้ รวมถึงแปลงคำสั่งจากโปรแกรมควบคุม PLC ซึ่งจะส่งข้อมูลในรูปแบบ serial ให้เปลี่ยนเป็นแพ็คเกจ TCP/IP ผ่านอินเทอร์เน็ตได้ ส่วน Factory Site จะทำหน้าที่แยกคำสั่งที่อาจส่งมาจากคอมพิวเตอร์พกพา หรือโทรศัพท์เคลื่อนที่ จัดการอุปกรณ์ปลายทางภายในโรงงาน จัดการด้าน Security ของระบบ มีรายละเอียดดังนี้

3.2 Remote Site ส่วนควบคุมจากระยะไกล

ในการทำงานของระบบเริ่มที่ฝั่ง Remote Site เป็นฝั่งที่อยู่ที่ได้ก็ได้ที่สามารถเชื่อมต่อเข้าเครือข่ายอินเทอร์เน็ต โดยผู้ใช้ที่ฝั่ง Remote Site นี้จะใช้โปรแกรมเดิมที่ใช้ในการควบคุม PLC จากคอมพิวเตอร์ Notebook หรือจะใช้โปรแกรมควบคุมที่พัฒนาขึ้นเองเพื่อสั่งจากโทรศัพท์เคลื่อนที่ก็ได้ สำหรับกรณีที่เป็นการสั่งจากเครื่องคอมพิวเตอร์ Notebook นั้นจะใช้โปรแกรมควบคุมเดิมที่ผู้ผลิตกำหนดมาควบคุม PLC เครื่องนั้นๆ เนื่องจากมีฟังก์ชันการทำงานที่ครบ แต่เนื่องจากโปรแกรมที่ใช้ควบคุม PLC นั้นจะส่งคำสั่งเพื่อควบคุมผ่านทาง Serial Port เป็นหลัก แต่ระบบนี้เป็นการควบคุมจากระยะไกลจึงต้องมีส่วน Data Converter เพื่อมารับ

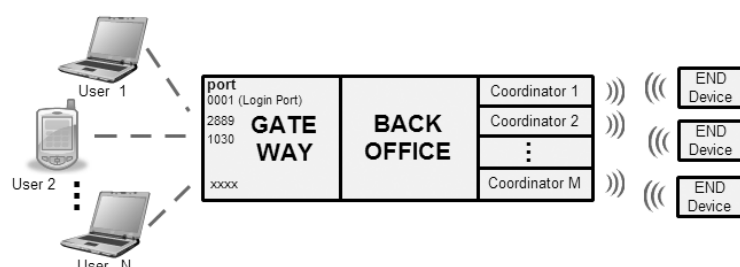
คำสั่งที่ส่งมาจากโปรแกรมที่ใช้ควบคุม PLC ซึ่ง Data Converter ประกอบด้วย ส่วนการทำงาน คือ Virtual Serial Port ซึ่งจะทำหน้าที่สร้างพอร์ต Serial จำลองขึ้นมาบนคอมพิวเตอร์พกพา เพื่อรอรับข้อมูลจากโปรแกรมที่ใช้ควบคุม PLC เมื่อ Virtual Serial Port ได้รับคำสั่งแล้วก็จะส่งไปสร้างเป็น TCP/IP Packet ก่อนจะส่งออกไปยังเครือข่ายอินเทอร์เน็ตผ่านระบบ Wireless LAN แต่ถ้าเป็นกรณีของการส่งคำสั่งจากโทรศัพท์เคลื่อนที่ซึ่งใช้โปรแกรมที่พัฒนาขึ้นเอง สามารถนำคำสั่งที่ใช้ควบคุม PLC ที่เข้ารหัสเพื่อรักษาความลับและสร้าง HMAC เพื่อควบคุมความถูกต้องของการส่งข้อมูล แล้วจึงไปสร้างเป็น TCP/IP Packet แล้วส่งออกเครือข่ายอินเทอร์เน็ตได้โดยตรง ไม่จำเป็นต้องมีส่วนของ Virtual Serial Port

3.3 Factory Site ระบบควบคุมในโรงงาน

ฝั่ง Factory Site ซึ่งอยู่ภายในโรงงาน จะรอรับคำสั่งจาก Remote Site ที่จะเข้ามายัง TCP/IP Port ที่เปิดรอไว้ โดย TCP/IP Packet นั้นถูกส่งเข้าไปยังส่วน GATEWAY ซึ่งทำหน้าที่ทำให้เกิดการติดต่อระหว่าง Remote Site และ Factory Site และดูแลการรับส่งข้อมูลของการติดต่อนั้นให้ถูกต้อง มีรายละเอียดดังนี้

3.3.1 หน้าที่ของ GATEWAY

3.3.1.1 กำหนด TCP Service Port ให้ผู้ใช้ กล่าวคือ เมื่อผู้ใช้ Login โดยติดต่อไปยัง Login Port เรียบร้อยแล้ว ก็จะต้องมีการกำหนด TCP Service Port สำหรับการเชื่อมต่อให้กับผู้ใช้แต่ละคนด้วยการสุ่มหมายเลขพอร์ตให้ โดยข้อมูลของผู้ใช้แต่ละคนจะถูกรับและส่งใน TCP Port ของตนที่ถูกกำหนดให้เท่านั้น เพื่อมิให้ข้อมูลของผู้ใช้แต่ละคนปะปนกัน ทำให้ไม่ต้องรอให้ Port ว่างก่อนจะส่งข้อมูล และ ทำให้สามารถรองรับผู้ใช้ได้หลายๆ คนพร้อมๆ กันแบบ Multi User ดังภาพที่ 3.2



ภาพที่ 3.2 แสดงแนวคิด Multi User และ Multi Device

3.3.1.2 ตรวจสอบ User Authentication โดยการ Login ด้วย User และ Password และต้องจัดการ Session การติดต่อนั้นจน Logout โดยเมื่อ Login สำเร็จแล้ว ต้องมีการจัดเก็บ IP Address ของผู้ที่อยู่ในระบบเพื่อใช้คัดกรอง TCP/IP Packet ข้อมูลต่อไป

3.3.1.3 คัดกรองเฉพาะข้อมูลหรือคำสั่งจากผู้ทำการ Login อย่างถูกต้องเท่านั้น ที่จะสามารถส่งข้อมูลผ่าน GATEWAY เข้าไปยังส่วนอื่นในระบบได้ ถ้าส่งมาจากผู้ที่ไม่ได้ Login อย่างถูกต้อง จะถูกทิ้งไปทั้งหมด

เมื่อ GATEWAY ตรวจสอบแล้วทุกอย่างถูกต้อง GATEWAY ก็จะส่งข้อมูลหรือคำสั่งที่อยู่ภายใน TCP/IP Packet ซึ่งยังอยู่ในรูปการเข้ารหัสข้อมูลไปยังส่วน BACK OFFICE ซึ่งมีหน้าที่ในการจัดการด้านความปลอดภัยและควบคุมกลุ่มของอุปกรณ์ปลายทาง มีรายละเอียดดังนี้

3.3.2 หน้าที่ของ BACK OFFICE

3.3.2.1 ถอดรหัสข้อมูลหรือคำสั่งที่อยู่ภายใน TCP/IP Packet ที่ได้รับมา

3.3.2.2 ตรวจสอบความถูกต้องของ TCP/IP PACKET ที่ส่งเข้ามามี เป็น TCP/IP Packet จากผู้ส่งตัวจริง ไม่ได้ถูกแก้ไขระหว่างทาง โดยใช้หลักการของการตรวจ HMAC

3.3.2.3 แปลงรูปแบบข้อมูลระหว่างชนิดของข้อมูลแบบ TCP/IP–Serial เนื่องจากโปรแกรมที่ใช้ควบคุม และ PLC จะติดต่อสื่อสารกันผ่าน Serial Port ผ่านสายเคเบิล เมื่อเปลี่ยนเป็นการควบคุมระยะไกลผ่านอินเทอร์เน็ต จึงต้องมีการแปลงข้อมูลให้เป็น TCP/IP Packet เพื่อให้สามารถส่งผ่านเครือข่ายอินเทอร์เน็ตได้ โดย BACK OFFICE ต้องแปลงข้อมูลรูปแบบ TCP/IP Data Packet จาก Remote Site เป็น Serial Line Data Packet เพื่อส่งให้กับ PLC หรือส่วนประมวลผลของ Sensor และต้องแปลง Serial Line Data Packet เป็น TCP/IP Data Packet เพื่อส่ง respond กลับไปยัง Remote Site

3.3.2.4 Multi-User Port To Serial Line Control กล่าวคือ BACK OFFICE ต้องเก็บสถานะการใช้อุปกรณ์ปลายทางเพื่อตรวจสอบสถานะว่าอุปกรณ์ปลายทางที่ต้องการว่างหรือไม่เมื่อมีคำร้องขอใช้อุปกรณ์ โดย BACK OFFICE ต้องกำกับการขนถ่ายข้อมูลจาก TCP/IP Port ผ่านทาง Coordinator Node ที่ถูกต้อง ไปยังอุปกรณ์ปลายทางที่ต้องการติดต่อได้ ดังภาพที่ 3.2

โดยส่วนของ GATEWAY และ BACK OFFICE จะถูก Implement เป็น Software ซึ่งจะทำงานอยู่ภายใน Microcontroller ในรูปแบบ Embedded System เพื่อการประหยัดพลังงาน และ ประหยัดพื้นที่ที่ใช้ในการติดตั้งระบบนี้

3.3.3 หน้าที่ของ Coordinator Node

เมื่อข้อมูลหรือคำสั่ง ถูกส่งผ่านออกมาจาก BACK OFFICE ได้ แสดงว่า เป็นข้อมูลที่ถูกแปลงกลับให้อยู่ในรูปแบบ Serial Line Data Packet แล้ว และเป็นข้อมูลที่ส่งมาจากจากผู้ที่มีสิทธิ Access จากการตรวจสิทธิและแปลงรูปแบบ TCP/IP เป็น Serial ของ GATEWAY นอกจากนี้ยังเป็นข้อมูลหรือคำสั่งที่ถูกส่งออกมายัง Serial Line ที่ถูกต้องแล้วด้วย จากการตรวจสอบของ BACK OFFICE ขึ้นต่อไป ข้อมูลหรือคำสั่งที่ออกจาก BACK OFFICE นี้จะเข้าไปยังส่วนของ Coordinator Node ซึ่ง Coordinator Node นี้จะทำหน้าที่ในการแปลงข้อมูล Serial Line Data ที่รับมาจากส่วน BACK OFFICE ให้อยู่ในรูปแบบของ RF Packet for Transmission เพื่อใช้ในการส่งต่อไปยัง Device Node ปลายทางด้วยการส่งแบบไร้สายต่อไป

เพื่อให้ผู้ใช้หลายคนสามารถเข้ามาควบคุม PLC หลายๆ ตัวได้พร้อมๆ กัน จึงมีการออกแบบให้มีการใช้ Coordinator Node หลายๆ ตัว โดยในการ Implement Coordinator Node ในงานวิจัยนี้ จะ พัฒนาโดยใช้ Zigbee RF Module จำนวน 2 Module ซึ่งทั้ง 2 Module ทำงานในโหมดที่ต่างกัน ตามวัตถุประสงค์ที่ต่างกัน กล่าวคือ กำหนดให้ Zigbee RF Module ที่หนึ่งทำงานใน Transparent Mode เพื่อให้สามารถกำหนดคู่ของการสื่อสารปลายทางได้ว่า ต้องการติดต่อกับ Device Node ไດ การเลือกใช้ Transparent Mode นี้เพื่อให้สามารถจับคู่ระหว่าง Coordinator Node กับ Device Node เพื่อให้ประสิทธิภาพในการรับและส่งข้อมูลระหว่าง Zigbee แบบไร้สาย มีประสิทธิภาพสูงสุด นอกจากนี้ยังสามารถเปลี่ยนคู่การสื่อสารเป็น Device Node อื่น ได้จากอุปกรณ์ควบคุมจากระยะไกลได้ทันที ทำให้สามารถเลือกที่จะควบคุม PLC ปลายทางตัวใดก็ได้ ด้วยการเปลี่ยนคู่การสื่อสาร

สำหรับ Zigbee RF Module ตัวที่ 2 กำหนดให้ทำงานใน API Mode เพื่อให้ Zigbee Module ซึ่งเป็น Coordinator Node นี้สามารถส่งคำสั่งให้คอนโทรลเลอร์ของ Device Node ทำการประมวลผลคำสั่งแล้วทำการอ่านค่าจาก Sensor ที่ต้องการแล้วทำการตอบผลลัพธ์กลับมาให้กับ Coordinator Node ซึ่ง Coordinator Node จะถอด Frame ผลลัพธ์ออกเป็น Serial Line Data แล้วส่งผ่าน BACK OFFICE และ GATEWAY กลับไปยังอุปกรณ์ควบคุมระยะไกล เพื่อใช้แสดงเป็นผลลัพธ์ต่อไป

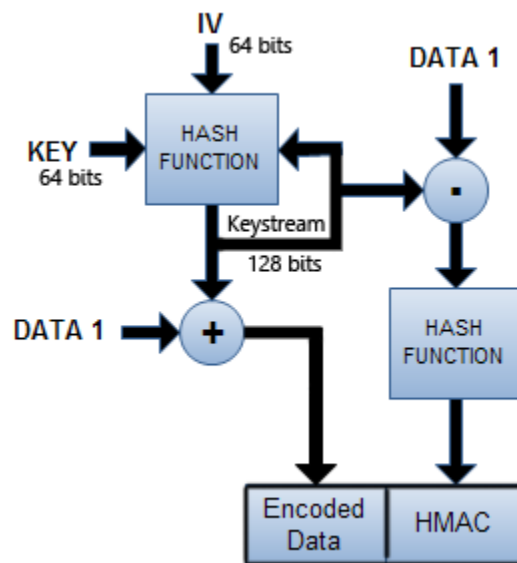
3.3.4 หน้าที่ของ Device Node

Device Node ทำหน้าที่เปลี่ยน RF Packet for Transmission ที่ได้รับมาจาก Coordinator Node ให้กลับมาอยู่ในรูป Serial Line Data แล้วส่งให้อุปกรณ์ เช่น PLC หรือ Sensor ทำงาน ในทางกลับกัน Device Node ก็ต้องทำหน้าที่รับข้อมูลจากอุปกรณ์ปลายทาง ซึ่งอยู่ในรูปแบบ Serial Line Data Packet แล้วแปลงให้อยู่ในรูปแบบ RF Packet For Transmission แล้วส่งออกไปยัง Coordinator Node อีกด้วย ในการ Implement Device Node นี้ จะ Implement ด้วย Zigbee RF Module โดยกำหนดให้มีโหมดการทำงาน 2 Mode เช่นเดียวกับ Coordinator Node นั่นคือ Transparent Mode และ API Mode โดย Device Node ที่กำหนดให้ทำงานแบบ Transparent Mode จะเชื่อมต่ออยู่กับ PLC ด้วย Port RS-232 เพื่อใช้รับส่งข้อมูล ซึ่ง PLC นี้เองที่เป็นอุปกรณ์ปลายทางอย่างแรกที่อุปกรณ์ควบคุมระยะไกลต้องการควบคุมตรวจสอบ สำหรับ Device Node ที่กำหนดให้ทำงานแบบ API Mode จะ Implement ผังลงอยู่กับ Sensor Board เพื่อลดขนาดของชุด Sensor ซึ่ง Sensor Board นี้เองเป็นอุปกรณ์ปลายทางอย่างที่สองที่อุปกรณ์ควบคุมระยะไกลต้องการติดต่อด้วย

3.4 ความมั่นคงของข้อมูล

3.4.1 การเข้ารหัสลับ และการควบคุมความถูกต้องของข้อมูล

เนื่องจากระบบที่นำเสนอนี้เป็นการควบคุมผ่านเครือข่ายอินเทอร์เน็ต จึงต้องคำนึงถึงความปลอดภัยและความมั่นคงของข้อมูล ในงานวิจัยนี้ใช้การเข้ารหัสลับแบบ Keystream เพื่อเข้ารหัสลับข้อมูล และใช้ HMAC เพื่อเป็นการยืนยันตัวตนของผู้ส่งและตรวจสอบว่าข้อมูลถูกแก้ไขระหว่างทางหรือไม่ ซึ่งหลักการที่ใช้ได้แสดงในดังภาพที่ 3.3



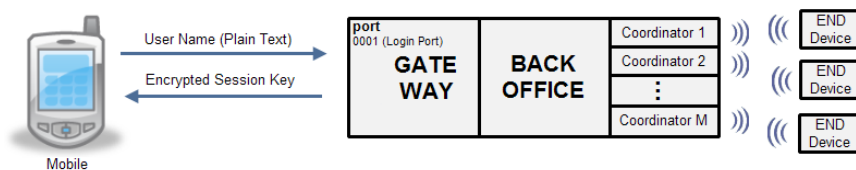
ภาพที่ 3.3 แสดงการเข้ารหัสข้อมูลและสร้าง HMAC

กระบวนการในการเข้ารหัสข้อมูลและสร้าง HMAC ในงานวิจัยนี้ จะทำโดยการสร้าง Keystream ขึ้นมาด้วยการนำ Initial Vector ขนาด 64 Bits เริ่มต้น มาเชื่อมต่อกับ Key ขนาด 64 Bits ที่กำหนดไว้ล่วงหน้า แล้วนำไปผ่าน Hash Function เช่น MD5 จะได้ Output ที่เป็นค่า Hash ออกมา มีขนาด 128 Bits แล้วนำค่า Hash ที่ได้นี้ ไปแทนที่ค่า KEY และ IV ในรอบถัดไป จึงทำให้ได้ Keystream เพื่อใช้ในการเข้ารหัส และใช้สร้าง HMAC ต่อไป โดยในการเข้ารหัส จะนำ Data มา Exclusive OR กับ Keystream ได้ Encoded Data ส่วน HMAC นั้นสร้างโดยการนำ Keystream ที่ได้นี้ มา Concat กับ Data แล้วนำไปผ่าน Hash Function ได้ผลลัพธ์ออกมาเพื่อใช้เป็น HMAC ปะท้าย Encoded Data เพื่อส่งออกไป

3.4.2 การยืนยันตัวเองของผู้ใช้ระบบ

ในการเข้าใช้งานระบบแต่ละครั้ง ผู้ใช้งานระบบจะต้องยืนยันตัวเอง เพื่อที่จะรับ Session Key เพื่อใช้ในการเข้ารหัสลับและควบคุมความถูกต้องของข้อมูลที่ส่ง ซึ่งข้อดีคือ Session Key ที่ใช้ในการติดต่อในแต่ละครั้งจะแตกต่างกันออกไป ทำให้สามารถแก้ปัญหา Reuse Attack ของการทำ Stream Cipher เช่น RC4 ได้ โดยการยืนยันตัวเองนี้ จะใช้หลักการของการ Challenge - Response ซึ่งมีขั้นตอนดังต่อไปนี้

ผู้ต้องการใช้ระบบจะส่งคำขอ ซึ่งมี User Name ไปให้กับ GATEWAY ซึ่ง GATEWAY จะใช้ Key ของผู้ใช้นั้นในการเข้ารหัสลับ Session Key ของผู้ใช้นั้น แล้วส่งกลับไปให้ผู้ใช้นั้น เมื่อผู้ใช้ได้รับข้อความซึ่งเข้ารหัสลับมาแล้ว ก็จะทำการป้อน Password ของตนเองเข้าไป ซึ่งโปรแกรมของฝั่งผู้ใช้ จะแปลง Password ให้เป็น Key ของผู้ใช้ โดย Key ที่ได้นี้จะนำไปถอดรหัส Session Key สำหรับการเข้าใช้งานครั้งนั้นมา ดังที่ได้แสดงในภาพการติดต่อขณะ Authentication ผู้ใช้ ดังภาพ 3.4



ภาพที่ 3.4 แสดงการติดต่อขณะกำลัง Authentication

โดยในงานวิจัยนี้จะเปลี่ยน Password ให้เป็น Key โดยใช้วิธีการป้อน Password เข้าไปยัง Hash Function

สำหรับข้อดีของการยืนยันตนเองด้วยวิธีนี้คือ ไม่ต้องมีการส่ง Password ผ่านเครือข่าย ทำให้ปลอดภัยจากการดักจับ Password ระหว่างส่งผ่านเครือข่ายอินเทอร์เน็ตด้วยวิธีต่างๆ ได้

3.5 การจัดการอุปกรณ์ปลายทางในโรงงาน

หลังจากการทำงานของส่วน BACK OFFICE นั้นข้อมูลและคำสั่งก็จะถูกส่งต่อไปให้ส่วน Coordinator Node ของ Zigbee เพื่อสื่อสารกับอุปกรณ์ปลายทางต่อไป โดยสภาพแวดล้อมในโรงงานอุตสาหกรรมอัตโนมัติ มักจะมีการใช้ PLC และ Sensor อยู่เป็นจำนวนมาก ดังนั้นเพื่อ

ประโยชน์สูงสุดของการจัดการระยะไกลจึงมีการออกแบบระบบซึ่งตอบสนองความต้องการ 2 ประการ คือ

- 1) ผู้ใช้สามารถเลือกและสลับ PLC ที่ต้องการควบคุมได้ด้วยตนเองจากระยะไกล
- 2) ผู้ใช้สามารถตรวจสอบสถานะของโรงงาน เช่น อุณหภูมิ คุณภาพอากาศ จาก Sensor ที่ติดตั้งในจุดต่างๆ ภายในโรงงานได้จากระยะไกล

ในการสื่อสารระหว่าง BACK OFFICE กับอุปกรณ์ที่ต้องการควบคุมในงานวิจัยนี้ จะใช้ระบบ Zigbee ซึ่งเป็นระบบสื่อสารไร้สายระยะใกล้ มีการรบกวนกับการทำงานของระบบ WIFI น้อย มีการจัดการด้านความปลอดภัยในการส่งแบบไร้สายระยะใกล้ที่ดี มีโหมดการทำงานที่ครอบคลุมความต้องการ

สำหรับ Zigbee Module ที่เลือกใช้ สามารถกำหนดให้ทำงานได้ 2 โหมด คือ

1) Transparent Mode เป็นโหมดที่ Zigbee Module จะติดต่อรับส่งข้อมูลกันแบบไร้สายในลักษณะ Point to Point ซึ่งเหมาะที่จะใช้ติดต่อระหว่าง Coordinator Node กับ End Device Node ของ PLC เนื่องจากสามารถกำหนดให้ติดต่อกันเฉพาะคู่ที่กำหนดไว้เท่านั้น จึงสามารถส่งข้อมูลจาก Coordinator ไปยัง PLC ได้ด้วยความเร็วสูงสุด นอกจากนี้ยังสามารถเปลี่ยนคู่ของการสื่อสารจากระยะไกลด้วยคำสั่ง AT Command (หรือจะพัฒนาให้ใช้งานขึ้นในอินเทอร์เฟซแบบ GUI ก็ได้) ซึ่งจะทำให้สามารถสลับไปควบคุม PLC ตัวอื่นๆ จากระยะไกลได้ง่าย

2) API Mode เป็นโหมดที่เหมาะสมที่จะประยุกต์ใช้กับ Sensor เพื่อให้สามารถติดต่อกับ Sensor จำนวนมากที่กระจายอยู่ในโรงงานได้ เนื่องจากโหมดนี้จะทำงานในรูปแบบเครือข่าย ซึ่งจัดตั้งเป็นเครือข่ายไร้สาย Zigbee โดย Coordinator Node จะทำหน้าที่เป็นศูนย์กลางในการกำกับดูแลกิจกรรมต่างๆ ภายใน Zigbee Network ส่วน Device Node ซึ่งเป็นสมาชิกของ Zigbee Network จะมี Sensor เชื่อมต่ออยู่ เพื่อให้อุปกรณ์เหล่านั้นสามารถรับคำสั่งและส่งผลลัพธ์ได้ตอบกลับไปผ่านเครือข่ายไร้สาย Zigbee ได้

บทที่ 4

การพัฒนาระบบไร้สายโดยใช้ ZigBee เพื่อควบคุมและติดตามสถานะ เครื่องจักรและเซ็นเซอร์ในโรงงานผ่านเครือข่ายอินเทอร์เน็ต

การพัฒนาระบบจากแนวคิดที่ได้นำเสนอไว้ให้สามารถนำไปใช้ประโยชน์ได้จริงนั้น ควรพิจารณาถึงความต้องการของแต่ละระบบที่ต้องการนำไปใช้ด้วย เช่น บางระบบมีผู้ใช้งานมาก บางระบบมีผู้ใช้น้อย บางระบบมีอุปกรณ์ที่ต้องการควบคุมมาก บางระบบมีอุปกรณ์ที่ต้องการควบคุมน้อย บางระบบสะดวกในการเลือกพัฒนาส่วนโปรแกรมในการควบคุมอุปกรณ์จากระยะไกลขึ้นมาเอง บางระบบก็เลือกที่จะใช้โปรแกรมในการควบคุมที่มีอยู่แล้ว หรือบางระบบก็เลือกที่จะใช้โปรแกรมในการควบคุมที่มีผู้พัฒนาไว้และจัดจำหน่ายให้เลือกใช้อยู่แล้ว เป็นต้น ซึ่งการเลือกพัฒนาระบบโดยยึดแนวคิดที่ได้นำเสนอไปแล้วเป็นหลักนี้ สามารถยืดหยุ่นได้ตามความเหมาะสมของสภาวะความต้องการของแต่ละสถานที่ที่มีความแตกต่างกันออกไปได้

อย่างไรก็ตาม วิทยานิพนธ์ฉบับนี้ จะนำเสนอรูปแบบการพัฒนาระบบจากแนวคิดในแบบพื้นฐานเพื่อให้เห็นภาพการทำงานตามแนวคิดได้จริง ดังนั้นในขั้นตอนการพัฒนานี้ จึงมีการเลือกใช้อุปกรณ์และพัฒนาโปรแกรมประยุกต์ที่จำเป็นดังนี้

4.1 ฝั่ง Remote Site

เป็นฝั่งที่ Remote User จะใช้อุปกรณ์เช่น Notebook PC และ โทรศัพท์เคลื่อนที่ เพื่อทำการสั่งงาน PLC จากระยะไกล โดยคุณสมบัติของอุปกรณ์และ Software ที่ใช้ในฝั่ง Remote Site มีดังนี้

4.1.1 เครื่องคอมพิวเตอร์ Notebook PC ในการควบคุม

4.1.1.1 Hardware ของเครื่องคอมพิวเตอร์ Notebook ที่ใช้ในวิทยานิพนธ์ครั้งนี้

คือ

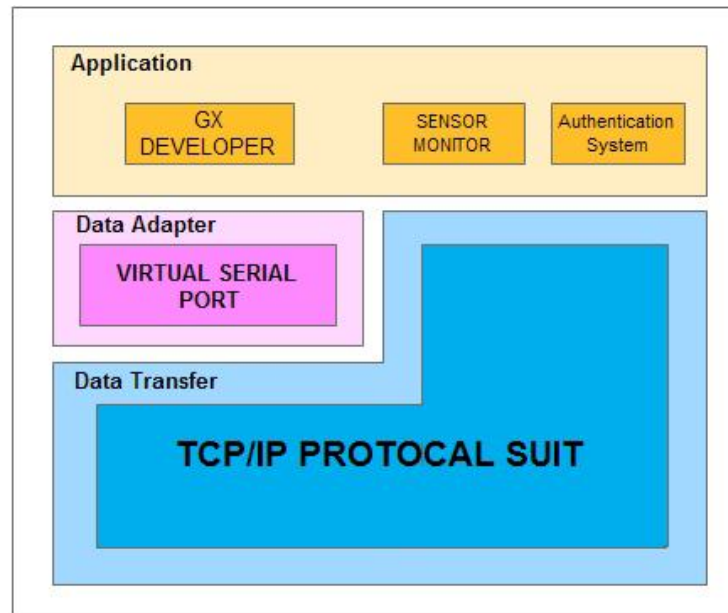
ตาราง 4.1 แสดงข้อมูลจำเพาะของเครื่องคอมพิวเตอร์ที่ใช้

msi CR460	
CPU	Intel® Core™ i3-2350M @2.30 GHz
Chipset	Intel® HM65
RAM	4.0 GB
Harddisk	SSD OCZ VERTEX 4 60GB
Wireless Lan	IEEE 802.11 b/g/n
OS	Windows® 7 Ultimate 32 Bit

4.1.1.2 Software ที่ใช้ใน Notebook PC

- 1) MELSOFT series GX Developer ใช้สำหรับการควบคุม PLC ผ่านเครือข่าย Internet
- 2) โปรแกรมสำหรับอ่านค่า Sensor เป็นโปรแกรมที่พัฒนาขึ้นเองเพื่อส่งคำสั่งในการสั่งให้มีการอ่านค่าจาก Sensor ซึ่งติดตั้งอยู่ภายในโรงงานผ่านทางเครือข่าย Internet พร้อมทั้งรับผลลัพธ์จาก Sensor ที่จะส่งกลับมาเพื่อแสดงผลอีกด้วย
- 3) Data Converter ซึ่งประกอบด้วยการทำงานสองส่วน คือ Virtual Serial Port Device Driver และ Serial to TCP/IP Packet Converter โดยในการ Implement ส่วน Software แบบที่ควบคุมบน Notebook PC นี้ จะเป็นการเลือกใช้ Software ซึ่งมีผู้พัฒนาไว้แล้ว โดยจะเลือก Software ที่มีความสามารถทั้งสองส่วน คือ สามารถสร้าง Virtual Serial Port Device Driver ขึ้นมาในระบบ และมีส่วนการทำงานในการแปลง Serial Line Data Packet เป็น TCP/IP Data Packet ได้

4.1.1.3 Software Architecture ของระบบ Software ที่ใช้บน Notebook PC
 สำหรับความสัมพันธ์ของ Software ที่ใช้บน Notebook PC นั้น แสดงได้ด้วยภาพแสดง
 Software Architecture บน Notebook PC ดังภาพ 4.1



ภาพที่ 4.1 แสดง Software Architecture ที่ใช้บน Notebook PC

4.1.2 โทรศัพท์เคลื่อนที่ในการควบคุม

โทรศัพท์เคลื่อนที่ SmartPhone ในยุคปัจจุบัน มีแนวโน้มของการพัฒนาทางด้าน Hardware ในด้านต่างๆ เช่น เพิ่มความเร็วของหน่วยประมวลผล เพิ่มจำนวนหน่วยประมวลผล เพิ่มหน่วยความจำหลัก เพิ่มพื้นที่เก็บข้อมูล ในขณะที่ราคาถูกลง เข้าถึงได้ง่ายขึ้น พกพาได้สะดวก

4.1.2.1 คุณสมบัติด้าน Hardware ของโทรศัพท์เคลื่อนที่ สำหรับโทรศัพท์เคลื่อนที่ที่ใช้ในการควบคุมระยะไกลในวิทยานิพนธ์ฉบับนี้ มีรายละเอียดดังนี้

ตาราง 4.2 แสดงข้อมูลจำเพาะของโทรศัพท์เคลื่อนที่ที่ใช้

	HTC EVO 3D
CPU Processing Speed	dual core ,1.2 GHz
RAM	1 GB
Storage	Internal Phone Storage 1 GB
Wireless Internet Connection	Cellular, EDGE , IEEE 802.11 b/g/n
OS	Android 4.0 (Ice Cream Sandwich)

4.1.2.2 โปรแกรมที่ใช้ทำการควบคุม PLC จากโทรศัพท์มือถือ

จากการพัฒนาอย่างต่อเนื่องของหน่วยประมวลผล หน่วยความจำหลัก รวมถึงพื้นที่เก็บข้อมูล ทำให้มีประสิทธิภาพสูงขึ้นอย่างมาก ในขณะที่มีขนาดเล็กลงจนนำไปใช้ในอุปกรณ์พกพาได้ เช่น โทรศัพท์เคลื่อนที่ คอมพิวเตอร์พกพา Tablet ส่งผลให้แนวคิดของการออกแบบระบบปฏิบัติการของโทรศัพท์เคลื่อนที่ซึ่งเปลี่ยนจากเดิมที่การที่การรับส่งข้อมูลเป็นส่วนเสริมของการสื่อสารด้วยเสียง เป็นการเน้นข้อมูลในการสื่อสารเป็นหลักมากกว่าการสื่อสารด้วยเสียงเพียงอย่างเดียว

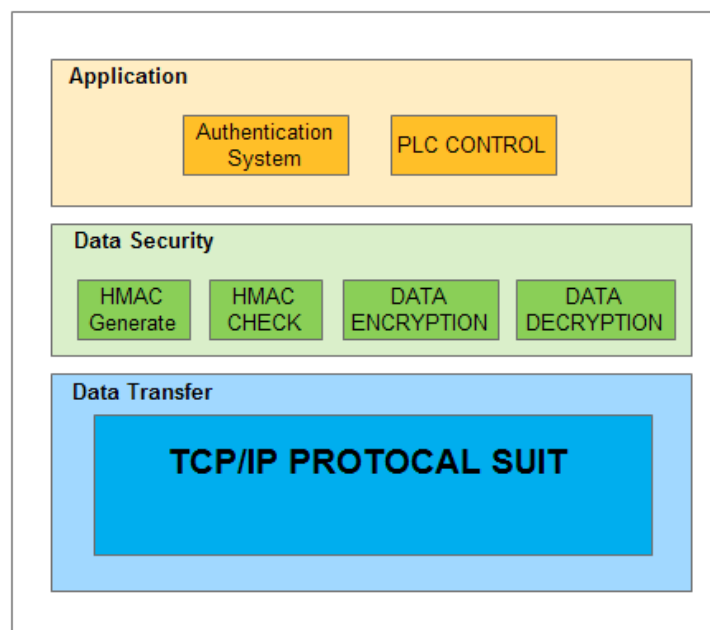
ด้วยแนวคิดของการออกแบบระบบปฏิบัติการของโทรศัพท์เคลื่อนที่ที่เปลี่ยนไปนี้เอง ทำให้ระบบปฏิบัติการสำหรับโทรศัพท์เคลื่อนที่ซึ่งมีผู้พัฒนาออกมาแข่งขันกัน มีการพัฒนาความสามารถให้สามารถทำงานได้เหมือนกับเครื่องคอมพิวเตอร์ PC เช่นในระบบ Android OS นั้นใช้ Kernel เดียวกันกับ Linux บน PC เป็นต้น โดยเราสามารถนำ Smart phone ในการทำงานเหมือนกับบน PC เช่นรับส่งข้อความทุกประเภท ดาวน์โหลดโปรแกรมประยุกต์ เช็คเมล ฟังเพลง ดูวิดีโอ ส่งซื้อขายหุ้น ท่องเว็บ เป็นต้น

ด้วยการที่โทรศัพท์เคลื่อนที่ได้พัฒนาทั้งทางด้าน Hardware และ OS ที่ทำให้ทำงานได้เร็ว และมีประสิทธิภาพ ครอบคลุมความต้องการ มีขนาดเล็ก พกพาติดตัวได้สะดวก จึงทำให้มีแนวคิดที่จะนำโทรศัพท์เคลื่อนที่แบบ Smart phone มาใช้เป็นส่วนหนึ่งของระบบควบคุมดังที่ได้นำเสนอในงานวิจัยนี้

ในการพัฒนาโปรแกรม Android สำหรับโทรศัพท์เคลื่อนที่ซึ่งใช้ในงานวิจัยนี้จะพัฒนาด้วยภาษา Java โดยใช้ Android SDK

4.1.2.3 Software Architecture ของ Software ที่ใช้บนโทรศัพท์เคลื่อนที่

ความสัมพันธ์ของ Software ที่ใช้ในการทำงานจากโทรศัพท์เคลื่อนที่ แสดงได้ด้วยภาพ Software Architecture บนโทรศัพท์เคลื่อนที่ ดังภาพที่ 4.2

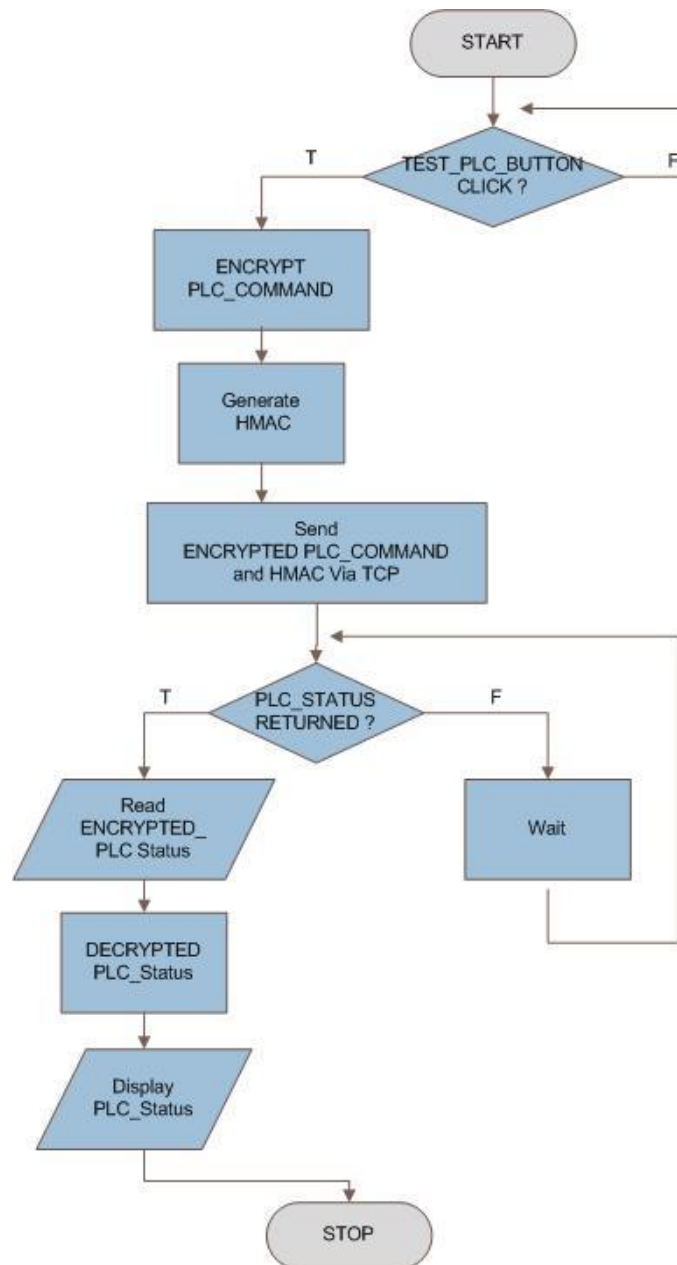


ภาพที่ 4.2 แสดง Software Architecture ของ software บนโทรศัพท์เคลื่อนที่

โปรแกรมที่พัฒนาขึ้นเองสำหรับ Android OS นี้ ใช้โปรแกรม Eclipse เวอร์ชัน Indigo ซึ่งติดตั้ง Android SDK เป็นส่วนเขียนโค้ดโปรแกรม คอมไพล์และทดสอบแก้ไขจนทำงานได้เสร็จสมบูรณ์ โดยโปรแกรมที่พัฒนาขึ้นจะมีส่วนของการทำงานในการส่งคำสั่งออกไปยัง PLC โดยผ่านระบบไร้สายแบบ 3G หรือ Wi-Fi โดยใช้ Protocols TCP/IP ในการส่งข้อมูลผ่าน Internet โดยคำสั่งที่ส่งออกจากโทรศัพท์มือถือนี้จะต้องมีการเข้ารหัสก่อนส่งออกไปและถอดรหัสเมื่อรับข้อมูลเข้ามาก่อนเสมอ รวมทั้ง ต้องมีการเช็คความถูกต้องของคำสั่งด้วยทุกครั้งโดยใช้หลักการของการ Stream Cipher

4.1.2.4 ขั้นตอนการทำงานของโปรแกรมที่พัฒนาขึ้นบนโทรศัพท์เคลื่อนที่

สำหรับลำดับการสั่งงานจากโทรศัพท์เคลื่อนที่นั้น จะมีลำดับขั้นตอนการทำงานในส่วนของการตรวจสอบสถานะของ PLC หลังจาก Login เรียบร้อยแล้ว ดังแสดงได้ด้วย ภาพ 4.3 แสดง Flowchart การทำงานของการส่งคำสั่งจากโทรศัพท์เคลื่อนที่



ภาพที่ 4.3 แสดงลำดับขั้นตอนการทำงานของโปรแกรมบนโทรศัพท์เคลื่อนที่

4.2 ฝั่ง Factory Site

ฝั่ง Factory Site เป็นฝั่งที่อยู่ภายในโรงงานจริง โดยจะมีอุปกรณ์ที่รองรับการส่งงานจาก Remote Site จากระยะไกล ซึ่ง Factory Site จะพัฒนาด้วย Hardware และ Software ดังนี้

4.2.1 GATEWAY ต้องทำหน้าที่ 3 ประการ ได้แก่

4.2.1.1 ควบคุมการ Login รวมถึงจัดการ Session การติดต่อที่ Login นั้น จนกว่าจะ Logout ออกจากระบบไป

4.2.1.2 กำหนด TCP/IP Port Service ให้ผู้ใช้แต่ละราย หลังจาก Login เข้าระบบได้อย่างถูกต้องแล้ว

4.2.1.3 คัดกรองเฉพาะข้อมูลที่ส่งจากผู้ Login อย่างถูกต้องเท่านั้นที่จะสามารถส่งผ่าน GATEWAY เข้าไปยัง BACK OFFICE ได้

4.2.2 BACK OFFICE ต้องทำหน้าที่ 4 ประการ ได้แก่

4.2.2.1 ถอดรหัสข้อมูลที่อยู่ใน TCP/IP Packet ที่ได้รับมา

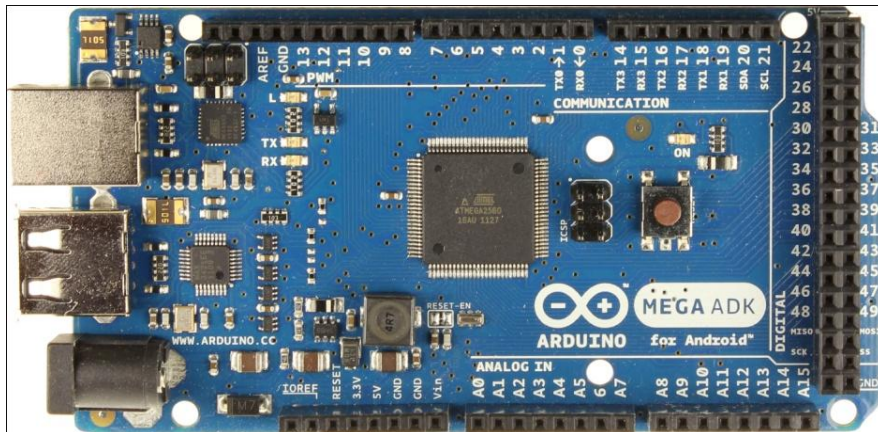
4.2.2.2 ตรวจสอบความถูกต้องของ Data Packet ที่รับมา ด้วยหลักการตรวจ HMAC

4.2.2.3 แปลงรูปแบบข้อมูลที่ใช้รับส่งระหว่างเครือข่ายอินเทอร์เน็ตกับอุปกรณ์ซึ่งทำงานโดยใช้ Serial Port

4.2.2.4 จัดการบริหารผู้ใช้ที่อยู่ในระบบและอุปกรณ์ปลายทางที่มี ในรูปแบบ Multi-User To Serial Line Control

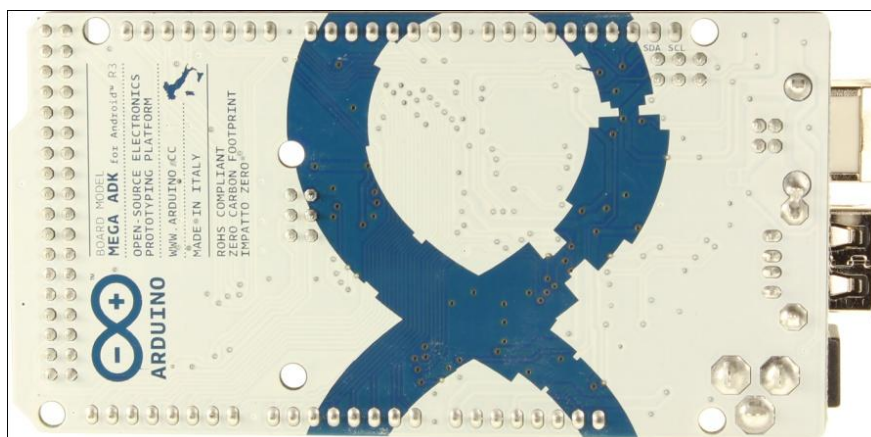
4.2.3 Hardware ที่ใช้ในการพัฒนา

ในการพัฒนาส่วน GATWEWAY และ BACK OFFICE นี้จะพัฒนาขึ้นมาเองในรูปแบบของ Software ซึ่งทำงานโดย Microcontroller ซึ่งการเลือกใช้ Microcontroller นั้นก็เพื่อให้ระบบมีลักษณะเป็น Embedded System สำหรับ Microcontroller ที่เลือกใช้ มีคุณสมบัติ ดังนี้



ภาพที่ 4.4 แสดงภาพด้านบนของ Microcontroller Arduino ADK 2560 R3

แหล่งที่มา: Arduino.cc, 2012.



ภาพที่ 4.5 แสดงภาพด้านล่างของ Microcontroller Arduino ADK 2560 R3

แหล่งที่มา: Arduino.cc, 2012.

คุณสมบัติด้าน Hardware ของ Microcontroller Arduino ADK 2560 R3 มีดังนี้

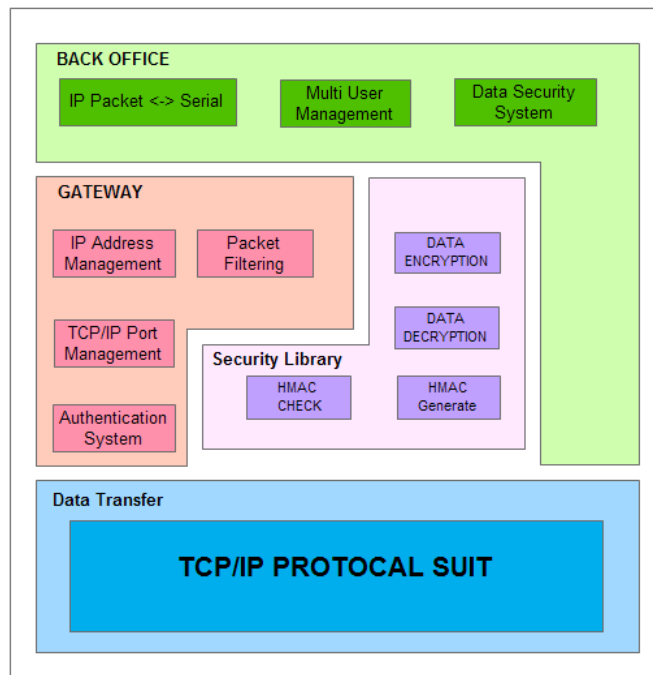
ตาราง 4.3 แสดงข้อมูลจำเพาะของ Microcontroller Arduino ADK 2560 R3

Arduino ADK 2560 R3	
Microcontroller	ATmega2560
Digital I/O Pins	54 (of which 15 provide PWM output)
Analog Input Pins	16
Flash Memory	256 KB of which 8 KB used by bootloader
SRAM	8 KB
EEPROM	4 KB
Clock Speed	16 MHz

4.2.4 Software Architecture ของ GATEWAY และ BACK OFFICE

ในการ Implement GATEWAY และ BACK OFFICE นี้จะพัฒนาขึ้นมาเองในรูปแบบของ SOFTWARE โดยจะพัฒนารวมกันทั้งส่วน GATEWAY และ BACK OFFICE บน Microcontroller ARDUINO

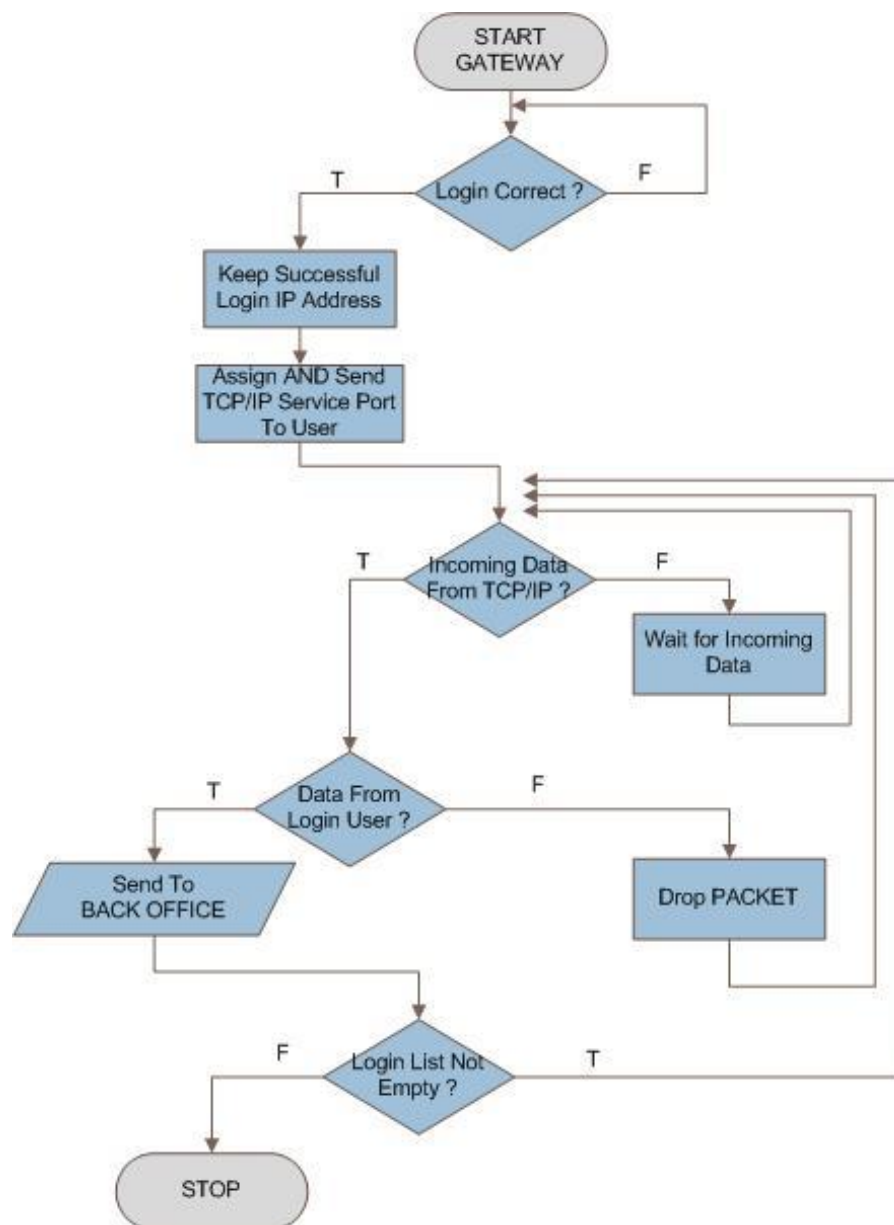
ความสัมพันธ์ของ Software ซึ่งพัฒนามบน Microcontroller Arduino ADK 2560 R3 นั้น แสดงได้ด้วยภาพ Software Architecture ซึ่งมีรายละเอียดดังภาพ 4.6



ภาพที่ 4.6 แสดง Software Architecture ซึ่งทำงานบน Microcontroller

4.2.5 ขั้นตอนการทำงาน GATEWAY

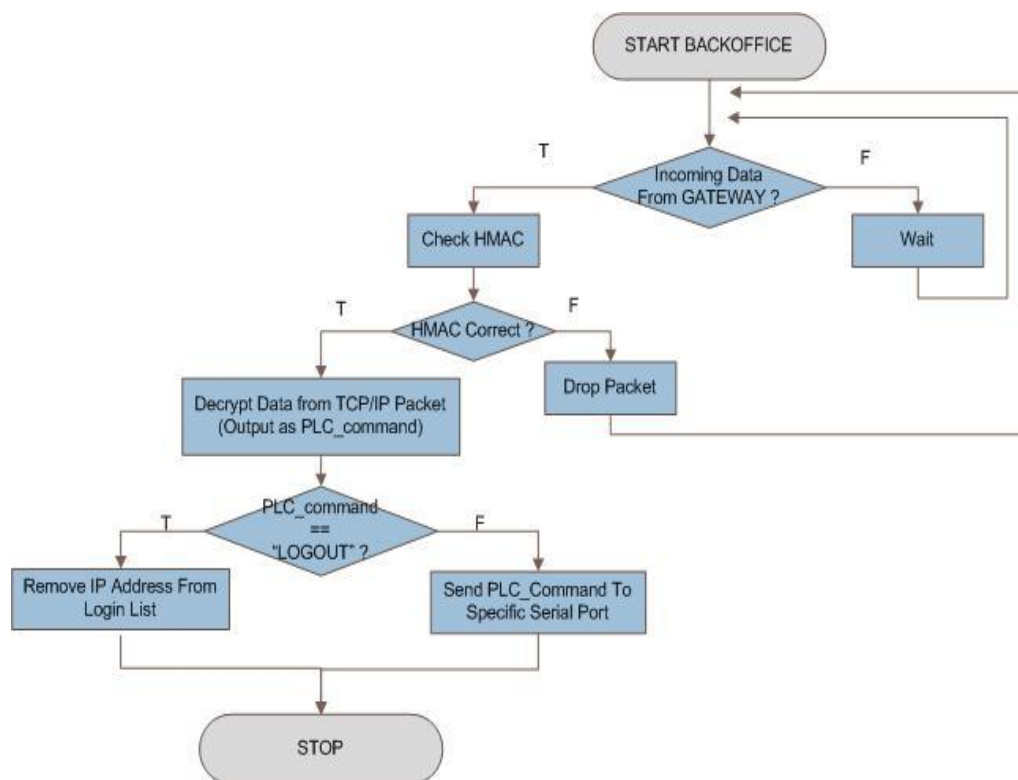
ภาพ 4.7 แสดงส่วนโปรแกรมการทำงานของ GATEWAY เมื่อมีการส่งคำสั่งทดสอบสถานะ PLC มาจากโทรศัพท์เคลื่อนที่ จะมีลำดับขั้นตอนการทำงาน ดังนี้



ภาพที่ 4.7 แสดงลำดับขั้นตอนการทำงานของ GATEWAY

4.2.6 ขั้นตอนการทำงานของ BACK OFFICE

เมื่อ GATEWAY ทำการคัดกรองเฉพาะข้อมูลที่ส่งมาจากผู้ที่มีสิทธิส่งข้อมูลเข้าระบบแล้ว GATEWAY ก็ส่งต่อข้อมูลหรือคำสั่งนั้น ให้กับส่วน BACK OFFICE ทำงานต่อไป โดยขั้นตอนการทำงานของ BACK OFFICE เมื่อได้รับข้อมูลเข้ามา จะมีลำดับการทำงานดังนี้



ภาพที่ 4.8 แสดงลำดับขั้นตอนการทำงานของ BACK OFFICE

4.2.7 Coordinator Node การควบคุมในระดับ Personal Area Network (PAN) ภายในโรงงาน เลือกใช้อุปกรณ์ Zigbee ในการสื่อสารระยะใกล้ ซึ่ง Zigbee Module ที่เลือกใช้มีคุณสมบัติด้าน Hardware ดังนี้

1) General

- (1) Power output:: 1mW (+0 dBm)
- (2) Indoor/Urban range: Up to 100 ft (30 m)
- (3) Outdoor/RF line-of-sight range: Up to 300 ft (90 m)
- (4) RF data rate: 250 Kbps
- (5) Interface data rate: Up to 115.2 Kbps
- (6) Operating frequency: 2.4 GHz
- (7) Receiver sensitivity: -92 dBm
- (8) Frequency band: 2.4000 - 2.4835 GHz
- (9) Interface options: 3V CMOS UART

2) Networking

- (1) Spread Spectrum type: DSSS (Direct Sequence Spread Spectrum)
- (2) Networking topology: Point-to-point, & peer-to-peer
- (3) Error handling: Retries & acknowledgements
- (4) Filtration options: PAN ID, Channel, and 64-bit addresses
- (5) Channel capacity: 16 Channels
- (6) Addressing: 65,000 network addresses available for each channel

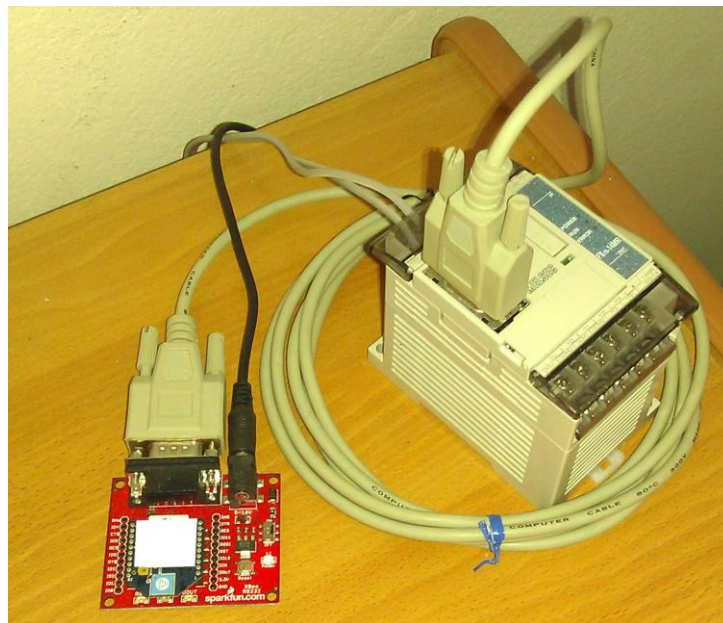
3) Power

- (1) Supply voltage: XBee: 2.8 - 3.4 VDC
- (2) XBee Footprint Recommendation: 3.0 - 3.4 VDC
- (3) Transmit current: XBee: 45 mA (@ 3.3 V) boost mode 35 mA
(@ 3.3 V) normal mode

4.2.8 Device Node คือ Node การสื่อสารระดับ PAN ซึ่งเชื่อมต่ออยู่กับอุปกรณ์ที่ต้องการ Monitor หรือควบคุม ในการ Implement จริงจะแบ่ง Device Node ได้เป็นสองชนิด ตามโหมดการทำงานร่วมกับ Coordinator Node ดังนี้

4.2.8.1 Device Node ใน Transparent Mode

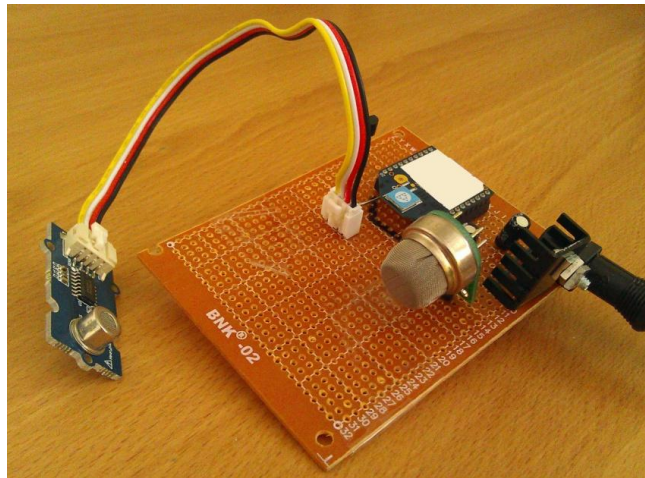
เพื่อให้สามารถสื่อสารที่ความเร็วสูงสุดของ Zigbee จึงเลือกใช้โหมดการทำงานนี้ในการเชื่อมต่อกับ PLC เพื่อให้สามารถรับส่งข้อมูลหรือคำสั่งกับ PLC ด้วยความเร็วสูงสุดได้ อีกทั้งการเปลี่ยนคู่การสื่อสารไปควบคุม PLC ตัวอื่นก็สามารถทำได้สะดวกจากระยะไกลอีกด้วย ในการ Implement จริง เพื่อให้สามารถเชื่อมต่อเข้ากับ PLC สะดวก จึงเลือกใช้ Zigbee Module ร่วมกับ Extension Board ดังรูป



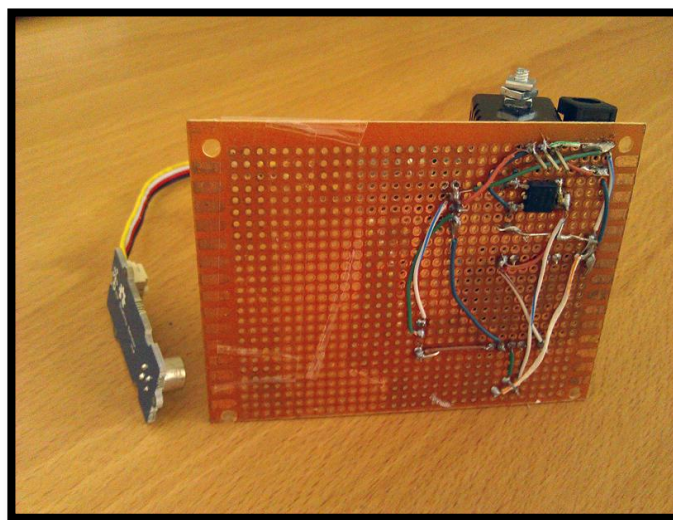
ภาพที่ 4.9 แสดงการเชื่อมต่อ Device Node เข้ากับ PLC ในการทำงาน Transparent Mode

4.2.8.2 Device Node ใน API Mode

เพื่อให้สามารถตรวจสอบสถานะของ Sensor ในรูปแบบ Zigbee Network จึงเลือกใช้ Zigbee ในโหมด API Command นี้ในการ Implement เพื่อให้ Sensor Module นี้มีขนาดเล็ก ประหยัดไฟ ติดตั้งง่าย ใช้น้อย จึง Implement Sensor Module โดย Integrate Zigbee Module รวมไปกับ Sensor 3 ชนิดบน Board เดียวกัน ซึ่งทำให้ Sensor Module นี้มีขนาดเล็ก ติดตั้งง่าย ตามความต้องการ ซึ่ง Sensor Module ที่พัฒนาขึ้น มีรูปแบบ ดังนี้

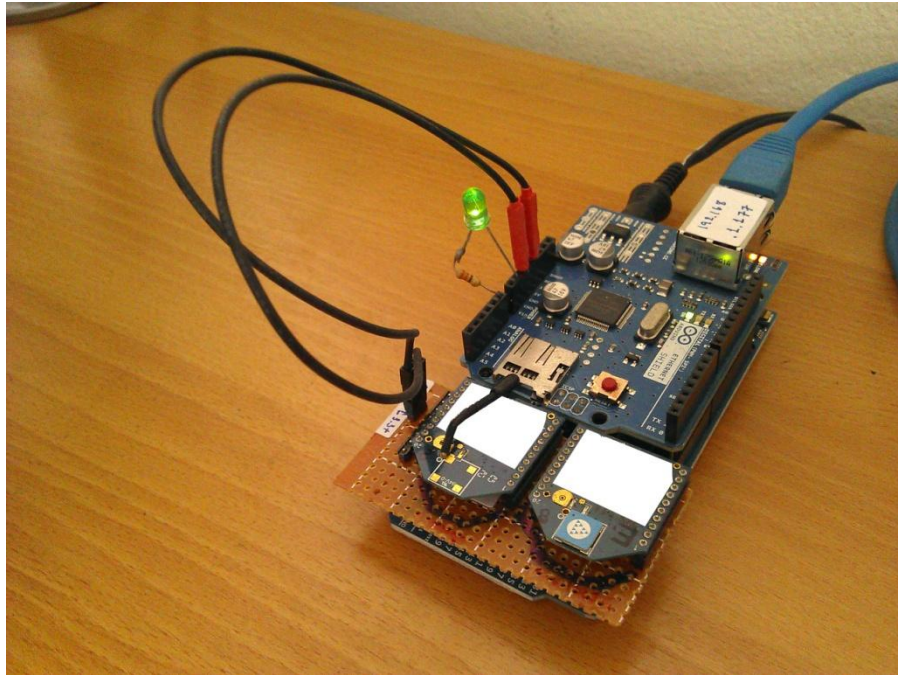


ภาพที่ 4.10 แสดง Device Node ซึ่งมีอุปกรณ์เป็น Sensor โดยมีการทำงานแบบ API Mode



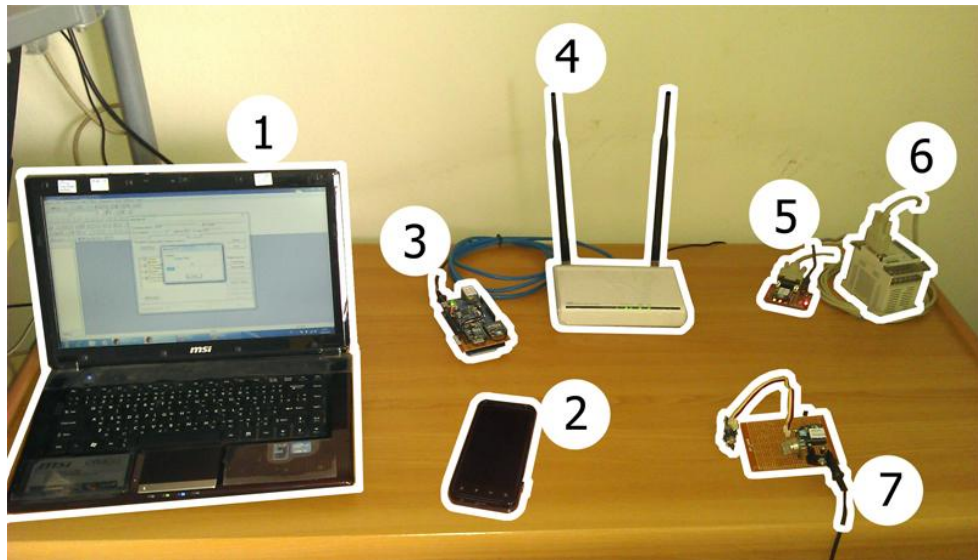
ภาพที่ 4.11 แสดงภาพด้านล่างของ Sensor Board ที่ทำงานแบบ API Mode

และเพื่อให้การสื่อสารในระดับ PAN สามารถส่งงานอุปกรณ์ได้พร้อมกันในรูปแบบที่ได้
นำเสนอแนวคิดไว้ คือ Transparent Mode และ API Mode ในการ Implement จึงได้เลือกใช้
Zigbee Module จำนวนสอง Module โดยในการ Implement จริงจะเชื่อม Zigbee Module ทั้ง
สอง Module เข้ากับ Microcontroller board เพื่อความสะดวกในการใช้งานและติดตั้ง ดังภาพ



ภาพที่ 4.12 แสดง Coordinator Node ซึ่งมีการทำงานทั้ง Transparent Mode และ API Mode

4.3 ระบบที่ได้พัฒนาในการทดลอง



ภาพที่ 4.13 แสดงระบบที่ได้พัฒนาขึ้นในการทดสอบการควบคุม

ระบบที่ใช้ในการทดลอง ประกอบด้วย

1) เครื่องคอมพิวเตอร์ที่ฝั่ง Remote Site ซึ่งใช้ในการสั่งงาน PLC ผ่านเครือข่ายอินเทอร์เน็ต ใช้เครื่อง PC แบบพกพา ที่สามารถเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตผ่าน WI-FI โดยโปรแกรมที่ใช้ควบคุม PLC จาก PC ที่ใช้ในการทดสอบคือ GX Developer สำหรับควบคุม PLC ของ Mitsubishi

2) โทรศัพท์เคลื่อนที่ในฝั่ง Remote Site ที่มีการติดตั้งโปรแกรมที่พัฒนาขึ้นโดยเป็นโปรแกรมที่จะสามารถสั่งงาน PLC ได้บางส่วน เช่น ตรวจสอบสถานะของ PLC ผ่านเครือข่ายอินเทอร์เน็ต โดยใช้ช่องทางการสื่อสารที่สะดวกในพื้นที่นั้นๆ เช่น Wi-Fi GPRS หรือระบบ 3G เป็นต้น

3) ไมโครคอนโทรลเลอร์ รุ่น Arduino MEGA ADK R3 ในฝั่ง Factory Site มี Clock Speed 16 MHz Flash Memory 256 KB SRAM 8 KB EEPROM 4 KB มีความสามารถในการประมวลผลคำสั่ง 16 MIPS ใช้ภาษา C++ ในการพัฒนาโปรแกรมการทำงาน โดยพัฒนาในรูปแบบ Embedded System ประกอบด้วยส่วนที่ทำหน้าที่ติดต่อกับ Remote Site และส่วนควบคุมภายในโรงงาน ซึ่งก็คือ GATEWAY และ BACK OFFICE นั่นเอง โดยต้องกำหนดให้มี IP ADDRESS ซึ่ง Remote Site สามารถเข้าถึงได้โดยตรงจากเครือข่ายอินเทอร์เน็ต ในงานวิจัยนี้ได้

รวมส่วน Coordinator Node เข้ากับ I/O port บนบอร์ดหลักของไมโครคอนโทรลเลอร์ด้วยเพื่อลดการเดินสายไฟภายนอก ทำให้การจัดเก็บ ติดตั้ง และใช้งาน มีความเหมาะสมในรูปแบบ Embedded System

4) Wi-Fi Router ในฝั่ง Factory Site ใช้ทดสอบการควบคุมจากคอมพิวเตอร์ Notebook ด้วยเครือข่าย Wi-Fi (สำหรับโทรศัพท์เคลื่อนที่ทดสอบด้วยเครือข่าย 3G)

5) เป็นส่วนของ Device Node ในฝั่ง Factory Site ซึ่งถูก Implement ด้วย Zigbee Module ซึ่งทำงานใน Transparent Mode โดย Device Node จะเชื่อมต่ออยู่กับ PLC ด้วยสายเคเบิล

6) เป็นส่วนอุปกรณ์ปลายทางที่ทำงานจริงคือ PLC นั้นเอง

7) เป็นอุปกรณ์ปลายทางอีกประเภท คือ Sensor Board ซึ่ง Integrate ส่วนการทำงานหลักสองส่วนบนบอร์ดหลัก คือ Device Node ซึ่ง Implement ด้วย Zigbee Module โดยทำงานใน API Mode และอีกส่วนคือ End Device ซึ่งได้แก่อุปกรณ์ Sensor 3 ชนิด ได้แก่ Thermometer Sensor Air Quality Sensor และ LPG Sensor

บทที่ 5

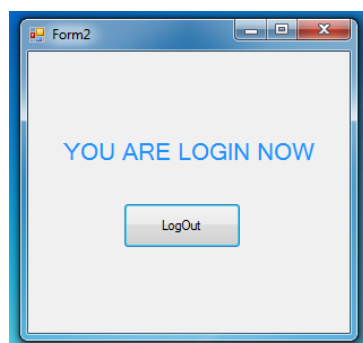
ผลการทดลองการใช้งาน

5.1 ผลการทดลองจากเครื่องคอมพิวเตอร์ PC

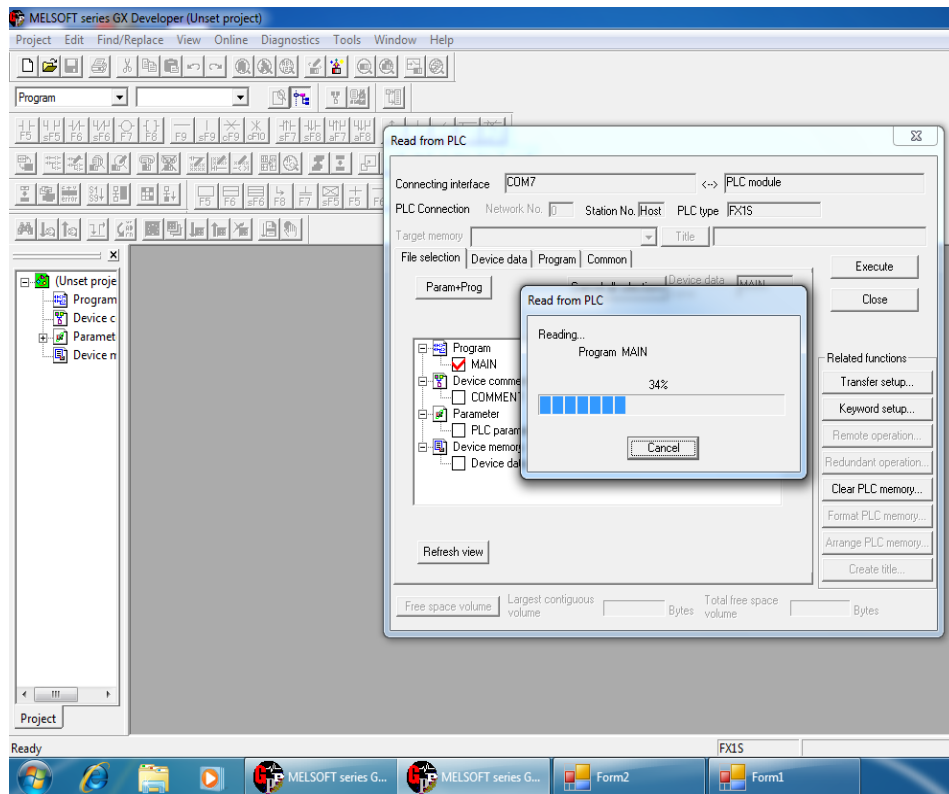
ผลการทดสอบจากระบบที่พัฒนาขึ้นจริง พบว่าในการควบคุม PLC โดยใช้เครื่องคอมพิวเตอร์ Notebook สามารถทำการ Login เพื่อเข้าสู่ระบบ แล้วสั่งงานได้ครบทุกฟังก์ชันการทำงานจากโปรแกรม GX Developer ผ่านเครือข่ายอินเทอร์เน็ตได้ทันที เสมือนว่าใช้การเชื่อมต่อโดยตรงด้วยสายเคเบิลอยู่ ดังที่ได้แสดงตัวอย่างการอ่านข้อมูลจากหน่วยความจำภายใน PLC ผ่านเครือข่ายอินเทอร์เน็ตกลับมายังโปรแกรม GX Developer ซึ่งได้แสดงไว้ในภาพที่ 5.3



ภาพที่ 5.1 แสดงหน้าจอขณะ Login เข้าสู่ระบบ บนเครื่องคอมพิวเตอร์ Notebook

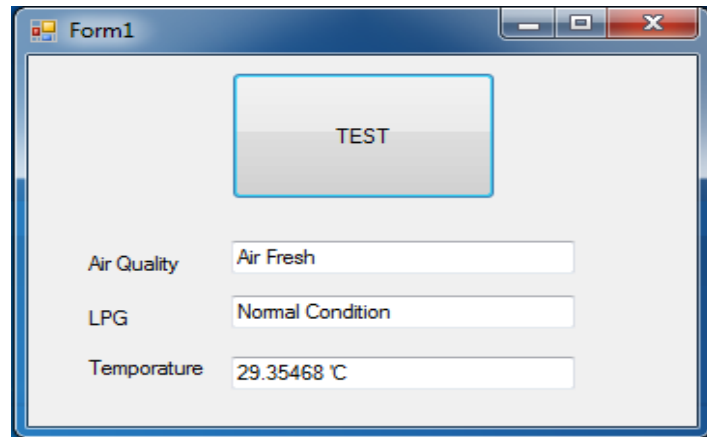


ภาพที่ 5.2 แสดงหน้าจอผลลัพธ์การเข้าสู่ระบบ เมื่อทำการ Login ได้สำเร็จ



ภาพที่ 5.3 แสดงการทดสอบการอ่านข้อมูลจาก PLC ด้วยโปรแกรม GX Developer

นอกจากการใช้โปรแกรม GX Developer แล้ว ยังสามารถใช้โปรแกรมที่พัฒนาขึ้นมาเอง
สั่งให้ Sensor Board ทำการเก็บค่าตัวอย่างของ อุณหภูมิ คุณภาพของอากาศ และ ระดับของก๊าซ
LPG บริเวณจุดที่ติดตั้ง Sensor Board โดยแสดงตัวอย่างของค่าที่ได้จาก Sensor ดังภาพที่ 5.4

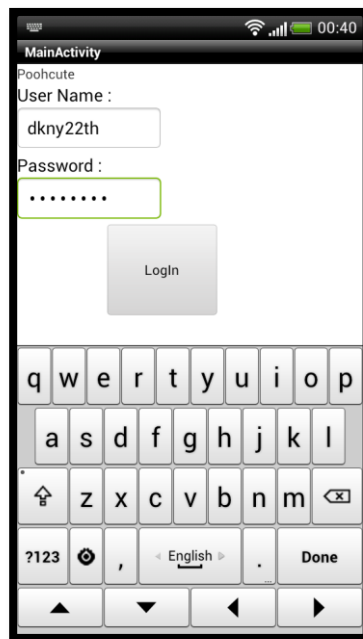


Form1	
TEST	
Air Quality	Air Fresh
LPG	Normal Condition
Temperature	29.35468 °C

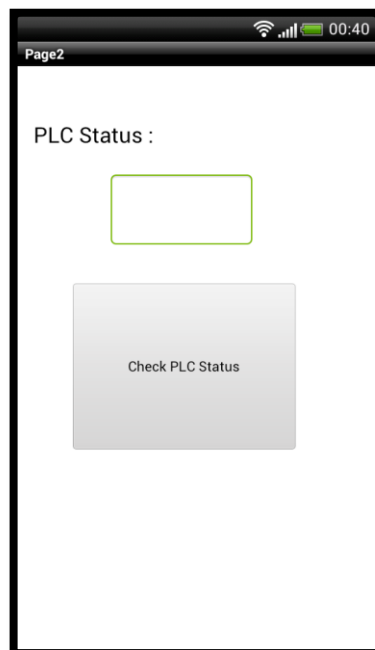
ภาพที่ 5.4 แสดงหน้าจอผลของค่าที่ได้จาก Sensor Board

5.2 ผลการทดลองจากโทรศัพท์เคลื่อนที่

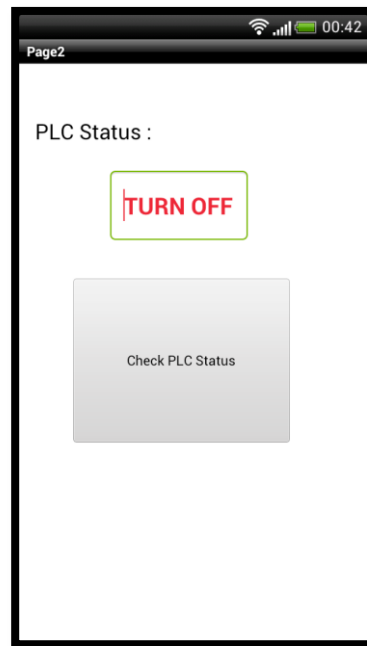
ในส่วนของการทดสอบระบบควบคุมที่พัฒนาขึ้นบนโทรศัพท์เคลื่อนที่ พบว่าสามารถใช้
โทรศัพท์เคลื่อนที่เพื่อ Login เข้าระบบและตรวจสอบสถานะของ PLC ผ่านเครือข่ายอินเทอร์เน็ต
และได้ผลลัพธ์ที่ตอบกลับมาได้อย่างถูกต้อง โดยมีส่วนของการทำงาน ดังนี้



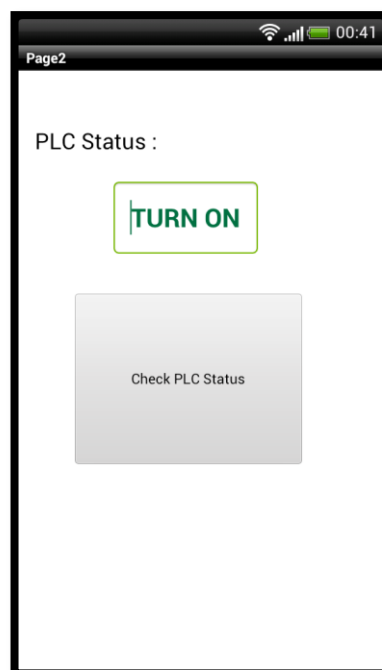
ภาพที่ 5.5 แสดงขั้นตอนการ Login จากโปรแกรมที่พัฒนาขึ้นบน Android



ภาพที่ 5.6 แสดงส่วนการตรวจสอบสถานะของ PLC หลังจากที่ทำกร Login เรียบร้อยแล้ว



ภาพที่ 5.7 แสดงผลลัพธ์การตรวจสอบสถานะของ PLC ซึ่งกำลังทำงานอยู่ในโหมด STOP



ภาพที่ 5.8 แสดงผลลัพธ์การตรวจสอบสถานะของ PLC ซึ่งกำลังทำงานอยู่ในโหมด RUN

ผลการทดลองของการทดลองใช้โมโครคอนโทรลเลอร์ในการ Generate Keystream แบบ MD5 โดยมี Initial Vector รวมกับ Key เป็นความยาว 51 ตัวอักษร ใช้เวลาเฉลี่ย 1,440 microsecond สำหรับเวลาเฉลี่ยที่ GATEWAY และ BACK OFFICE ใช้ในการทำงานทั้งหมดในฝั่ง Factory Site มีดังตารางที่ 5.1 ดังนี้

ตารางที่ 5.1 แสดงเวลาเฉลี่ยที่ดำเนินไปของการทำงานในแต่ละขั้น

สถานะการทำงาน	เวลาที่ดำเนินไป (microsecond)
พร้อมรับ TCP/IP Packet จาก Secure Port	
รับ HMAC จาก Remote Site	0 - 372
รับ Encode Data จาก Remote Site	372 - 774
Generate Key stream เพื่อใช้ Decode ในฝั่ง Factory Site แบบ MD5 โดยใช้ IV+KEY ขนาด 51 อักขร	774 - 2294
Generate HMAC ของฝั่ง Factory Site แบบ MD 5 โดยใช้ IV+KEY ขนาด 33 ตัวอักษร เพื่อใช้เปรียบเทียบ	2294 - 3746
ตรวจ message Integrity ของ HMAC ที่รับเข้ามาจาก Remote Site กับที่ Generate ขึ้นใน Factory Site ด้วยการ XOR กัน	3746 - 3866
ถอดรหัสข้อมูลที่ได้รับจาก Remote Site ด้วยการ XOR กับ Key stream	3866 - 4116

สำหรับเวลาเฉลี่ยที่ใช้ในการส่งงานจากภายในโรงงาน โดยทดสอบด้วยการส่งงานจากโทรศัพท์เคลื่อนที่ซึ่งเชื่อมเข้ากับเครือข่ายอินเทอร์เน็ตภายในโรงงานด้วยระบบไร้สายแบบ Wi-Fi ภายในโรงงาน ใช้เวลาตั้งแต่กดส่งงานบนโทรศัพท์จนได้ผลลัพธ์ตอบกลับมานบนหน้าจอโทรศัพท์ โดยทดลองซ้ำ 30 ครั้ง ใช้เวลาเฉลี่ย 2:30 วินาที

เวลาเฉลี่ยที่ระบบนี้ใช้ในการทำงานจริงในการทดสอบแบบระยะไกล โดยทดสอบด้วยการส่งงานจาก Remote Site ด้วยโทรศัพท์เคลื่อนที่ซึ่งเชื่อมเข้ากับเครือข่ายอินเทอร์เน็ตด้วยเครือข่าย 3G โดยผู้ให้บริการคือ TOT ไปยังระบบในฝั่ง Factory Site โดยจับเวลาตั้งแต่กดส่งงานบนโทรศัพท์ จนถึงได้ผลลัพธ์ตอบกลับมายังหน้าจอโทรศัพท์ ทดลองซ้ำ 30 ครั้ง ใช้เวลาเฉลี่ย 4:41 วินาที

บทที่ 6

บทสรุป

6.1 สรุปผลการวิจัย

งานวิจัยนี้เสนอแนวคิดของระบบที่สามารถควบคุม PLC และติดตามสถานะของ Sensor จากระยะไกล ทั้งจากคอมพิวเตอร์ Notebook และ โทรศัพท์เคลื่อนที่ โดยนำเสนอแนวคิดของการแปลงรูปแบบคำสั่งให้ส่งผ่านอินเทอร์เน็ตได้ การจัดการระบบแบบ Multi User และแนวคิดด้านการจัดการความมั่นคงปลอดภัยของระบบ โดยระบบที่ Implement ขึ้นตามแนวคิดนี้สามารถเพิ่มประสิทธิภาพและความสะดวกในการใช้งาน PLC โดยไม่ต้องจำกัดระยะทางของเครื่องควบคุมด้วยสายเคเบิลอีกต่อไป

ผลการวิจัยที่ได้จากการทดลอง Implement ระบบขึ้นจริงพบว่า ระบบสามารถทำงานได้อย่างถูกต้อง เชื่อถือได้ เนื่องจากมีการควบคุมด้านความถูกต้องของการส่งข้อมูลทั้งระบบ โดยการรับส่งข้อมูลระยะไกลแบบไร้สายในโรงงานจะถูกควบคุมความถูกต้องด้วย Zigbee Protocol Stack ส่วนการรับส่งข้อมูลระยะไกลระหว่างอินเทอร์เน็ต จะควบคุมความถูกต้องด้วย TCP/IP Protocol Suit

สำหรับปัจจัยที่มีผลให้ความเร็วในการตอบสนองของระบบในฝั่ง Remote Site มีความแตกต่างกันออกไปก็คือ ประสิทธิภาพและความหนาแน่นของเครือข่ายอินเทอร์เน็ตที่มีความแตกต่างกันออกไปในแต่ละพื้นที่ ส่วนประสิทธิภาพของระบบที่ทำงานอยู่ในฝั่ง Factory Site นั้นขึ้นอยู่กับความเหมาะสมของการเลือกใช้อุปกรณ์ที่ใช้ Implement ในส่วน GATEWAY และ BACK OFFICE เป็นสำคัญ

ประโยชน์ที่สำคัญอีกประการของระบบนี้คือสามารถนำไปปรับใช้ควบคุมอุปกรณ์อื่นๆ ที่ใช้การเชื่อมต่อแบบ Serial Interface ได้ทันที

สำหรับข้อจำกัดของระบบที่พัฒนาขึ้นคือ ระบบนี้ถูกออกแบบมาให้ใช้ควบคุมอุปกรณ์ที่ใช้การเชื่อมต่อแบบ Serial Interface เท่านั้น

6.2 ข้อเสนอแนะ

เพื่อให้กระบวนการ Authentication เข้าระบบของผู้ใช้ครบถ้วนสมบูรณ์ตามหลัก Challenge-Response จึงควรเพิ่มกระบวนการ Response กลับจากผู้ใช้ไปยัง GATEWAY เมื่อทำการป้อน Password แล้วด้วย โดยอาจกำหนดให้ GATEWAY สร้าง Random Number ขึ้นมาอีกค่าหนึ่ง แล้วส่งไปพร้อมกับ Session Key ด้วย เมื่อผู้ใช้ถอดรหัสได้ Session Key และ Random Number ที่ถูกต้องนี้ได้ ก็ส่ง Random Number กลับมาเพื่อให้ GATEWAY ตรวจสอบความถูกต้อง โดยถ้าตรวจสอบแล้วพบว่าผู้ใช้ได้ Random Number ที่ไม่ถูกต้อง ก็สามารถปฏิเสธการ Login ในครั้งนั้นได้ทันที แล้วทำการคืนทรัพยากรทั้งหมดให้กับระบบ ทำให้ระบบมีการรักษาความปลอดภัยที่รัดกุมยิ่งขึ้น

เพื่อให้ระบบมีการรักษาความปลอดภัยที่ดียิ่งขึ้นในการทำงานแบบหลายผู้ใช้หลายอุปกรณ์ จึงควรมีการกำหนดสิทธิการใช้อุปกรณ์ของผู้ใช้แต่ละคนตามความเหมาะสมกับขอบเขตงานที่รับผิดชอบ

ในกรณีที่การรักษาความปลอดภัยในการควบคุมเป็นสิ่งสำคัญ ควรเลือกใช้การพัฒนาส่วน Data Converter ที่ใช้บนคอมพิวเตอร์ Notebook ขึ้นเอง เนื่องจากการเลือกใช้ Virtual Serial Port ที่มีขายในท้องตลาดนั้นจะทำให้ไม่สามารถเพิ่มส่วนการเข้ารหัสและเช็คความถูกต้องของข้อมูลด้วย HMAC เข้าไปได้ แต่ถ้าพัฒนาส่วน Virtual Serial Port ขึ้นเองก็จะสามารถนำผลลัพธ์จาก Virtual Serial Port ไปผ่านกระบวนการรักษาความปลอดภัยตามที่ได้กำหนดไว้ได้อย่างครบถ้วนสมบูรณ์

สิ่งที่ต้องคำนึงถึงในการนำระบบนี้ไปประยุกต์ใช้ คือ รูปแบบของการเกิด Time out และเวลาที่กำหนดให้เป็น Time out ของแต่ละชุดโปรแกรมควบคุมกับอุปกรณ์ที่ถูกควบคุมจะแตกต่างกันออกไป ดังนั้นจึงควรที่จะศึกษารูปแบบและระยะเวลาการเกิด Time out ของอุปกรณ์ที่ต้องการควบคุมอย่างละเอียด เพื่อปรับจังหวะการส่งผ่านข้อมูลจากโปรแกรมที่ใช้ควบคุมไปยังอุปกรณ์ได้อย่างมีประสิทธิภาพ รวมถึงในการพัฒนาระบบเพื่อใช้จริง ควรพิจารณาความสามารถของอุปกรณ์ที่นำมาพัฒนาในแต่ละส่วน ว่าสามารถรองรับภาระงานที่เกิดขึ้นได้เพียงพอตามความต้องการใช้งานหรือไม่

บรรณานุกรม

- About El-Ela, M. and Alkanhel, M.. 2007. Bluetooth Based Telemetry/ PLC system. In **AEIC'2007 Al-Azhar Engineering Ninth International Conference**. Cairo: [S.n.].
- Android Developers. 2013. **Building and Running**. Retrieved July 18, 2013 from <http://developer.android.com/tools/building/index.html>
- Android Open Source Project. 2013. **Porting Android to Devices**. Retrieved July 1, 2013 from <http://source.android.com/devices/index.html>
- Arduino.cc . 2012. **Arduino ADK**. Retrieved Mar 22, 2012 from <http://arduino.cc/en/Main/ArduinoBoardADK>
- Forouzan, Behrouz A. 2007. **Data Communications and Networking**. New York: McGraw-Hill.
- Digi International. 2007. **XBee™ Series 2 OEM RF Modules**. Retrieved Aug 15, 2012 from <http://docs-europe.origin.electrocomponents.com/webdocs/0b04/0900766b80b04c09.pdf>
- Digi International. 2008. **XBee®/XBee-PRO® OEM RF Modules**. Retrieved May 16, 2012 from ftp://ftp1.digi.com/support/documentation/90000982_A.pdf
- Hui, Li and Jing, Zhang. 2011. Study on Remote PLC Experiment System Based on Web. In **Mechanic Automation and Control Engineering**. Hohhot: [S.n.]. Pp.1683-1686.
- Gill, Khusvinder; Shuang-Hua, Yang; Fang, Yao and Xin, Lu. 2009. A zigbee-based home automation system. **IEEE Transactions on Consumer Electronics**. 55(May): 422-430.
- Li, Pengfei and Li, Jiakun. 2009. Application of Communication and Remote Control in PLC Based on ZigBee. **Computational Intelligence and Security**. 2(Dec): 533-536.
- Stallings, William. 2003. **Cryptography and network security : principles and practice**. New Jersey: Prentice Hall.
- Wikipedia. 2013. **IEEE 802.15.4**. Retrieved May 5, 2013 from https://en.wikipedia.org/wiki/IEEE_802.15.4
- Wikipedia. 2013. **ZigBee**. Retrieved JUNE 23, 2013 from <http://en.wikipedia.org/wiki/ZigBee>

Zigbee Alliance. 2013. **ZigBee FAQ**. Retrieved May 2, 2013 from <http://www.zigbee.org/About/FAQ.aspx>

ประวัติผู้เขียน

ชื่อ ชื่อสกุล

นายพูนศักดิ์ ทรัพย์เพิ่มพูน

ประวัติการศึกษา

ศิลปศาสตรบัณฑิต (สารสนเทศศึกษา)
มหาวิทยาลัยรามคำแหง พ.ศ. 2553

ประสบการณ์ทำงาน

เข้าร่วมนำเสนอผลงานวิจัยในการประชุมทาง
วิชาการระดับชาติด้านคอมพิวเตอร์และ
เทคโนโลยีสารสนเทศ ครั้งที่ 9 ณ มหาวิทยาลัย
เทคโนโลยีพระจอมเกล้าพระนครเหนือ