สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัยในหมู่บ้าน

NETWORK SYSTEM FOR VILLAGE SECURITY SYSTEM

โดย

นายคมสันต์ ประพันธเทวา

นายจตุเดช วิวัฒน์สมวงศ์

อาจารย์ที่ปรึกษา

รศ.สมศักดิ์ มิตะถา

อ.อวัชริน นาชิน

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2545

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เลขหมู่.....
เลขทะเบียน 49915
วัน,เดือน,ปี 2 เม.ย. 2547

.b.....
.i.....

ปริญญานิพนธ์ ปีการศึกษา 2545

ภาควิชาคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัยในหมู่บ้าน

NETWORK SYSTEM FOR VILLAGE SECURITY SYSTEM

คณะผู้จัดทำ นายคมสันต์ ประพันธเทวา รหัส 42010041

นายจตุเดช วิวัฒน์สมวงศ์ รหัส 42010045

.....อาจารย์ที่ปรึกษา

(รศ.สมศักดิ์ มิตะถา)

.....อาจารย์ที่ปรึกษา

(อ.อวัชริน นาชิน)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบเครือข่ายสำหรับระบบรักษาความปลอดภัยในหมู่บ้าน

นายคมสันต์ ประพันธเทวา 42010041
นายจตุเดช วิวัฒน์สมวงศ์ 42010045
รศ.สมศักดิ์ มิตะถา อาจารย์ที่ปรึกษา
อ.อวัชริน นาชิน อาจารย์ที่ปรึกษา
ปีการศึกษา 2545

บทคัดย่อ

ปริญญานิพนธ์ฉบับนี้ เป็นการออกแบบระบบเครือข่ายสำหรับระบบรักษาความปลอดภัยในหมู่บ้านซึ่งเป็นการนำไมโครคอมพิวเตอร์และ ไมโครคอนโทรเลอร์ มาทำหน้าที่ในการรับและส่งข้อมูลผ่านเครือข่ายแบบอนุกรมอ้างอิงมาตรฐานRS-485 โดยเป็นระบบเครือข่ายที่มีคุณสมบัติคือ มีความรวดเร็วและมีประสิทธิภาพในการรับและส่งข้อมูล มีความปลอดภัยของข้อมูล และ มีความน่าเชื่อถือ โดยทำการออกแบบกระบวนการรับและส่งข้อมูล มีการควบคุมการไหลของข้อมูล (Flow control) มีเฟรมข้อมูลที่กระชับและรองรับการทำงานที่ต้องการได้ครบถ้วน และได้นำกระบวนการปกปิดข้อมูลโดยใช้อัลกอริทึมแบบ DES (Data Encryption Standard) มาประยุกต์ใช้บนไมโครคอมพิวเตอร์ และไมโครคอนโทรเลอร์ นอกจากนั้นยังมีการรับประกันข้อมูลว่าไปถึงผู้รับหรือไม่อย่างไร โดยการใช้เฟรมการตอบรับสัญญาณ (Acknowledge) และการทำช่วงเวลาการตอบรับสัญญาณ (Request time)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Network System for Village Security System

Mr. Komsan Prapantathewa
Mr. Jatudate Wiwatsomwong
Assoc.Prof. Somsak Mitatha Advisor
Mr. Awacharin Nachin Advisor

ABSTRACT

This thesis is a designing of network system for village security system which microcomputers and microcontrollers are applied for transmitting and receiving data over standard serial network, RS-485. The advantages of this network are having high quality of speed, performance, security and reliability of data transmission. We designed a new data transmission protocol which has a qualified flow control and the data frame is designed to be compact and versatile. DES (Data Encryption Standard) algorithm is applied to microcomputers and microcontrollers for data encryption and decryption. To ensure that the data is received by the receiver, the acknowledge frame and request time interval is also implemented to this project.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้คงไม่อาจเสร็จได้ด้วยดี หากไม่ได้รับความช่วยเหลือ และร่วมมือจากหลายๆ ฝ่าย ด้วยกัน บุคคลแรกที่ต้องกล่าวถึงเพราะเป็นส่วนสำคัญที่ทำให้วิทยานิพนธ์นี้เสร็จลงได้ก็คือรศ.สมศักดิ์ มิตะถา และ อาจารย์ อวัชริน นาชิน อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ให้ความเอาใจใส่ แนะนำ และช่วยเหลือเสมอมา ซึ่งต้องขอขอบพระคุณเป็นอย่างมาก

ขอขอบคุณเพื่อนๆ พี่ๆ น้องๆ ที่คอยให้ความช่วยเหลือ และต้องขอขอบพระคุณบุคคลสำคัญที่สุดที่ทำให้ข้าพเจ้ามีวันนี้ ก็คือ บิดา มารดา อันเป็นที่เคารพรักยิ่ง ซึ่งได้เลี้ยงดูผู้เขียนมาเป็นอย่างดี พร้อมทั้งให้โอกาสในการศึกษาอย่างเต็มที่ และยังให้กำลังใจ เอาใจใส่เสมอมา ในทุกๆ ด้านอันหาที่เปรียบมิได้ ข้าพเจ้าขอระลึกในพระคุณอันสุดประมาณ และขอกราบขอบพระคุณมา ณ ที่นี้

จตุเดช วิวัฒน์สมวงศ์
คมสันต์ ประพันธเทวา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่1
บทนำ

1.1 ความสำคัญและที่มา

ในปัจจุบันสภาพความเป็นอยู่โดยเฉพาะผู้ที่อาศัยอยู่ในเมืองใหญ่ๆจะพบว่าทั้งหัวหน้าครอบครัวและแม่บ้านจะต้องออกไปทำงานนอกบ้าน ดังนั้นจึงใช้เวลาส่วนใหญ่อยู่นอกบ้านเป็นหลัก จึงเป็นการง่ายต่อการถูกโจรกรรมของมิจฉาชีพหรืออุบัติเหตุต่างๆที่อาจจะเกิดขึ้น เช่นไฟไหม้ เป็นต้น นอกจากนั้นบ้านแบบที่เป็นหมู่บ้านซึ่งมีบ้านเป็นจำนวนมากก็ยิ่งเสี่ยงต่ออุบัติภัย หรือการดูแลได้ไม่ทั่วถึงของเจ้าหน้าที่ ดังนั้น ระบบรักษาความปลอดภัยซึ่งทำงานได้ตลอดเวลาจึงสามารถที่จะป้องกันหรือลดโอกาสที่จะถูกเหตุการณ์ต่างๆที่ไม่คาดฝันเหล่านั้นได้

ระบบรักษาความปลอดภัยในหมู่บ้านได้รับการพัฒนามาอย่างต่อเนื่อง ระบบจะทำงานทั้งแบบเดี่ยว (Stand Alone) และแบบเครือข่าย (Network) โดยหลักการนั้นคือ เมื่อมีเหตุผิดปกติเกิดขึ้นในบ้าน ระบบรักษาความปลอดภัยที่อยู่ในบ้านจะทำการส่งสัญญาณเตือนภัยไปสองส่วนคือ ส่วนหนึ่งส่งไปยังส่วนควบคุมภายในบ้านให้ทำการร้องเตือนภัย หรือการหมุนโทรศัพท์ไปแจ้งเหตุผิดปกติ ในขณะที่อีกส่วนหนึ่งส่งไปยังศูนย์รักษาการผ่านระบบเครือข่ายภายใน (Area Network) และแสดงผลบนเครื่องคอมพิวเตอร์ ทำให้เจ้าหน้าที่รักษาความปลอดภัยสามารถทราบความผิดปกติได้ทันที

ดังนั้น จะเห็นได้ว่า ระบบเครือข่าย ซึ่งเป็นส่วนเป็นทางผ่านของข้อมูลระหว่างศูนย์ควบคุมหลักกับวงจร เป็นส่วนที่มีความสำคัญต่อระบบโดยรวมเป็นอย่างยิ่ง ถ้าหากระบบเครือข่ายขาดความปลอดภัยของข้อมูล หรือขาดระบบการจัดการข้อมูลที่ดี ระบบโดยรวมก็ถือว่าไม่มีประสิทธิภาพเช่นกัน

โครงงานระบบเครือข่ายสำหรับระบบรักษาความปลอดภัยในหมู่บ้าน เป็นโครงงานเพื่อพัฒนาระบบเครือข่ายสำหรับการควบคุมและตรวจสอบข้อมูลสำหรับระบบรักษาความปลอดภัยในหมู่บ้าน เป็นการออกแบบระบบเครือข่ายสำหรับระบบรักษาความปลอดภัยในหมู่บ้านซึ่งเป็นการนำไมโครคอมพิวเตอร์และ ไมโครคอนโทรเลอร์ มาทำหน้าที่ในการรับและส่งข้อมูล ผ่านเครือข่ายแบบอนุกรมอ้างอิงมาตรฐานRS-485 โดยเป็นระบบเครือข่ายที่มีคุณสมบัติคือ มีความรวดเร็วและมีประสิทธิภาพในการรับและส่งข้อมูล มีความปลอดภัยของข้อมูล และ มีความน่าเชื่อถือ โดยทำการออกแบบกระบวนการรับและส่งข้อมูลที่สั้นมีการควบคุมการไหลของข้อมูล(Flow control) มีเฟรมข้อมูลที่กระชับและรองรับการทำงานที่ต้องการได้ครบถ้วน และนำกระบวนการปกปิดข้อมูลโดยใช้อัลกอริทึมแบบ DES(Data Encryption Standard)มาประยุกต์ใช้บนไมโครคอมพิวเตอร์และไมโครคอนโทรเลอร์ และทำการออกแบบเฟรมการตอบรับสัญญาณ(Acknowledge) การทำช่วงเวลาการตอบรับสัญญาณ (Request time) เพื่อให้ทราบได้ว่าข้อมูลที่ส่งไปไปถึงผู้รับหรือไม่อย่างไร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

เนื่องจากในปัจจุบัน มีการนำไมโครคอนโทรเลอร์มาใช้ในงานควบคุมและรับข้อมูลจากอุปกรณ์ต่างๆเป็นจำนวนมาก ซึ่งส่วนใหญ่ระบบเครือข่ายและกระบวนการรับ-ส่งข้อมูลจะถูกออกแบบโดยปราศจากการรักษาความปลอดภัยของข้อมูลบนเครือข่าย และ ขาดการออกแบบกระบวนการรับ-ส่งข้อมูล (Protocol) ที่ดี

ดังนั้น วัตถุประสงค์ของการศึกษาก็เพื่อ ออกแบบระบบเครือข่าย และรูปแบบการรับ-ส่งข้อมูล ที่มีประสิทธิภาพโดยมีคุณสมบัติดังต่อไปนี้

1.2.1 ความเชื่อถือได้และความถูกต้องของข้อมูล(Reliable & Integrity) ด้วยการออกแบบและปรับปรุงระบบการรับ-ส่งข้อมูล เพิ่มเติมการตอบสนอง(Acknowledge)ให้กับอุปกรณ์

1.2.2 ระบบที่มีความปลอดภัยของข้อมูล(Security) ด้วยการศึกษาถึงกระบวนการปกปิดข้อมูล (Cryptography)ในรูปแบบต่างๆ โดยพิจารณาถึงความเหมาะสมที่จะนำมาใช้ประมวลผลในไมโครคอนโทรเลอร์MCS-51 แล้วนำมาใช้กับโครงงานนี้

1.2.3 ระบบที่มีการทำงาน การตอบสนองที่รวดเร็ว(Response) ศึกษามาตรฐานการรับ-ส่งข้อมูลที่สั้น กระชับ และสามารถรองรับการทำงานที่ต้องการได้ แล้วนำมาประยุกต์ใช้กับโครงงานนี้

1. 3 ขอบเขตของโครงงาน

งานวิจัยชิ้นนี้จะทำการออกแบบระบบเครือข่าย และทำการสร้างระบบรักษาความปลอดภัยในหมู่บ้าน ซึ่งใช้ไมโครคอนโทรเลอร์MCS-51 ในการควบคุมการประมวลผล การรับและส่งข้อมูล โดยอ้างอิงมาตรฐาน RS-485 ทั้งนี้จะมีการเพิ่มเติมกระบวนการปกปิดข้อมูล และรูปแบบการรับ-ส่งข้อมูลที่รวดเร็วและเชื่อถือได้ เพื่อให้บรรลุตามวัตถุประสงค์ที่วางไว้ ผู้จัดทำจึงกำหนดขอบเขตของโครงงานคือ

1.3.1 การออกแบบ กระบวนการรับและส่งข้อมูล(Protocol) เพื่อใช้ในระบบรักษาความปลอดภัยในหมู่บ้าน

1.3.2 การออกแบบเฟรมข้อมูล การตอบรับข้อมูล และการควบคุมการไหลของข้อมูล

1.3.3 การนำกระบวนการเพื่อใช้ในการปกปิดข้อมูล โดยใช้อัลกอริทึมแบบ DES มาใช้บนไมโครคอนโทลเลอร์ MCS-51 และโปรแกรม

1.3.4 การเขียนโปรแกรม เพื่อใช้ในการแสดงผลและสั่งงานผ่านทางคอมพิวเตอร์

1.3.5 การทำเครือข่ายจำลองระบบการทำงาน โดยประยุกต์ใช้กับระบบรักษาความปลอดภัยในหมู่บ้าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.4 วิธีการดำเนินงาน

งานวิจัยนี้ เริ่มต้นด้วยการศึกษาองค์ประกอบต่างๆของระบบรักษาความปลอดภัยในหมู่บ้าน ได้แก่ การต่อวงจรฮาร์ดแวร์ การศึกษากระบวนการทำงานของโปรแกรมที่มีการเขียนไว้ รวมถึงกระบวนการรับ-ส่งข้อมูล และรูปแบบการทำงาน หลังจากนั้นจึงทำการศึกษาถึงปัญหาที่พบในระบบเดิมซึ่งบนปัญหาของระบบเครือข่ายดังที่กล่าวมาข้างต้น จึงทำการออกแบบรูปแบบการรับ-ส่งข้อมูล โดยอ้างอิงตาม มาตรฐาน ISO (Seven layers) การออกแบบวงจรฮาร์ดแวร์ซึ่งต้องศึกษาข้อมูลของอุปกรณ์ต่างๆ ได้แก่ MSC-51, MAX232, SN75176 และ MC14551

เมื่อได้โครงสร้างของอุปกรณ์ฮาร์ดแวร์ และทำการสร้างวงจรแล้ว ต่อไปจึงเป็นการศึกษาการเขียนโปแกรมสำหรับไมโครคอนโทรเลอร์ MCS-51 โดยใช้ภาษา C ซึ่งทำให้ง่ายต่อการพัฒนาโปรแกรม มีการเขียนควบคุมการรับ และส่งข้อมูล โดยในขั้นแรก จะทำการทดลองบนมาตรฐานแบบ RS-232 ก่อน เพราะง่ายต่อการตรวจเช็ค ทดสอบและหาข้อผิดพลาด เมื่อกระบวนการทำงานต่างๆ สามารถทำงานได้ตามวัตถุประสงค์แล้ว ก็ทำการทดลองบนมาตรฐานแบบ RS-485 โดยมีจำนวนของอุปกรณ์มากขึ้น ทำการออกแบบกระบวนการไหลของข้อมูลและลักษณะเฟรมข้อมูล เพื่อให้สามารถรองรับการทำงานอันได้แก่ การตรวจสอบสถานะ การสั่งงาน และการตอบรับสัญญาณเมื่อมีเหตุผิดปกติขึ้น เมื่อการรับและส่งข้อมูลเป็นไปตามที่ออกแบบไว้แล้ว จึงทำการเพิ่มเติมกระบวนการทำงานในส่วนของระบบความปลอดภัยบนเครือข่าย ได้แก่ การปกปิดข้อมูลโดยศึกษากระบวนการที่เป็นที่ยอมรับ และพิจารณาตามความเหมาะสมในการนำมาใช้กับไมโครคอนโทรเลอร์ ซึ่งได้เลือกการเข้ารหัสและถอดรหัสโดยใช้อัลกอริทึมแบบ DES มาใช้บนไมโครคอนโทรเลอร์และไมโครคอมพิวเตอร์

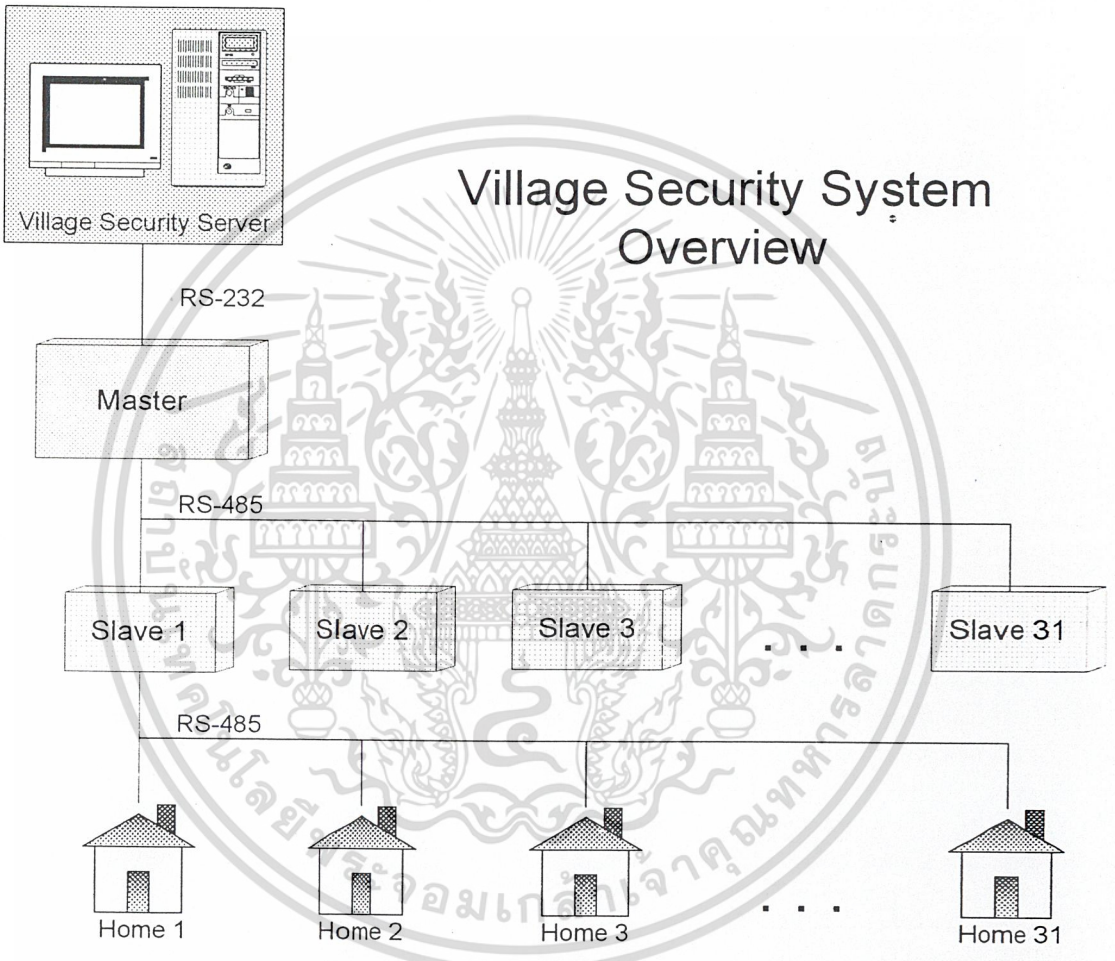
และในส่วนสุดท้าย คือส่วนควบคุมบนไมโครคอมพิวเตอร์ จะมีการเขียนโปรแกรมโดยใช้ MS Visual Basic เพื่อเป็นส่วนควบคุมและสั่งงาน โดยเชื่อมต่อกับฐานข้อมูลของ MS SQL Server เพื่อเพิ่มความปลอดภัยในการจัดเก็บข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่2

ภาพรวมของระบบรักษาความปลอดภัยในหมู่บ้าน

ระบบรักษาความปลอดภัยในหมู่บ้านโดยผ่านระบบเครือข่ายคอมพิวเตอร์ มีภาพรวมดังรูปที่ 2-1



รูปที่ 2-1 แสดงภาพรวมของระบบ

ระบบรักษาความปลอดภัยในหมู่บ้าน สามารถแบ่งได้เป็น 3 ส่วนใหญ่ๆ คือ

1. ส่วนระบบเครือข่าย(Network)
2. ส่วนของไมโครคอนโทรเลอร์และวงจรHardware
3. ส่วนแสดงผลและสั่งงานบนไมโครคอมพิวเตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1 ส่วนระบบเครือขาย (Network)

ระบบเครือข่ายของโครงงานนี้ อ้างอิงตามมาตรฐานของ RS-485 เนื่องจากมีความเหมาะสมที่สุด เพราะ ข้อกำหนดของมาตรฐาน RS-485 จะสามารถต่ออุปกรณ์ที่เป็นตัวรับและตัวส่ง (Device) ได้มากถึง 32 ตัวภายใน 1 คู่สายสัญญาณ นอกจากนั้นยังสามารถรับส่งข้อมูลได้เป็นระยะทางไกลสูงสุดถึง 4000 ฟุต

การทำงานของระบบ เป็นการทำงานแบบ 2 ระดับแบบ แม่ลูก (Master/Slave) นั่นคือ ความสามารถในการรองรับจำนวนของอุปกรณ์ที่เป็นตัวรับและตัวส่งจะได้มากถึง 31*31 = 961 ตัว ทั้งนี้ ข้อมูลที่อยู่บนระบบเครือข่ายจะเป็นข้อมูลที่ถูกเข้ารหัส ด้วยกระบวนการแบบ Data Encryption Standard(DES) เพื่อเพิ่มความปลอดภัยของข้อมูลบนเครือข่าย

2.2 ส่วนระบบไมโครคอนโทรเลอร์

ระบบใช้วงจรซึ่งควบคุมโดยไมโครคอนโทรเลอร์(MCS) มีรายละเอียดของวงจรต่างๆคือ

2.2.1 วงจร Master ใช้ไมโครคอนโทรเลอร์ตระกูล MCS-51 เป็นส่วนประมวลผล โดยต่อกับ Multiplexer MC14551 เพราะต้องการเชื่อมต่อกับ MAX232 ให้สามารถติดต่อกับไมโครคอมพิวเตอร์ผ่านพอร์ทอนุกรม (Serial port) และต่อกับ SN75176 เพื่อให้สามารถติดต่อกับวงจรในระดับ Slave แบบอนุกรมอ้างอิงมาตรฐานแบบ RS-485 ทำหน้าที่ในการเป็นส่วนเชื่อมต่อระหว่าง RS-232 และ RS-485

2.2.2 วงจร Slave ใช้ไมโครคอนโทรเลอร์ตระกูล MCS-51 โดยต่อกับ Multiplexer MC14551 เพราะต้องการเชื่อมต่อกับ SN75176 จำนวน 2 ชุด เพื่อให้สามารถติดต่อกับวงจรในระดับ Master และ Slave แบบอนุกรมอ้างอิงมาตรฐานแบบ RS-485 ทำหน้าที่ในการรับข้อมูล และส่งข้อมูลต่อไปยัง วงจร Home

2.2.3 วงจร Home ใช้ใช้ไมโครคอนโทรเลอร์ตระกูล MCS-55wd เป็นส่วนประมวลผล โดยเชื่อมต่อกับ Multiplexer SN74LS42N ซึ่งทำหน้าที่ในการขยายพอร์ทในการควบคุมอุปกรณ์รับและส่งสัญญาณ โดยเชื่อมต่อกับ Dip-Switchซึ่งเป็นเหมือนอุปกรณ์ส่งข้อมูล และเชื่อมต่อกับไดโอดเปล่งแสง (LED)ซึ่งเป็นเหมือนอุปกรณ์รับข้อมูล และเชื่อมต่อกับหน่วยความจำขนาด 32 กิโลไบต์ UT62256CPC เพราะไมโครคอนโทรเลอร์จะถูกโปรแกรมกระบวนการเข้าและถอดรหัสแบบDES ซึ่งต้องใช้หน่วยความจำในการประมวลผลเกินกว่าที่มีใน MCS-55 โดยหน้าที่ของวงจรนี้คือการตรวจสอบสถานะของอุปกรณ์ไฟฟ้า และรับข้อมูลความผิดปกติจากอุปกรณ์ตรวจจับ เพื่อแจ้งไปยังศูนย์ควบคุมหลัก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

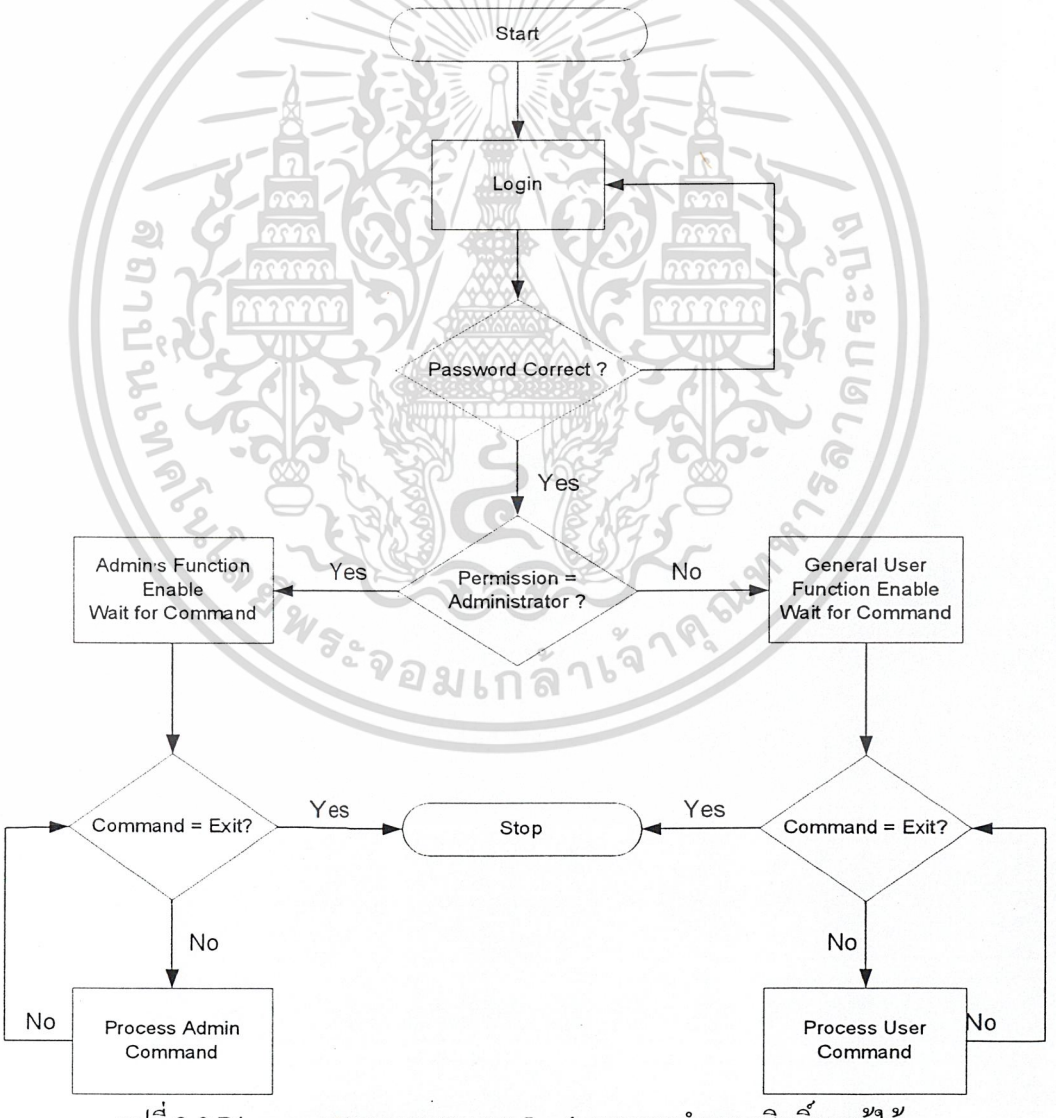
2.3 ส่วนแสดงผลและสั่งงานบนไมโครคอมพิวเตอร์

ส่วนแสดงผลและสั่งงาน ใช้โปรแกรม MS Visual Basic ในการทำส่วนติดต่อกับผู้ใช้ (User Interface) โดยกำหนดสิทธิในการใช้โปรแกรม (Permission) ตามประเภทของผู้ใช้ โดยจะต้องทำการ Login เข้าสู่โปรแกรมก่อน สำหรับประเภทของผู้ใช้แบ่งเป็น

2.3.1 ผู้ใช้ทั่วไป (General User) สามารถตรวจสอบสถานะของอุปกรณ์ต่างๆที่เชื่อมต่อบนระบบเครือข่าย เช่น สถานะของอุปกรณ์ไฟฟ้าต่างๆภายในบ้าน หรือการสั่งเปิด-ปิดอุปกรณ์ไฟฟ้า

2.3.2 ผู้ดูแลระบบ (Administrator) สามารถใช้งานได้เหมือนผู้ใช้ทั่วไป และยังสามารถเพิ่มเติมหรือแก้ไขข้อมูล เช่น ลดจำนวนบ้านในระบบเครือข่าย แก้ไขรายละเอียดของระบบ เป็นต้น

ทั้งนี้ การกำหนดสิทธิ์ของโปรแกรม จะขึ้นอยู่กับประเภทของผู้ใช้ และข้อมูลชื่อผู้ใช้และรหัสผ่าน จะถูกจัดเก็บอยู่ในฐานข้อมูลบนโปรแกรม MS SQL Server เพื่อความปลอดภัยของข้อมูล แสดงได้ดังรูป



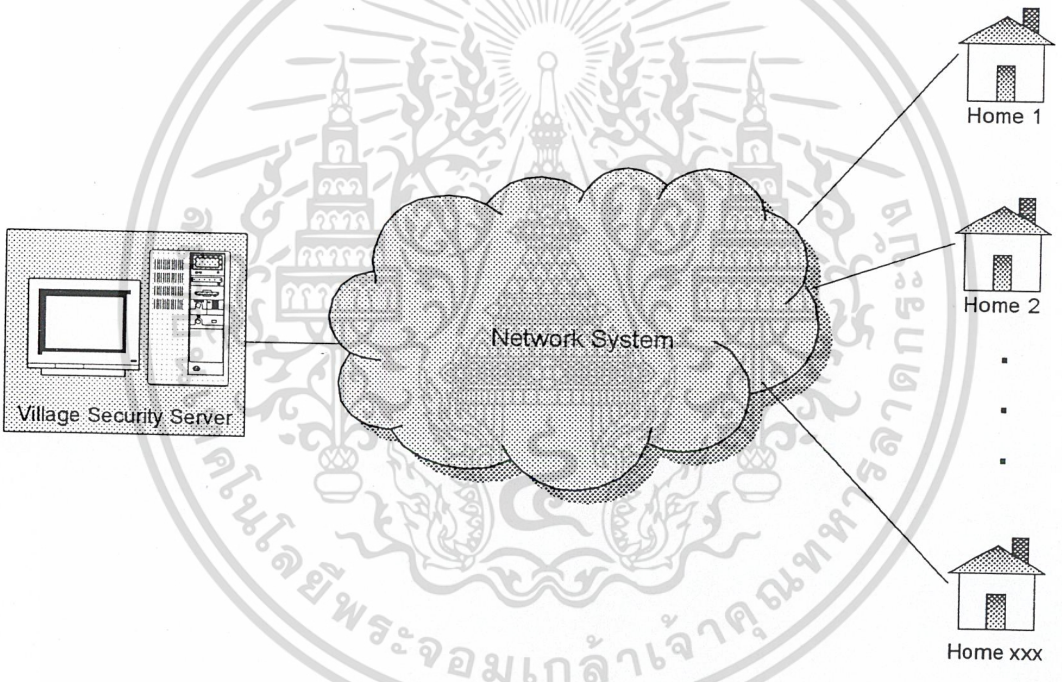
รูปที่ 2-2 Diagram แสดงกระบวนการ Loginและการกำหนดสิทธิ์ของผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
ระบบเครือข่าย

3.1 ภาพรวมของระบบเครือข่าย

ระบบรักษาความปลอดภัยในหมู่บ้านมีลักษณะการทำงานโดยทั่วไปคือ ในแต่ละบ้านจะมีไมโครคอนโทรเลอร์เพื่อใช้ในการตรวจจับสัญญาณจาก Sensor และนอกจากนั้นยังส่งสัญญาณเตือนภัยไปยังศูนย์รักษาความปลอดภัยของหมู่บ้าน โดยผ่านระบบเครือข่าย ขณะเดียวกัน ศูนย์รักษาความปลอดภัย ก็ยังสามารถตรวจสอบสถานะต่างๆของบ้านแต่ละหลังในหมู่บ้าน ผ่านระบบเครือข่ายเดียวกันนี้ได้ โดยที่รูปแบบของการติดต่อตามหลักการมีลักษณะดังรูปที่ 3-1



รูปที่ 3-1 แผนผังเครือข่ายในอุดมคติ

จากรูปที่ 3-1 มีการกำหนดให้มีการวางสายส่งข้อมูลไปยังบ้านแต่ละหลังมีเพียง 1 คู่เท่านั้น ทั้งนี้เนื่องจากการนำไปใช้กับระบบหมู่บ้าน ซึ่งบ้านแต่ละหลังมีระยะห่างที่ไกลจากศูนย์รักษาความปลอดภัยมาก การใช้สายส่งข้อมูลเพียง 1 คู่ ก็เพื่อประหยัดค่าใช้จ่าย มีความสะดวกในการติดตั้งใช้งานและสามารถทำงานได้ครบถ้วนถูกต้อง

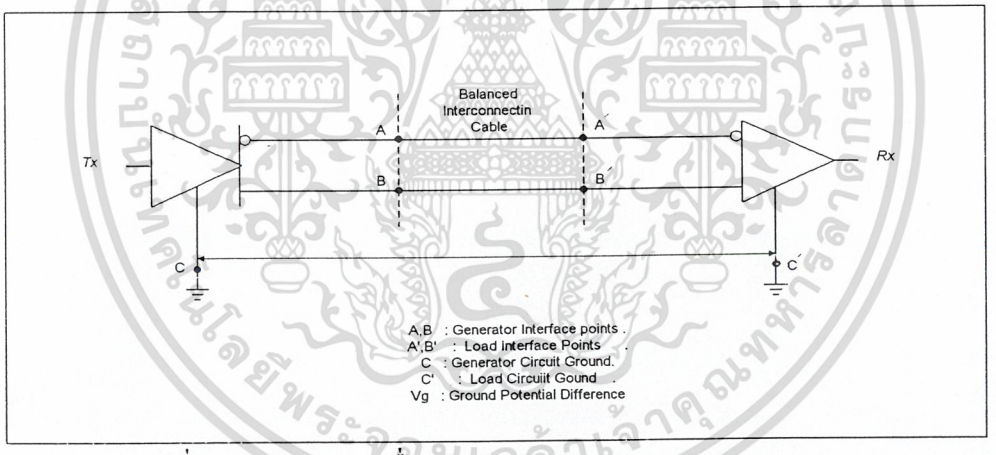
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2 มาตรฐานการรับ-ส่งสัญญาณในเครือข่าย

การพิจารณามาตรฐานการรับ-ส่งสัญญาณ ต้องพิจารณาจากเงื่อนไข ความเหมาะสมของการนำมาใช้ เนื่องจากการเชื่อมต่อของอุปกรณ์เป็นแบบอนุกรม การพิจารณาขั้นแรกจึงมุ่งเน้นที่การรับ-ส่งสัญญาณข้อมูลแบบอนุกรมในโหมดอะซิงโครนัส ซึ่งมีด้วยกันหลายมาตรฐาน คือ RS-232, RS-422 และ RS-485 ซึ่งถูกกำหนดมาตรฐานโดยสถาบันEIA (Electronic International Associate) และเป็นที่นิยมใช้กันเป็นยอมรับในสากล นอกจากนั้นเครื่องไมโครคอนโทรเลอร์ในปัจจุบัน แทบทุกเครื่องจะต้องประกอบด้วย Port อนุกรม มาตรฐาน RS-232 ดังนั้น จึงได้นำมาตรฐานแบบ RS-485, RS-232, RS-422 มาพิจารณามาตรฐานการรับ-ส่งข้อมูล

3.2.1 มาตรฐาน RS-485

มาตรฐานแบบ RS-485 พัฒนาขึ้นมาจาก RS-422 โดยรูปแบบการต่อใช้งานจะเป็นตามรูปที่ 3-2 จะใช้วงจรเชื่อมโยงแบบ Balanced Line ซึ่งแต่ละสัญญาณมี 2 ตัวนำ และสัญญาณในตัวนำที่ 2จะตรงกันข้ามกับตัวนำแรก RS-485 Receiver ตอบสนองต่อความแตกต่างแรงดันระหว่าง 2 ตัวนำ เงื่อนไข อื่นๆ สำหรับชนิดนี้มาตรฐานของการวัดคือแบบ Differential Measurement ในทางตรงกันข้าม RS-232

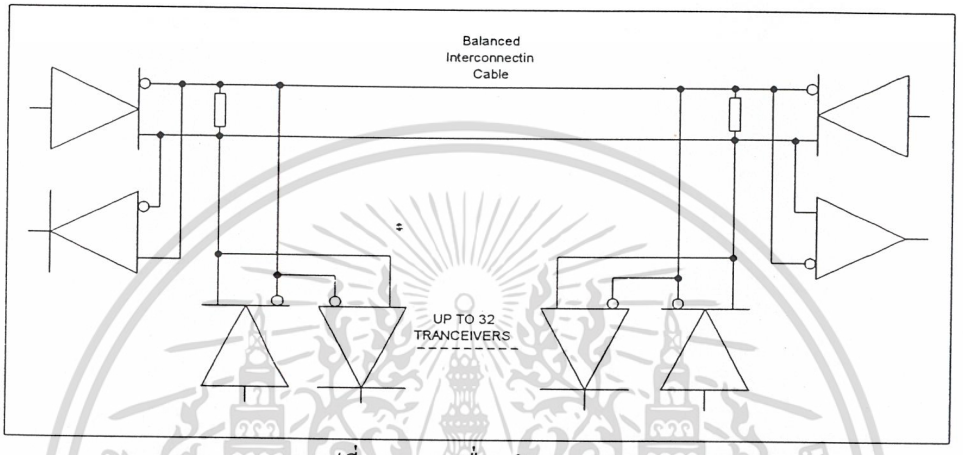


รูปที่ 3- 2 หลักการการเชื่อมโยงของมาตรฐาน RS-422, 485

การสื่อสารข้อมูลแบบ Unbalanced line ที่ซึ่งแต่ละสัญญาณมีเพียง 1 ตัวนำ และตัว Receiver ตอบสนองต่อความแตกต่างของแรงดันระหว่างตัวนำนี้ และตัวนำที่เป็นกราวด์รวมถูกนำมาใช้กับสัญญาณทั้งหมด มาตรฐานการวัดนี้เป็นแบบ Single-ended แบบ Balanced line มีข้อดีที่เหนือกว่าแบบ Unbalanced Line ข้อที่ 1 ก็คือเรื่องสัญญาณรบกวนต่างๆ (Voltage spikes , oscillations หรือ interference) จะถูกตัดทิ้งไป ในแบบ Unbalanced line กระแสย้อนกลับของสัญญาณผ่านสายกราวด์ สามารถผลิตสัญญาณรบกวนขึ้นที่ตัวรับ ในแบบ Balanced Line สัญญาณแบบ Differenced จะผลิตสัญญาณขึ้นมา 2 สัญญาณที่เท่ากันแต่ส่งกระแสตรงกันข้ามกัน ตั้งแต่กระแสเพิ่มขึ้นจนถึง 0 สำหรับทุกๆวัตถุประสงค์ในทางปฏิบัติไม่มีการส่งกระแสย้อนกลับในทางปฏิบัติที่จะเป็นสาเหตุให้เกิดปัญหา ข้อดีอื่นๆของแบบ Balanced มีภูมิคุ้มกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(ข้อจำกัดภายใน) ต่อความแตกต่างระหว่างความต่างศักย์ของกราวด์ระหว่างโหนด ในเครือข่ายที่มีสายยาวๆความต่างศักย์ของกราวด์ อาจเปลี่ยนแปลงหลายๆโวลต์จากโหนดหนึ่งไปยังโหนดอื่นๆ แต่แบบ Differential Measurement ไม่สนใจเกี่ยวกับความแตกต่างนี้ โดยเหตุที่มันวัดเพียง แรงดันระหว่าง 2 สายสัญญาณตัวนำ การนำเอาแบบ Balanced line มาใช้ประโยชน์คือเหตุผลหลักว่าทำไม RS-485 สามารถที่จะส่งข้อมูลได้ไกลกว่าแบบ RS-232 พร้อมทั้งยังสามารถเพิ่มจุดต่อ Terminal ได้สูงสุดถึง 32 ชุด ดังแสดงตามรูปที่ 3-3



รูปที่ 3-3 การเชื่อมโยง RS-422, 485

วงจรเชื่อมโยงแบบ RS-485 ใช้สายเคเบิลแบบ Twisted Pair ซึ่งประกอบด้วย 2 สายตัวนำที่มีฉนวนหุ้มตีเกลียวมีขนาดตามมาตรฐาน AWG22 ถึงแม้ว่า RS-485 อินเตอร์เฟสโดยปกติจะใช้แรงดันไฟเลี้ยง 5 โวลต์ ระดับลอจิกที่ตัว Driver และตัว Receiver ไม่ได้เป็น มาตรฐานแรงดัน 5 โวลต์ TTL หรือ CMOS สายสัญญาณทั้ง 2 ที่แสดงไว้ก็คือ A และ B ที่ระดับแรงดันที่ถูกต้องความแตกต่างแรงดันระหว่างเทอร์มินัล A และ เทอร์มินัล B สามารถที่จะยอมได้ถึง 1.5 โวลต์ ถึงแม้ว่าจะเป็นแบบที่ใช้ความแตกต่างแรงดัน 5 โวลต์ ถ้าเทอร์มินัล A มีค่าแรงดันน้อยที่สุดเป็นบวก 1.5 โวลต์เมื่อเทียบกับเทอร์มินัล B เอาท์พุทจะเป็นลอจิก “0” และถ้าเทอร์มินัล A มีค่าแรงดันน้อยที่สุดเป็นไฟลบ 1.5 โวลต์เมื่อเทียบกับเทอร์มินัล B เอาต์พุตจะเป็นลอจิก “1” ถ้าค่าความแตกต่างของแรงดันน้อยกว่า 1.5 โวลต์เอาต์พุตที่ได้จะไม่แสดงความหมายเป็นลอจิกใดๆ ที่ RS-485 Receiver ความแตกต่างแรงดันระหว่าง เทอร์มินัล A และ B แรงดันอินพุทเหมาะสมที่ต้องการ คือ 0.2 โวลต์สำหรับระดับลอจิกที่ถูกต้อง ถ้าเทอร์มินัล A มีค่าน้อยที่สุดเป็นบวก 0.2 โวลต์เมื่อเทียบกับเทอร์มินัล B ตัว Receiver จะมองเห็นเป็นเป็นลอจิก “0” และถ้าเทอร์มินัล B มีค่าน้อยที่สุดบวก 0.2 โวลต์เมื่อเทียบกับเทอร์มินัล A ตัว Receiver จะมองเห็นเป็นลอจิก “1” เช่นกันถ้าความแตกต่างของแรงดันระหว่างเทอร์มินัล A และ B น้อยกว่า 0.2 โวลต์เอาต์พุตที่ได้จะไม่ได้แสดงความหมายเป็นลอจิกใดๆ ความแตกต่างระหว่างแรงดันที่ต้องการที่ตัว Driver และ Receiver หมายความว่าสัญญาณนั้นสามารถลดทอนลงได้มากถึง 1.3 โวลต์ตามความยาวสายตัวนำของเครือข่ายสำหรับตัว Receiver ที่ยังจดจำคุณสมบัติของมัน ถ้าตัว Driver ผลิตความแตกต่างแรงดัน 5 โวลต์ออกมาขอบเขตของแรงดันจะมากขึ้นที่ระดับแรงดัน 4.8 โวลต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Specification	RS-232	RS-423	RS-422	RS-485
Transmission Mode	Unbalanced	Unbalanced	Balanced	Balanced
Max.Cable Length	50 Feet	100 Feet	4,000 Feet	4,000 Feet
Max.speed	20Kbps	100Kbps	10Mbps	10Mbps
Min.Driver O/P	+/-5 v	+3.6 v	+ 2 v	+/-1.5 v
Max.Driver O/P	+15 v	+/-6 v	+/- 5 v	+/-6 v
Receiver Sent.	+3 volts	+0.2 volts	+0.2 v	+0.2 v
Max.Drivers	1	1	1	32
Max.Receivers	1	10	10	32
Driver Load (Ω)	3-7 KΩ	450 Ω Min	100 Ω Min	60 Ω

ตารางที่ 3-1 การเปรียบเทียบมาตรฐานการสื่อสารข้อมูลอนุกรม 4 แบบ

3.3 หลักการพิจารณาและออกแบบ

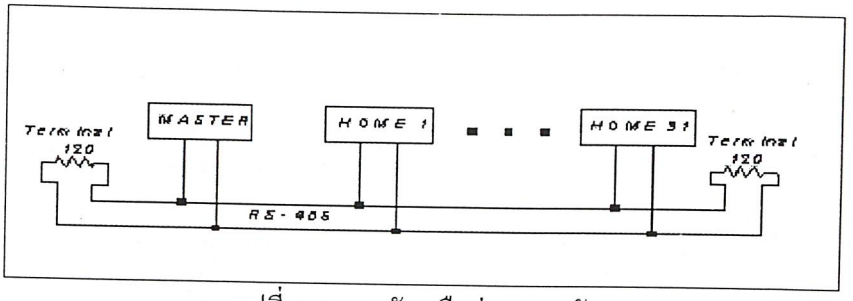
3.3.1 การออกแบบเครือข่าย

จากการศึกษามาตรฐาน RS-422,RS-485 และ RS-232 ในการนำมาใช้เป็นระบบเครือข่าย พบว่า RS-232 ไม่สามารถนำมาใช้สร้างระบบเครือข่ายได้เพราะสามารถต่อ Driverและ Receiver ได้เพียง 1 ตัว สำหรับ RS-422,RS-485 มีความเป็นไปได้ที่จะนำมาใช้สร้างระบบเครือข่าย เพราะสามารถต่ออุปกรณ์ได้หลายชุดต่อสายนำสัญญาณ 1 คู่ โดยเฉพาะ RS-485 นั้นสามารถต่ออุปกรณ์ Terminal Transceiver ได้ถึง 32 ชุด อีกทั้งยังต่อได้ระยะทางไกลถึง 4000 ฟุต ดังนั้น มาตรฐาน RS-485 จึงมีความเหมาะสมมากที่สุด

สำหรับลักษณะของการต่อระบบเครือข่าย ออกแบบเป็น 2 ระดับ คือแม่กับลูก (Master/Slave) โดยตอบสนองสัญญาณแบบ Polling ในส่วนของอุปกรณ์ซึ่งทำหน้าที่ในการควบคุมและประมวลผลในระบบเครือข่าย เลือกใช้ไมโครคอนโทนเลอร์ ตระกูล MCS-51 เพราะมีความเร็วในการประมวลผลที่สูง จากการศึกษาพบว่า หนึ่งชุดคำสั่งการทำงานนั้น จะใช้เวลาเพียง 1 ไมโครเซคชั่น(1 ใน 1 ล้านวินาที) ที่การใช้สัญญาณนาฬิกาความถี่ 12 เมกกะเฮิร์ต และ เป็นชิพที่มีจำหน่ายในประเทศ ราคาไม่แพง นอกจากนั้นยังมีพอร์ทสำหรับรับและส่งข้อมูลอนุกรมภายในชิพ ซึ่งเป็นระบบ Hardware และสามารถเลือกใช้งานแบบตรวจจับการรับสัญญาณแบบวิธี Interrupt

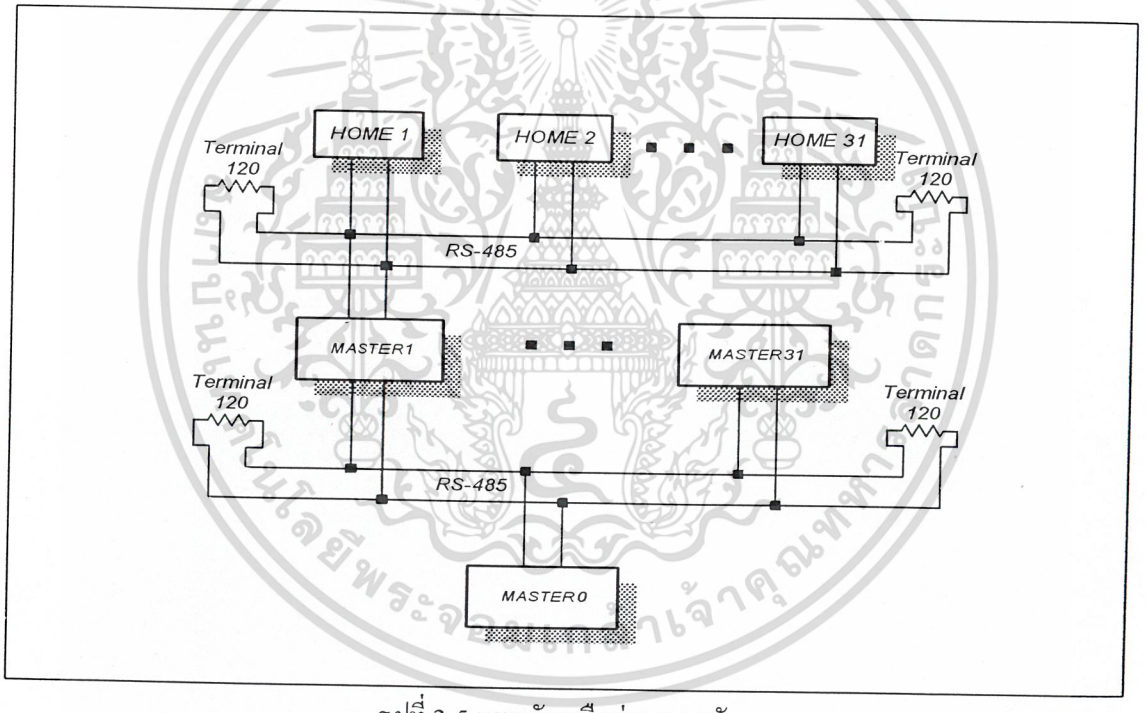
การทดลองเพื่อหารูปแบบการสร้างระบบเครือข่ายที่สามารถรองรับจำนวนอุปกรณ์ได้ในจำนวนที่เพียงพอ ขั้นเริ่มต้น ได้นำ การต่อเครือข่ายอ้างอิงมาตรฐาน RS-485 ได้ดังรูปที่ 3-4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3-4 แผนผังเครือข่าย 1 ระดับ

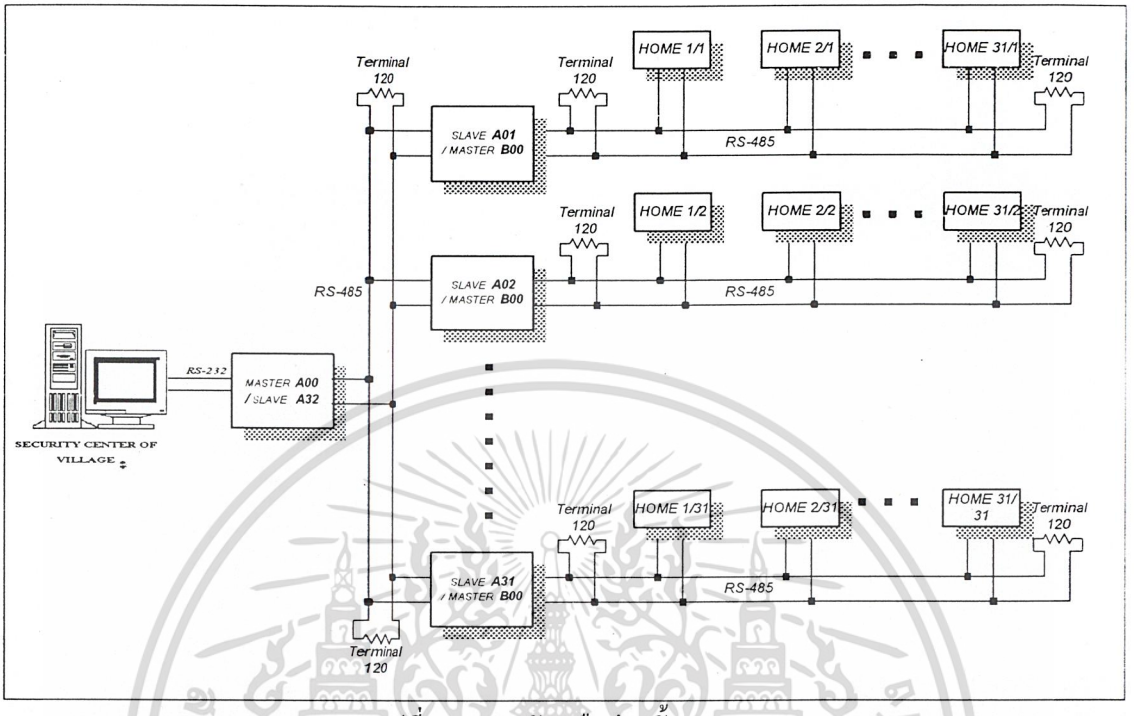
จากรูปที่ 3-4 จะเห็นว่า จำนวนของอุปกรณ์ที่สามารถเชื่อมต่อใน 1 คู่สายสัญญาณ หรือจุดติดต่อกับบ้านนั้น มีได้สูงสุดเพียง 31 จุดเท่านั้น เพราะอีก 1 ชุดจะทำหน้าที่เชื่อมต่อกับสถานีแม่ เนื่องจากระบบเป็นการออกแบบเพื่อใช้กับระบบรักษาความปลอดภัยในหมู่บ้าน ดังนั้น ยังมีความจำเป็นต้องขยายจำนวนจุดเชื่อมต่อเพิ่มขึ้น โดยทำการออกแบบชุดของ RS-485 เพิ่มขึ้นอีก 1 ระดับ แสดงได้ดังรูปที่ 3-5



รูปที่ 3-5 แผนผังเครือข่าย 2 ระดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3-5 พบว่าระบบจะมีจุดเชื่อมต่อกับบ้านได้สูงสุดถึง 931 หลัง(31*31) ซึ่งถือว่าพียงพอสำหรับใช้ในหมู่บ้าน ซึ่งเมื่อติดต่อกับส่วนของไมโครคอมพิวเตอร์ จะแสดงได้ดังรูปที่ 3-6



รูปที่ 3-6 แผนผังเครือข่ายทั้งระบบ

3.3.2 การออกแบบโพรโตคอล

ในการรับส่งสัญญาณระยะไกลนั้นสิ่งที่จำเป็นก็คือ การกำหนดรูปแบบวิธีของการรับ-ส่งข้อมูลโดยฝ่ายรับและส่งต้องตกลงกันก่อน ซึ่งเรียกว่า โพรโตคอล (Protocol) ทั้งนี้ การออกแบบโพรโตคอลที่ดี ต้องพิจารณาถึงปัจจัยต่างๆ เช่น

3.3.2.1 ความรวดเร็วของโพรโตคอล โพรโตคอลที่ดี ในหนึ่งรอบการทำงานจะต้องมีกระบวนการที่สั้น และสามารถทำงานได้ตามความต้องการของระบบ

3.3.2.2 ความสามารถในการรองรับงานต่างๆ โพรโตคอลต้องสามารถทำงานได้ตามความต้องการของผู้ออกแบบ ซึ่งออกแบบมาให้รองรับการทำงานของระบบ

3.3.2.3 ความถูกต้องของข้อมูล ข้อมูลจากผู้รับควรจะไปถึงผู้ส่งอย่างถูกต้อง หรือแม้จะมีข้อผิดพลาด ก็ควรเป็นข้อผิดพลาดที่สามารถตรวจสอบได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.3 โพรโตคอล

ในการออกแบบโพรโตคอลทางการได้แบบการทำงานออกเป็น Layer ต่างๆ เพื่อลดการซับซ้อนของหน้าที่การทำงานและยังสามารถช่วยให้มีการพัฒนางานได้อย่างระบบระเบียบ โดยเราศึกษาการทำงานของ OSI Model เพื่อเป็นแนวทางในการออกแบบโดยมีการดูหน้าที่การทำงานของโพรโตคอลและวิธีการจัดการกับปัญหาที่เกิดขึ้นในระบบแบบต่างๆ

Application layer	User application 1		...	
Presentation layer	Encryption/ decryption		compression/ expansion	Choice of syntax
Session layer	Session control	Session synch.	Session to transport mapping	Session management
Transport layer	Layer and flow control		Error recovery	Multiplexing
Network layer	Connection control		Routing	Addressing
Link layer	Data link establishment		Error control / Flow control	Synch / Framing
Physical layer	Access to trasmit media		Physical and electrical interface	Activation/ deactivation of con.

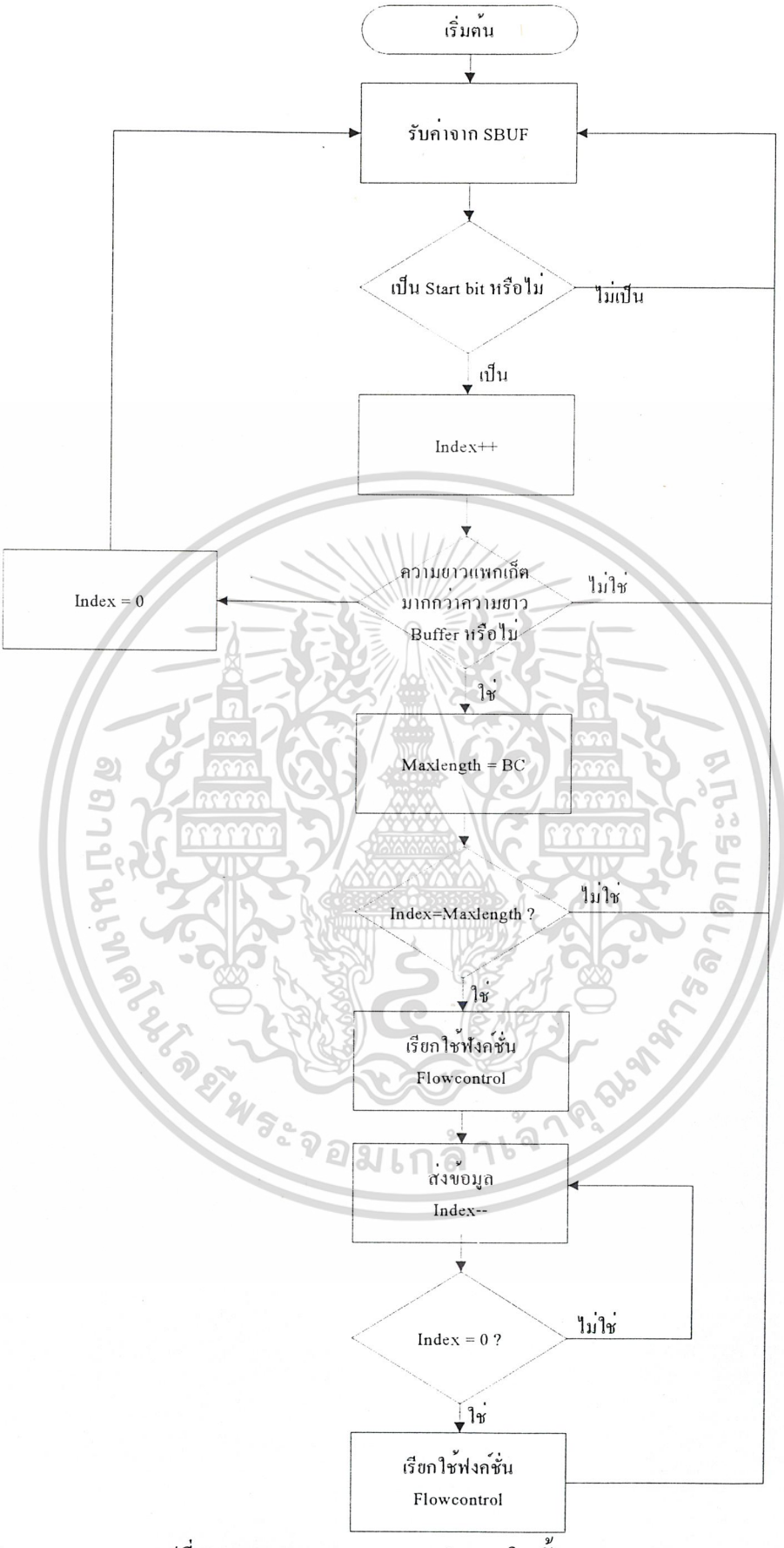
รูปที่ 3-7 OSI Model และหน้าที่การทำงาน

การออกแบบเพื่อใช้กับระบบรักษาความปลอดภัยในหมู่บ้าน ได้ทำการออกแบบในส่วนต่างๆ คือ Physical Layer, Data link Layer, Flow Control, Application โดยมีรายละเอียดดังต่อไปนี้

3.3.3.1 Physical Layer ใช้การเชื่อมต่ออ้างอิงมาตรฐาน RS-485 ทั้งนี้ เพราะสามารถส่งสัญญาณได้เป็นระยะทางไกล เหมาะกับการนำมาใช้ในหมู่บ้าน

3.3.3.2 Data link Layer ทำการออกแบบกระบวนการการรับส่งข้อมูลระหว่างไมโครคอมพิวเตอร์ และไมโครคอนโทรเลอร์ นอกจากนั้นยังมีการออกแบบแพกเก็ต เช่น ความยาวของเฟรม บิตที่ใช้ในการเริ่มต้นในการส่งข้อมูลและจำนวนข้อมูล เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



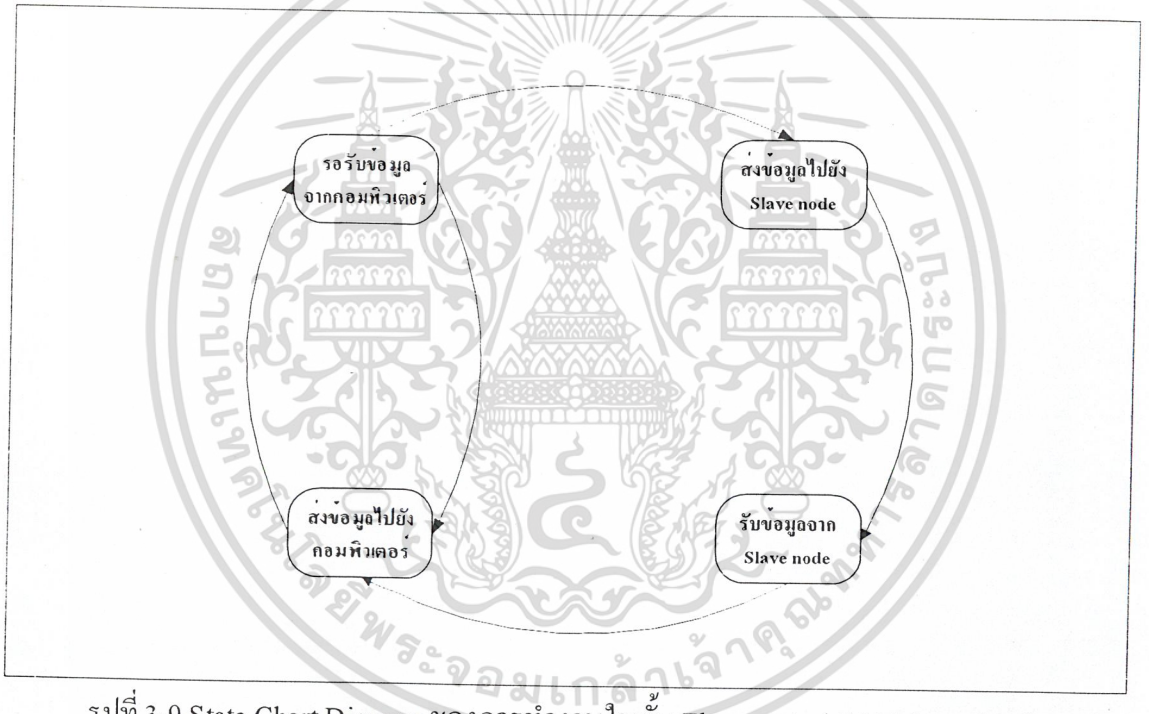
รูปที่ 3-8 Flow Chart ของการทำงานในชั้น Data Link

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.3.3 Flow control

ดังที่กล่าวมาข้างต้น สำหรับในชั้น data link เมื่อสามารถรับข้อมูลและส่งข้อมูลได้จนครบทั้งแพ็กเก็ตแล้ว ในชั้นนี้จะทำการควบคุมทิศทางการทำงาน ว่าจะส่งข้อมูลไปให้ทิศทางไหน ไปยังผู้รับคือใคร และยังมีหน้าที่การทำงานในการตรวจสอบสถานะของเครือข่ายว่า ส่วนใดทำงานอยู่บ้าง โดยการทำงานจะต่างไปตาม Master Node, Slave Node, Home Node ดังต่อไปนี้

3.3.3.3.1 Master Node การทำงานใน Master จะรับข้อมูลจาก คอมพิวเตอร์ เพื่อส่งข้อมูลไปให้ Slave Node เท่านั้น โดยมีข้อยกเว้นคือการตรวจสอบการทำงานของ Master Node เท่านั้นที่จะส่งข้อมูลโดยตรงไปสู่ศูนย์ควบคุม.

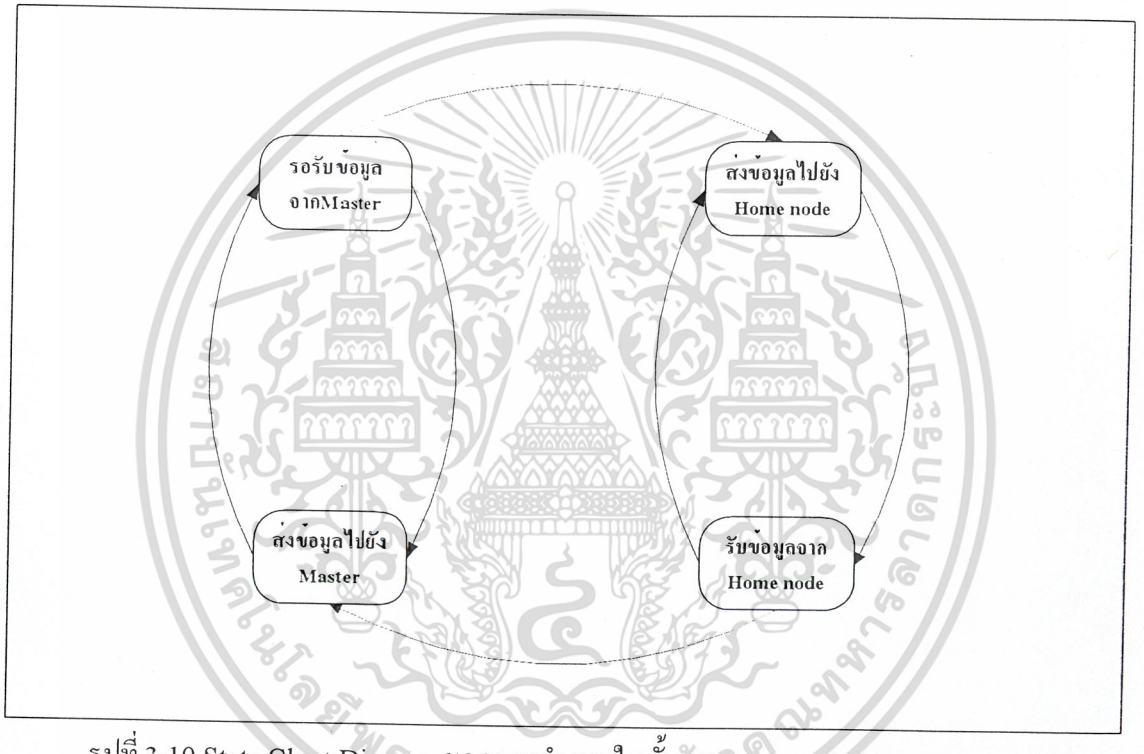


รูปที่ 3-9 State Chart Diagram ของการทำงานในชั้น Flow control ของ Master Node

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.3.3.2 Slave Node เป็นส่วนที่มีความซับซ้อนที่สุดในเรื่อง โพรโตคอลเพราะมีหน้าที่ที่จะต้องเป็นตัวเก็บข้อมูลของ Home Node ให้กับศูนย์ควบคุมหลักโดยผ่านทาง Master node โดยจะรอรับคำสั่งจาก Master node ให้ทำการตรวจสอบสถานะและเก็บข้อมูลจาก Home node อีกทีเพื่อให้มีการทำงานที่เป็นจังหวะและไม่เกิดการชนการข้อมูล

เมื่อได้รับคำสั่งจะเปลี่ยนทิศทางการทำงานไปยัง Home Node เพื่อทำการไล่ตรวจสอบข้อมูลทั้งหมดของ Home Node และจัดทำเก็บข้อมูลและตรวจสอบว่าข้อมูลมีการเปลี่ยนแปลงหรือเปล่าด้วย

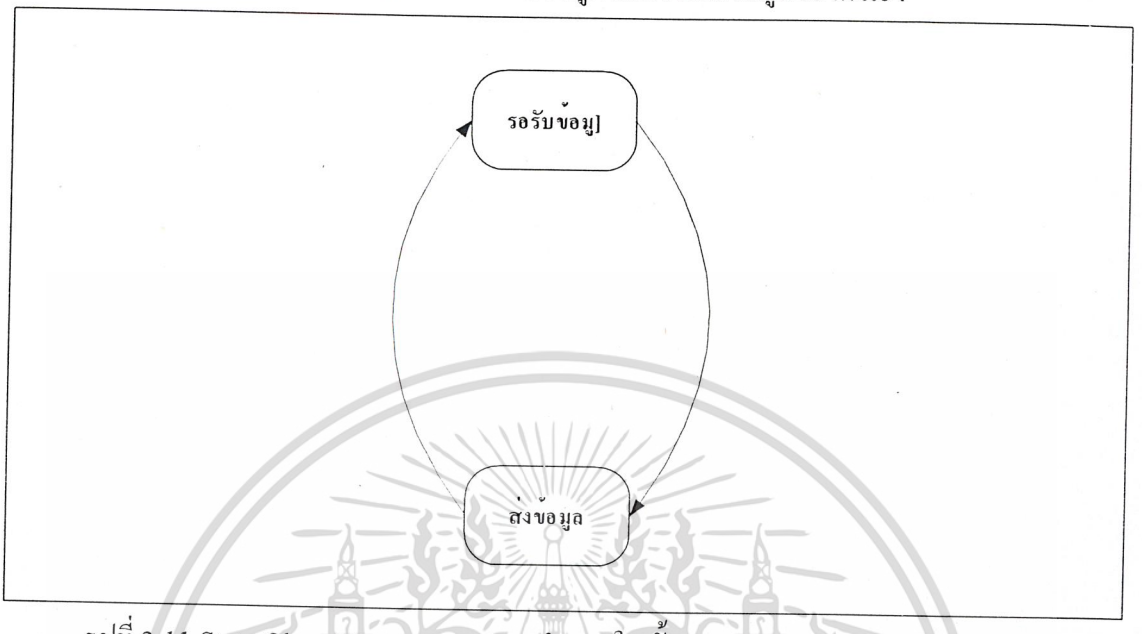


รูปที่ 3-10 State Chart Diagram ของการทำงานในชั้น Flow control ของ Slave Node

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

3.3.3.3.3 Home Node การทำงานในส่วนนี้ จะทำตรวจสอบความเป็นเจ้าของของข้อมูล ว่าเป็นข้อมูลของตัวเองหรือเปล่า ถ้าเป็นข้อมูลตัวเองก็จะรับข้อมูลไปทำงานต่อไปถ้าไม่ใช่ก็จะรอรับข้อมูลจนกว่าจะมีข้อมูลของตัวเอง



รูปที่ 3-11 State Chart Diagram ของการทำงานในชั้น Flow control ของ Home Node

3.3.3.4 Application จะมีการทำงานเฉพาะในส่วนHome node เท่านั้น โดยในชั้น Flow control จะดูข้อมูลว่าเป็นข้อมูลของตัวเองหรือเปล่า ในชั้น Application ก็จะส่งข้อมูลมาให้ เพื่อจะได้ทำงานตามคำสั่งนั้นๆ และยังเป็นส่วนที่ทำงานในส่วนของการเข้ารหัสและถอดรหัส สำหรับกระบวนการ และการทำงานของการเข้ารหัส จะกล่าวอีกครั้งใน บทที่ 5 ความปลอดภัยของข้อมูลบนเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

49915

3.3.4 การออกแบบ Frame ข้อมูล

ในการออกแบบจะคำนึงถึงความต้องการของ โพรโตคอลของระบบว่าต้องการอะไรบ้างเพื่อให้สามารถรองรับการทำงานกับตัวโพรโตคอลได้อย่างดี นอกจากนั้นการออกแบบเฟรมจะต้องสั้น กะทัดรัด และสามารถทำงานได้ถูกต้อง สำหรับ Application ที่ใช้งานในระบบรักษาความปลอดภัยในหมู่บ้าน แบ่งเป็น 2 กลุ่มใหญ่ๆคือ Application สำหรับการตรวจสอบสถานะและApplication สำหรับการควบคุมสั่งงาน

3.3.4.1 ส่วนของการตรวจสอบสถานะ โดยในส่วนนี้จะมีหน้าที่ในการตรวจสอบสถานะต่างๆ ของเครือข่าย แบ่งตามการทำงานได้ดังนี้

- **Frame การร้องข้อการตรวจสอบสถานะของ Node ต่างๆ**
  ประกอบไปด้วยที่อยู่ผู้ส่ง (Sender Address) ที่อยู่ผู้รับ (Home Address) และคำสั่งซึ่งใช้ในการแสดงการร้องขอการตรวจสอบสถานะ (Command) แสดงได้ดังรูป

ADDS	ADDH	CMD

- **Frame การตอบรับการตรวจสอบสถานะของ Node**
  ประกอบไปด้วยที่อยู่ผู้ส่ง (Sender Address) ที่อยู่ผู้รับ (Home Address) และคำสั่งซึ่ง ใช้ในการแสดงการตอบรับ (Command) แสดงได้ดังรูป

ADDS	ADDH	CMD

- **Frame การตอบรับข้อมูลภายใน บ้าน**
  ประกอบไปด้วยที่อยู่ของHomeที่ตอบรับ ข้อมูลสถานะของอุปกรณ์ตรวจจับและอุปกรณ์ไฟฟ้าแสดงได้ดังรูป

ADDH	SEN1	SEN2	DEV1	DEV2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.4.2 ส่วนการสั่งงาน โดยส่วนนี้มีจุดประสงค์เพื่อสั่งงานให้ อุปกรณ์ทำงานจากส่วนควบคุมหลัก เฟรมข้อมูลจะประกอบไปด้วยที่อยู่ของผู้ส่ง ที่อยู่ของผู้รับ หรือ Home node และข้อมูลของอุปกรณ์ที่ต้องการสั่งงาน

ADDS	ADDH	DEV1	DEV2

โดย ฟิลด์ ต่างจะมีความหมายดังนี้

ADDS : คือ ที่อยู่ของ Slave Node และ ถ้ามีค่าเป็น 0 จะหมายถึง Master

ADDH : คือ ที่อยู่ของ Home Node

CMD : จะเป็นส่วนกำหนดว่าจะเป็นคำสั่งอะไร มีคำสั่งต่อไปนี้

CMD=1 : เป็นการร้องข้อมูลการตรวจสอบสภานะ

CMD=2 : เป็นการสั่งงาน

CMD=3 : เป็นการตอบรับว่าสถานะว่ายังทำงานอยู่

SEN1-2 : แสดงสถานะของ Sensor

DEV1-2 : แสดงสถานะของ Device และคำสั่งให้ Device ทำงาน

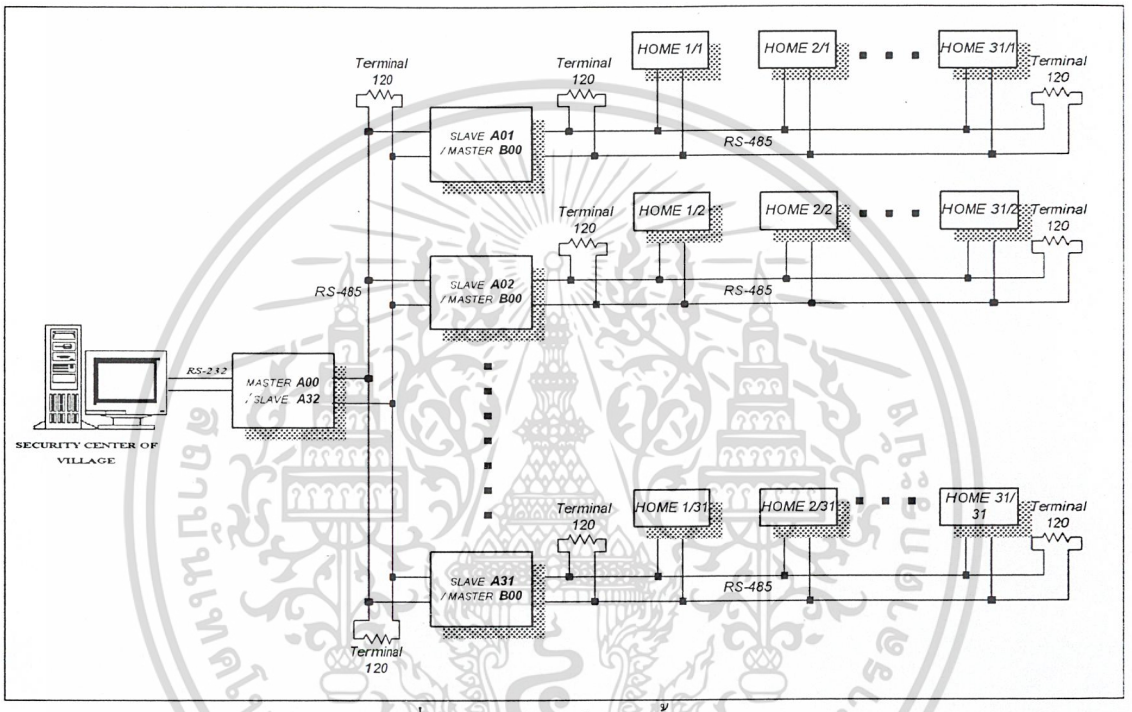
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

ระบบHardware และวงจร

4.1 การออกแบบHardware

จากการออกแบบระบบเครือข่ายแสดงแผนผังเครือข่ายทั้งระบบได้ดังรูปที่ 4-1

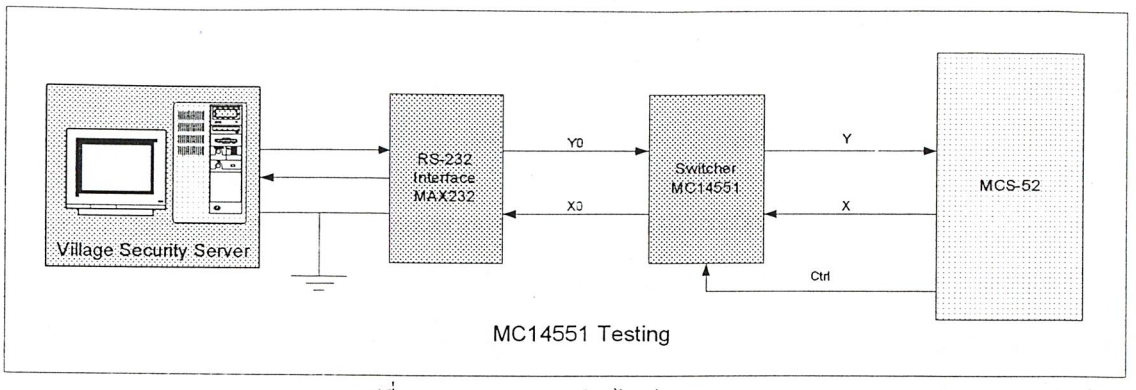


รูปที่ 4-1 แผนผังเครือข่ายทั้งระบบ

การออกแบบHardwareที่ระดับชั้นที่ 1 พบว่า วงจรจะต้องมีพอร์ทอนุกรม RS-232 ติดต่อกับเครื่องไมโครคอมพิวเตอร์ และ RS-485 ติดต่อกับเครือข่าย ดังนั้น การออกแบบจึงใช้อุปกรณ์ Switching เพื่อสลับการติดต่อระหว่าง RS-485และ RS-232 โดยเลือกชิชิพไอซีเบอร์ MC14551 เนื่องจากมีสายสัญญาณได้ถึง 4 ชุด ในขณะที่ถ้าหากเลือกใช้ ชิพเบอร์ 4016 ซึ่งเป็น Bilateral Switch จะต้องใช้สายควบคุม RS-485 อีก ทำให้สิ้นเปลืองไป

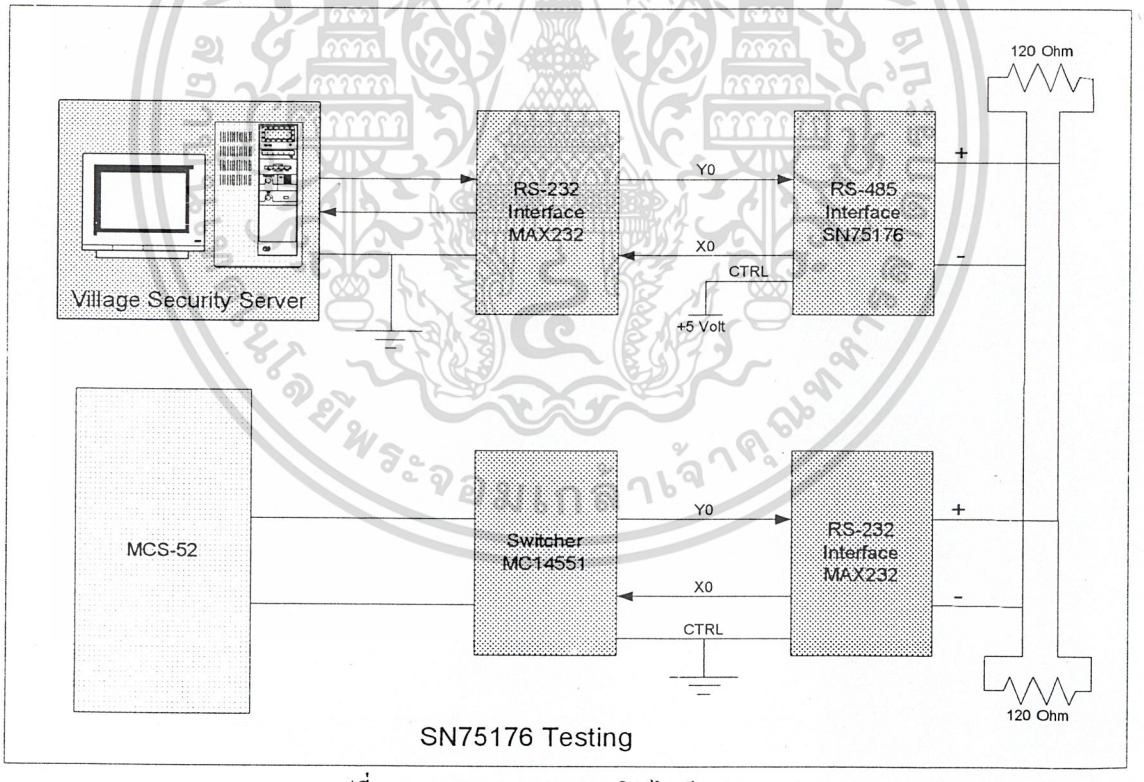
MC14551 ถูกออกแบบให้ทำงานเป็นแบบ Multiplex/Demultiplex จึงมีความเหมาะสมที่จะนำมาใช้เป็น Switching สำหรับการสลับการติดต่อระหว่างพอร์ททั้งสอง จากการทดสอบการทำงานโดยต่อวงจรบนแผงทดลอง(Photo board) ทำการต่อชุดวงจร MCS-51 เพื่อทำการติดต่อกับไมโครคอมพิวเตอร์ผ่าทางพอร์ทอนุกรมแบบ RS-232 โดยใช้ชิพเบอร์ MAX232 ซึ่งมีหน้าที่ในการแปลงแรงดันค่า + - 25 โวลต์ เป็น +5 โวลต์ และ 0 โวลต์ โดยส่งผ่าน MC14551 ดังแสดงตามรูปที่ 4-2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4-2 การทดสอบชิพไอซี MC14551

จากการทดลองพบว่า ไมโครคอนโทรเลอร์สามารถทำงานผ่านพอร์ทอนุกรม RS-232 ได้ความเร็วที่ 19,200 Baud ข้อมูลที่ได้รับจากไมโครคอนโทรเลอร์สามารถทำงานได้ตามปกติ ในขั้นตอนถัดไป เป็นการทดสอบการรับ-ส่งสัญญาณผ่าน RS-485 โดยใช้ชิพเบอร์ SN75173 ซึ่งในขั้นตอนนี้ เราใช้วงจรที่ทดสอบ MC14551 ดังรูปที่ 4-2 เพื่อทำหน้าที่เป็นส่วนแปลงสัญญาณจาก RS-232 มาเป็น RS-485 แล้วเชื่อมต่อกับเครือข่าย RS-485 ดังการทดลองรูปที่ 4-3



รูปที่ 4-3 แสดงการทดสอบชิพไอซี SN75176

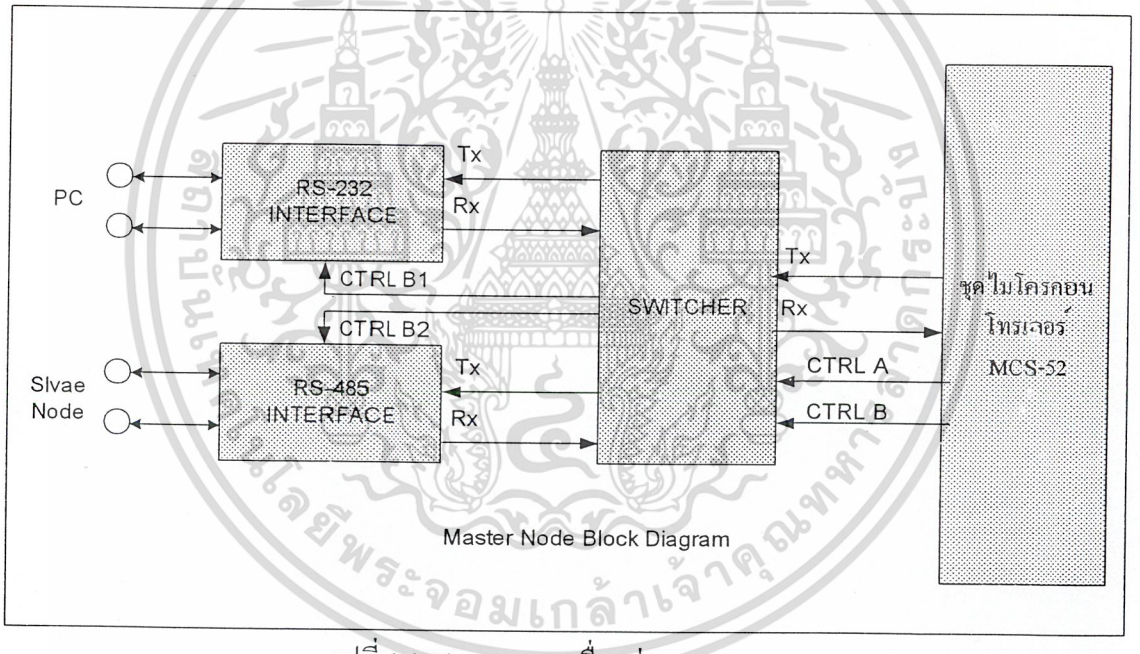
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากการทดลอง การรับและส่งข้อมูลจากเครื่องไมโครคอมพิวเตอร์ไปยังไมโครคอนโทรเลอร์ พบว่า ที่ความเร็ว 19,200 Baud บอร์ดไมโครคอนโทรเลอร์ไม่สามารถรับข้อมูลได้อย่างถูกต้อง แสดงว่า ไอซี SN75176 ไม่สามารถทำงานที่ความเร็วนี้ได้ จึงทำการทดลองที่ความเร็ว 9,600 Baud โดยใช้โปรแกรม Hyper Terminal ในการรับและส่งข้อมูลผ่านทางพอร์ท RS-232 พบว่า ไมโครคอนโทรเลอร์สามารถทำงานได้ถูกต้องทั้งการรับและส่งข้อมูล

จากผลการทดลอง จึงสามารถออกแบบวงจร Hardware ของ Node ทั้ง 3 ส่วน ได้แก่

4.1.1 วงจร Master

ใช้ MCS-52 เป็นส่วนประมวลผล โดยต่อกับ Multiplexer MC14551 เพราะต้องการเชื่อมต่อกับ MAX232 ให้สามารถติดต่อกับไมโครคอมพิวเตอร์ผ่านพอร์ทอนุกรม (Serial port) และต่อกับ SN75176 เพื่อให้สามารถติดต่อกับวงจรในระดับ Slave แบบอนุกรมอ้างอิงมาตรฐานแบบ RS-485 แสดงรายละเอียดดังรูปที่ 4-4

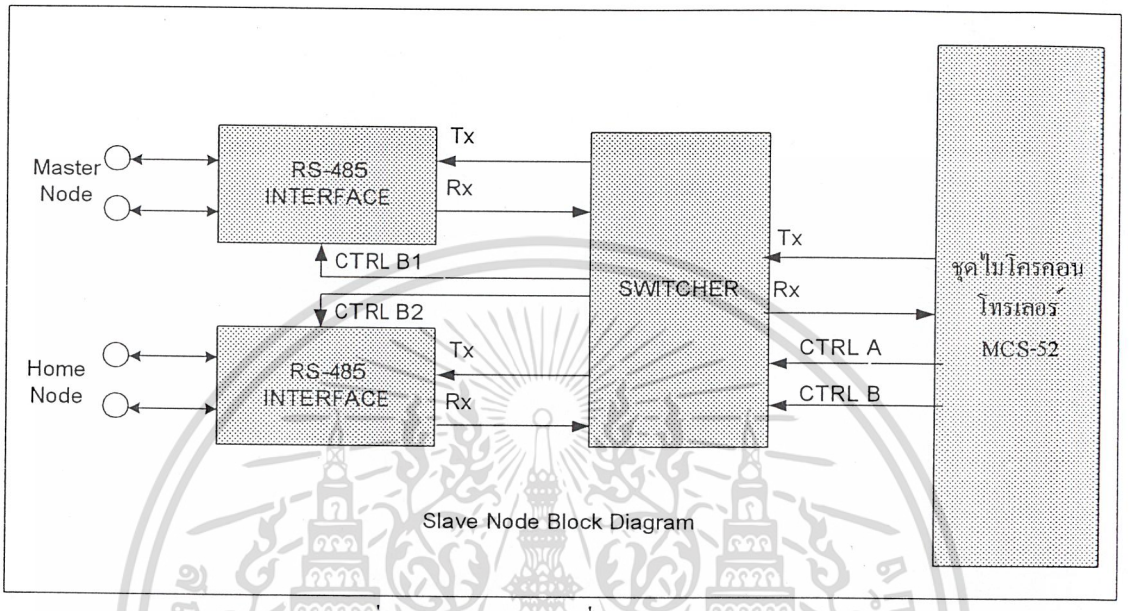


รูปที่ 4-4 Diagram การเชื่อมต่อวงจร Master

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.2 วงจร Slave

ใช้ MCS-52 เป็นส่วนประมวลผล โดยต่อกับ Multiplexer MC14551 เพราะต้องการเชื่อมต่อกับ SN75176 จำนวน 2 ชุด เพื่อให้สามารถติดต่อกับวงจรในระดับ Master และ Slave แบบอนุกรมอ้างอิงมาตรฐานแบบ RS-485 แสดงรายละเอียดได้ดังรูปที่ 4-6

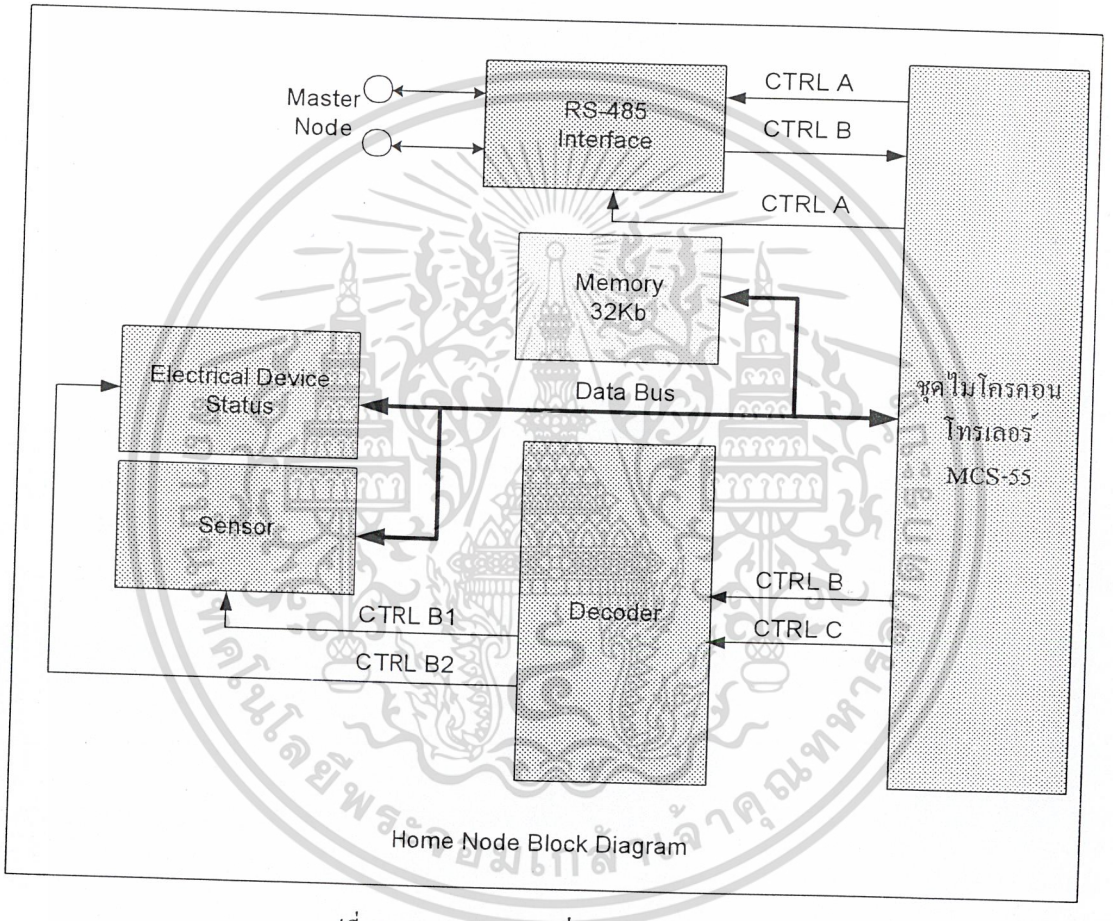


รูปที่ 4-5 Diagram การเชื่อมต่อวงจร Slave

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.3 วงจร Home

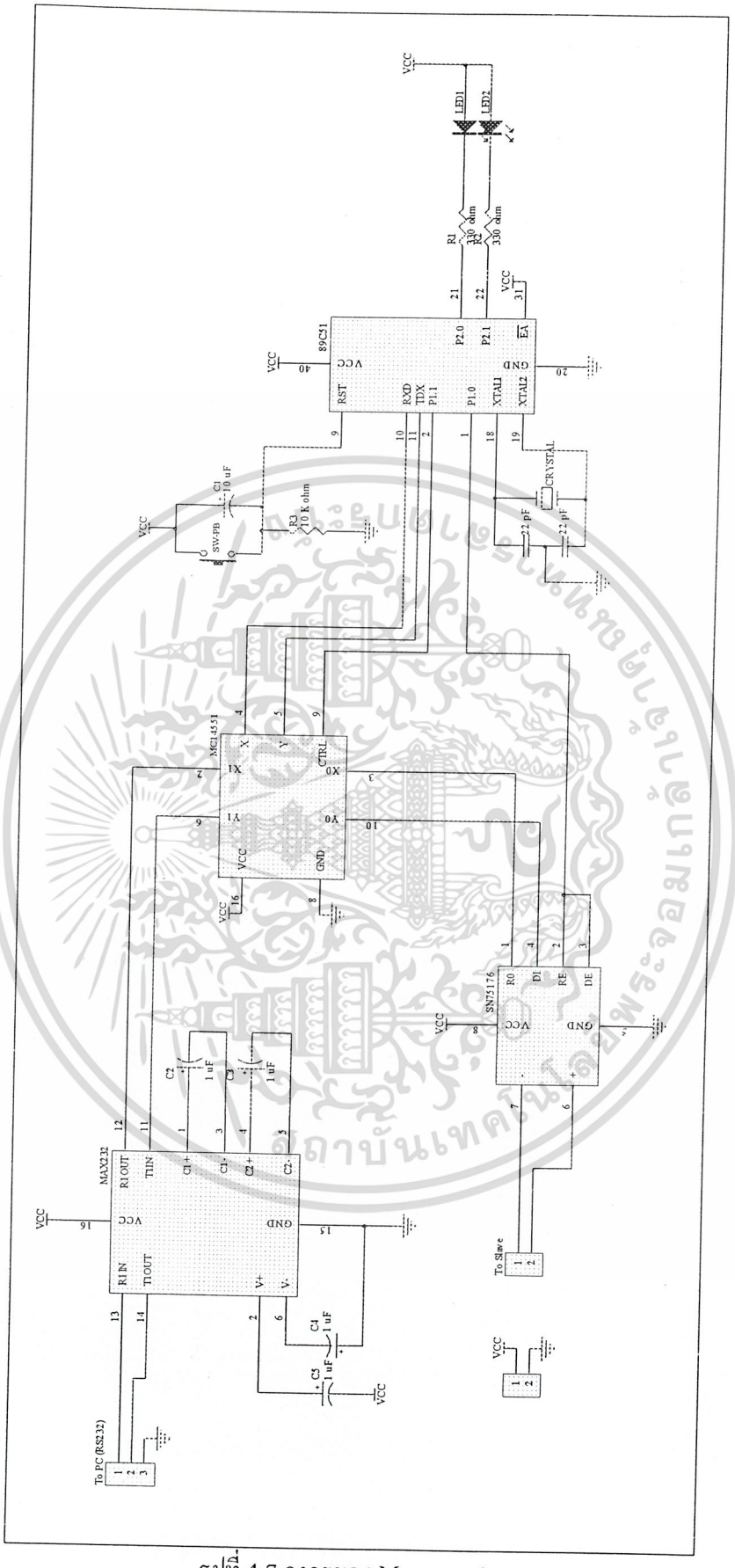
ใช้ MCS-55wd เป็นส่วนประมวลผล โดยเชื่อมต่อกับ Multiplexer SN74LS42N ซึ่งทำหน้าที่ในการขยายพอร์ทในการควบคุมอุปกรณ์รับและส่งสัญญาณ โดยเชื่อมต่อกับ Dip-Switchซึ่งเป็นเหมือนอุปกรณ์ส่งข้อมูล และเชื่อมต่อกับไดโอดเปล่งแสง (LED) ซึ่งเป็นเหมือนอุปกรณ์รับข้อมูล และเชื่อมต่อกับหน่วยความจำขนาด 32 กิโลไบต์ UT62256CPC เพราะไมโครคอนโทรเลอร์จะถูกโปรแกรมกระบวนการเข้าและถอดรหัสแบบ DES ซึ่งต้องใช้หน่วยความจำในการประมวลผลเกินกว่าที่มีใน MCS-55 แสดงรายละเอียดได้ดังรูปที่ 4-6



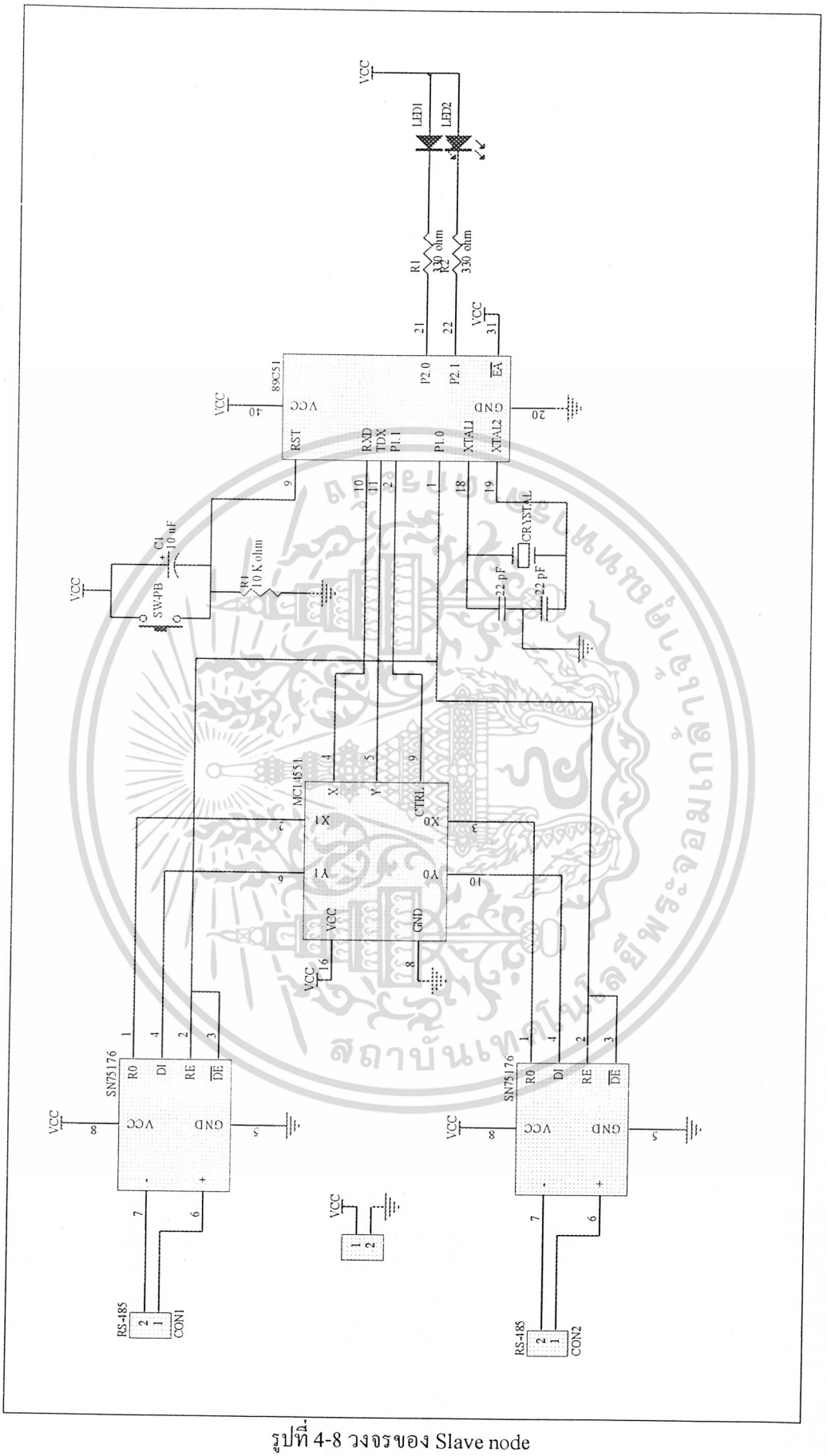
รูปที่ 4-6 Diagram การเชื่อมต่อวงจร Home

จากรูป Diagram รูปที่ 4-4,4-5,4-6 สามารถที่จะออกแบบเป็น Schematic circuit Diagram ดังรูปที่ 4-7 เป็นวงจรของ Masterที่ทำหน้าที่เป็นส่วนเชื่อมต่อระหว่างศูนย์รักษาความปลอดภัยไปยังเครือข่าย รูปที่ 4-8 เป็นวงจร Slave node ระดับที่ 1 และ รูปที่ 4-9 เป็นวงจร Slave node ระดับที่ 2 หรือเป็นส่วนของวงจร Home ซึ่งก็คือบ้านแต่ละหลังนั่นเอง

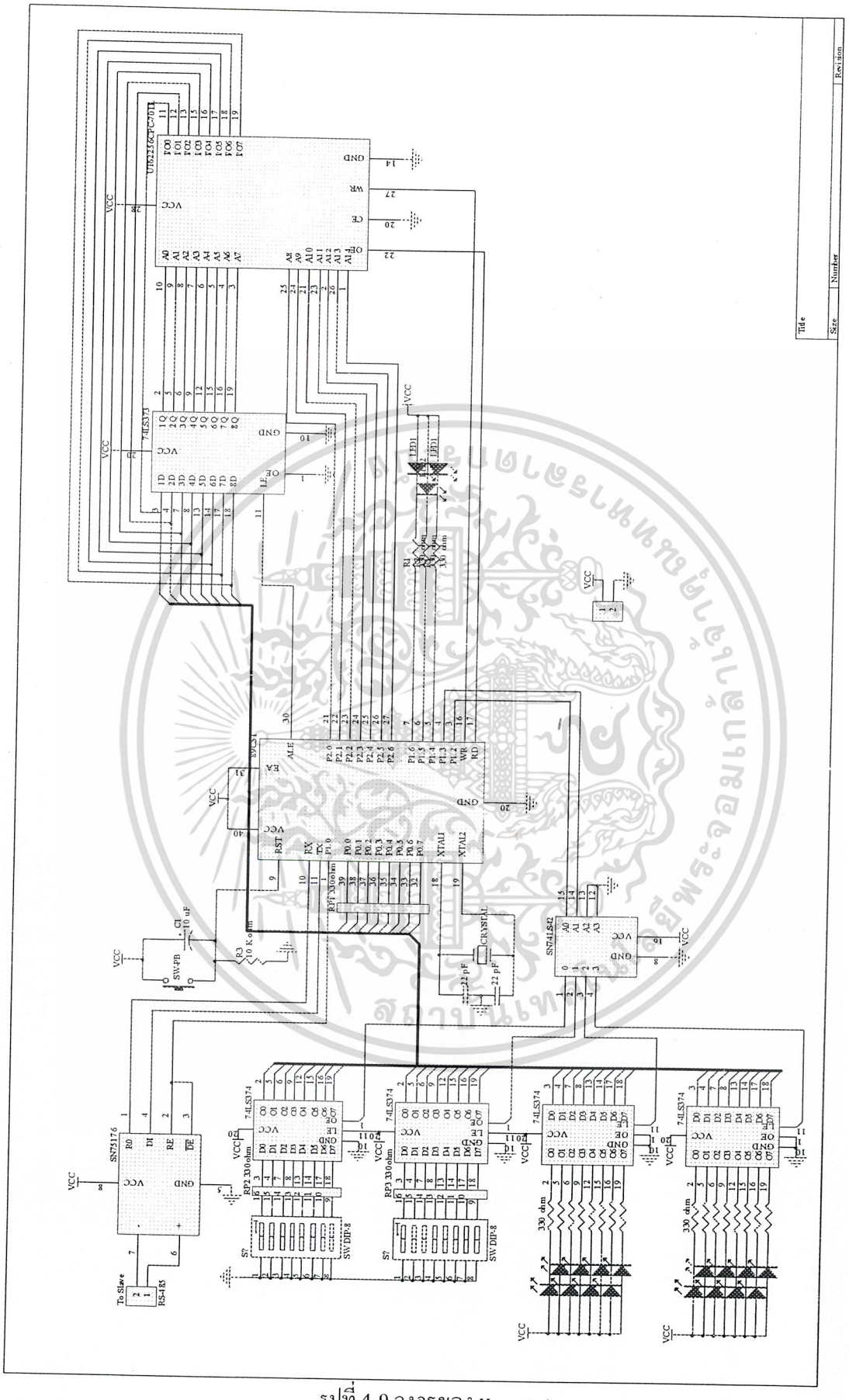
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4-7 วงจรของ Master node



รูปที่ 4-8 วงจรของ Slave node



รูปที่ 4-9 วงจรของ Home node

4.2 การพัฒนาโปรแกรมบนระบบเครือข่าย

4.2.1 ภาษาสำหรับการโปรแกรม

ในส่วนการพัฒนาโปรแกรมเพื่อใช้บนไมโครคอนโทรเลอร์นั้น ต้องทำการพิจารณาเลือกภาษาที่ใช้ในการเขียนโปรแกรม สำหรับไมโครคอนโทรเลอร์ ซึ่งได้แก่ ภาษา Assembly และ ภาษาซี สำหรับการพัฒนาโปรแกรม ของโครงงานนี้ เลือกใช้ภาษาซี สำหรับ ไมโครคอนโทรเลอร์ เนื่องจาก การเขียนโปรแกรมเพื่อควบคุมการทำงานของไมโครคอนโทรเลอร์โดยการใช้ภาษาซีนั้น มีข้อได้เปรียบมากกว่าการเขียนโดยภาษาแอสเซมบลีอย่างมากเพราะโครงสร้างของภาษาแอสเซมบลีจะดูได้ยากกว่า การควบคุมก็เข้าใจได้ยาก ซึ่งทำให้เป็นอุปสรรค์อย่างยิ่งต่อการนำไปพัฒนาต่อโดยผู้ที่ไม่ใช่ผู้เขียนคนแรก

ดังนั้น โครงงานชิ้นนี้จึงทำการโปรแกรมกระบวนการทำงานที่ออกแบบไว้ใหม่ทั้งหมด โดยใช้ภาษาซี ซึ่งสามารถใช้กับงานที่ซับซ้อนได้ ด้วยการใช้คอมไพเลอร์ภาษาซีของ Keil ซึ่งสามารถใช้ได้กับตัวแปรทุกประเภท และมีไลบรารีทางคณิตศาสตร์ให้มาอีกด้วย

4.2.2 การโปรแกรม

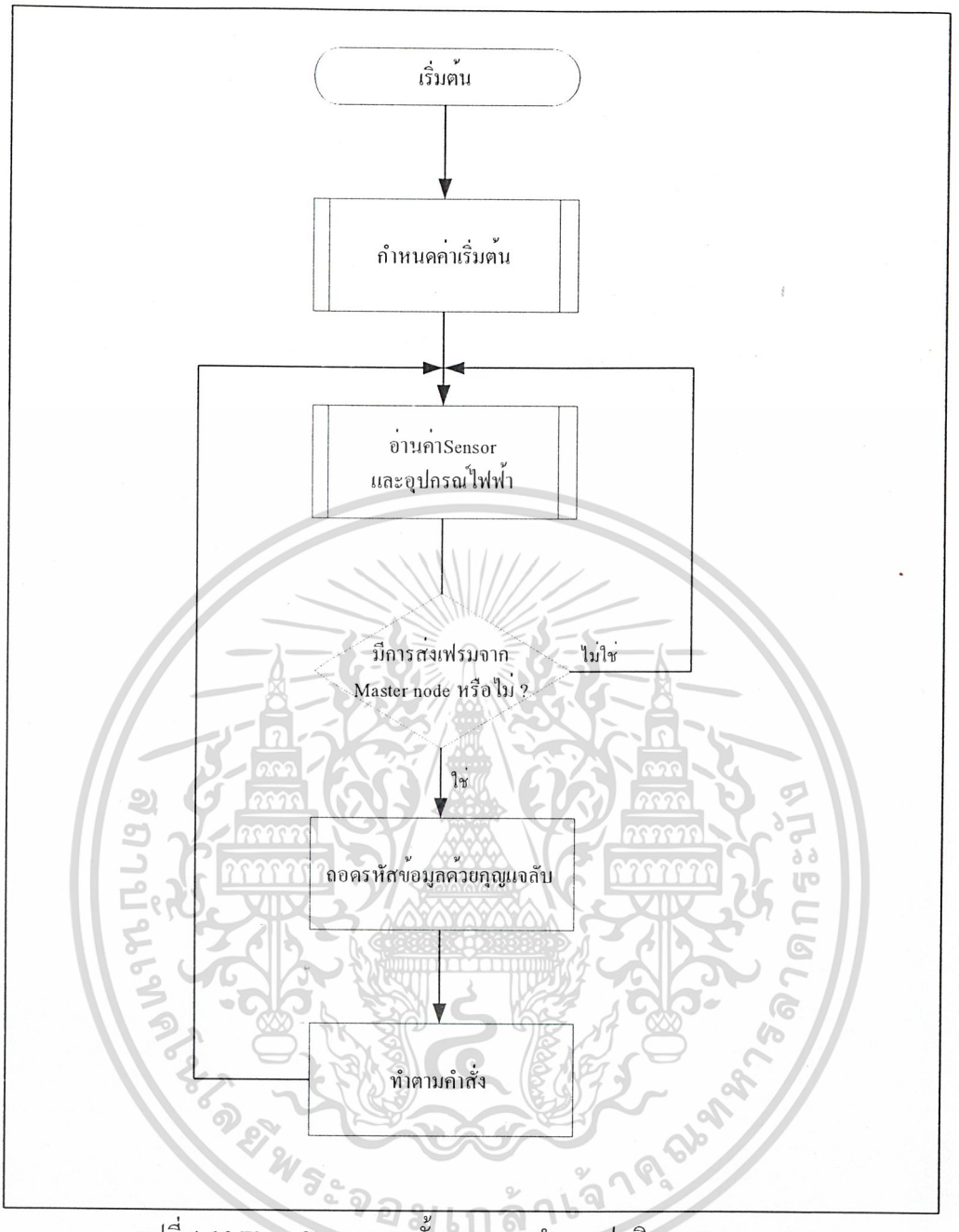
ในส่วนของการพัฒนาโปรแกรมแบ่งได้เป็น

1. ส่วนที่ทำหน้าที่เป็นระบบเตือนภัยในบ้านหรือ Home node
2. ส่วนที่ทำหน้าที่เป็น Slave node
3. ส่วนที่ทำหน้าที่เป็น Master node

4.2.2.1 ส่วนที่ทำหน้าที่เป็นระบบเตือนภัยในบ้านหรือ Home node

เป็นส่วนที่ต้องคอยตรวจสอบสถานะของอุปกรณ์ไฟฟ้าและอุปกรณ์ตรวจจับอยู่เสมอ สามารถแสดงขั้นตอนการทำงานหลักได้ดังรูป

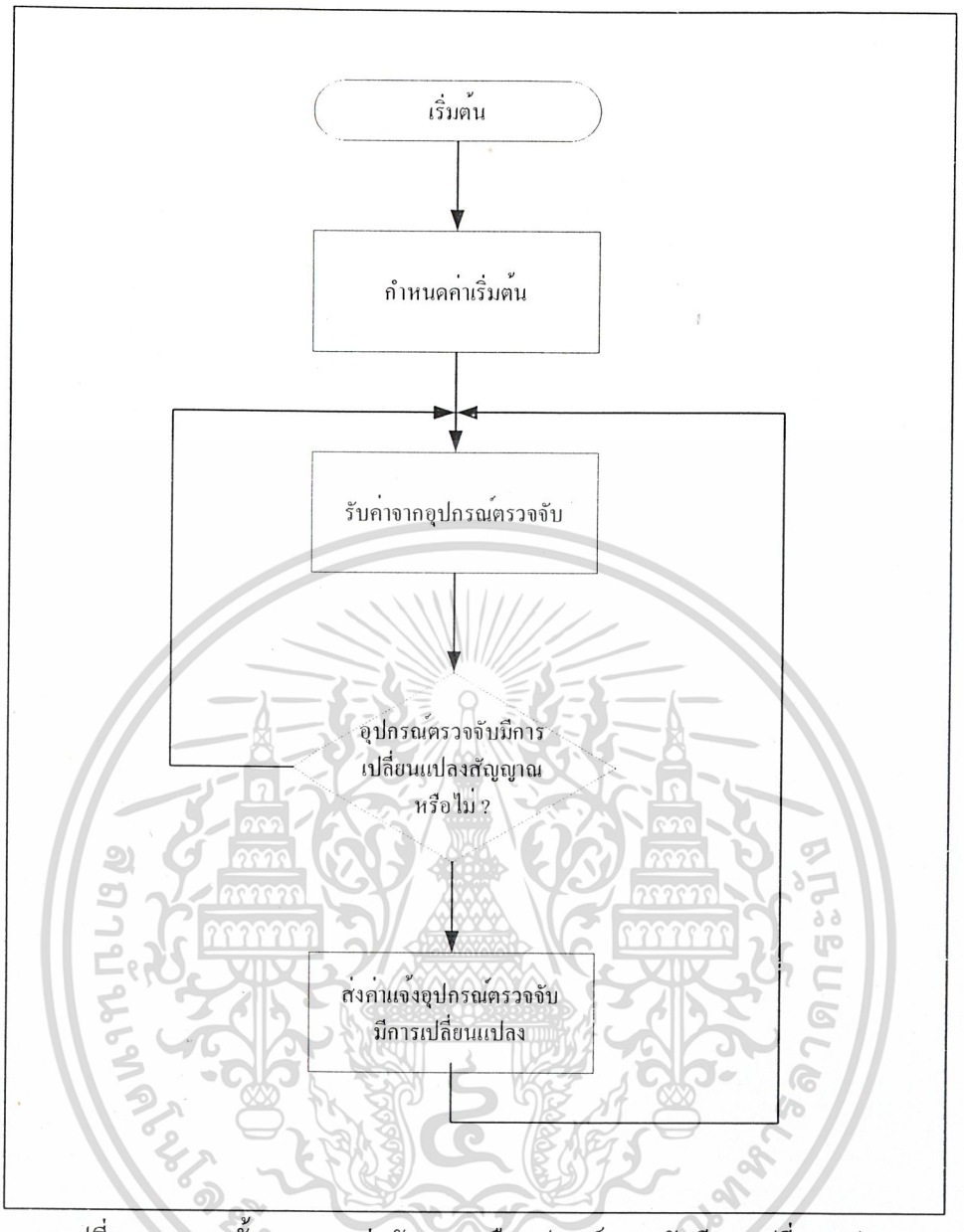
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4-10 Flow Chart แสดงขั้นตอนการทำงานปกติของHome node

สำหรับการส่งค่าข้อมูลของอุปกรณ์ตรวจจับ หลังจากที่เริ่มต้นการทำงานแล้ว Home node จะมีการวนตรวจสอบอุปกรณ์ตรวจจับอยู่ตลอดเวลา และจะมีการส่งข้อมูลไปแจ้งศูนย์ควบคุมเฉพาะกรณีที่ อุปกรณ์ตรวจจับมีการเปลี่ยนแปลงสัญญาณเท่านั้น แสดงได้ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

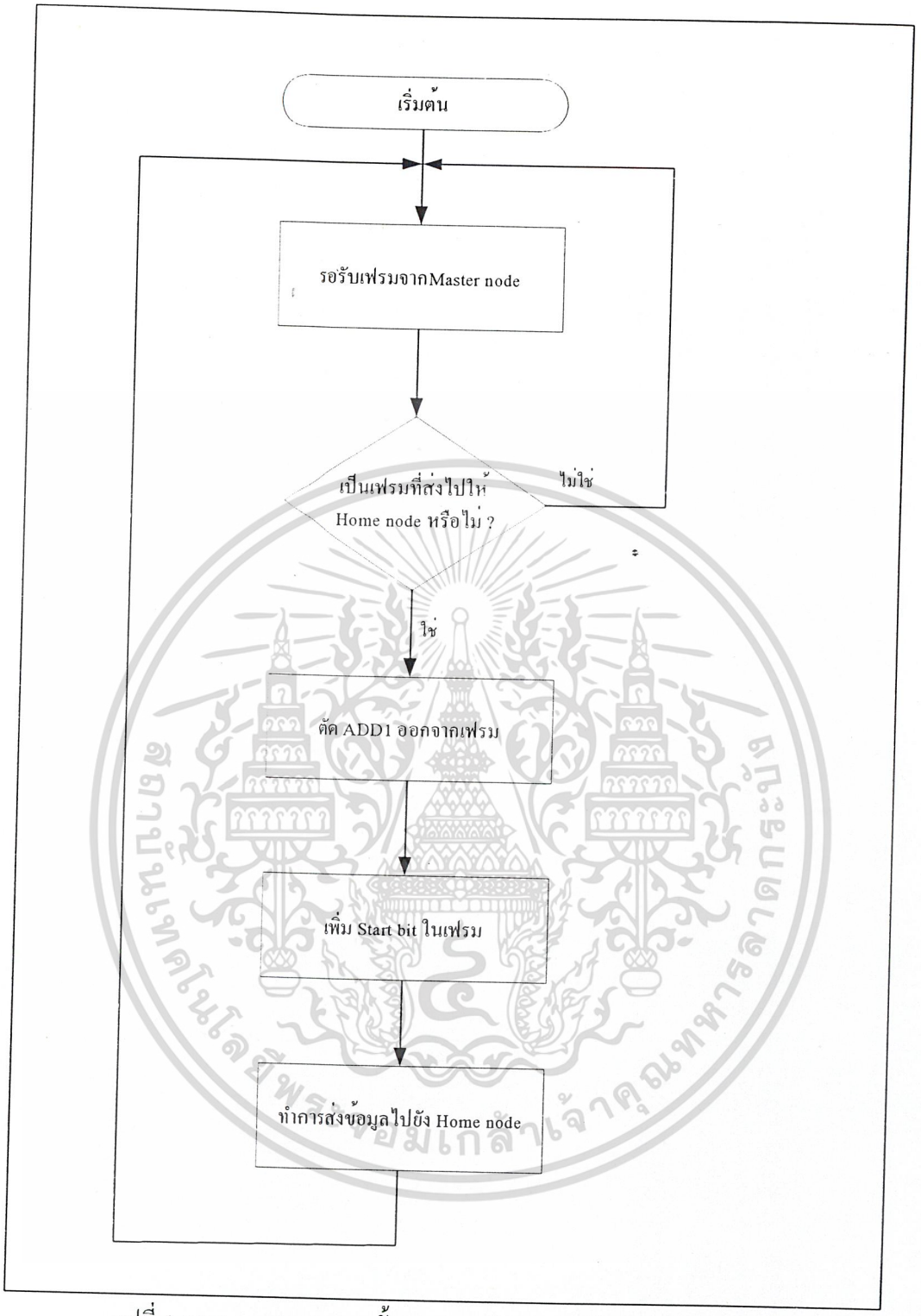


รูปที่ 4-11 แสดงขั้นตอนการส่งสัญญาณเมืออุปกรณ์ตรวจจับมีการเปลี่ยนแปลง

4.2.2.2 ส่วนที่ทำหน้าที่เป็น Slave Node

มีหน้าที่หลักๆในการทำงาน คือ การรับและส่งต่อเฟรมข้อมูลไปบนเครือข่าย RS-485 โดยมีการทำงานคือ เมื่อรับเฟรมข้อมูลมาแล้ว ก่อนที่จะส่งต่อจะต้องตัด ADD1 (Address ของSlave) ออก ก่อนที่จะส่งต่อไปยัง Home node โดยการทำงานสามารถแสดงได้ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4-12 Flow Chart แสดงขั้นตอนการรับและส่งเฟรมของSlave node

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.2.3 ส่วนที่ทำหน้าที่เป็น Master node

มีหน้าที่หลักเหมือนกับ Slave node เพียงแต่ ไม่มีการตัดข้อมูล หรือต่อข้อมูลใดๆทั้งสิ้น เพราะ Master node ทำหน้าที่เป็นเพียงส่วนแปลงสัญญาณระหว่างมาตรฐานของ RS-485 และ RS-232 ดังนั้น จึงมีลักษณะการทำงานเหมือนกับ Slave node คือการรับแล้วส่งต่อ สามารถศึกษาได้ดังรูป 4-13 ข้างต้น

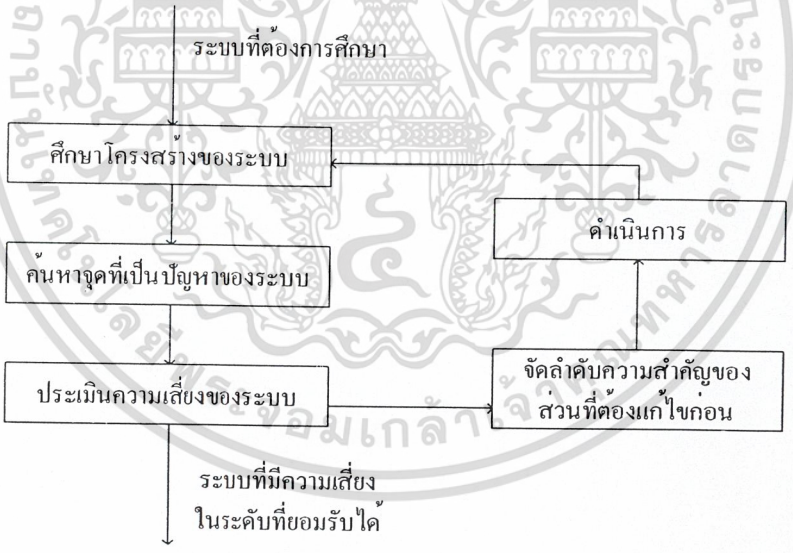
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
ความปลอดภัยของข้อมูลบนเครือข่าย

5.1 ความจำเป็นในการสร้างความปลอดภัยให้กับข้อมูล

ระบบรักษาความปลอดภัยในหมู่บ้านใช้ระบบเครือข่ายอ้างอิงตามมาตรฐาน RS-485 ซึ่งเป็นสายตีเกลียว(Twist pair) เนื่องจากเป็นระบบที่ใช้สายส่งสัญญาณ(Media) เป็น Cable ทำให้ง่ายต่อการดักจับสัญญาณ (Wire Tapping) ถ้าหากสัญญาณถูกปลอมแปลงโดยที่ไม่สามารถตรวจสอบได้ว่า เป็นสัญญาณที่ส่งมาจากผู้ส่งที่แท้จริง หรือผู้รับเป็นผู้รับที่แท้จริง ก็อาจจะทำให้ระบบถูกรบกวนโดยการปลอมแปลงข้อมูลทำให้เกิดความผิดปกติอย่างรุนแรง เช่น ส่งสัญญาณประเภทควบคุมไปควบคุมการเปิด ปิดอุปกรณ์ไฟฟ้าภายในบ้าน , ส่งสัญญาณไปแจ้งศูนย์ควบคุมว่าระบบยังเป็นปกติอยู่ทั้งที่จริงแล้วบ้านนั้นกำลังถูกโจรขึ้นบ้านอยู่ เป็นต้น

จากการศึกษาระบบเครือข่ายของระบบรักษาความปลอดภัยในหมู่บ้านพบว่า ข้อมูลที่อยู่บนเครือข่าย ไม่มีการเข้ารหัสเพื่อทำการปกปิดข้อมูลใดๆทั้งสิ้น ในการสร้างหรือเพิ่มระบบรักษาความปลอดภัย เราสามารถทำตามกระบวนการวิศวกรรมระบบการรักษาความปลอดภัย ได้ตามรูปที่ 5-1



รูปที่ 5-1 แสดง Diagramวิศวกรรมระบบการรักษาความปลอดภัย (System Security Engineering Process)

จากกระบวนการวิศวกรรมระบบการรักษาความปลอดภัย เราสามารถศึกษาถึงระบบรักษาความปลอดภัยในหมู่บ้าน ตามลำดับของ Diagram ได้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.1 การศึกษาโครงสร้างของระบบ

ระบบรักษาความปลอดภัยในหมู่บ้านใช้ไมโครคอนโทรเลอร์ในการควบคุมอุปกรณ์รับและส่งสัญญาณ โดยวงจรไมโครคอนโทรเลอร์จะส่งข้อมูลผ่านทางเครือข่ายซึ่งเชื่อมต่อโดยอ้างอิงตามมาตรฐานแบบ RS-485 ส่งข้อมูลไปยังศูนย์รักษาความปลอดภัยซึ่งใช้ไมโครคอมพิวเตอร์ในการแสดงสถานะ และส่งคำสั่ง โดยใช้ส่วนติดต่อกับผู้ใช้ (GUI) ซึ่งโปรแกรมโดย MS Visual Basic

5.1.2 ค้นหาจุดที่เป็นปัญหาของระบบ

จุดที่เป็นปัญหาของระบบ เราแบ่งการพิจารณาออกเป็น 3 ส่วนใหญ่ๆ ได้แก่

5.1.2.1 ส่วนของโปรแกรม MS Visual Basic ซึ่งทำงานบนไมโครคอมพิวเตอร์

ปัญหาที่พบคือ โปรแกรมยังขาดการจัดเก็บข้อมูลที่เป็นชื่อและรหัสผ่าน (User/Password) ที่ปลอดภัย เพราะ โปรแกรมเดิมใช้การเก็บข้อมูลดังกล่าวเป็น Text file ไม่มีการเข้ารหัสข้อมูลใดๆทั้งสิ้น ทำให้ง่ายต่อการมีผู้ไม่ประสงค์ดี เข้ามาก่อกวนระบบ ผ่านทางโปรแกรมควบคุมที่ศูนย์ควบคุมระบบรักษาความปลอดภัยในหมู่บ้าน

5.1.2.2 ส่วนของวงจรHardware ได้แก่ Master , Slave , Home node

ปัญหาที่พบคือ วงจรHardware มีโอกาสที่จะถูกลอกเลียนแบบทั้งวงจร รวมถึงโปรแกรมภายในไมโครคอนโทรเลอร์ ทำให้เกิดโอกาสที่จะมีผู้ลอกเลียนวงจร Hardware แล้วนำวงจรที่ลอกเลียนแบบ เข้ามารบกวน หรือแทนที่วงจรชุดเดิม ซึ่งทำให้ศูนย์ควบคุมแสดงสถานะที่ผิดพลาดไปจากความจริงได้

5.1.2.3 ส่วนของระบบเครือข่าย

ปัญหาที่พบคือ ข้อมูลบนระบบเครือข่ายเป็นข้อมูลซึ่งไม่มีการปกปิดใดๆ ทำให้ง่ายต่อการถูกดักจับข้อมูลด้วยวิธีการดักจับจากสายสัญญาณ(Wire Tapping) ซึ่งข้อมูลเหล่านั้น เป็นข้อมูลที่สำคัญต่อระบบรักษาความปลอดภัยอย่างมาก เพราะ ข้อมูลจะบ่งบอกถึง ตำแหน่งของบ้าน (Address) ข้อมูลของอุปกรณ์ตรวจจับหรือSensor ทั้งSensor ที่ทำงานอยู่และไม่ได้ทำงานอยู่ และยังรวมไปถึงข้อมูลของอุปกรณ์ไฟฟ้าว่า เปิด/ปิด อย่างไรบ้าง ทำให้โอกาสที่ผู้บุกรุกจะนำข้อมูลเหล่านี้ไปจัดทำเป็นสถิติและหาโอกาส วิธีการต่างๆ เข้ามาโจรกรรม เป็นไปได้อย่างง่ายดาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.3 ประเมินความเสี่ยงของระบบ

การประเมินความเสียงของระบบ ทำได้โดยการวิเคราะห์ความสำพันธ์ของความสำคัญที่มีต่อระบบ(Criticality) และความพยายามที่ต้องใช้ในการโจมตี (Effort) โดยสามารถใช้สูตรเพื่อคำนวณหาค่าความเสี่ยง คือ

$$\text{ความเสี่ยง (Risk)} = \frac{\text{ความสำคัญที่มีต่อระบบ (Criticality)}}{\text{ความพยายามที่ต้องใช้ในการโจมตี (Effort)}}$$

ถ้ากำหนดค่าให้

0 = น้อย, 5 = ปานกลาง และ 10 = มาก

สามารถวิเคราะห์ความเสี่ยง โดยพิจารณาตามปัญหาที่อาจจะเกิดขึ้น แสดงเป็นตารางได้ดังตารางที่ 5-1

ความเสี่ยงที่อาจเกิด	ระดับความสำคัญต่อระบบ (Criticality)	ความพยายามที่ต้องใช้ในการโจมตี (Effort)	ค่าความเสี่ยง Risk=C/E
1.ก่อกวนหรือดูข้อมูลผ่านทางศูนย์ควบคุม	8	2	4
2.ลอกเลียนแบบวงจร Hardware ในระบบ	6	5	1.2
3.ดักจับข้อมูลด้วยวิธี Wire Tapping	8	1	8
4.ส่งข้อมูลชุดเดิม (Reply Attack)	8	2	4
5.ตัดสายสัญญาณ	5	2	2.5

ตารางที่ 5-1 แสดงอัตราความเสี่ยงของเหตุการณ์ที่อาจจะเกิดขึ้น

เมื่อพิจารณาจากค่าความเสี่ยง เราสามารถจัดลำดับความสำคัญของเหตุการณ์ที่ควรจะแก้ไขก่อน โดยเรียงตามลำดับค่าความเสี่ยงที่มากที่สุดก่อน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.4 จัดลำดับความสำคัญของส่วนที่ต้องทำการแก้ไขก่อน

การจัดลำดับความสำคัญของเหตุการณ์ที่ควรจะแก้ไขก่อน พิจารณาจากตารางที่ 5-2 ได้ดังนี้

เหตุการณ์ที่ควรจะแก้ไขก่อน	ค่าความเสี่ยง	แนวทางการแก้ไข
1. ดักจับข้อมูลด้วยวิธี Wire Tapping	8	เข้าปกปิดข้อมูลด้วยกระบวนการที่เป็นที่ยอมรับ
2. การส่งข้อมูลชุดเดิม (Reply Attack)	8	เพิ่มเติมส่วนของลำดับข้อมูล(Data Sequenc) ในเฟรมข้อมูล
3. ก่อกวนหรือดูข้อมูลผ่านทางศูนย์ควบคุม	4	เก็บข้อมูลและรหัสผ่าน(User/Password) ในDatabase ที่มีการเข้ารหัส หรือต้อง Log in
4.ตัดสายสัญญาณ	2.5	ฝังสายสัญญาณไว้ใต้ดินหรือวางสายสัญญาณในที่ลับ
5.ลอกเลียนแบบวงจร Hardware ในระบบ	1.2	ทำการ lock การอ่านข้อมูลจากไมโครคอนโทรเลอร์

ตารางที่ 5-2 แสดงลำดับความสำคัญของเหตุการณ์ที่ควรจะแก้ไขก่อน

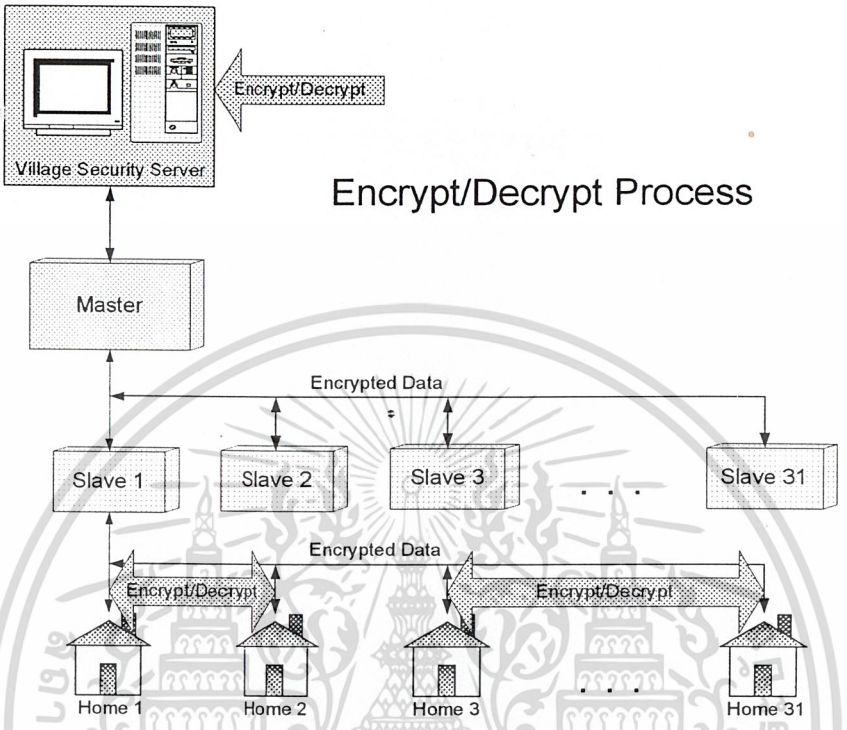
จากตารางแสดงให้เห็นว่า สิ่งที่ควรทำเป็นอันดับแรกและอันดับต่อๆไปคือ การปกปิดข้อมูลด้วยกระบวนการที่เป็นที่ยอมรับ การเพิ่มเติมส่วนของลำดับของข้อมูลในเฟรมข้อมูล ปรับปรุงการเก็บข้อมูลและรหัสผ่านของโปรแกรมที่ใช้ในศูนย์ควบคุม ซึ่งทั้ง 3 ส่วนนี้ มีค่าความเสี่ยงที่ควรจะปรับปรุง เพื่อให้ระบบมีความปลอดภัยในระดับที่ยอมรับได้

5.1.5 ขั้นตอนการดำเนินการ

การดำเนินการเพื่อปรับปรุงระบบ จะต้องพิจารณาถึงความเหมาะสมหลายๆอย่างของระบบ โดยสามารถแบ่งขั้นตอนการดำเนินงานเป็นข้อๆ ตามแนวทางการแก้ไขได้เรียงตามลำดับดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.5.1 การปกปิดข้อมูล สามารถทำได้ด้วยการเข้ารหัสซึ่งมีหลายวิธี เช่น การเข้า รหัสแบบ DES , 3DES , AES เป็นต้น สำหรับส่วนที่จะต้องทำการเข้ารหัสและถอดรหัสในระบบ คือ ส่วนของโปรแกรมศูนย์หลัก และส่วนของวงจรไมโครคอนโทรเลอร์ที่บ้าน Home node แสดงได้ดังรูปที่ 5-2

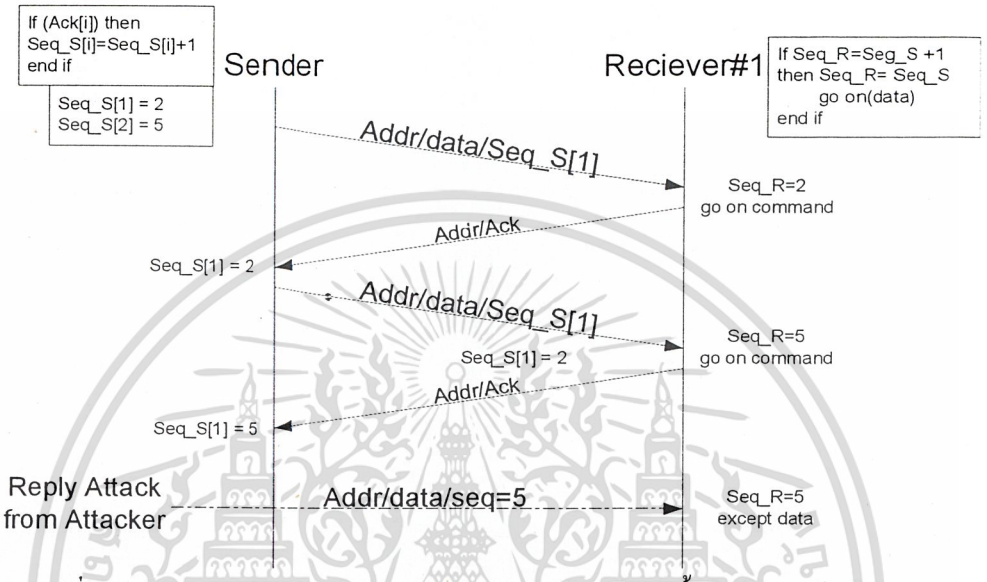


รูปที่ 5-2 แสดงตำแหน่งของการเข้ารหัสและถอดรหัส

จากรูปที่ 5-2 แสดงให้เห็นว่า การเข้ารหัสและถอดรหัสทันทีที่ ข้อมูลออกมาจากแหล่งส่งและรับข้อมูล จะทำให้ข้อมูลที่อยู่บนเครือข่าย เป็นข้อมูลที่ถูกเข้ารหัสแล้ว (Encrypted data) สำหรับการเลือกวิธีการในการเข้ารหัส จะต้องดูถึงความเหมาะสมในการนำมาใช้กับไมโครคอนโทรเลอร์เป็นหลัก เพราะถ้ากระบวนการนั้น มีความซับซ้อนมาก ก็จะยิ่งทำให้เวลาที่ใช้ในการเข้ารหัสบนไมโครคอนโทรเลอร์มากขึ้นตามไปด้วย และเนื่องด้วยการที่ไมโครคอนโทรเลอร์จะต้องทำงานหน้าที่อื่นด้วย เช่น การตรวจสอบอุปกรณ์ไฟฟ้า การรับและส่งข้อมูลบนเครือข่าย ดังนั้น วิธีการที่นำมาใช้ จึงไม่ควรยากจนเกินไป แต่ก็สามารถป้องกัน หรือสร้างความปลอดภัยให้แก่ข้อมูลได้ดี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.5.2 การเพิ่มลำดับของข้อมูลในเฟรมข้อมูล การเพิ่มลำดับของเฟรมข้อมูล เป็นเทคนิคที่ใช้เพื่อป้องกันการส่งข้อมูลซ้ำ(Reply Attack) อธิบายได้คือ ถ้าหากผู้บุกรุก สามารถดักจับสัญญาณข้อมูล แล้วส่งสัญญาณเดิมซ้ำๆ ระบบจะไม่มีทางรู้ได้เลยว่า ข้อมูลนั้นเป็นข้อมูลปลอม ระบบก็จะทำงานตามและทำงานผิดพลาด การเพิ่มลำดับเฟรมของข้อมูล สามารถป้องกันการบุกรุกแบบนี้ได้ แสดงได้ดังรูป 5-3



รูปที่ 5-3 Transition Diagram แสดงการป้องกันการส่งข้อมูลซ้ำด้วยวิธีลำดับข้อมูล

จากรูป ผู้ส่ง(Sender) จะเก็บลำดับ (Sequence) ของผู้รับไว้ ในส่วนของผู้รับ (Receiver) จะเก็บลำดับของเฟรมหลังสุดที่เคยรับไว้ ถ้าหากเฟรมที่ผู้รับ ได้รับ มีลำดับเป็นลำดับถัดไป แสดงว่า เป็นเฟรมที่มาจากผู้ส่งที่แท้จริง ผู้รับก็จะทำงานตามคำสั่งหรือข้อมูลที่ได้รับมา แต่ถ้าหากเฟรมดังกล่าว ลำดับเฟรมที่ไม่ถูกต้องตามลำดับ เฟรมนั้นก็จะถูกยกเลิกไป

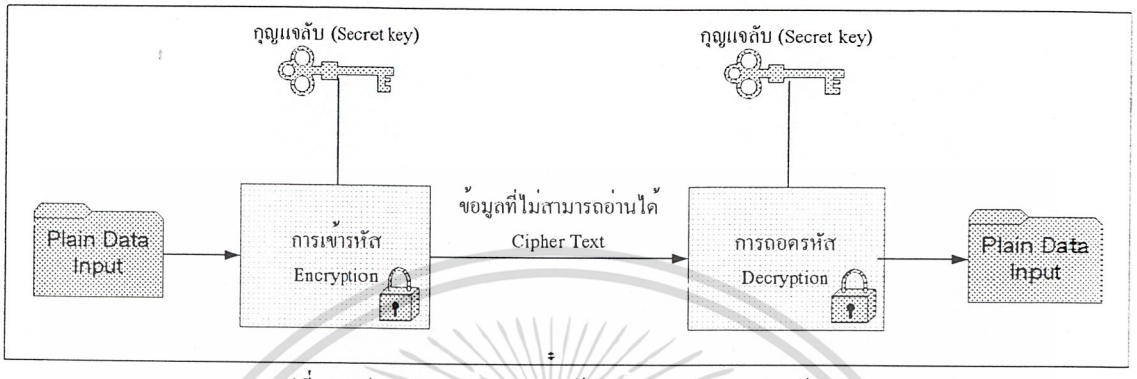
5.1.5.3 การปรับปรุงโปรแกรมที่ใช้งานบนไมโครคอมพิวเตอร์ที่ศูนย์ควบคุมหลัก โดยการเพิ่มเติมความปลอดภัยให้กับข้อมูลของชื่อผู้ใช้และรหัสผ่าน ด้วยการเก็บข้อมูลไว้ในตารางฐานข้อมูลของโปรแกรม MS SQL Server ซึ่งสามารถป้องกันการดูข้อมูลดังกล่าวได้โดยการใช้รหัสผ่านกับฐานข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.2 การเข้ารหัสและถอดรหัสข้อมูล

5.2.1 ทฤษฎีการเข้ารหัสและถอดรหัสข้อมูล

การเข้ารหัสข้อมูล เป็นการรักษาความลับของข้อมูลหรือปกปิดข้อมูล โดยที่ข้อมูลนั้นจะถูกเปิดเผยต่อบุคคลที่ได้รับอนุญาตเท่านั้น หลักการของการเข้ารหัสแสดงได้ดังรูปที่ 5-4



รูปที่ 5-4 แสดงกระบวนการเข้ารหัสและถอดรหัสข้อมูล

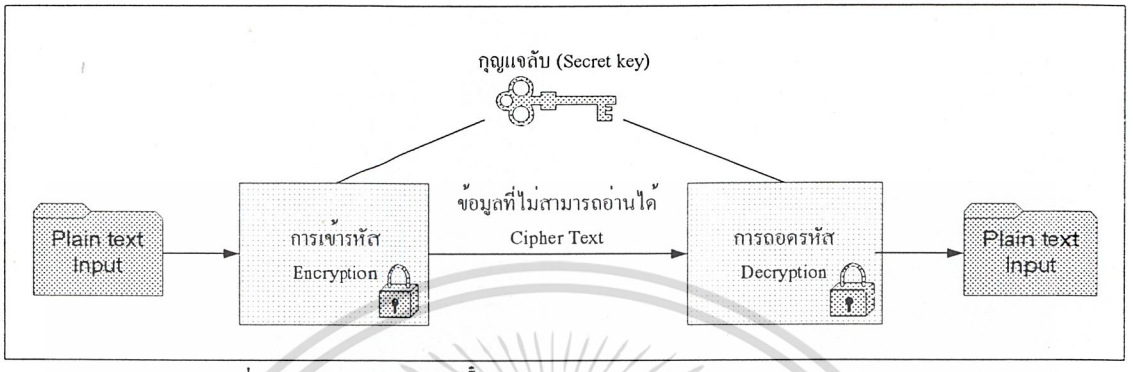
โดยที่

- Plain Data : ข้อมูลแรกเริ่มซึ่งยังไม่ได้มีการปกปิดข้อมูล
- Encryption : เป็นการใช้กระบวนการ(Algorithm)เข้ารหัส โดยรูปแบบของการแปลงข้อความของกระบวนการในการเข้ารหัส จะขึ้นอยู่กับกุญแจลับ(Secret) ที่ป้อนเข้าไป
- กุญแจลับ : เป็นรหัส เช่น ตัวอักษร ตัวเลข ที่ต้องป้อนเข้าไปในกระบวนการเข้ารหัส โดยรูปแบบการแปลงข้อความของอัลกอริทึมในการเข้ารหัส จะขึ้นกับกุญแจลับที่ป้อนเข้าไป
- Cipher text เป็นผลลัพธ์ที่ได้จากการเข้ารหัส โดยจะขึ้นกับข้อมูลแรกเริ่มและกุญแจลับที่ป้อนเข้าไป ข้อความที่เหมือนกันแต่มีกุญแจต่างกัน จะให้ผลลัพธ์ที่ต่างกันด้วย
- Decryption : เป็นการใช้กระบวนการย้อนกลับของการเข้ารหัสเพื่อทำการถอดรหัส โดยเมื่อใส่ข้อมูลที่ถูกเข้ารหัส (Cipher text) และกุญแจ ที่ถูกต้องเข้าไปจะต้องได้ข้อมูลเหมือนเดิม(Plain Data) ออกมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

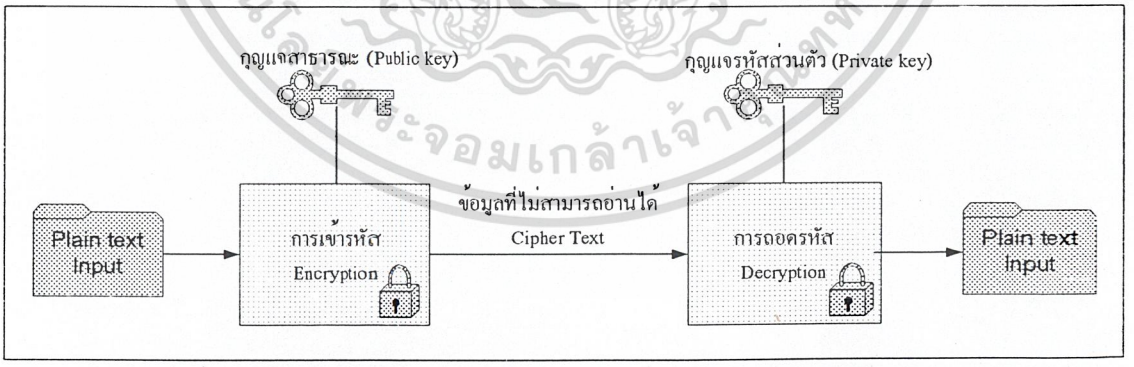
การเข้ารหัสโดยการใช้กุญแจในการเข้ารหัส แบ่งได้เป็น 2 วิธี คือ

1. การเข้ารหัสแบบสมมาตร หรือ Symmetric Encryption มีลักษณะคือ กระบวนการเข้ารหัสและถอดรหัสที่เป็นกระบวนการเดียวกัน โดยการใช้กุญแจเดียว(Single Key)คือทั้งการเข้ารหัส และถอดรหัสจะใช้กุญแจเดียวกัน แสดงได้ดังรูปที่ 5-5



รูปที่ 5-5 รูปแบบการเข้ารหัสแบบสมมาตร(Symmetric Encryption)

2. การเข้ารหัสแบบไม่สมมาตร หรือ Asymmetric-Key Encryption มีลักษณะการใช้กุญแจรหัสที่แตกต่างไปจากแบบสมมาตร นั่นคือ กุญแจที่ใช้ในการเข้ารหัสและถอดรหัส จะประกอบไปด้วย กุญแจคู่หนึ่ง คือ กุญแจรหัสลับ และ กุญแจรหัสสาธารณะ โดยที่กุญแจรหัสสาธารณะ ไม่จำเป็นต้องเก็บไว้เป็นความลับ สามารถแจกจ่ายไปให้ใครก็ได้ที่อยู่ในระบบ ส่วนกุญแจรหัสลับ จะเป็นกุญแจที่ถูกเก็บไว้เป็นความลับเฉพาะบุคคล ไม่มีการแจกจ่ายไปให้ใคร ดังนั้น แม้ผู้อื่นจะได้รับข้อความ ก็ไม่อาจทำการถอดรหัสได้เพราะไม่มีกุญแจรหัสลับ แสดงขั้นตอนการทำงานได้ดังรูปที่ 5-6



รูปที่ 5-6 รูปแบบการเข้ารหัสแบบอสมมาตร (Asymmetric-Key Encryption)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการใช้งานการเข้ารหัสในแบบกุญแจลับนี้ จะมีความจำเป็น 2 ประการเพื่อให้การใช้งานได้ผลดี คือ

1. อัลกอริทึมในการเข้ารหัส จะต้องมีความแข็งแกร่ง (Strong) ทั้งนี้เนื่องจากอัลกอริทึมที่เป็นแบบกุญแจลับ นี้ มักจะมีการเปิดเผยวิธีการอยู่แล้ว ดังนั้นผู้อื่นก็ย่อมจะรู้วิธีการเข้าและถอดรหัสเช่นเดียวกัน ดังนั้นจากส่วนประกอบของกระบวนการเข้ารหัส ผู้อื่นก็จะรู้ถึง Cipher text เพราะสามรถดักได้จากกระบวนการส่ง และสามารถรู้อัลกอริทึม แต่สิ่งที่ผู้อื่นไม่รู้ก็คือกุญแจลับ ดังนั้นเพื่อให้ได้ข้อความต้นฉบับกลับมา ก็ต้องหากุญแจลับ เพื่อจะได้ใช้ในการถอดรหัสได้ ดังนั้นอัลกอริทึมนี้ จะต้องมีความแข็งแกร่งมากพอที่จะปิดบังกุญแจลับเอาไว้ แม้ว่าจะได้ทั้ง Plain Data และ Cipher text ก็ไม่สามารถหากุญแจลับได้
2. จากที่ได้กล่าวมา จะเห็นได้ว่าหัวใจของกระบวนการการเข้ารหัสแบบนี้ คือกุญแจลับ ซึ่งจะเห็นได้ว่า แม้จะทราบถึงส่วนประกอบต่าง ๆ ทั้งหมด แต่ไม่ทราบกุญแจลับ ก็ไม่สามารถจะบุกรุกหรือรบกวนกระบวนการได้ ดังนั้นการรักษากุญแจลับไว้ จึงมีความสำคัญอย่างยิ่ง และวิธีการเข้ารหัสในแบบกุญแจลับนี้ ก็จะถือว่า กระบวนการรับส่ง หรือ แจกจ่ายกุญแจลับจะต้องมีความปลอดภัย โดยจะถือว่าผู้รับสารและผู้ส่งสาร จะต้องมีช่องทางในการรับส่งกุญแจลับอย่างปลอดภัยอยู่แล้ว เพราะถ้าหากมีผู้อื่นได้กุญแจลับไป กระบวนการเข้ารหัสเพื่อรักษาความลับ ก็จะไม่เป็นความลับต่อไป

จากที่กล่าวมา จะเห็นความปลอดภัยของการเข้ารหัส หรือ การรักษาความลับระหว่างการรับส่งข้อมูล ของวิธีการเข้ารหัสแบบกุญแจลับ นี้จะขึ้นกับความลับของกุญแจลับ ไม่ใช่ความลับของอัลกอริทึม ทั้งนี้เนื่องจากการได้มาซึ่งอัลกอริทึมสัก 1 ตัวที่ความสามรถตามความต้องการของหลักการเข้ารหัสแบบกุญแจลับ นั้นเป็นเรื่องไม่ง่ายนัก ดังนั้นหากใช้วิธีให้ความลับอยู่ที่อัลกอริทึมแล้วหากถูกเปิดเผยก็ต้องสร้างอัลกอริทึมใหม่ขึ้นมา ในขณะที่ใช้วิธีให้ความลับอยู่ที่กุญแจลับแล้ว หากกุญแจลับมีการเปิดเผย ก็เพียงแต่สร้างกุญแจลับใหม่ขึ้นมาเท่านั้น ซึ่งเป็นเรื่องง่ายกว่ามาก

และโดยการเปิดเผยอัลกอริทึมนี้เอง ที่ทำให้การใช้งานการเข้ารหัสแบบกุญแจลับ สามารถใช้งานได้อย่างกว้างขวาง เพราะไม่จำเป็นที่แต่ละคนจะต้องสร้างอัลกอริทึมในการเข้ารหัสของตัวเองขึ้นมา แต่ใช้สิ่งที่เป็นมาตรฐานเหมือน ๆ กัน แต่ใช้กุญแจลับที่ต่างกัน และจากการที่ทุกคนรู้อัลกอริทึม ก็ไม่จำเป็นที่จะต้องบอกวิธีการให้อีกฝ่ายทราบ เพียงแต่เข้าใจตรงกันว่ากำลังใช้อัลกอริทึมไหน และใช้กุญแจ อะไรอยู่ก็พอแล้ว นอกจากนั้นยังสามารถสร้างการเข้ารหัสในรูปแบบของฮาร์ดแวร์ได้ด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.2.2 การเข้ารหัส

ระบบการเข้ารหัสนั้น โดยทั่วไปจะมีการพิจารณาใน 3 มุมมองด้วยกัน คือ

1. รูปแบบของการกระทำที่ใช้ในการแปลงจาก Plain text ไปเป็น Cipher text ในอัลกอริทึมของการเข้ารหัสทุกรูปแบบ มักจะตั้งอยู่บนหลักการ 2 หลัก คือ การแทนที่ (Substitution) และการสลับที่ (Transposition) โดยหลักการแทนที่ จะใช้วิธีแทนส่วนประกอบของข้อมูลที่จะทำการส่งหรือ Plain text (บิต กลุ่มของบิต ไบต์ หรือตัวอักษร) ด้วยส่วนประกอบอีกกลุ่มหนึ่ง และวิธีการสลับที่นั้น จะเป็นการจัดลำดับของบิต กลุ่มของบิต ไบต์ หรือตัวอักษร ใหม่ให้มีรูปแบบที่เปลี่ยนไป โดยในระหว่างกระบวนการทำนั้น จะต้องไม่มีข้อความ หรือส่วนใดๆของข้อความที่หายไป ทั้งนี้ก็เพื่อให้กระบวนการย้อนกลับสามารถทำได้
2. จำนวนของกุญแจที่ใช้ในการเข้ารหัส ถ้าหากผู้รับและผู้ส่งใช้กุญแจเดียวกันจะเรียกวิธีในการเข้ารหัสนั้น ว่า Symmetric Key ในขณะที่ ถ้าหากผู้รับและผู้ส่งใช้กุญแจที่แตกต่างกัน ก็จะเรียกว่า Asymmetric Key
3. ลักษณะที่อัลกอริทึมทำกับข้อความต้นฉบับ โดยจะแบ่งเป็น 2 แบบ คือ Block Cipher เป็นการแบ่งข้อมูลออกเป็นส่วนๆที่มีความยาวเท่ากัน แล้วจึงประมวลผลข้อมูลออกไปทีละ Block โดยจะได้ผลลัพธ์เป็น Block ในขณะที่อีกแบบ คือ Stream Cipher เป็นการประมวลผลทีละกลุ่ม โดยผลลัพธ์ก็จะออกมาในลักษณะเดียวกัน

5.2.3 การถอดรหัส

การถอดรหัสมีกระบวนการได้หลายรูปแบบ หลายวิธี ทั้งนี้ต้องขึ้นกับกระบวนการเข้ารหัส ซึ่งโดยทั่วไปแล้วการออกแบบอัลกอริทึมในการเข้ารหัสนั้น จะถือว่าประสบความสำเร็จในการรักษาความปลอดภัย เมื่อรหัสที่สร้างขึ้นมาโดยอัลกอริทึมนั้น มีค่าใช้จ่ายที่ต้องใช้ในการถอดรหัสจะต้องมากกว่ามูลค่าของข้อมูลที่เข้ารหัส หรือ เวลาที่ใช้ในการถอดรหัสจะต้องมากกว่าอายุการใช้งานของข้อมูลนั้น

เนื่องจากความต้องการข้อมูลที่เข้ารหัส ก็เนื่องจากความต้องการนำข้อมูลนั้นไปใช้ประโยชน์ แต่ถ้าหากค่าใช้จ่ายที่ต้องใช้ในการถอดรหัส มีมูลค่ามากกว่าตัวข้อมูลเองแล้ว ก็ไม่มีความคุ้มค่าในการถอดรหัส แต่การประเมินค่าของข้อมูลเป็นเรื่องที่พิจารณาได้ยาก ดังนั้นโดยส่วนใหญ่จึงมักจะประเมินความปลอดภัยของอัลกอริทึมเพราะเป็นสิ่งที่พิจารณาได้ง่าย ดังนั้นถ้าหากอัลกอริทึมที่ออกแบบมาไม่มีจุดอ่อน การถอดรหัสจะต้องใช้วิธีที่เรียกว่า Brute-Force เพียงอย่างเดียว

สำหรับวิธี Brute-Force เป็นวิธีการที่ลองเดาค่าของกุญแจในทุกๆค่าที่เป็นไปได้ ซึ่งหมายความว่าวิธีการนี้ สามารถที่จะถอดรหัสได้อย่างแน่นอน แต่ทั้งนี้ เวลาที่ใช้ในการถอดรหัสจะขึ้นอยู่กับจำนวนบิตของกุญแจ ซึ่งสามารถอ้างอิงได้จากตารางที่ 5-3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขนาดของกุญแจ(Bits)	จำนวนของกุญแจที่เป็นไปได้	เวลาที่ใช้ เมื่อความเร็วในการถอดรหัสคือ 1 Decryption / μS	เวลาที่ใช้ เมื่อความเร็วในการถอดรหัสคือ 10^6 Decryption / μS
32	4.3×10^9	35.8 นาที	2.15 ล้านวินาที
56	7.2×10^{16}	1142 ปี	10 ชั่วโมง
128	3.4×10^{38}	5.4×10^{24} ปี	5.4×10^{18} ปี
168	3.7×10^{50}	5.9×10^{36} ปี	5.9×10^{30} ปี

ตารางที่ 5-3 แสดงเวลาที่ใช้ในการถอดรหัสแบบ Brute-Force

5.3 อัลกอริทึมการเข้ารหัสและถอดรหัส

กระบวนการในการเข้ารหัส(Algorithm) ในปัจจุบันมีมากมายหลายวิธี เช่น Blowfish , Data Encryption Standard (DES) , Triple Data Encryption Algorithm (Triple DES) , Advanced Encryption Standard (AES) ,Secure Hash Algorithm (SHA-1) , Secure Hash Algorithm (SHA-256) , Secure Random Number Generator (RNG) , Old-style Random Number Generator (RAN) ในที่นี้ จะกล่าวถึงวิธีที่ได้นำมาใช้ในโครงงานนี้เท่านั้น นั่นคือ อัลกอริทึมแบบ DES ทั้งนี้ เนื่องมาจาก อัลกอริทึมนี้ ไม่ยากและซับซ้อนจนเกินไป เหมาะที่จะนำมาใช้กับไมโครคอนโทรเลอร์ และเป็นวิธีการที่ได้รับการยอมรับอย่างกว้างขวาง

5.3.1 DES (Data Encryption Standard)

เป็นวิธีการเข้ารหัสที่ใช้กันอย่างแพร่หลายที่เป็นพื้นฐาน Data Encryption Standard (DES) ที่พัฒนาขึ้นในปี 1977 โดย National Bureau of Standards ซึ่งปัจจุบันคือ Federal Information Processing Standard 46 (FIPS PUB46) สำหรับ DES ข้อมูลจะถูกเข้ารหัสเป็นบล็อกขนาด 64 บิต ซึ่งใช้คีย์ 56 บิต โดยการจัดการกับข้อมูล 64 บิตที่เข้ามาเพื่อแปลงเป็นข้อมูล 64 บิตออกไป และใช้คีย์เดียวกันนี้ในการถอดรหัส

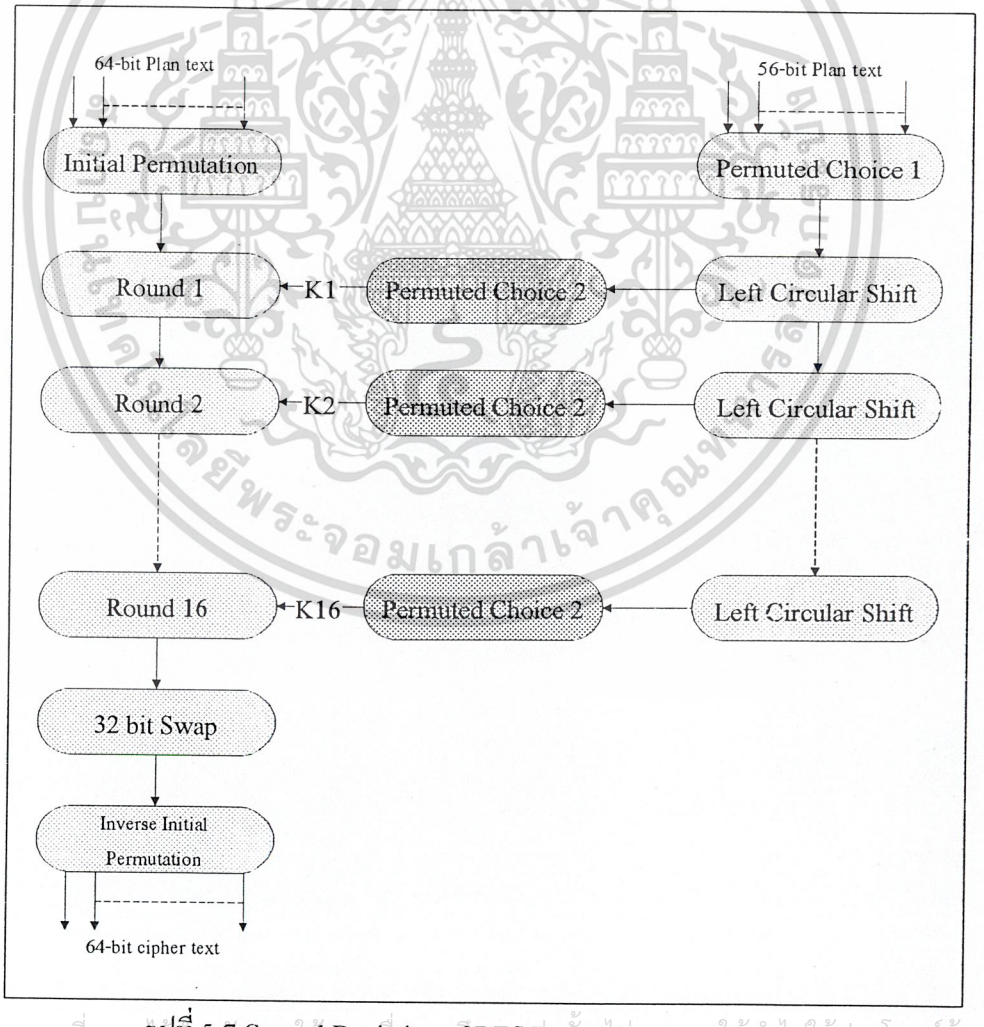
ระบบการเข้ารหัส และถอดรหัสแบบ DES ในกลุ่ม 64 bit block มีการใช้กุญแจแบบ 64 bit โดยระบบนี้สามารถที่จะปกป้องข้อมูลได้ เพราะข้อมูลจะถูกเปลี่ยนจากข้อมูลดิบหรือข้อความที่สามารถอ่านเข้าใจได้ (Clear/plain Text) ไปเป็นข้อมูลที่ไม่สามารถจะอ่านและเข้าใจได้ (Cipher Text) เพราะว่า DES ทำงานบนกลุ่มข้อมูลของ block ที่มีขนาดเท่ากัน และ DES สามารถใช้ได้ ทั้งการสลับที่กันและการแทนที่กันในระบบการคำนวณแบบอัลกอริทึม DES จึงเป็นทั้ง block cipher และเป็นผลลัพธ์ (output) ของข้อมูลที่ไม่สามารถอ่านเข้าใจได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

DES เป็นระบบแบบ 16 รอบ ซึ่งหมายความว่า อัลกอริทึมหลักจะถูกทำซ้ำ 16 ครั้งเพื่อเปลี่ยนข้อมูลให้ไม่สามารถจะอ่านและเข้าใจได้ ระบบ DES ถูกพบว่าจำนวนรอบมีสัดส่วนสัมพันธ์กับจำนวนเวลาที่ต้องการใช้ในการหากุญแจเข้ารหัสลับแบบ exponential ด้วยการใส่ข้อมูลแบบมั่วๆ ไร้เหตุผล ด้วยจำนวนรอบที่เพิ่มขึ้น ระบบรักษาความปลอดภัยแบบ algorithm จะเพิ่มขึ้นตามแบบ exponential

แม้ว่า DES ถูกนำมาใช้งานตั้งแต่ช่วงทศวรรษที่ 70 (ค.ศ.1960-1970) และได้รับการตอบรับอย่างดีจากนักวิเคราะห์รหัส (Cryptanalysis) อย่างแพรหลาย แต่ก็เป็นข้อถกเถียงกันเป็นอย่างมากถึงเรื่อง DES นั้นจะปลอดภัยหรือไม่มีความปลอดภัยมากน้อยขนาดไหน แต่ปัจจุบันเราก็ยังไม่พบช่องโหว่ของ DES ตามเอกสารที่ตีพิมพ์เป็นสาธารณะ แม้ว่าจะใช้คีย์เพียงไม่กี่บิตก็ตาม ในทางตรงกันข้ามแนวคิดแบบ IDEA กลับใช้คีย์แบบ 128 บิต (ซึ่งมากกว่า 2 เท่าของ DES) และได้รับการตอบรับจากสาธารณะตั้งแต่ทศวรรษที่ 90 (ค.ศ.1980-1990) (แต่ดีไม่เท่าตอนประกาศใช้ DES) IDEA มีความปลอดภัยมากกว่า DES และสามารถประมวลผลได้เร็วกว่า DES อย่างไรก็ตาม IDEA ยังต้องรอการตรวจสอบจากผู้เชี่ยวชาญอีกมากถึงเรื่องช่องโหว่ของความปลอดภัย

5.3.1.1 อัลกอริทึมของการเข้ารหัสแบบ DES



รูปที่ 5-7 General Depiction of DES Encryption Algorithm

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อัลกอริทึมการทำงานของ DES แสดงไว้ดังรูป 5-7 โดย DES จะใช้บล็อกข้อมูลขนาด 64 บิต และใช้คีย์ขนาด 56 บิต โดยหากข้อมูลมีขนาดใหญ่กว่า 64 บิตก็จะแบ่งเป็นบล็อกละ 64 บิต จากรูปทางด้านฝั่งซ้าย จะแสดงการนำบล็อกข้อมูลมาแบ่งออกเป็น 3 ช่วงย่อย โดยช่วงแรกจะเป็นการนำเอาบล็อกข้อมูลมาผ่านการสลับบิตขั้นต้น (Initial Permutation) ซึ่งจะสลับบิตทั้งหมดเสียใหม่ จากนั้นจะเข้าสู่ช่วงที่ 2 โดยประกอบด้วยการทำฟังก์ชัน Round จำนวน 16 ครั้ง และช่วงสุดท้าย จะประกอบไปด้วยการสลับกลุ่มข้อมูล 32 บิตซ้ายและขวา จากนั้นจะนำมาผ่านการสลับบิตย้อนกลับ (Reverse Initial Permutation) อีกครั้งก็จะได้ออกมาเป็น Cipher text ที่มีความยาวเท่ากับ Plaintext ที่เข้าไปคือ 64 บิต

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

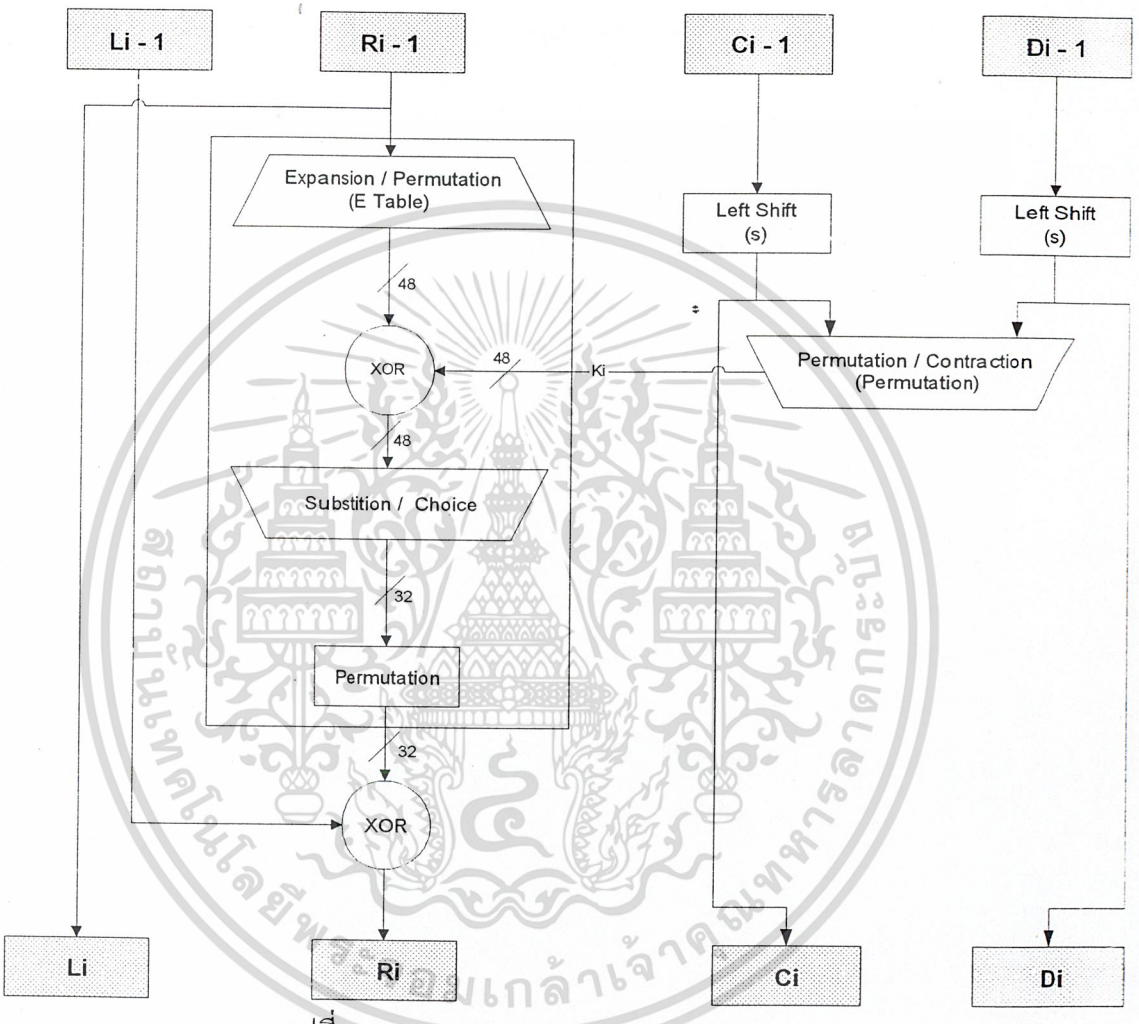
ตารางที่ 5-4 ตาราง Initial Permutation

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

ตารางที่ 5-5 ตารางInverse Permutation

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำหรับทางด้านฝั่งขวา จะแสดงกระบวนการในการสร้างคีย์ย่อย โดยเริ่มต้นคีย์หลักที่มีความยาว 56 บิต จะผ่านฟังก์ชันการสลับบิต 1 จากนั้นจะนำผลลัพธ์ที่ได้ไปใช้ในการสร้างคีย์ย่อยจำนวน 16 คีย์ ในแต่ละครั้งของการสร้างคีย์ย่อยนั้น จะมีการทำ Circular Shift และนำผลลัพธ์ที่ได้ไปผ่านฟังก์ชันการสลับบิต 2 จากทั้งหมดที่ได้กล่าวมา คงจะเห็นภาพรวมของการเข้ารหัสแบบ DES สำหรับรายละเอียดของการเข้ารหัสในแต่ละรอบนั้น ได้แสดงไว้ในรูปที่ 5-8



รูปที่ 5-8 Single Round of DES Algorithm

จากรูปจะเห็นได้ว่าในแต่ละรอบการทำงานนั้น จะมีการแบ่งข้อมูลออกเป็น 64 บิตที่ได้จากผลของการทำงานในรอบก่อนหน้าออกเป็นข้อมูล 32 บิต 2 ชุด โดยจะเรียกว่าชุด L และชุด R โดยสมการการสร้างชุดข้อมูล L และ R ในรอบ I ได้ดังนี้

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_i\text{-}1, K_i)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำหรับฟังก์ชัน F นั้นเป็นฟังก์ชันที่มีการทำงานในแบบที่มีการสลับบิต (Permutation) และการแทนที่ (Substitution) โดยผ่าน E Table และ S-BOX โดย E Table จะเป็นการสลับบิตในแบบที่มีการขยายข้อความยาวด้วย โดยตาราง E สามารถดูได้จากตารางข้างล่างนี้ จากนั้นจะนำผลลัพธ์ที่ขยายเป็น 48 บิตไป XOR กับคีย์ย่อย จากนั้นเมื่อผ่าน S-BOX แล้วจะถูกลดความยาวลงเหลือ 32 บิตเท่าเดิม และนำไปผ่านฟังก์ชันสลับบิต P อีกครั้ง

E-bit Selection Table					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

ตารางที่ 5-6 ตาราง E-bit Selection

P Permutation			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

ตารางที่ 5-7 ตาราง P Permutation

สำหรับกระบวนการในการถอดรหัส DES ก็จะมีลักษณะเช่นเดียวกับการเข้ารหัสทุกประการ ซึ่งถือว่าเป็นสิ่งสำคัญ โดยจะเป็นอัลกอริทึมเดียวกัน เพียงแต่เปลี่ยนอินพุตเป็น Cipher text และฟังก์ชั่นที่สร้างคีย์จะต้องสร้างออกมาในลำดับที่ย้อนกลับกันเท่านั้น ทั้งนี้เนื่องจากการเข้ารหัสนี้โดยภาพรวมแล้ว จะเป็นการสลับบิตข้อมูลไปมา โดยผ่านตารางที่มีรูปแบบตายตัว ซึ่งเป็นกระบวนการที่ย้อนกลับได้ และผ่าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ฟังก์ชัน XOR ซึ่งเป็นกระบวนการที่ย้อนกลับได้เช่นเดียวกัน ดังนั้นการออกแบบอัลกอริทึมที่เหมาะสม ก็ทำให้การถอดรหัสง่าย (หากทราบคีย์) แต่จะการแกะจะทำได้ยาก เพราะข้อมูลมีการเปลี่ยนไปมาก

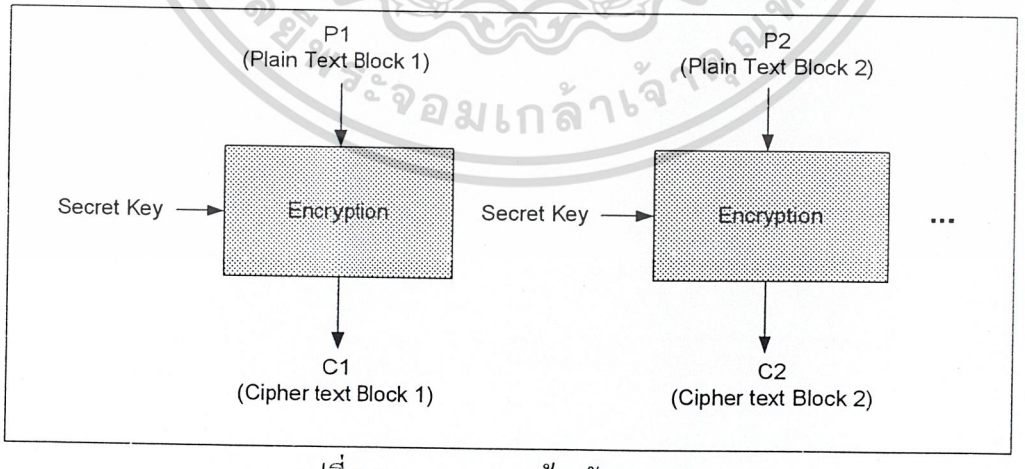
5.3.1.2 กระบวนการถอดรหัสแบบ DES

ระบบ ALGORITHM จะถูกใช้เพื่อการเข้ารหัสและถอดรหัสเพื่อปกป้องข้อมูลโดยวิธีการก็คือการเปลี่ยนกลุ่มข้อมูลที่สามารถอ่านได้เป็นข้อมูลที่ถูกเข้ารหัสหรือไม่สามารถอ่านได้ เพื่อที่จะถอดรหัสข้อมูลที่ไม่สามารถอ่านได้ให้เป็นข้อมูลต้นฉบับที่สามารถอ่านได้นั้น กระบวนการจะถูกทำซ้ำแต่กุญแจรหัสย่อยจะถูกใช้ในคำสั่งตรงกันข้ามจาก K[16]-K[1] นั่นคือขั้นที่2ของหน้าที่หลักตามโครงสร้างที่ได้กล่าวข้างต้น โดยเปลี่ยนจาก R[I-1] XOR K[I] เป็น R[I-1] XOR K[17-I] ยิ่งไปกว่านั้นการถอดรหัสจะถูกใช้กระบวนการเดียวกันกับการเข้ารหัส

5.3.1.3 โหมดการทำงานของอัลกอริทึม DES

5.3.1.3.1 ECB Electronic code book

ECBเป็นระบบการคำนวณพื้นฐาน DES algorithm ข้อมูลจะถูกแบ่งเป็น 64 bit block และแต่ละ block จะถูกเข้ารหัสครั้งเดียวและข้อมูลที่ถูกเข้ารหัสจะไม่ขึ้นต่อข้อมูลกลุ่มอื่นหมายความว่าถ้าข้อมูลที่ถูกส่งไปตามเครือข่าย network หรือตามสายโทรศัพท์ ความผิดพลาดจากการส่งข้อมูลจะมีผลกระทบต่อกลุ่มข้อมูลที่มีข้อผิดพลาดนั้นเท่านั้น อย่างไรก็ตามกลุ่มข้อมูลที่ผิดพลาดสามารถถูกจัดเรียงได้ใหม่ ดังนั้นกลุ่มข้อมูลที่ถูกรบกวนมากเกินกว่าที่จะรับได้ ก็จะไม่สามารถถูกตรวจพบ ECB จึงเป็นระบบที่ผิดพลาดมากที่สุดเพราะไม่มีระบบปกป้องข้อมูลอื่นใดถูกใช้นอกเหนือจากระบบพื้นฐานของ DES algorithm อย่างไรก็ตาม ECB เป็นระบบที่รวดเร็วที่สุด สะดวกที่สุด ในการใช้งานทำให้ วิธีการดำเนินงานแบบ ECB เป็นที่แพร่หลายในองค์การธุรกิจ แสดงกระบวนการได้ดังรูปที่ 5-9



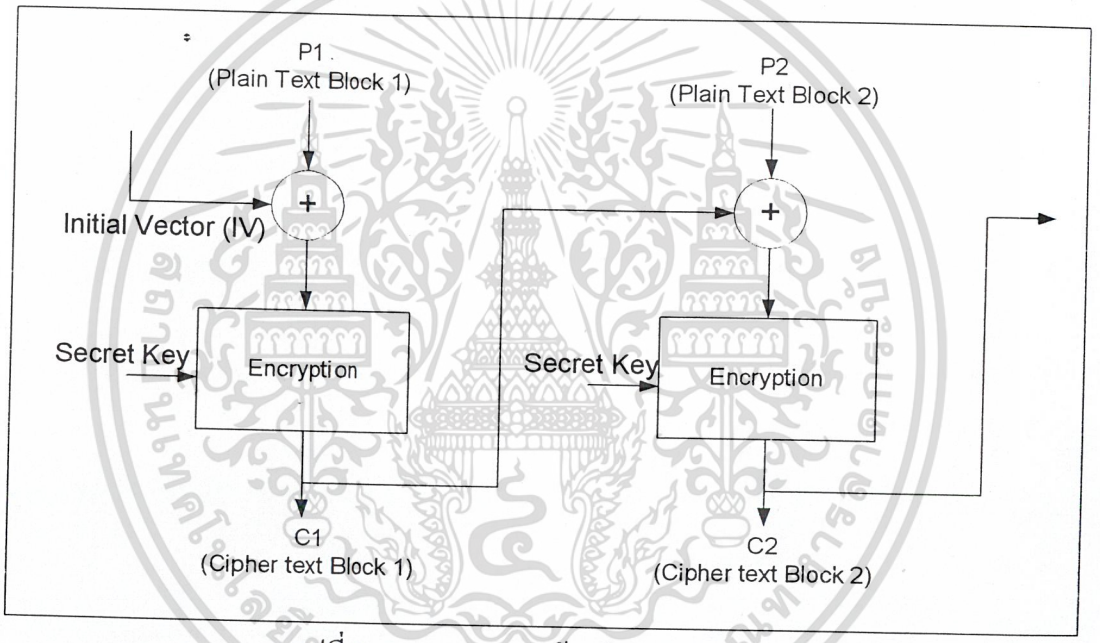
รูปที่ 5-9 กระบวนการเข้ารหัสแบบ ECB

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.3.1.3.2 CBC(Cipher Block Chaining)

ในวิธีการดำเนินงานนี้แต่ละ Block ข้อมูลของ ECBที่ถูกเข้ารหัสเป็น XOR กับกลุ่มข้อมูลที่สามารถอ่านได้กลุ่มถัดไปที่จะถูกเข้ารหัส ดังนั้นจะทำให้ กลุ่มข้อมูลทุก Block เป็นอิสระไม่ขึ้นกับข้อมูลที่ผ่านไปแล้ว นั้นคือการที่จะเจาะจงหา block ที่ต้องการจำเป็นต้องทราบถึงข้อมูลที่เข้ารหัสแล้ว กุญแจรหัส และข้อมูลที่ถูกเข้ารหัสก่อนหน้านั้น กลุ่มข้อมูล BLOCK แรกที่ถูกเข้ารหัสจะไม่มีข้อมูลที่ถูกเข้ารหัสก่อนหน้านั้น ดังนั้นข้อมูลดิบก็ เป็น XOR 16 บิต เรียกว่า Initialization Vector (IV)

ดังนั้นถ้าข้อมูลถูกส่งผ่านระบบเครือข่าย Network หรือสายโทรศัพท์และมีความผิดพลาดในการส่งเกิดขึ้น ข้อผิดพลาดจะถูกส่งผ่านไปในข้อมูลตัวต่อๆ ไปตามลำดับตั้งแต่ที่ผิดพลาดจนถึงข้อมูลกลุ่มสุดท้าย วิธีนี้เป็นวิธีการดำเนินงานที่ปลอดภัยกว่า ECB เพราะว่าจำนวนขั้นตอนที่เพิ่มขึ้นของ XOR จะเพิ่มกระบวนการเข้ารหัสมากกว่า 1 ขั้น แสดงได้ดังรูปที่ 5-10



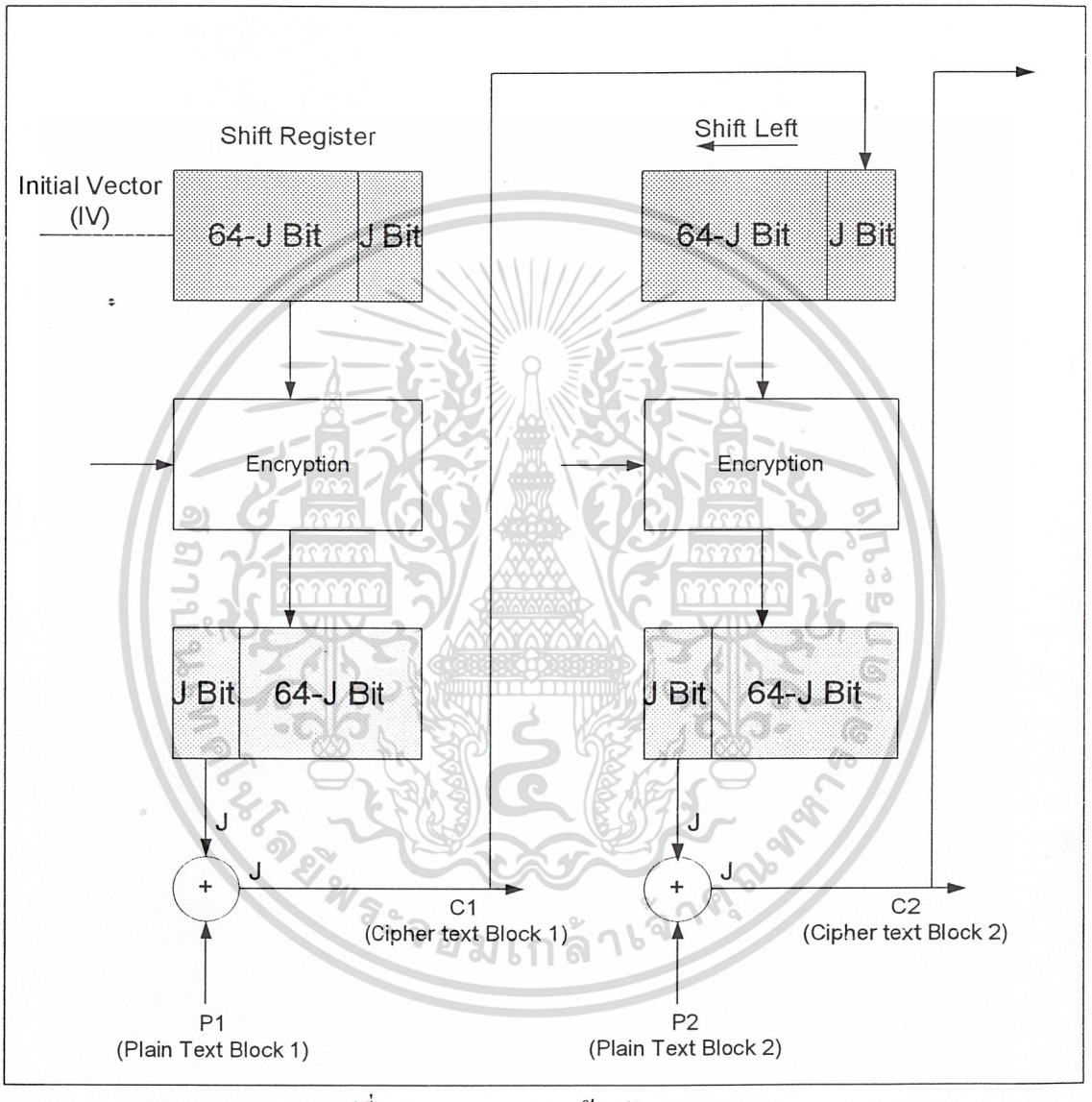
รูปที่ 5-10 กระบวนการเข้ารหัสแบบ CBC

ข้อดีของบล็อกไซเฟอร์ลักษณะนี้คือสามารถแก้ปัญหาการซ้ำกันของข้อมูลก่อนการเข้ารหัสเพราะต้องนำเพลนเท็กซ์มาเอ็กครูซีฟออร์ก่อนที่จะนำมาเข้ารหัส แต่มีข้อเสียเนื่องจากการเข้ารหัสแต่ละบล็อกต้องรอบล็อกข้างหน้ามันก่อนจึงจะทำการเข้ารหัสได้ไม่สามารถทำพร้อมกันได้ทำให้ช้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.3.1.3.3 CFB (Cipher Feed Back)

ขั้นแรกมี ชิฟรีจิสเตอร์ (Shift Register) ขนาด 64 บิต โดยกำหนดค่าเริ่มต้นเป็นเวคเตอร์เริ่มต้น (IV) แล้วนำมาเข้ารหัสกับคีย์ (K) จากนั้นนำ J บิต หน้าสุดมาเอ็กครูซีฟออร์กับเพลนเท็กซ์แล้วนำไซเฟอร์เท็กซ์ที่ได้ไปใช้ใน ชิฟรีจิสเตอร์ J บิตท้ายโดยเลื่อนไปด้านซ้าย ไป J บิตเพื่อนำไซเฟอร์เท็กเข้ามา ดังรูป 5-11 โดยส่วนใหญ่จะทำทีละ 8 บิตซึ่งคือ 1 ตัวอักษรโดยสามรถทำงานแบบเรียลไทม์ได้



รูปที่ 5-11 กระบวนการเข้ารหัสแบบ CFB

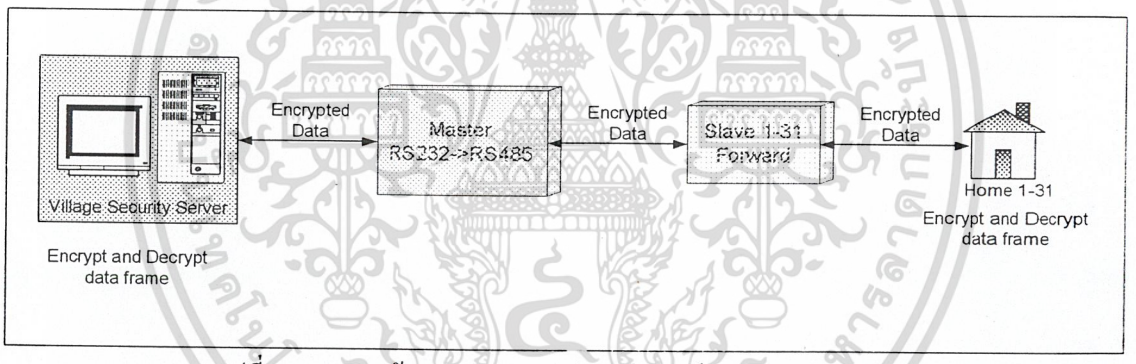
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.4 การปรับปรุงระบบด้วยการเพิ่มกระบวนการปกปิดข้อมูล

ระบบรักษาความปลอดภัยในหมู่บ้าน มีส่วนที่ทำหน้าที่หลักในการส่งข้อมูลและรับข้อมูลอยู่ 4 ส่วน ได้แก่

1. ส่วนโปรแกรมบนศูนย์ควบคุม ทำหน้าที่ในการประมวลผลคำสั่งเพื่อแสดงสถานะต่างๆของบ้าน และทำหน้าที่ในการส่งคำสั่งไปยังเครือข่าย
2. ส่วนของ Master node ทำหน้าที่ในการรับและส่งต่อเฟรมข้อมูลระหว่าง Computer กับ Slave node
3. ส่วนของ Slave node ทำหน้าที่ในการรับและส่งต่อเฟรมข้อมูลระหว่าง Master node กับ Home node
4. ส่วนของ Home node ทำหน้าที่ในการประมวลผลคำสั่ง และส่งสถานะ ต่างๆของอุปกรณ์ไฟฟ้าภายในบ้านแต่ละหลัง

จากส่วนการทำงานหลัก ทั้ง 4 ส่วน พบว่า ส่วนที่ทำหน้าที่ในการสร้างเฟรมคำสั่ง และส่งคำสั่งกับรับเฟรมคำสั่งและทำงาน ได้แก่ ส่วนของโปรแกรมควบคุมหลัก และ ส่วนของ Home node ดังนั้นจึงสามารถแสดงตำแหน่งของการเข้ารหัสและถอดรหัสได้ดังรูปที่ 5-12

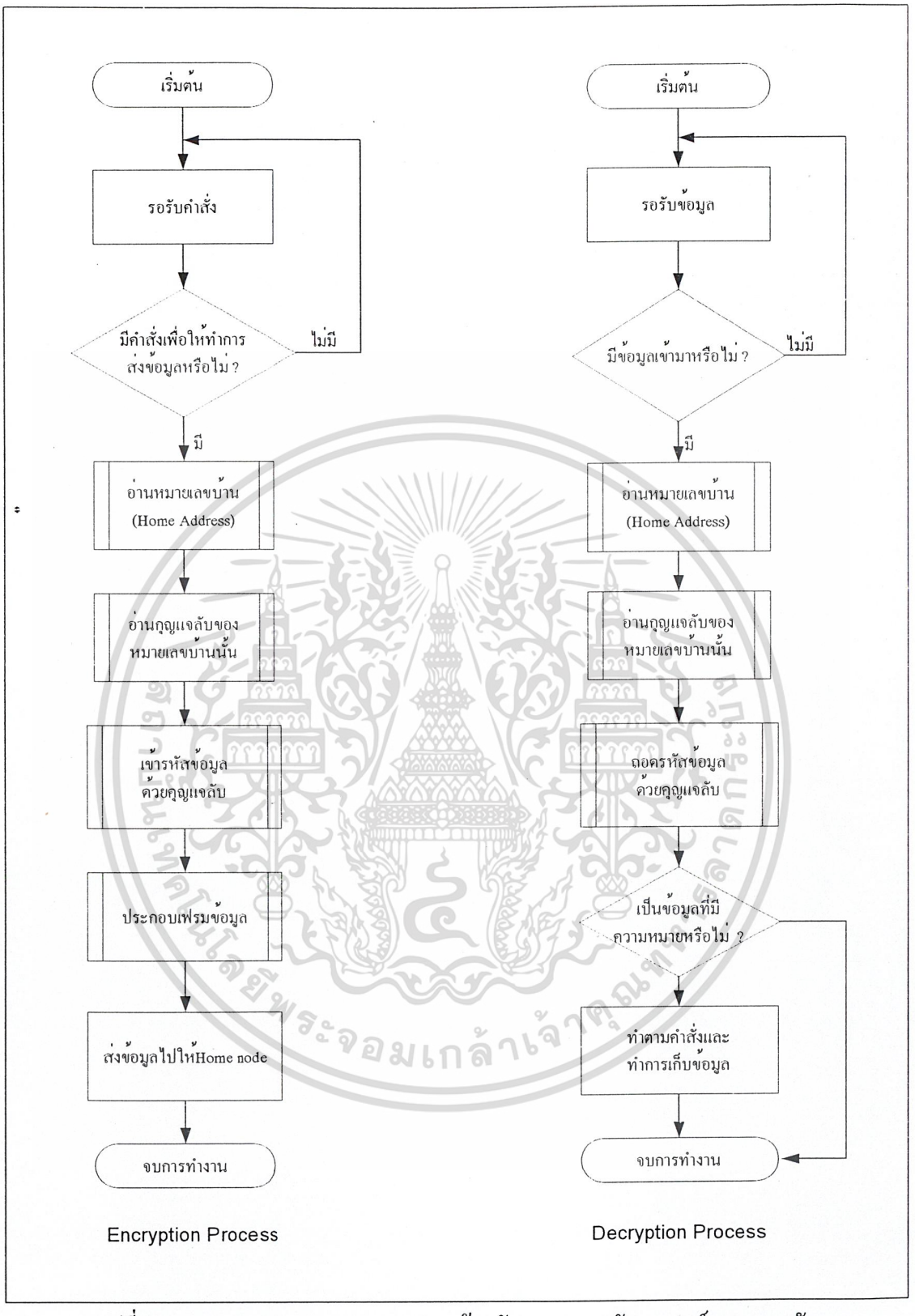


รูปที่ 5-12 แสดงข้อมูลและตำแหน่งของการเข้ารหัสและถอดรหัส

จากรูป 5-12 แสดงให้ว่า การเข้ารหัสข้อมูลที่ส่งมาจากโปรแกรมศูนย์ควบคุม และจาก Home node เป็นวิธีที่ทำให้ข้อมูลที่อยู่บนเครือข่ายถูกเข้ารหัสไว้ทั้งหมด ดังนั้น การออกแบบ จึงเลือกที่จะใช้อัลกอริทึม DES ที่ โปรแกรมศูนย์ควบคุมหลัก และ โปรแกรมในส่วนของไมโครคอนโทรเลอร์ที่ Home node

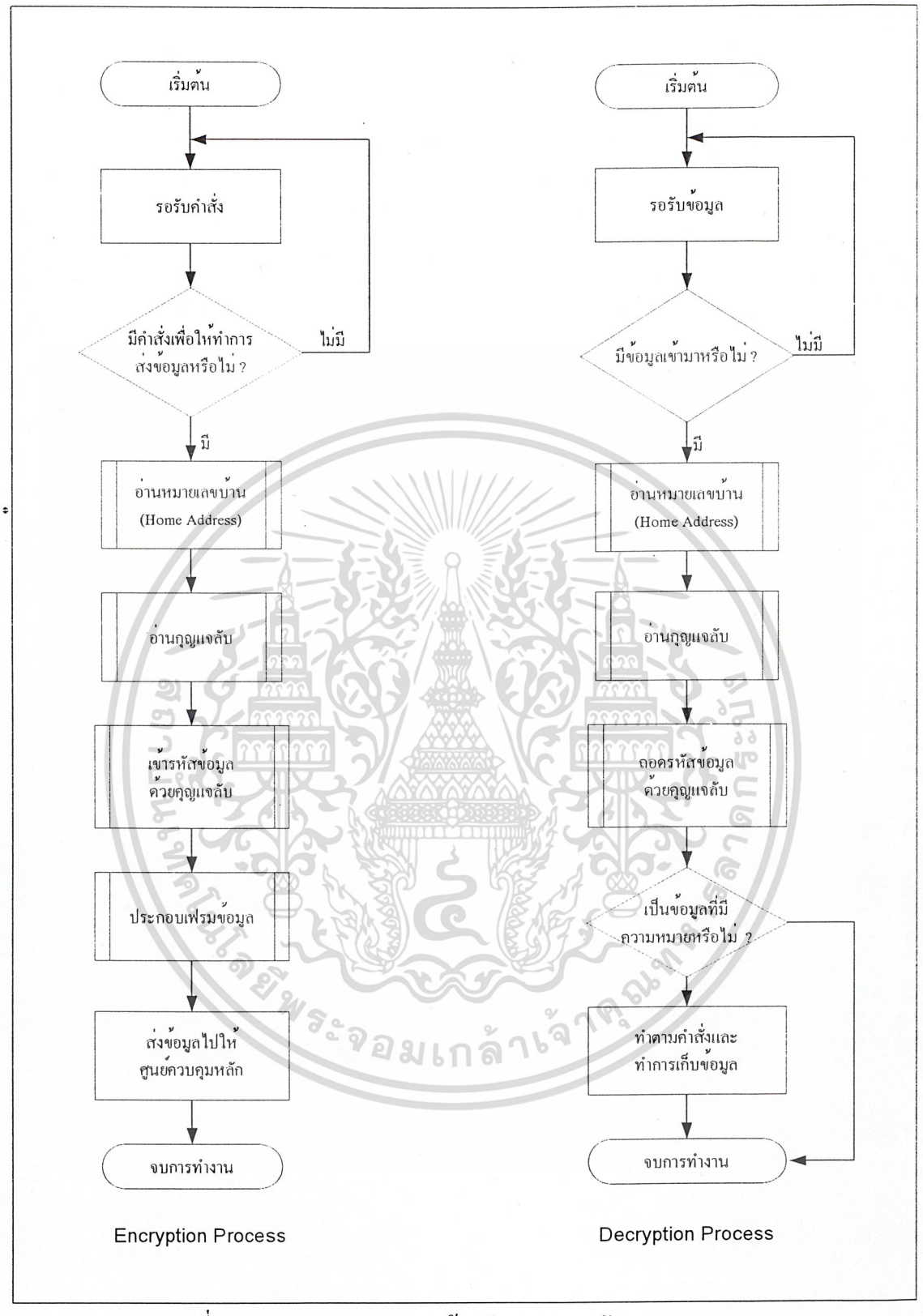
สำหรับกระบวนการในการเข้ารหัสและถอดรหัส สามารถแสดงกระบวนการโดย รูปที่ 5-13 Flow chart แสดงกระบวนการเข้ารหัสและถอดรหัสบนศูนย์ควบคุมหลัก รูปที่ 5-14 Flow chartแสดงการเข้ารหัสและถอดรหัสบนHome node

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5-13 Flow chart แสดงกระบวนการเข้ารหัสและถอดรหัสบนศูนย์ควบคุมหลัก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5-14 Flow chartแสดงการเข้ารหัสและถอดรหัสบนHome node

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 5-13 และ 5-14 แสดงให้เห็นถึงกระบวนการในการเข้ารหัสและถอดรหัสข้อมูล ซึ่งมีลักษณะใกล้เคียงกันระหว่างโปรแกรมศูนย์ควบคุมและโปรแกรมบน Home node คือ

ในขั้นตอนการเข้ารหัส เมื่อมีข้อมูลที่ต้องการจะส่ง จะทำการอ่านค่าของหมายเลขบ้านที่ต้องการส่งหรือหมายเลขบ้านของผู้ส่ง หลังจากนั้นถ้าเป็นโปรแกรมศูนย์ควบคุม จะต้องใช้หมายเลขบ้านดังกล่าวในการหากุญแจลับเพื่อใช้ในการเข้ารหัส ส่วนถ้าเป็นHome node จะใช้กุญแจลับซึ่งถูกเก็บไว้เป็นตัวแปร เมื่อได้กุญแจลับในการเข้ารหัส ขั้นตอนต่อไปจึงเป็นการเข้ารหัส และทำการประกอบเฟรมที่ได้ พร้อมส่งออกไป

สำหรับการถอดรหัส เมื่อมีข้อมูลเข้ามาจะทำการอ่านค่าของหมายเลขบ้านที่ส่งมาหรือหมายเลขบ้านของผู้รับ หลังจากนั้นถ้าเป็นโปรแกรมศูนย์ควบคุม จะต้องใช้หมายเลขบ้านดังกล่าว ในการหากุญแจลับเพื่อใช้ในการถอดรหัส ส่วนถ้าเป็นHome node จะใช้กุญแจลับซึ่งถูกเก็บไว้เป็นตัวแปร เมื่อได้กุญแจลับในการถอดรหัส ขั้นตอนต่อไปจึงเป็นการถอดรหัส ถ้าหากข้อมูลที่ได้หลังจากการถอดรหัสเป็นข้อมูลที่ไม่มีความหมาย ก็จะทำการละเลยข้อมูลนั้นทิ้งไป แต่ถ้าเป็นข้อมูลที่มีความหมาย ก็จะทำการตรวจคำสั่งทำตามคำสั่ง และบันทึกข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6
โปรแกรมของศูนย์ควบคุมหลัก

6.1 การออกแบบโปรแกรม

ระบบรักษาความปลอดภัยในหมู่บ้าน มีส่วนของโปรแกรมบนศูนย์ควบคุมหลักเพื่อใช้ในการแสดงผลและสั่งงานผ่านทางคอมพิวเตอร์ เนื่องจากเป็นระบบที่ต้องการความน่าเชื่อถือสูง เพราะว่าระบบจะต้องสามารถแจ้งการเตือนภัยในกรณีที่เกิดเหตุการณ์ผิดปกติได้อย่างรวดเร็ว

เนื่องจากโปรแกรมจะต้องนำไปใช้กับระบบรักษาความปลอดภัยในหมู่บ้าน ดังนั้น ความปลอดภัยภายในระบบไม่ว่าจะเป็นการจัดเก็บข้อมูล การสั่งงาน จึงควรมีความสำคัญมาก ใกล้เคียงกับความน่าเชื่อถือของระบบ จากเหตุผลดังกล่าว ในส่วนของการออกแบบโปรแกรม จึงควรเน้นหลักการออกแบบไว้ในส่วนดังต่อไปนี้

1. มีความปลอดภัยของโปรแกรมสูง
2. มีความน่าเชื่อถือสูง
3. โปรแกรมใช้งานง่าย
4. ยืดหยุ่นต่อการแก้ไข เพิ่มเติม
5. มีความรวดเร็วในการติดต่อ รับและส่งข้อมูล

สำหรับส่วนของภาษาที่จะนำมาใช้ในการจัดทำโปรแกรมของศูนย์ควบคุมหลัก พบว่า ภาษา Visual Basic เป็นภาษาที่มีความเหมาะสมกับหลักการการออกแบบได้อย่างดี ทั้งนี้เพราะว่า

1. MS Visual Basic สามารถอ้างอิงคอมโพเน้น(Component) หรือ Reference สำหรับการเชื่อมโยงกับฐานข้อมูล SQL ซึ่งเป็นฐานข้อมูลที่ได้ทำการเลือกไว้สำหรับเก็บข้อมูลที่มีความสำคัญ ทำให้เป็นส่วนสนับสนุนการสร้างความปลอดภัยให้กับโปรแกรมได้อย่างดี
2. MS Visual Basic มีความสามารถในการจัดการทรัพยากรของระบบได้ดี และสามารถทำงานได้ต่อเนื่องยาวนาน นอกจากนั้น ยังสามารถรายงานข้อผิดพลาดได้อย่างละเอียด
3. MS Visual Basic มี เครื่องมือ(Tools)สำหรับการทำส่วนติดต่อกับผู้ใช้ (User Interface) ให้มาค่อนข้างสมบูรณ์ และใช้งานง่าย
4. สนับสนุนการเชื่อมต่อกับฐานข้อมูลซึ่งต้องใช้ชื่อและรหัสผ่านสำหรับเข้าถึงข้อมูล
5. สนับสนุนการส่งข้อมูลผ่าน มาตรฐาน RS-485 โดยคอมโพเน้น MS Com Control 6.0

จะเห็นได้ว่า MS Visual Basic มีความเหมาะสมที่จะนำมาใช้เขียนโปรแกรม โดยที่ในการออกแบบโปรแกรม สามารถแบ่งการออกแบบเป็น 3 ส่วน คือ

1. ส่วนติดต่อกับผู้ใช้ (User Interface)
2. ส่วนติดต่อกับอุปกรณ์ Hardware เช่น Slave node และ Home node
3. ส่วนติดต่อกับฐานข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.1.1 ส่วนติดต่อกับผู้ใช้(User Interface)

ส่วนติดต่อกับผู้ใช้ ออกแบบเพื่อให้ผู้ใช้สามารถใช้งานโปรแกรมได้อย่างสะดวกและรวดเร็วต่อเหตุการณ์ที่เกิดขึ้น เช่น การเกิดสัญญาณเตือนภัยภายในบ้าน ผู้ใช้จะสามารถ ตรวจสอบความผิดปกติผ่าน User Interface ได้อย่างรวดเร็ว ก็สามารถทราบถึงเหตุการณ์ผิดปกติ ที่เกิดขึ้นได้

ส่วนติดต่อกับผู้ใช้สามารถแบ่งออกเป็นส่วนต่างได้ ดังนี้

1. ส่วน Login
2. ส่วนเมนูหลัก (Main Menu)
3. ส่วนที่ใช้จัดการเกี่ยวกับชื่อผู้ใช้ รหัสผ่านและการจัดการฐานข้อมูล
4. ส่วนที่ใช้สำหรับการกำหนดจำนวนบ้านและจำนวนSlaveในระบบ
5. ส่วนตรวจสอบและแสดงสถานะ
6. ส่วนควบคุมและสั่งงาน

6.1.1.1 ส่วน Login

เป็นส่วนที่ผู้ใช้จะต้องทำการแสดงตัวผู้ใช้ก่อนที่จะเข้าไปใช้งานในระบบต่อไปโดยโปรแกรมประกอบไปด้วย 3 ส่วนคือ

- Login เป็นส่วนที่ผู้ใช้จะต้องทำการกรอกชื่อผู้ใช้ และรหัสผ่าน ก่อนที่จะเข้าไปใช้งานในโปรแกรม
- Exit เป็นส่วนที่ใช้ในการออกจากโปรแกรม

6.1.1.2 ส่วนเมนูหลัก (Main Menu)

เป็นส่วนที่ใช้ควบคุมการใช้งานโปรแกรมทั้งหมด ซึ่งสามารถที่จะเข้าไปในส่วนต่างๆ ของโปรแกรมได้ จากส่วนของเมนูหลัก โดยประกอบไปด้วย 5 ส่วน คือ

- Login Management เป็นส่วนสำหรับผู้ดูแลระบบ(Admin) เพื่อใช้ในการจัดการเกี่ยวกับชื่อผู้ใช้ รวมไปถึงรหัสผ่าน
- Configuration เป็นส่วนสำหรับผู้ดูแลระบบ เพื่อใช้ในการแก้ไขข้อมูลจำนวนบ้าน จำนวนอุปกรณ์ตรวจจับ และจำนวนอุปกรณ์ไฟฟ้าที่ใช้ในบ้านแต่ละหลัง รวมไปถึงการแก้ไขข้อมูลเกี่ยวกับจำนวนบ้านในแต่ละโหนดของ Slave
- Status Report เป็นส่วนที่ใช้ในการตรวจสอบสถานะต่างๆของอุปกรณ์ตรวจจับและอุปกรณ์ไฟฟ้าในบ้านแต่ละหลัง
- Device Control เป็นส่วนสำหรับการสั่งงาน ควบคุมอุปกรณ์ไฟฟ้าภายในบ้าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.1.1.3 ส่วนที่ใช้จัดการเกี่ยวกับชื่อผู้ใช้ รหัสผ่านและการจัดการฐานข้อมูล

เป็นส่วนที่ติดต่อกับฐานข้อมูลของ MS SQL server ซึ่งจัดเก็บตารางของชื่อผู้ใช้และรหัสผ่าน ตารางสำหรับSlave node และตารางสำหรับHome node

6.1.1.4 ส่วนที่ใช้สำหรับการกำหนดจำนวนบ้านและจำนวนSlaveในระบบ

ใช้สำหรับการแก้ไขข้อมูล และเพิ่มเติมข้อมูล เช่น จำนวนบ้านในแต่ละ Node ของ Slave หรือ จำนวนอุปกรณ์ตรวจจับ อุปกรณ์ไฟฟ้า ในแต่ละบ้าน

6.1.1.5 ส่วนตรวจสอบและแสดงสถานะ

เป็นส่วนที่ใช้ในการตรวจสอบว่า ภายในบ้าน หรือ Slave ไหน มีเหตุผิดปกติเกิดขึ้นบ้าง และสามารถตรวจสอบได้ว่าเกิดจากบ้านหลังไหน โดยมีการแสดงสถานะสีของปุ่มทำให้สามารถเห็นได้อย่างชัดเจน

6.1.1.6 ส่วนควบคุมและสั่งงาน

เป็นส่วนที่ใช้ในการควบคุมอุปกรณ์ไฟฟ้า รวมทั้งสามารถตรวจสอบได้ว่าอุปกรณ์ไฟฟ้ามีการเปิดใช้งานทิ้งไว้หรือไม่ โดยสามารถเปิด และปิดอุปกรณ์เหล่านั้น ผ่านทางโปรแกรมศูนย์ควบคุมหลักได้

6.1.2 ส่วนติดต่อกับอุปกรณ์ Hardware

เป็นส่วนที่ไมโครคอมพิวเตอร์ใช้สำหรับการส่งข้อมูลไปยังเครือข่าย RS-485 โดยผ่านMaster node ซึ่งเชื่อมต่อตามมาตรฐานแบบ RS-232 กับไมโครคอมพิวเตอร์

6.1.3 ส่วนที่ใช้สำหรับการติดต่อฐานข้อมูล

เป็นส่วนที่โปรแกรมใช้ในการติดต่อกับฐานข้อมูลของ MS SQL Server โดยการใช้การอ้างอิงคอมโพเน้นที่ใช้ติดต่อกับฐานข้อมูลของโปรแกรม Visual Basic

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.2 การทำงานของโปรแกรมและการใช้งาน

การทำงานของโปรแกรม จะต้องทำการเตรียมโปรแกรมให้พร้อมเสียก่อน โดยสามารถศึกษาขั้นตอนการเตรียมโปรแกรมต่างๆก่อนใช้งานได้ที่ ภาคผนวก...

เมื่อทำการเปิดโปรแกรม จะมีการโหลด Form ของ Menu ต่างๆ เพื่อใช้ในการแสดงผลให้ผู้ใช้งานสามารถใช้งานได้อย่างง่าย โดยการเลือกปุ่มบน Menu ซึ่งแบ่งเป็น Form หลักๆ ได้ 6 Form คือ

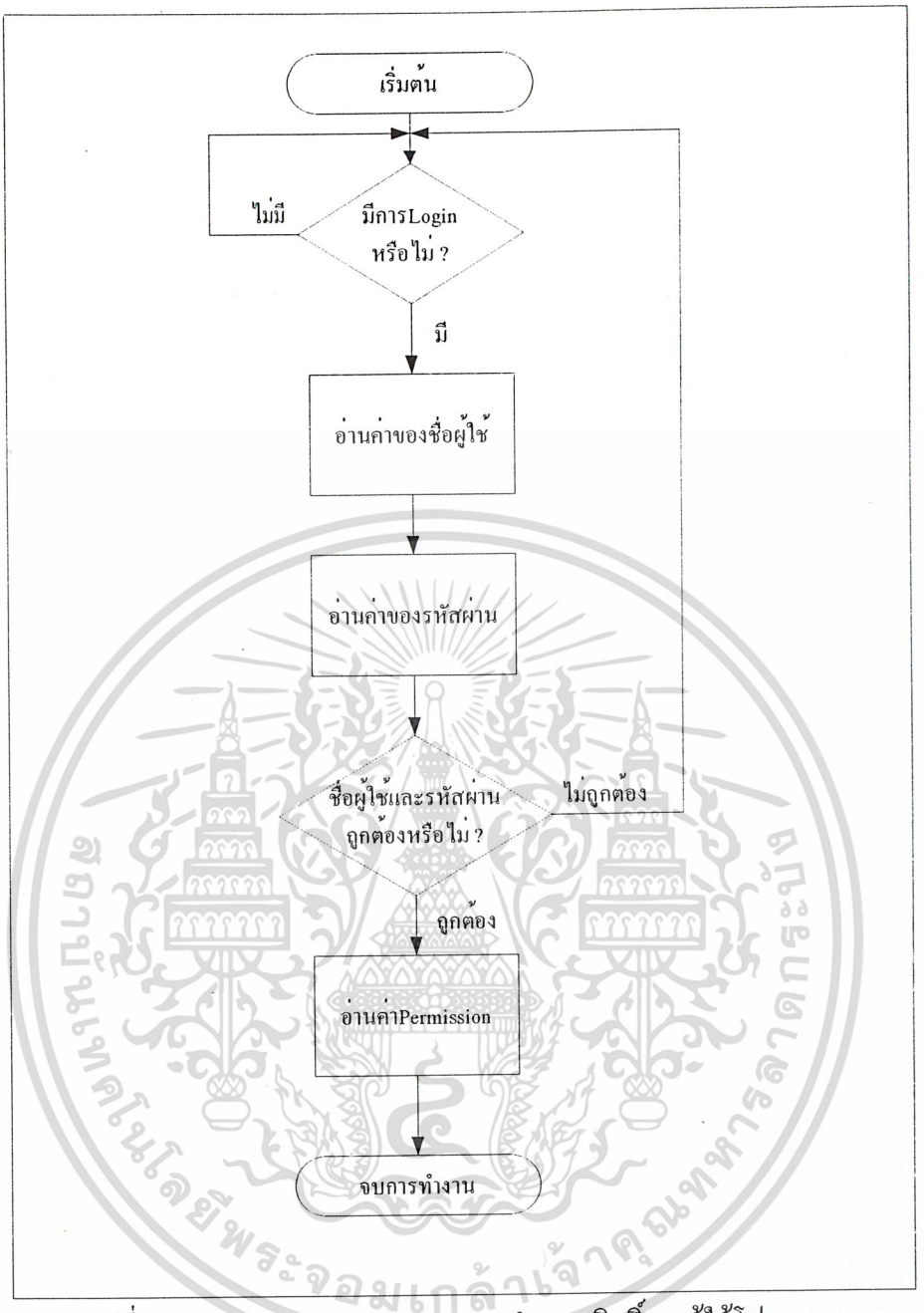
1. Form Login
2. Form Main Menu
3. Form Login Management
4. Form Configuration
5. Form Status Report
6. Form Device Control

6.2.1 Form Login

โดยการทำงานของโปรแกรม จะแบ่งประเภทของผู้ใช้ออกเป็น 2 แบบ คือ ผู้ใช้ที่เป็นผู้ดูแลระบบและผู้ใช้ที่เป็นผู้ใช้ทั่วไป สำหรับความแตกต่างของประเภทผู้ใช้ทั้ง 2 ก็คือ สิทธิ์ในการเข้าถึงฐานข้อมูลของระบบ ซึ่งผู้ใช้ที่เป็นผู้ดูแลระบบเท่านั้นที่จะสามารถใช้งานได้

ดังนั้น Form Login จะเป็นส่วนที่ให้ผู้ใช้กรอกชื่อผู้ใช้และรหัสผ่าน เพื่อโปรแกรมจะทำการกำหนดสิทธิของผู้ใช้(Permission) โดยมีขั้นตอนการทำงานในการกำหนดค่าสิทธิของผู้ใช้ แสดงได้ดังรูปที่ 6-1

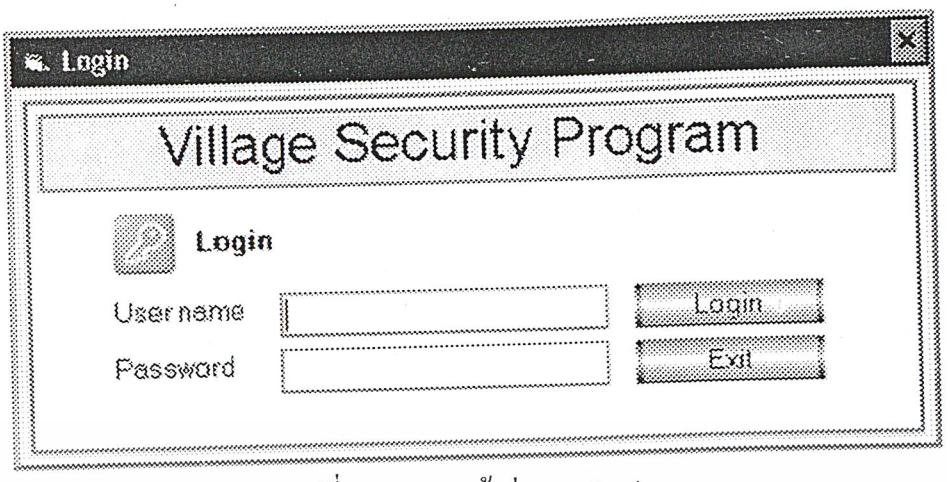
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6-1 Flow Chart แสดงกระบวนการกำหนดสิทธิ์ของผู้ใช้โปรแกรม

โดยสามารถแสดงหน้าต่างส่วนติดต่อกับผู้ใช้ ได้ดังรูปที่ 6-2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

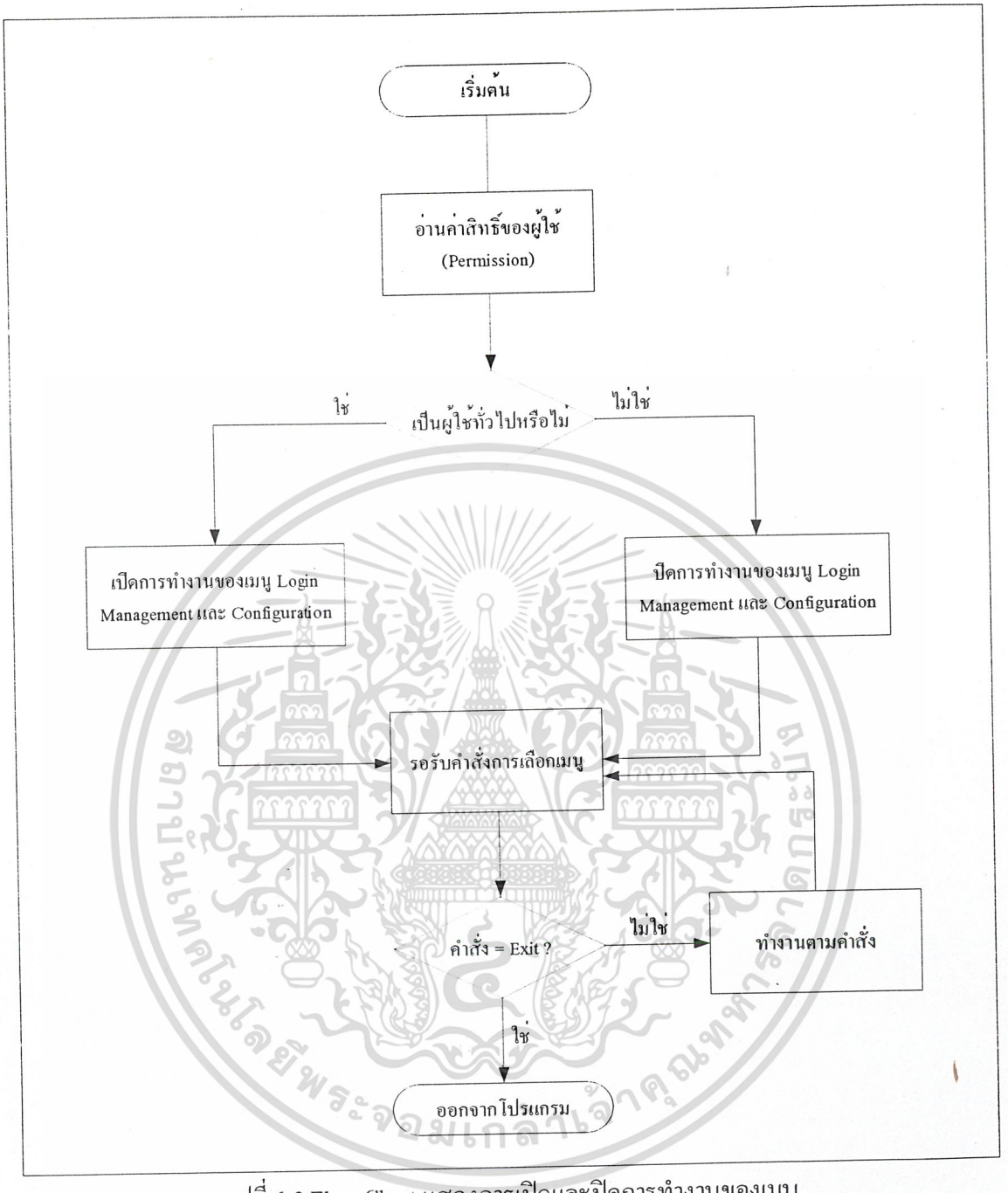


รูปที่ 6-2 แสดงหน้าต่างการ Login

6.2.2 Form Main Menu

เป็นส่วนเมนูหลักที่ใช้สำหรับเข้าไปใช้ในเมนูต่างๆ ซึ่งประกอบไปด้วย 4 เมนู คือ Menu Login Management ,Menu Configuration , Menu Status Report และ Menu Device Control โดยที่ในส่วนนี้ จะมีการกำหนดให้ Menu Login Management และ Menu Configuration ทำงาน(Enable) เมื่อผู้ใช้มีสิทธิ์เป็นผู้ดูแลระบบเท่านั้น ผู้ใช้ทั่วไปจะไม่สามารถใช้งานได้ โดยสามารถแสดงการทำงาน ได้ดังรูปที่ 6-2

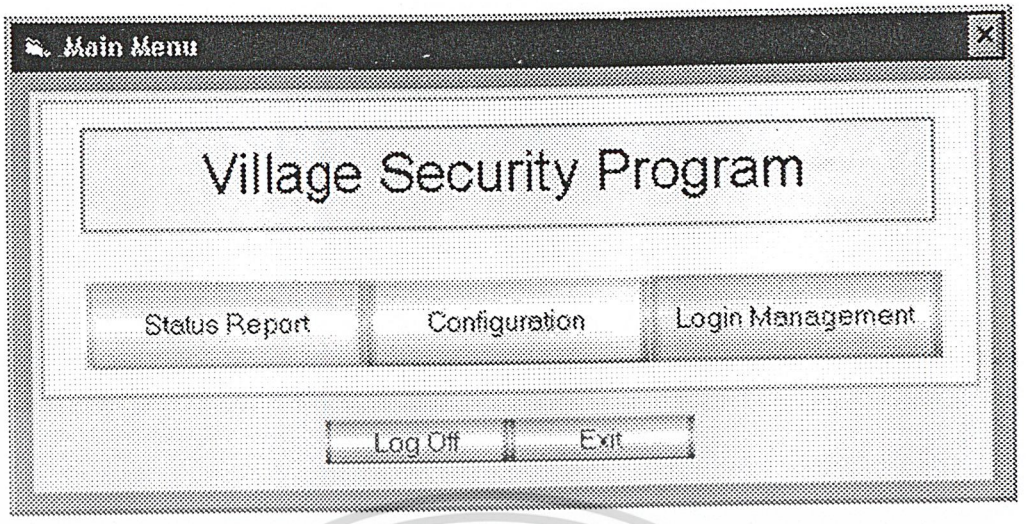
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



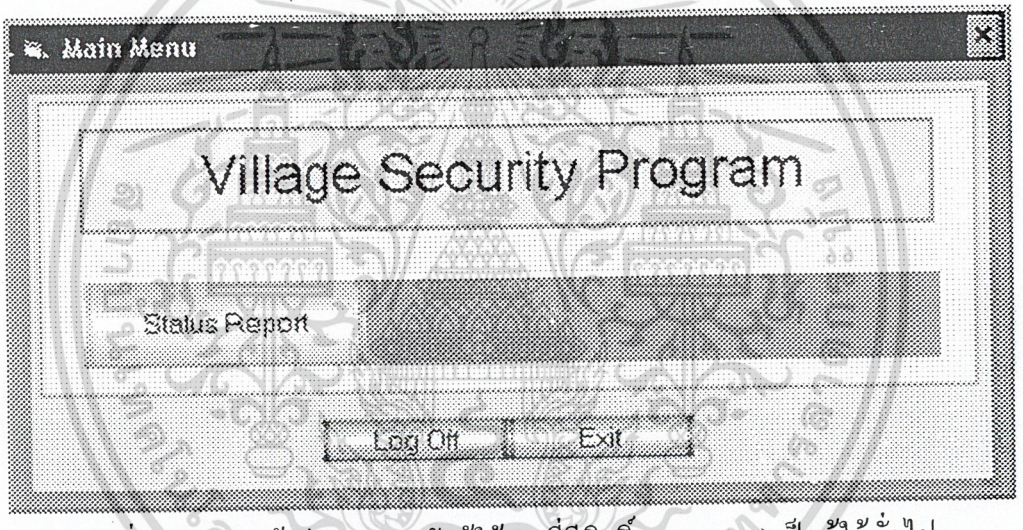
รูปที่ 6-3 Flow Chart แสดงการเปิดและปิดการทำงานของเมนู

โดยสามารถแสดงตัวอย่างของหน้าต่างสำหรับชื่อผู้ใช้ที่มีสิทธิ์ในการเข้าใช้เป็นผู้ดูแลระบบ ได้ดังรูปที่ 6-4 และ แสดงตัวอย่างของหน้าต่างสำหรับชื่อผู้ใช้ที่มีสิทธิ์ในการเข้าใช้เป็นผู้ใช้ทั่วไป ดังรูปที่ 6-5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6-4 แสดงหน้าต่างเมนูสำหรับผู้ใช้งานที่มีสิทธิ์(Permission) เป็นผู้ดูแลระบบ

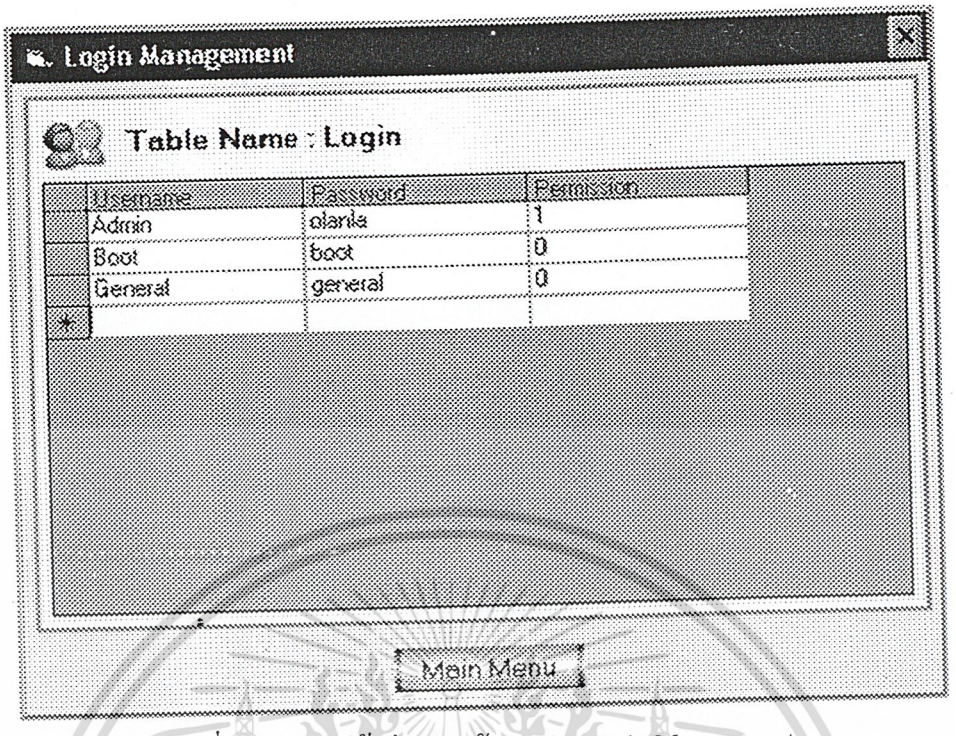


รูปที่ 6-5 แสดงหน้าต่างเมนูสำหรับผู้ใช้งานที่มีสิทธิ์(Permission) เป็นผู้ใช้ทั่วไป

6.2.3 Form Login Management

เป็นส่วนการทำงานที่ผู้ใช้ที่เป็นผู้ดูแลระบบเท่านั้น ที่จะสามารถใช้งานได้ มีหน้าที่ในการจัดการ Account หรือชื่อและรหัสผ่าน รวมไปถึงการกำหนดสิทธิ์ของผู้ใช้ที่จะใช้งานโปรแกรม โดยสามารถแสดงหน้าต่างการทำงานได้ดังรูปที่ 6-6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6-6 แสดงหน้าต่างสำหรับ Menu Login Management

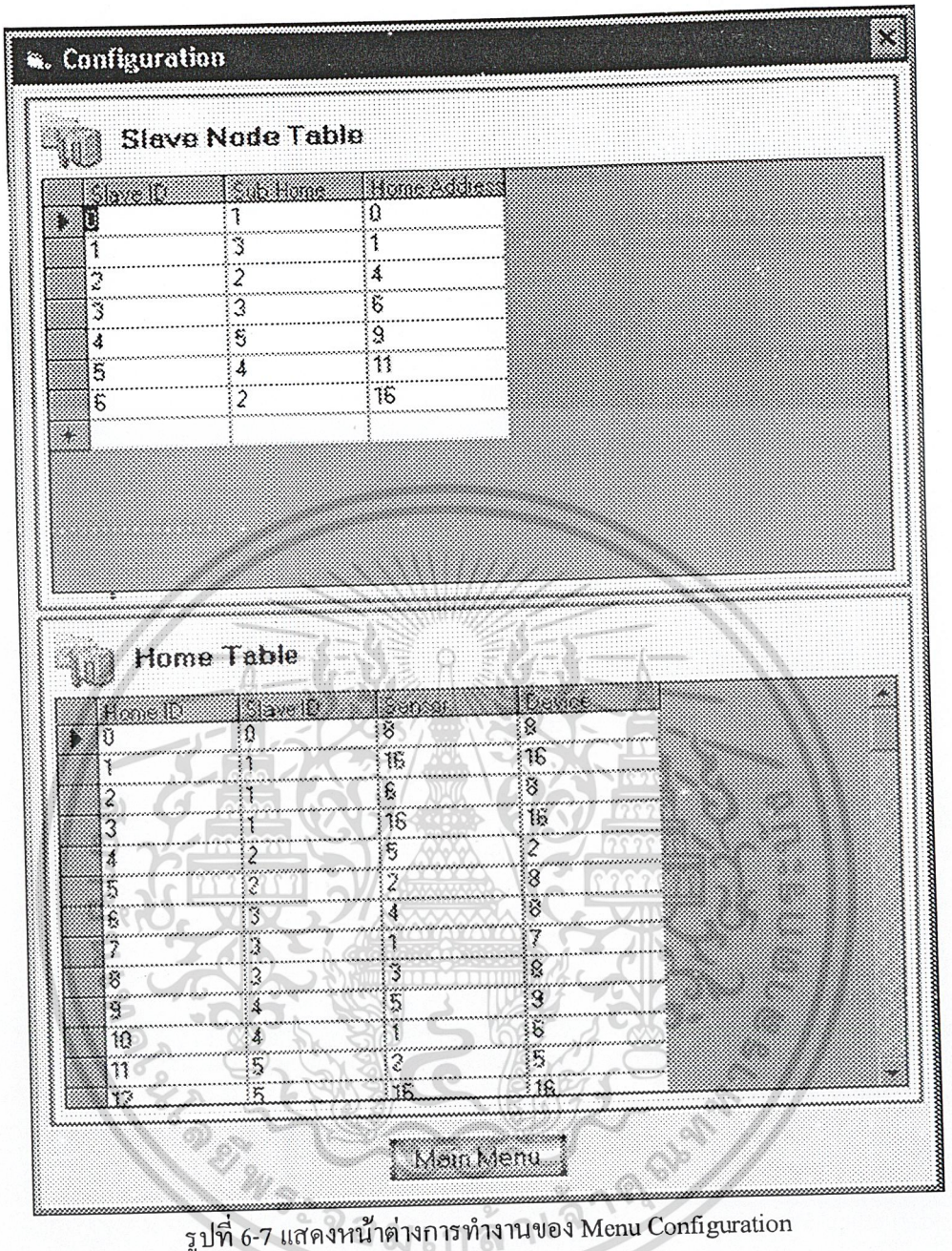
โดยที่ในหน้าต่าง Login Management ผู้ดูแลระบบ สามารถเพิ่ม ลบ แก้ไข ชื่อผู้ใช้และรหัสผ่าน รวมไปถึงการกำหนดสิทธิ์ ซึ่ง ถ้า สิทธิในการเข้าระบบมีค่าเป็น 0 แสดงว่า เป็นผู้ใช้ทั่วไป แต่ถ้ามีค่าเป็น1 แสดงว่าเป็นผู้ดูแลระบบ

นอกจากนั้น ยังมีหน้าต่างสำหรับการใช้คำสั่ง SQL เพื่อให้ผู้ดูแลระบบ สามารถจัดการฐานข้อมูลได้อย่างยืดหยุ่นและมีประสิทธิภาพ

6.2.4 Form Configuration

เป็นส่วนการทำงานที่ผู้ใช้ที่เป็นผู้ดูแลระบบเท่านั้น ที่จะสามารถใช้งานได้ มีหน้าที่ในการจัดการฐานข้อมูลเกี่ยวกับจำนวนของ Slave node และจำนวน Home node ที่Slave nodeนั้นมีอยู่ และยังจัดการเกี่ยวกับจำนวนอุปกรณ์ตรวจจับ และอุปกรณ์ไฟฟ้าที่แต่ละบ้านมี สามารถแสดงหน้าต่างได้ดังรูป ที่ 6-7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



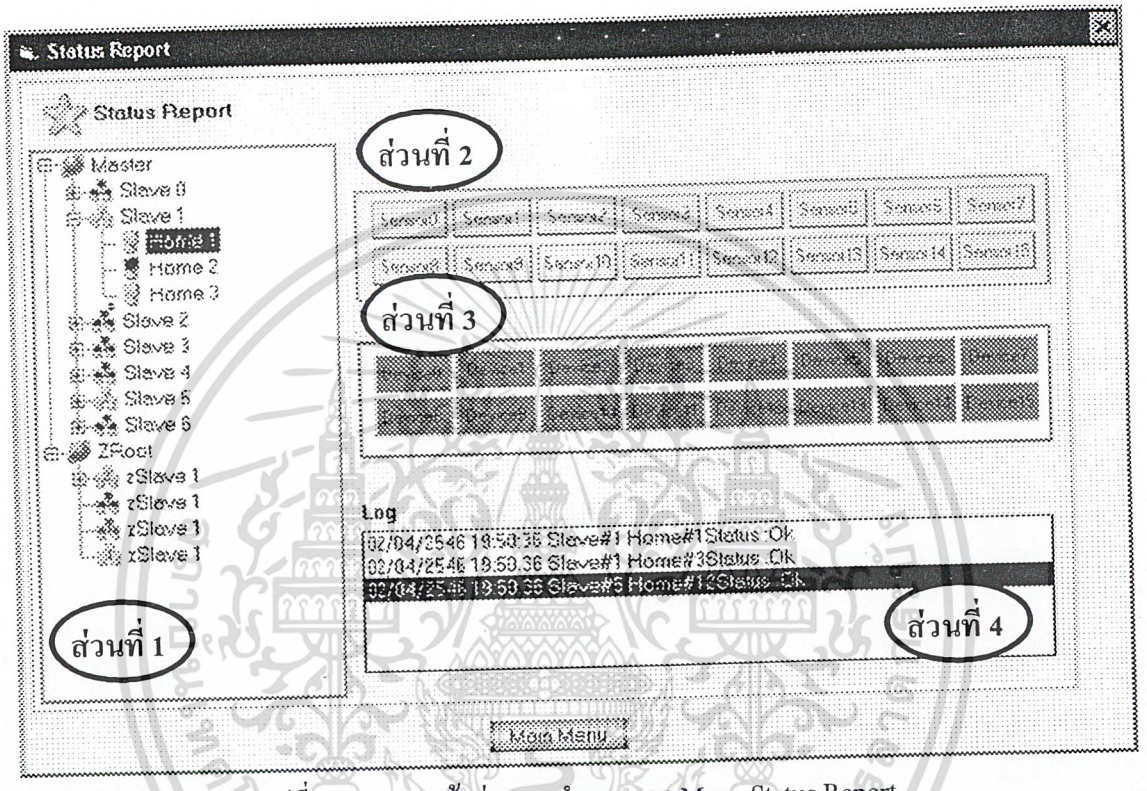
รูปที่ 6-7 แสดงหน้าต่างการทำงานของ Menu Configuration

การทำงานของฟอร์มนี้ อ้างอิงกับตาราง Slave และ ตาราง Home ซึ่งถูกสร้างไว้ใน MS SQL Server

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.2.5 Form Status Report

เป็นส่วนที่ผู้ใช้ทุกประเภทสามารถใช้งานได้ โดยขั้นตอนการทำงานคือ โปรแกรมจะรับเฟรมข้อมูลจากอุปกรณ์ Hardware และนำข้อมูลที่ได้มาแสดงผล ถ้าหาก มีวงจร Online อยู่บนเครือข่าย ปุ่มจะเป็นสีเขียว ถ้าหากวงจรเกิดปัญหาขึ้น ปุ่มจะขึ้นเป็นสีแดง สำหรับ ส่วนที่ไม่ได้ทำงานอยู่ ปุ่มจะไม่มีสี และสำหรับเมนูที่ทำงานอยู่ จะแสดงเป็นกรอบสีเหลือง แสดงหน้าต่างได้ดังรูปที่ 6-8



รูปที่ 6-8 แสดงหน้าต่างการทำงานของ Menu Status Report

จากรูป หน้าต่าง Status Report ประกอบไปด้วยส่วนแสดงผล 4 ส่วนหลักๆ ได้แก่

ส่วนที่ 1 แผนผังต้นไม้ จะแสดงรายระเอียดของทั้งระบบ ว่า แต่ละ Slave มีบ้านกี่หลัง และเมื่อทำการเลือกบ้านที่ต้องการ ส่วนอื่นๆจะมีการเปลี่ยนแปลงไปตามข้อมูลของบ้านนั้น

ส่วนที่ 2 ส่วนอุปกรณ์ตรวจจับ แสดงสถานะของอุปกรณ์ตรวจจับแต่ละจุดในบ้านนั้น ถ้าหากมีเหตุผิดปกติเกิดขึ้น จะแสดงเป็นสีแดง แต่ถ้าเหตุการณ์เป็นปกติ จะแสดงเป็นสีเขียว

ส่วนที่ 3 ส่วนอุปกรณ์ไฟฟ้า แสดงสถานะของอุปกรณ์ไฟฟ้าแต่ละชิ้นในบ้านนั้น ถ้าอุปกรณ์นั้นใช้งานอยู่ จะแสดงเป็นสีเขียว แต่ถ้าหากไม่ได้ใช้งานจะแสดงเป็นสีเทาทึบ และถ้าหากต้องการสั่งเปิดหรือปิดอุปกรณ์ก็ทำได้โดยการคลิ้กไปยังอุปกรณ์ไฟฟ้าที่ต้องการ

ส่วนที่ 4 ส่วนบันทึกเหตุการณ์ จะแจ้งเหตุการณ์ที่มีการเปลี่ยนแปลงขึ้น เช่น สถานะของบ้านเมื่ออุปกรณ์ตรวจจับผิดปกติ จะแสดงข้อความ “Status: Sensor Detected” เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สถานะต่างๆในแต่ละส่วนจะแสดงโดยใช้สีที่แตกต่างกัน คือ

สีเหลือง : เกิด Request time out เนื่องมาจากสายสัญญาณถูกตัดขาด หรืออุปกรณ์ชำรุด

สีแดง : เกิดเหตุการณ์ผิดปกติ มีสัญญาณจากอุปกรณ์ตรวจจับ

สีเขียว : อุปกรณ์ทำงานตามปกติ

สีเท่าดำ : อุปกรณ์ไม่ได้ทำงาน หรือ ไม่ได้ใช้งาน

การแสดงส่วนบันทึกเหตุการณ์หรือส่วนที่4 ได้แก่

Status : Ok แสดงว่า อุปกรณ์ทำงานตามปกติ

Status : Request time out แสดงว่า อุปกรณ์นั้นถูกตัดขาดจากระบบ เนื่องมาจาก สายสัญญาณถูกตัดขาด หรืออุปกรณ์ชำรุด

Status : Sensor Detected แสดงว่า มีการตรวจจับความผิดปกติจากอุปกรณ์ตรวจจับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 7

การทดลองและผลการทดลอง

การทดลองการทำงานของระบบนั้น สามารถแบ่งตามส่วนต่างได้เป็น

1. การทดลองความเร็วของระบบ
2. การทดลองการ login เข้าสู่ระบบ
3. การทดลองการปรับแต่งฐานข้อมูล โดยผู้ใช้ที่เป็นผู้ดูแลระบบ
4. การทดลองการแสดงผลสถานะของ Node
5. การทดลองการสั่งงานเพื่อควบคุมอุปกรณ์ไฟฟ้า
6. การทดลองการตัดสายสัญญาณเชื่อมต่อระหว่าง Master node และ Slave node
7. การทดลองการตัดสายสัญญาณเชื่อมต่อระหว่าง Slave node และ Home node

โดยจะทำการอธิบายรายละเอียดแต่ละหัวข้อดังต่อไปนี้

7.1 การทดลองความเร็วของระบบ

การทดลองนี้ เป็นการทดสอบความเร็วสูงสุดที่วงจรHardware จะทำงานได้ โดยการวนส่งคำสั่งตรวจสอบสถานะไปยังวงจรที่บ้าน และใช้ช่วงเวลาระหว่างการส่งที่ลดลงเรื่อยๆ จนกว่าสัญญาณที่ตอบกลับจากHome node มีความผิดปกติเกิดขึ้นซึ่งแสดงว่า ระบบไม่สามารถทำงานได้ทัน ณ ช่วงเวลานั้น

ขั้นตอนการทดลอง

1. ทำการติดตั้งระบบเครือข่าย
2. เขียนโปรแกรมเพื่อทำการ Polling ส่งคำสั่งการตรวจสอบสถานะไปยังบ้าน Home-1 โดยมีลักษณะของโปรแกรมคือ

```
While (true)
{
        ส่งคำสั่งตรวจสอบสถานะไปยัง Home-1
        Delay (time)
}
```

3. กำหนดค่าของ time ไว้ที่ 1 วินาที แล้วให้โปรแกรมทำงาน
4. สังเกตสัญญาณตอบกลับจาก Home-1
5. ลดค่าของ time ลง 0.05 วินาที แล้วให้โปรแกรมทำงาน
6. สังเกตสัญญาณตอบกลับจาก Home-1
7. ทำซ้ำข้อ 5 จนกระทั่งสัญญาณตอบกลับจาก Home-1 ผิดพลาด
8. บันทึกค่าของ time

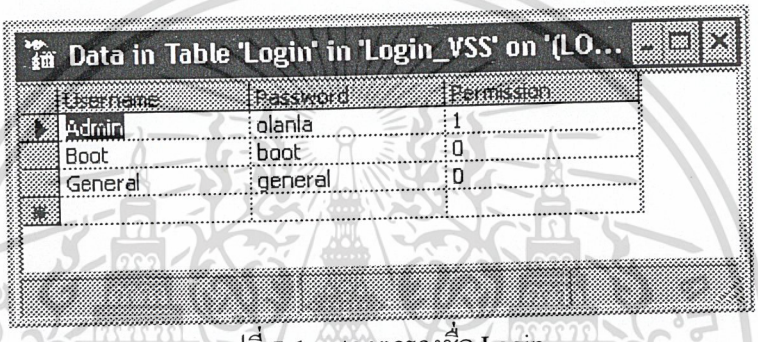
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งไม่อนุญาตให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผลการทดลอง

เมื่อทำการทดลองที่ delay 1 วินาทีปรากฏว่า สัญญาณตอบกลับจาก Home-1 ยังทำงานได้ถูกต้อง และ หลังจากทำการลดเวลาลงทุกๆ 0.05 วินาที พบว่า ช่วงเวลา delay ที่ต่ำกว่า 0.07 วินาที Home-1 จะตอบสัญญาณกลับไม่ทัน หรือมีความผิดพลาดของข้อมูลขึ้น นั่นแสดงว่า เวลาต่ำสุดที่ระบบรองรับ ในการสั่งงาน 1 รอบ (Master -> Slave -> Home / Home-> Slave -> Master) คือ 0.07 วินาที

7.2 การทดลองการ Login เข้าสู่ระบบ

การทดลองนี้ จะเป็นการทดลองเพื่อทดสอบชื่อผู้ใช้ รหัสผ่าน และสิทธิ์ในการใช้งาน ซึ่งได้ทำการตั้งค่าไว้ใน ตารางชื่อ Login ใน MS SQL Server แสดงตารางได้ดังรูป



รูปที่ 7-1 แสดงตารางชื่อ Login

แบ่งการทดลองในการ Login เข้าระบบได้เป็น 3 แบบ คือ

1. เข้าระบบด้วย Account ที่เป็นผู้ดูแลระบบ
2. เข้าระบบด้วย Account ที่เป็นผู้ใช้งานทั่วไป
3. เข้าระบบด้วย Account ที่ไม่มีอยู่ในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

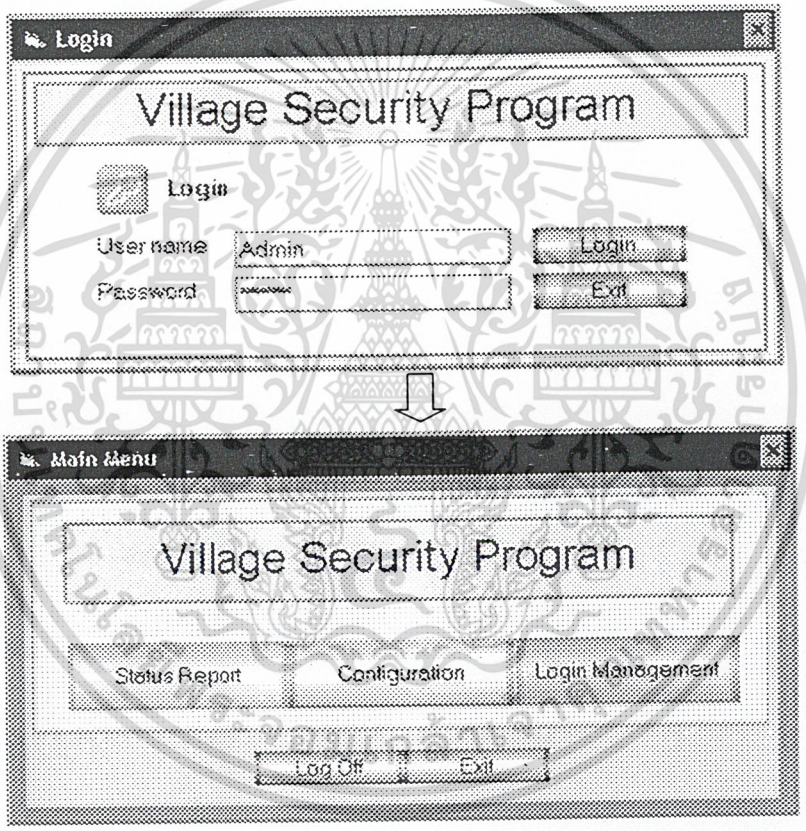
7.2.1 การทดลองเข้าระบบด้วย Account ของผู้ดูแลระบบ

ขั้นตอนการทดลอง

1. ทำการป้อนชื่อผู้ใช้ เป็น Admin
2. ทำการป้อนรหัสผ่านเป็น olanla
3. ทำการ Login
4. สังเกตการณ์ทำงานของโปรแกรม

ผลการทดลอง

หลังจากการทดลอง พบว่า สามารถ Login เข้าระบบ และใช้ Menu ที่ปรากฏขึ้นได้ครบทุก Menu ซึ่งตรงกับ Permission ของ Account นี้ที่เป็นผู้ดูแลระบบ แสดงได้ดังรูป



รูปที่ 7-2 แสดงการเข้าระบบด้วย Account ของผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

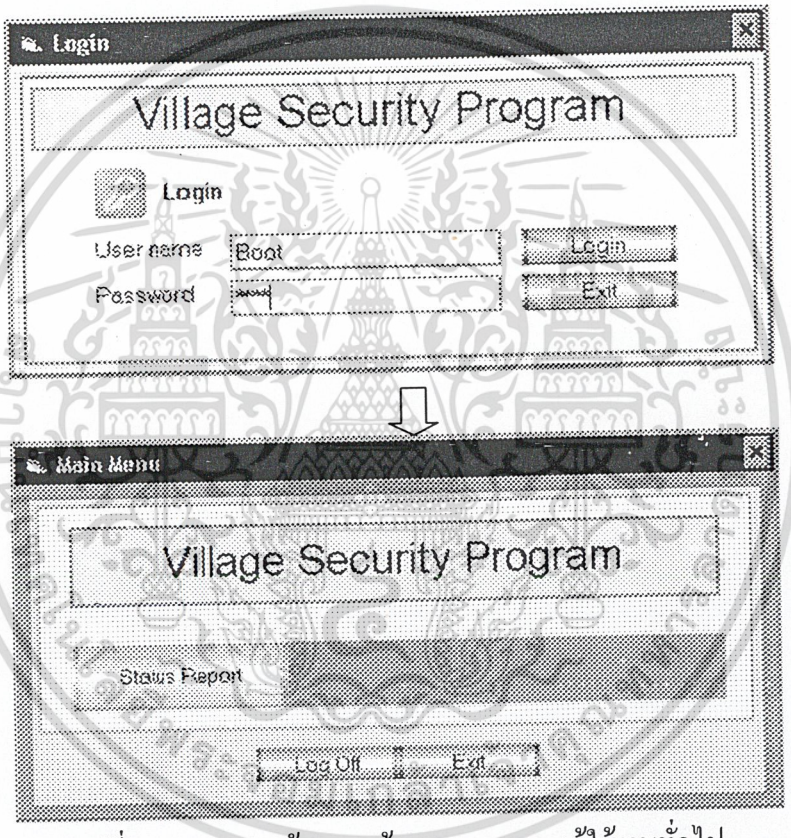
7.2.2 การทดลองเข้าระบบด้วย Account ของผู้ดูแลระบบ

ขั้นตอนการทดลอง

1. ทำการป้อนชื่อผู้ใช้ เป็น General
2. ทำการป้อนรหัสผ่านเป็น general
3. ทำการ Login
4. สังเกตการณ์ทำงานของโปรแกรม

ผลการทดลอง

หลังจากการทดลอง พบว่า สามารถ Login เข้าระบบ และไม่สามารถใช้ Menu ที่เกี่ยวข้องกับการแก้ไขฐานข้อมูลได้ ซึ่งตรงกับ Permission ของ Account นี้ที่เป็นผู้ใช้ทั่วไป แสดงได้ดังรูป



รูปที่ 7-3 แสดงการเข้าระบบด้วย Account ของผู้ใช้งานทั่วไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

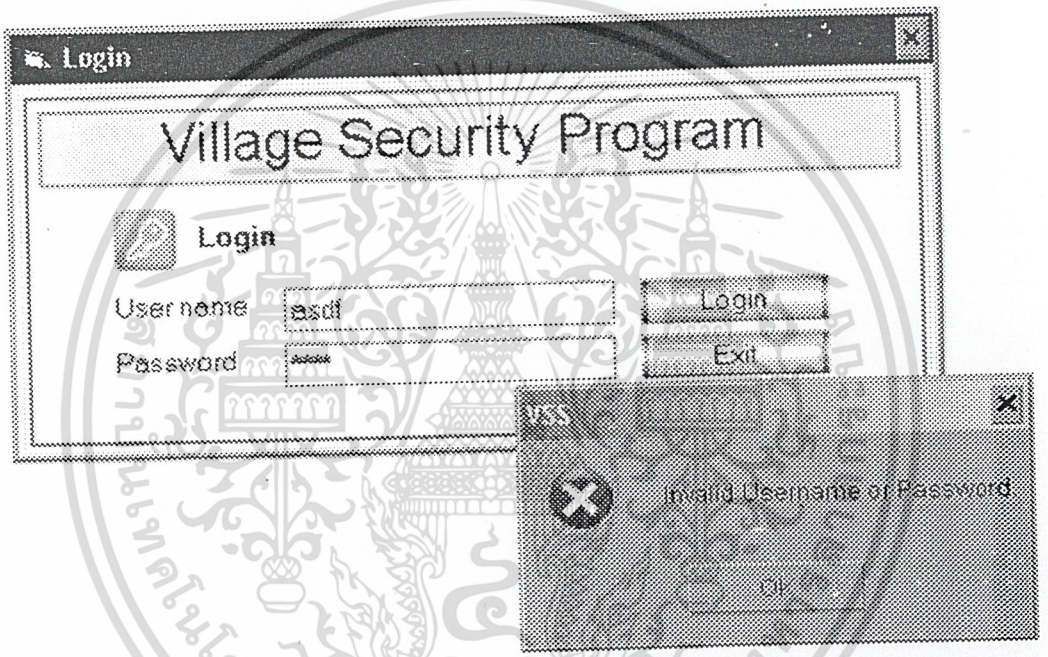
7.2.3 การทดลองเข้าระบบด้วย Account ที่ไม่มีอยู่ในระบบ

ขั้นตอนการทดลอง

1. ทำการป้อนชื่อผู้ใช้ เป็น asdf
2. ทำการป้อนรหัสผ่านเป็น asdf
3. ทำการ Login
4. สังเกตการณ์ทำงานของโปรแกรม

ผลการทดลอง

หลังจากการทดลอง พบว่า ไม่สามารถ Login เข้าระบบได้



รูปที่ 7-4 แสดงการเข้าระบบด้วย Account ที่ไม่อยู่ในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.3 การทดลองการปรับแต่งฐานข้อมูล โดยผู้ใช้ที่เป็นผู้ดูแลระบบ

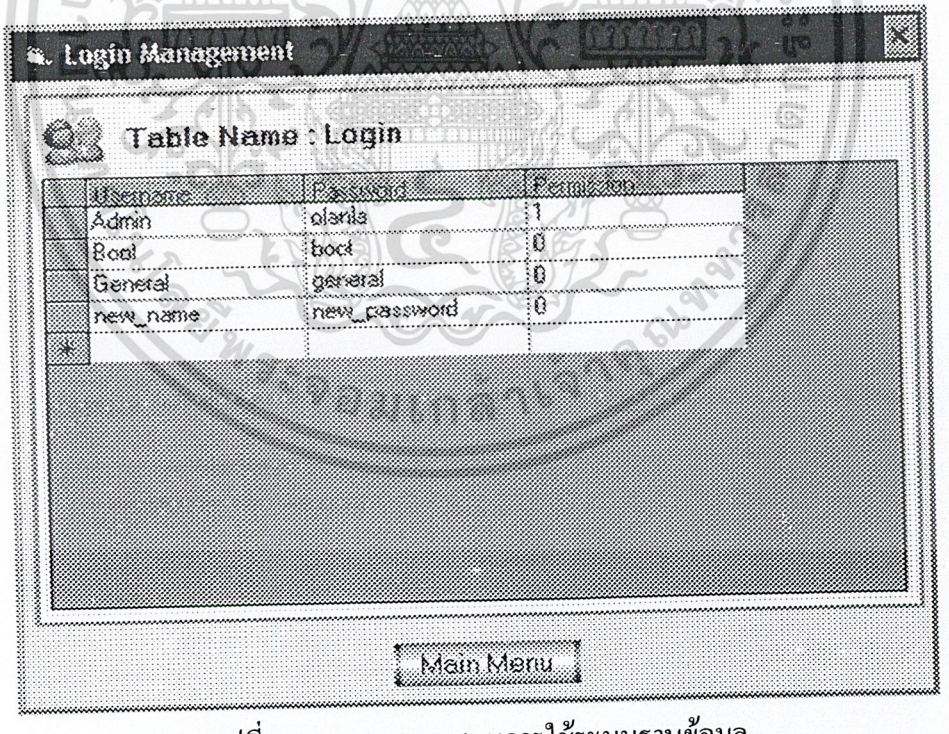
เป็นการทดสอบการใช้คำสั่ง SQL ผ่าน Component ของ Visual Basic โดยมีขั้นตอนการทดลองโดยการใช้ Form Menu Account Management ในการทดสอบ เพราะมีกระบวนการครบถ้วน เช่น การ insert, delete หรือ update

ขั้นตอนการทดลอง

1. Login เข้าระบบด้วย Account ของผู้ดูแลระบบ
2. เลือกเมนู Account Management
3. ทำการเพิ่มชื่อผู้ใช้และรหัสผ่านใหม่
4. สังเกตการณ์เปลี่ยนแปลงของตาราง
5. ทำการลบชื่อผู้ใช้
6. สังเกตการณ์เปลี่ยนแปลงของตาราง

ผลการทดลอง

การทดลองแก้ไขตาราง สามารถทำได้ถูกต้อง เมื่อมีการแก้ไขใดๆเกิดขึ้น ตารางที่อยู่บนฐานข้อมูลของ MS SQL ก็จะมีการเปลี่ยนแปลงไปตามการแก้ไขนั้นๆ



รูปที่ 7-5 แสดงการทดสอบการใช้ระบบฐานข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

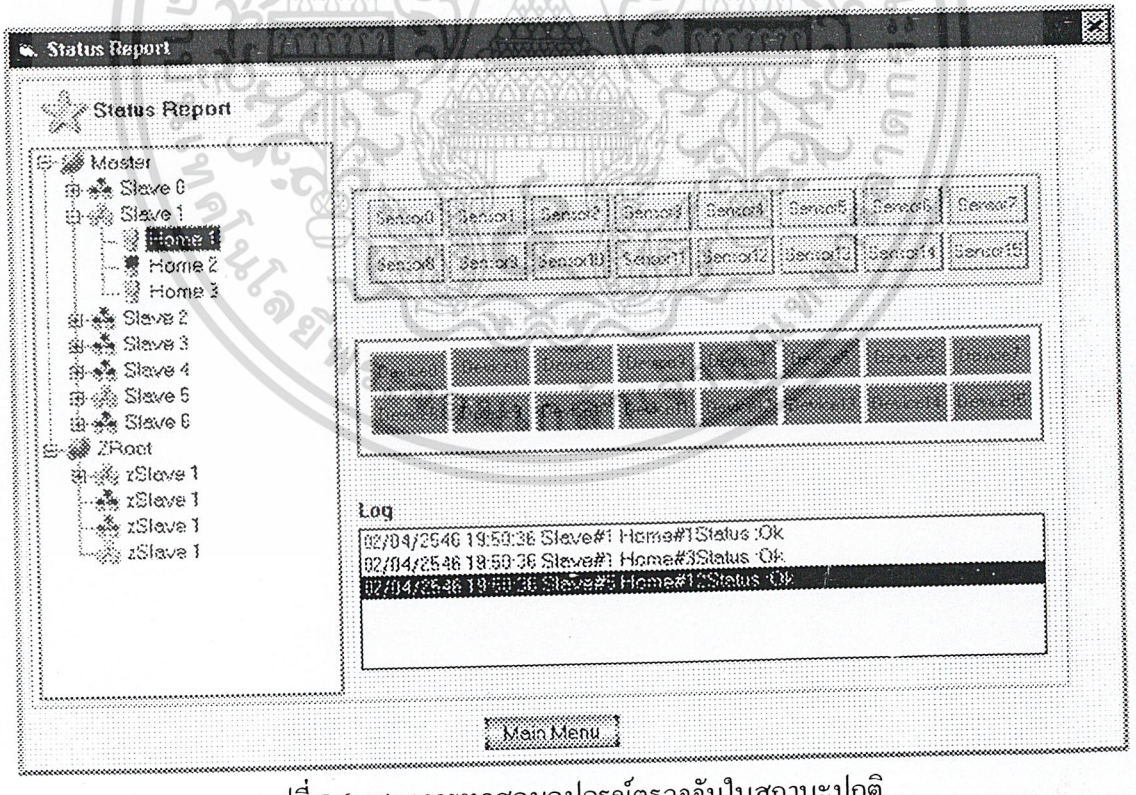
7.4 ทดสอบการแสดงสถานะของ Node

การทดสอบ จะทำการทดสอบการแสดงผลสถานะของ Node ว่าตรวจสอบได้ตรงตามที่กำหนดไว้หรือไม่ โดยมีขั้นตอนการทดลองคือ

1. ทำการติดตั้งระบบเครือข่าย
2. เปิดโปรแกรมศูนย์ควบคุมหลัก
3. เปิดเมนู Status Report
4. ทดสอบโดยให้ Sensor อยู่สถานะปกติ
5. สังเกตผลการทดลอง
6. ทดสอบโดยให้Sensor อยู่ในสถานะผิดปกติ
7. สังเกตผลการทดลอง

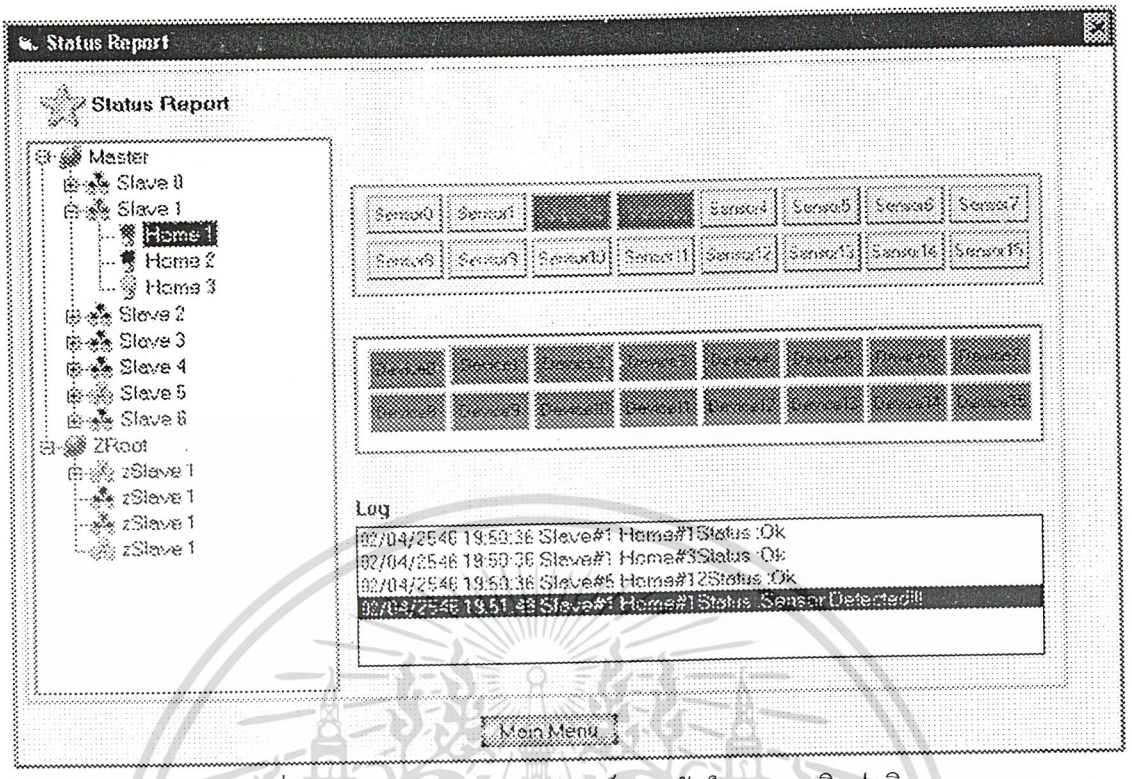
ผลการทดลอง

จากการทดลองข้างต้น พบว่า เมื่อสถานะของ Sensor เป็นปกติ ปุ่มแสดง Sensor จะขึ้นสีเขียว ดังรูปที่ 7-6 และเมื่อสถานะของ Sensor เป็นภาวะผิดปกติ ปุ่มแสดง Sensor จะเป็นสีแดง และสีของปุ่มที่ Home จะเป็นสีแดงเช่นกัน ดังรูปที่ 7-7 และมีการแจ้งข้อความสถานการณ์เปลี่ยนแปลงในช่อง Log ซึ่งเป็นไปตามที่ออกแบบไว้



รูปที่ 7-6 แสดงการทดสอบอุปกรณ์ตรวจจับในสถานะปกติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 7-7 แสดงการทดสอบอุปกรณ์ตรวจจับในสถานะผิดปกติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

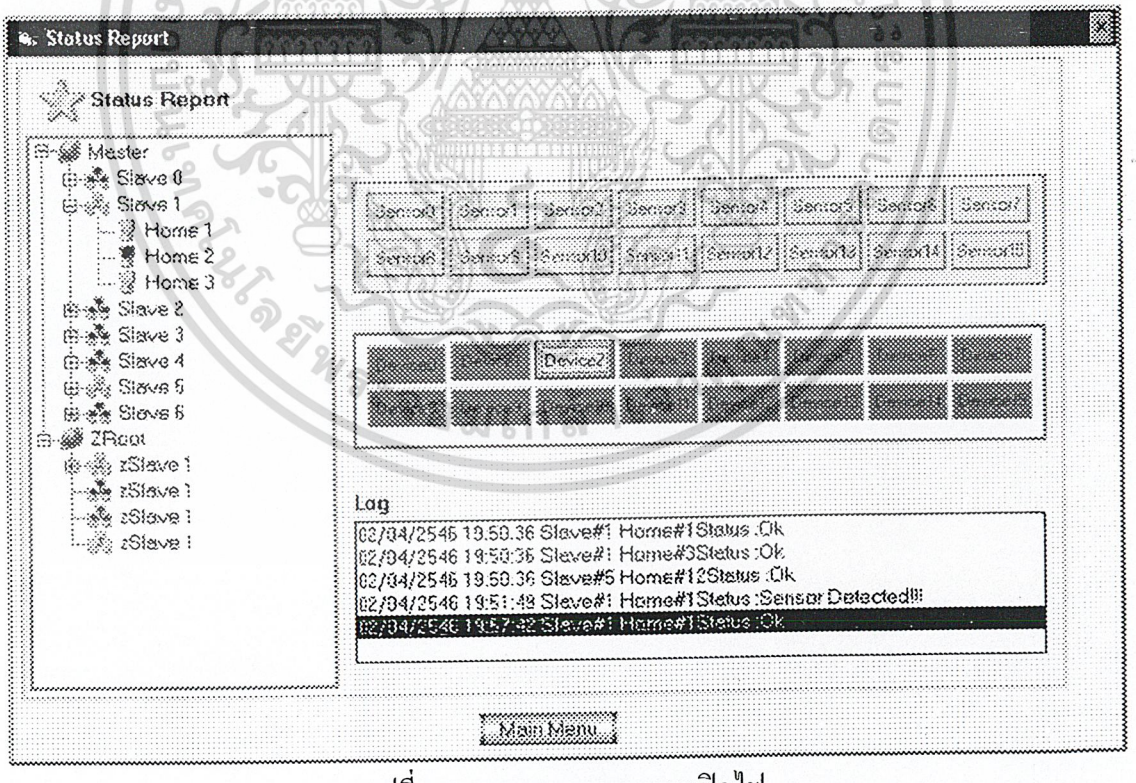
7.5 การทดลองการสั่งงานเพื่อควบคุมอุปกรณ์ไฟฟ้า

การทดสอบ เป็นการสั่งงานผ่านทางศูนย์ควบคุม เพื่อให้ Home node ทำการเปิด หรือปิดไฟ ซึ่งเป็นการจำลองการควบคุมอุปกรณ์ไฟฟ้า โดยมีขั้นตอนการทดลองคือ

1. ทำการติดตั้งระบบเครือข่าย
2. เปิดโปรแกรมศูนย์ควบคุมหลัก
3. เปิดเมนู Device Control
4. เลือก Slave 0 และ Home ที่ 3
5. สังเกตผลการทดลอง
6. เลือก Device 2 ให้เปิดไฟ
7. สังเกตผลการทดลอง

ผลการทดลอง

จากการทดลองข้างต้น พบว่า เมื่อทำการเลือก Slave 0 และ Home 3 แล้ว สถานะของอุปกรณ์ไฟฟ้า จะแสดงขึ้นเป็น สีทึบ จำนวน 16 ปุ่ม นั่นคือ อุปกรณ์ไฟฟ้ายังไม่ได้เปิดทำงาน เมื่อทำการเลือกอุปกรณ์ไฟฟ้าชิ้นที่ 3 หรือ Device 2 ไฟที่ Home 3 ควงที่ 3 ก็จะสว่างขึ้น และสถานะของ Device 2 ก็จะแสดงเป็นสีเขียว ซึ่งเป็นไปตามที่ได้ออกแบบไว้ แสดงได้ดังรูปที่ 7-8



รูปที่ 7-8 แสดงการทดลองการเปิดไฟ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.6 การทดลองการตัดสายสัญญาณเชื่อมต่อระหว่าง Master node และ Slave node

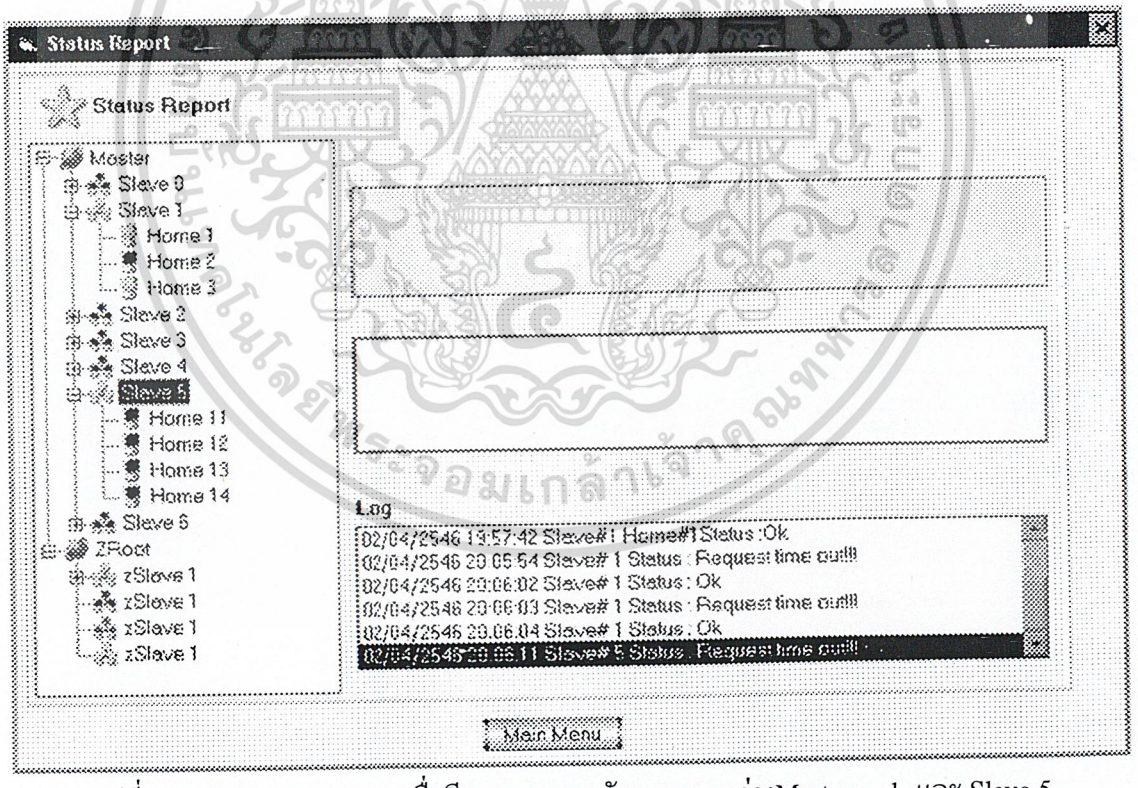
การทดสอบจะเป็นการตรวจสอบว่า เมื่อมีเหตุผิดปกติเกิดขึ้นกับ Slave node ไม่ว่าจะเป็นกรณีที่สายสัญญาณขาด หรือ Slave node ไม่ทำงาน จะมีการแสดงสถานะขึ้นบนส่วนควบคุมหลักอย่างไร

ขั้นตอนการทดลอง

1. ทำการติดตั้งระบบเครือข่าย
2. เปิดโปรแกรมศูนย์ควบคุมหลัก
3. เปิดเมนู Status report
4. ถอดสายสัญญาณระหว่าง Master node และ Slave node – 5
5. สังเกตผลการทดลอง

ผลการทดลอง

จากการทดลอง เมื่อทำการถอดสายสัญญาณออก โปรแกรมจะตรวจสอบได้ทันทีว่ามีเหตุผิดปกติเกิดขึ้นกับ Slave-5 โดยมีการแสดงผลที่ปุ่มของ Slave-5 เป็นสีเหลือง และแสดงข้อความเตือนใน Log เพื่อบอกว่าเกิด Request time out นั่นคือให้รีบไปตรวจสอบความผิดปกติ ซึ่งเป็นไปตามการออกแบบทุกประการ แสดงได้ดังรูป ที่ 7-9



รูปที่ 7-9 แสดงผลการทดลองเมื่อมีการถอดสายสัญญาณระหว่างMaster node และ Slave-5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.7 การทดลองการตัดสายสัญญาณเชื่อมต่อระหว่าง Slave node และ Home node

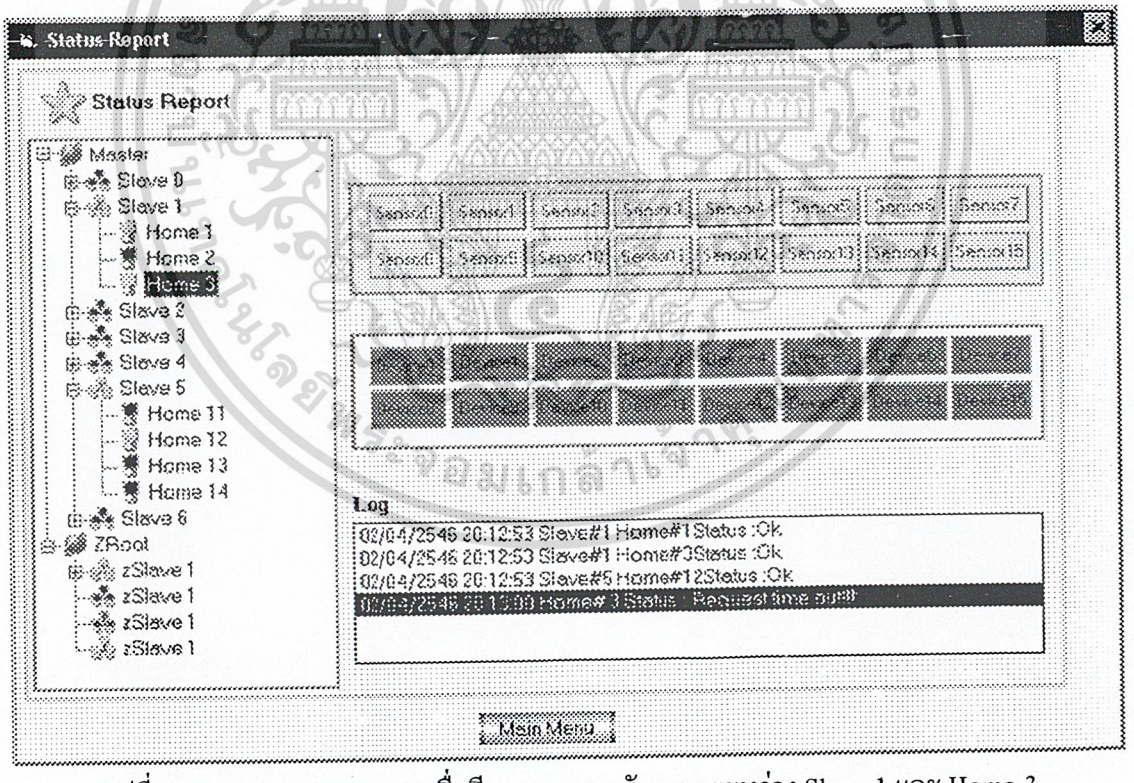
การทดสอบจะเป็นการตรวจสอบว่า เมื่อมีเหตุผิดปกติเกิดขึ้นกับ Home node ไม่ว่าจะเป็นกรณีที่สายสัญญาณขาด หรือ Home node ไม่ทำงาน จะมีการแสดงสถานะขึ้นบนส่วนควบคุมหลักอย่างไร

ขั้นตอนการทดลอง

1. ทำการติดตั้งระบบเครือข่าย
2. เปิดโปรแกรมศูนย์ควบคุมหลัก
3. เปิดเมนู Status report
4. ถอดสายสัญญาณระหว่าง Slave node-1 และ Home node – 3
5. สังเกตผลการทดลอง

ผลการทดลอง

จากการทดลอง เมื่อทำการถอดสายสัญญาณออก โปรแกรมจะตรวจสอบได้ทันทีว่ามีเหตุผิดปกติเกิดขึ้นกับ Home-3 โดยมีการแสดงผลที่ปุ่มของ Home-3 จะเป็นสีเหลือง และแสดงข้อความเตือนใน Log เพื่อบอกว่า Home-3 เกิด Request time out นั่นคือให้รีบไปตรวจสอบความผิดปกติ ซึ่งเป็นไปตามการออกแบบทุกประการ แสดงได้ดังรูปที่ 7-10



รูปที่ 7-10 แสดงผลการทดลองเมื่อมีการถอดสายสัญญาณระหว่าง Slave-1 และ Home-3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 8
สรุปและวิจารณ์ผลการทดลอง

จากการทำงานและทดลองระบบเพื่อให้เป็นไปตามที่ออกแบบไว้ กล่าวคือ

1. ระบบสามารถรับและส่งข้อมูลได้ถูกต้องทุกประการ
2. ระบบมีประสิทธิภาพในด้านของความเร็วในการรับและส่งข้อมูล จากเครื่องคอมพิวเตอร์ไปยัง Home node (PC->Master->Slave->Home / Home->Slave->Master->PC) มีความเร็วสูงสุดที่ 70 Millisecond
3. ระบบเครือข่ายมีความปลอดภัยของข้อมูล เพราะมีการเข้ารหัสก่อนที่จะสั่งข้อมูลออกไปยังเครือข่าย โดยใช้อัลกอริทึมแบบ DES มีกุญแจรหัสขนาด 8 บิต
4. ระบบเครือข่ายมีความเชื่อถือได้ เพราะมีการทำการตอบรับสัญญาณ และการกำหนดช่วงเวลาตอบกลับ (Request time) ถ้าหากวงจรมีความผิดปกติ หรือสายสัญญาณถูกตัดขาดจะเกิด Request time out ทำให้ทราบได้ทันท่วงที
5. โปรแกรมซึ่งใช้ควบคุมระบบมีความปลอดภัย เพราะผู้ใช้จะสามารถใช้ได้ก็ต่อเมื่อมี account ในฐานข้อมูลเท่านั้น
6. การโปรแกรมบนไมโครคอนโทรเลอร์ด้วยภาษาซี ง่ายต่อความเข้าใจ ทำให้ง่ายต่อการนำไปศึกษาและพัฒนาต่อ
7. การออกแบบวงจร Hardware ในส่วน Home node โดยการเพิ่ม decoder ให้กับสัญญาณ Control ทำให้สามารถรองรับจำนวนอุปกรณ์ไฟฟ้า และอุปกรณ์ตรวจจับ ได้มากขึ้นหลายเท่า

สำหรับปัญหาที่พบระหว่างการดำเนินงานนั้น สามารถสรุปได้เป็นดังนี้

1. ปัญหาเนื่องจากอุปกรณ์ Hardware

เนื่องจากอุปกรณ์ Hardware ที่ใช้ในการทดสอบทั้งหมด เป็นการนำบอร์ดไข่ปลา และวางสายด้วยการบัดกรีเอง ทำให้เป็นบ่อยครั้งที่พบปัญหาการทำงานไม่เป็นไปตามที่โปรแกรมไว้ เพราะสายที่วางไว้หลุด

2. IC บางเบอร์ไม่มีจำหน่ายในประเทศไทย

จากการศึกษาพบว่า มี IC หลายชนิดที่มีประสิทธิภาพสูงขึ้น สามารถใช้เข้ากับโครงงานนี้ได้ เช่น IC MAX3162/3163 ซึ่งเป็น Protocol Converter สามารถแปลงสัญญาณไฟจากมาตรฐาน RS-485 ไปเป็น RS-232 หรือจาก RS-232 เป็น RS-485 ได้ แต่จากการสอบถามร้านขาย IC ในประเทศไทย พบว่า ไม่มีการนำเข้ามาจำหน่าย ดังนั้น ถ้าหากมีการพัฒนาต่อไป ผู้จัดทำจึงอยากให้ศึกษา IC ดังกล่าวเพิ่มเติมด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นอกจากนั้น ยังมี IC ที่ทำหน้าที่ในการแปลงสัญญาณเป็นอนุกรมมาตรฐาน RS-485 ที่ต่อกับอุปกรณ์เพิ่มเติมได้ถึง 256 อุปกรณ์ ซึ่งเป็นการเพิ่มขีดจำกัดของการรองรับ อุปกรณ์บนเครือข่ายได้ถึง 255x 255 Node

3. ปัญหาจากการศึกษาโปรแกรมภาษา Assembly ทำได้ลำบากมาก

เพราะตัวโครงสร้างของ Assembly ทำให้ยากต่อการที่ผู้ที่ต้องการศึกษาโปรแกรมจะเข้าใจได้ ผู้จัดทำได้ตัดสินใจในการโปรแกรมไมโครคอนโทรเลอร์โดยใช้ภาษาซี เพราะมีโครงสร้างภาษาที่ง่ายต่อการเข้าใจ และผู้ที่ต้องการพัฒนาต่อสามารถศึกษาได้

แต่ถึงอย่างไร โครงงานนี้ก็เสร็จ สมบูรณ์และเป็นไปตามที่ออกแบบไว้ทุกประการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก

DES Programming for Microcontroller

โปรแกรม สำหรับการทำกระบวนการ Encrypt / Decrypt ซึ่งเป็นภาษาซี สำหรับไมโครคอนโทรเลอร์ 51

```
#include <string.h>
#define DES_ENCRYPT 1
#define DES_DECRYPT 0

unsigned char Key_Schedule[16][48];

/* left shift table for key schedule LS */
static const unsigned char LS[16] = { 1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1 };

/* permuted-choice tables for key schedule PC1, PC2 */
unsigned char PC1[56] = {
  57,49,41,33,25,17, 9, 1,58,50,42,34,26,18,10, 2,
  59,51,43,35,27,19,11, 3,60,52,44,36,63,55,47,39,
  31,23,15, 7,62,54,46,38,30,22,14, 6,61,53,45,37,
  29,21,13, 5,28,20,12, 4 };

unsigned char PC2[48] = {
  14,17,11,24, 1, 5, 3,28,15, 6,21,10,23,19,12, 4,
  26, 8,16, 7,27,20,13, 2,41,52,31,37,47,55,30,40,
  51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32 };

/* initial permutation IP */
unsigned char IP[64] = {
  58,50,42,34,26,18,10, 2,60,52,44,36,28,20,12, 4,
  62,54,46,38,30,22,14, 6,64,56,48,40,32,24,16, 8,
  57,49,41,33,25,17, 9, 1,59,51,43,35,27,19,11, 3,
  61,53,45,37,29,21,13, 5,63,55,47,39,31,23,15, 7 };

/* bit-selection table E */
unsigned char E[48] = {
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9, 8, 9,10,11,
12,13,12,13,14,15,16,17,16,17,18,19,20,21,20,21,
22,23,24,25,24,25,26,27,28,29,28,29,30,31,32, 1 };

/* substitution tables ST */
unsigned char ST[8][64] = {
 14, 4,13, 1, 2,15,11, 8, 3,10, 6,12, 5, 9, 0, 7,
  0,15, 7, 4,14, 2,13, 1,10, 6,12,11, 9, 5, 3, 8,
  4, 1,14, 8,13, 6, 2,11,15,12, 9, 7, 3,10, 5, 0,
 15,12, 8, 2, 4, 9, 1, 7, 5,11, 3,14,10, 0, 6,13,

 15, 1, 8,14, 6,11, 3, 4, 9, 7, 2,13,12, 0, 5,10,
  3,13, 4, 7,15, 2, 8,14,12, 0, 1,10, 6, 9,11, 5,
  0,14, 7,11,10, 4,13, 1, 5, 8,12, 6, 9, 3, 2,15,
 13, 8,10, 1, 3,15, 4, 2,11, 6, 7,12, 0, 5,14, 9,

 10, 0, 9,14, 6, 3,15, 5, 1,13,12, 7,11, 4, 2, 8,
 13, 7, 0, 9, 3, 4, 6,10, 2, 8, 5,14,12,11,15, 1,
 13, 6, 4, 9, 8,15, 3, 0,11, 1, 2,12, 5,10,14, 7,
  1,10,13, 0, 6, 9, 8, 7, 4,15,14, 3,11, 5, 2,12,

  7,13,14, 3, 0, 6, 9,10, 1, 2, 8, 5,11,12, 4,15,
 13, 8,11, 5, 6,15, 0, 3, 4, 7, 2,12, 1,10,14, 9,
 10, 6, 9, 0,12,11, 7,13,15, 1, 3,14, 5, 2, 8, 4,
  3,15, 0, 6,10, 1,13, 8, 9, 4, 5,11,12, 7, 2,14,

  2,12, 4, 1, 7,10,11, 6, 8, 5, 3,15,13, 0,14, 9,
 14,11, 2,12, 4, 7,13, 1, 5, 0,15,10, 3, 9, 8, 6,
  4, 2, 1,11,10,13, 7, 8,15, 9,12, 5, 6, 3, 0,14,
 11, 8,12, 7, 1,14, 2,13, 6,15, 0, 9,10, 4, 5, 3,

 12, 1,10,15, 9, 2, 6, 8, 0,13, 3, 4,14, 7, 5,11,
 10,15, 4, 2, 7,12, 9, 5, 6, 1,13,14, 0,11, 3, 8,
  9,14,15, 5, 2, 8,12, 3, 7, 0, 4,10, 1,13,11, 6,
  4, 3, 2,12, 9, 5,15,10,11,14, 1, 7, 6, 0, 8,13,
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
4,11, 2,14,15, 0, 8,13, 3,12, 9, 7, 5,10, 6, 1,
13, 0,11, 7, 4, 9, 1,10,14, 3, 5,12, 2,15, 8, 6,
 1, 4,11,13,12, 3, 7,14,10,15, 6, 8, 0, 5, 9, 2,
 6,11,13, 8, 1, 4,10, 7, 9, 5, 0,15,14, 2, 3,12,

13, 2, 8, 4, 6,15,11, 1,10, 9, 3,14, 5, 0,12, 7,
 1,15,13, 8,10, 3, 7, 4,12, 5, 6,11, 0,14, 9, 2,
 7,11, 4, 1, 9,12,14, 2, 0, 6,10,13,15, 3, 5, 8,
 2, 1,14, 7, 4,10, 8,13,15,12, 9, 0, 3, 5, 6,11 };

/* permutation table P */
unsigned char P[32] = {
 16, 7,20,21,29,12,28,17, 1,15,23,26, 5,18,31,10,
  2, 8,24,14,32,27, 3, 9,19,13,30, 6,22,11, 4,25 };

/* final permutation FP */
unsigned char FP[64] = {
 40, 8,48,16,56,24,64,32,39, 7,47,15,55,23,63,31,
 38, 6,46,14,54,22,62,30,37, 5,45,13,53,21,61,29,
 36, 4,44,12,52,20,60,28,35, 3,43,11,51,19,59,27,
 34, 2,42,10,50,18,58,26,33, 1,41, 9,49,17,57,25 };

/* unbit(to, from, len) -- unpack len bytes to bits */
void unbit(unsigned char *to,unsigned char *from,int len)
{
register int j,f;

        while(len--)
        {
                for (j = 8,f = *from++; j--;)
                {
                        *to++ = (f >> j) & 1;
                }
        }
}
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
/* pkbit(to from, len) -- pack bits to len bytes */
void pkbit(unsigned char *to, unsigned char *from, int len)
{
register int j,t;

        while (len--)
        {
                for (j = 8, t = 0; j--;)
                        t |= *from++ << j;
                *to++ = t;
        }
}

/* perm(to, OP, from, bits) -- do permutation */
void perm(unsigned char *to, const unsigned char *op, unsigned char *from, int bits)
{
register int i;

        for (i = 0; i < bits; i++)
                to[i] = from[op[i]-1];
}

/* rot(to, from, len, bits) -- rotate left */
void rot(unsigned char *r, int len, int bits)
{
register int i,t;

        if (len > 1)
        {
                for (i = 0; i<bits; i++)
                {
                        t = r[0];
                        memmove(&r[0], &r[1], len - 1);
                        r[len-1] = t;
                }
        }
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
}

/* add2(to, from, bits) -- add bits modulo 2 (that is, eor) */
void add2(unsigned char *to, unsigned char *from, int bits)
{
register int i;

        for (i=0; i<bits; i++)
                to[i] ^= from[i];
}

/* subs(o,i,s) -- substitute 6 bits to 4 bits using ST[s] */
void subs(unsigned char *o, unsigned char *i, int s)
{
register int t;

        t = ST[s][
                (i[0] << 5) | (i[5] << 4) | /* 1st and 6th bit, row index */
                (i[1] << 3) | (i[2] << 2) | /* 2nd to 5th bit, col index */
                (i[3] << 1) | i[4]];
        o[0] = (t >> 3) & 1;
        o[1] = (t >> 2) & 1;
        o[2] = (t >> 1) & 1;
        o[3] =  t & 1;
}

/* des_set_key(key,ks) -- generate a keyschedule */
int des_set_key(unsigned char *key)
{
int i;
unsigned char k[64],cd[56];

        unbit(k, key, 8);
        perm(cd, PC1, k, 56);
        for (i = 0; i < 16; i++)
        {
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
            rot(&cd[0], 28, LS[i]);
            rot(&cd[28], 28, LS[i]);
            perm(Key_Schedule[i], PC2, cd, 48);
        }
        return 1;
}

/* des_func(in,out,ks) -- des core function */
void des_func(unsigned char in[64], unsigned char out[64], unsigned char b[16][48], int enc)
{
int i,j;
unsigned char lr[64], rsto[32], si[48], so[32];
#define LEFT  lr
#define RIGHT  &lr[32]

        perm(lr, IP, in, 64); /* initial permutation */
        for (i = 0; i < 16; i++)
        { /* 16 rounds */
            memcpy(rsto, RIGHT,32); /* store right part */
            perm(si, E, RIGHT, 48); /* F-box: permute to subst. input */
            add2(si, b[enc ? i : 15-i], 48); /* add key (enc/dec order) */
            for (j = 0; j < 8; j++) /* 48 to 32 bit substitute */
                subs(&so[j*4],&si[j*6],j);
            perm(RIGHT, P, so, 32); /* permute substitution output: end F*/
            add2(RIGHT, LEFT, 32); /* add left part */
            memcpy(LEFT, rsto, 32); /* old right part will be new left */
        }
        memcpy(LEFT, RIGHT, 32); /* swap left and right part */
        memcpy(RIGHT,rsto, 32);
        perm(out,FP,lr,64); /* final permutation */
}

/* des_ecb_encrypt(in, out, ks, enc) -- des electronic code book mode */
int des_ecb_encrypt(unsigned char *in, unsigned char *out, int enc)
{
unsigned char o[64];
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
        unbit(o, (unsigned char *)in, 8);
        des_func((unsigned char *)o, (unsigned char *)o, Key_Schedule, enc);
        pkbit((unsigned char *)out, o, 8);
        return 8;
}

void DesECBEncrypt(unsigned char Key[16], unsigned char In[16], unsigned char Out[16])
{
        des_set_key(Key);
        des_ecb_encrypt(In, Out, DES_ENCRYPT);
}

void DesECBDecrypt(unsigned char Key[16], unsigned char In[16], unsigned char Out[16])
{
        des_set_key(Key);
        des_ecb_encrypt(In, Out, DES_DECRYPT);
}
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข

DES Source Code อ้างอิงกับ Library“diCryptoSys.dll”สำหรับVisual Basic

```
Public Function Bytes2HexStr(aBytes() As Byte, nBytes As Long) As String
   Bytes2HexStr = Str2Hex(Bytes2String(aBytes, nBytes))
End Function


Public Function HexStr2Bytes(sHex As String, aBytes() As Byte) As Integer
' Converts string <sHex> with hex values into array of bytes
' Returns # of bytes converted
' Assumes array is large enough
' E.g. "fedcba98" will be converted into {&HFE, &HDC, &HBA, &H98}
   Dim i As Integer
   Dim nBytes As Integer

   If Not IsValidHex(sHex) Then    ' Validation added Aug 2001
      Exit Function
   End If

   nBytes = Len(sHex) \ 2
   For i = 0 To nBytes - 1
      aBytes(i) = CByte("&H" & Mid(sHex, i * 2 + 1, 2))
   Next

   HexStr2Bytes = nBytes

End Function

Public Function HexStr2Words(sHex As String, aWords() As Long) As Integer
' Converts string <sHex> with hex values into array of words (long ints)
' Returns # of words converted
' Assumes array is large enough
' E.g. "fedcba9876543210" will be converted into {&HFEDCBA98, &H76543210}
   Const ncLEN As Integer = 8
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Dim i As Integer
Dim nWords As Integer

If Not IsValidHex(sHex) Then    ' Validation added Aug 2001
   Exit Function
End If

nWords = Len(sHex) \ ncLEN
For i = 0 To nWords - 1
   aWords(i) = CLng("&H" & Mid(sHex, i * ncLEN + 1, ncLEN))
Next

HexStr2Words = nWords

End Function

Public Function Words2HexStr(aWords() As Long, nWords As Long) As String
' Converts array of words (long ints), nWords long, into a string
' E.g. {&HFEDCBA98, &H76543210} will be converted to "FEDCBA9876543210"
   Const ncLEN As Integer = 8
   Dim i As Integer
   Dim sHex As String

   Words2HexStr = ""
   For i = 0 To nWords - 1
      sHex = Hex(aWords(i))
      sHex = String(ncLEN - Len(sHex), "0") & sHex
      Words2HexStr = Words2HexStr & sHex
   Next

End Function

Public Function String2Bytes(str As String, aBytes() As Byte) As Integer
' Converts string <str> directly into array of bytes
' String may contain any characters between &H00 and &HFF
' Returns # of bytes converted
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
' Assumes array is large enough
' E.g. "abc" will be converted to (&H61, &H62, &H63) i.e. (97, 98, 99)
    Dim i As Integer
    Dim nBytes As Integer

    nBytes = Len(str)
    For i = 0 To nBytes - 1
        aBytes(i) = Asc(Mid(str, i + 1, 1))
    Next

    String2Bytes = nBytes

End Function

Public Function Bytes2String(aBytes() As Byte, nBytes As Long) As String
' Converts array of bytes, nBytes long, into a string
' E.g. (&H61, &H62, &H63) will be converted to "abc"
    Dim i As Integer
    Dim str As String

    For i = 0 To nBytes - 1
        str = str & Chr(aBytes(i * 2))
    Next

    Bytes2String = str

End Function

Public Function String2Words(str As String, aWords() As Long) As Long
' Converts string of ascii chars into an array of 32-bit words
' E.g. "abcdefgh" will be converted to {&H61626364, &H65666768}
    Dim sTemp As String
    sTemp = Str2Hex(str)
    String2Words = HexStr2Words(sTemp, aWords)
End Function
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Public Function Str2Hex(str As String) As String
' Converts string <str> of ascii chars to string in hex byte format
' E.g. "abc" will be converted to "616263"
    Dim byt As Byte
    Dim i As Integer
    Dim n As Integer
    Dim sHex As String
    sHex = ""

    n = Len(str)
    For i = 1 To n
       byt = CByte(Asc(Mid(str, i, 1)))
       If Len(Hex(byt)) = 1 Then
          sHex = sHex & "0" & Hex(byt)
       Else
          sHex = sHex & Hex(byt)
       End If
    Next
    Str2Hex = sHex

End Function

Public Function Hex2Str(sHex As String) As String
' Version 3.1: New function added August 2001
' Converts string <sHex> in hex format to string of ascii chars
' E.g. "6162632E" will be converted to "abc."
    Dim i As Integer
    Dim nBytes As Integer

    Hex2Str = ""
    If Not IsValidHex(sHex) Then
       Exit Function
    End If
    nBytes = Len(sHex) \ 2
    For i = 0 To nBytes - 1
       Hex2Str = Hex2Str & Chr(CByte("&H" & Mid(sHex, i * 2 + 1, 2)))
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
    Next

End Function

Public Function IsValidHex(strToCheck As String)
' Vesrion 3.1: New function added August 2001
' Returns True if strToCheck only contains valid hexadecimal digits
    Const scHEXDIGITS As String = "0123456789ABCDEFabcdef"
    ' NB Include both uc and lc just in case Binary Compare mode
    Dim i As Integer
    Dim nLen As Long

    IsValidHex = True
    nLen = Len(strToCheck)
    For i = 1 To nLen
      If InStr(scHEXDIGITS, Mid(strToCheck, i, 1)) = 0 Then
        IsValidHex = False
        Exit For
      End If
    Next
End Function

Public Function XorBytes(aByt1() As Byte, aByt2() As Byte, nBytes As Long)
' XOR's bytes in array aByt1 with array aByt2
' Returns results in aByt1
' i.e. aByt1 = aByt1 XOR aByt2
    Dim i As Long
    For i = 0 To nBytes - 1
      aByt1(i) = aByt1(i) Xor aByt2(i)
    Next
End Function

Public Function CopyBytes(aDest() As Byte, aSrc() As Byte, nBytes As Long)
' Copies nBytes from array aSrc() into aDest()
' Assumes aDest is large enough.
    Dim i As Long
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
  For i = 0 To nBytes - 1
    aDest(i) = aSrc(i)
  Next
End Function

Public Function LoadByteArray(aBytes() As Byte, ParamArray List() As Variant) As Integer
' Copies a list of values <List> into array of bytes <aBytes>.
' Returns number of bytes read.
' Checks length of array first.
' E.g. LoadByteArray(aBytes, &HFE, &HDC, &HBA, &H98) will return 4 and set
' aBytes(0) = &HFE, aBytes(1) = &HDC, aBytes(2) = &HBA, aBytes(3) = &H98
  Dim nLen As Integer, i As Integer

  nLen = UBound(List())     ' NB Zero-base, so one less than real length
  If UBound(aBytes()) < nLen Then
    nLen = UBound(aBytes())
  End If

  For i = 0 To nLen
    aBytes(i) = CByte(List(i))
  Next

  LoadByteArray = nLen + 1

End Function

' Version 3: ShiftLeft and ShiftRight functions improved.
' Thanks to Doug J Ward for these.
' Identical functions are also used as private functions in basRadix64
Public Function ShiftLeft(ByVal bytValue As Byte, intShift As Integer) As Byte
  If intShift > 0 And intShift < 8 Then
    ShiftLeft = bytValue * (2 ^ intShift) Mod 256
  ElseIf intShift = 0 Then
    ShiftLeft = bytValue
  Else
    ShiftLeft = 0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
    End If
End Function

Public Function ShiftRight(ByVal bytValue As Byte, intShift As Integer) As Byte
    If intShift > 0 And intShift < 8 Then
        ShiftRight = bytValue \ (2 ^ intShift)
    ElseIf intShift = 0 Then
        ShiftRight = bytValue
    Else
        ShiftRight = 0
    End If
End Function

Public Function PadHexString(strData As String, nblocklen As Long) As String
' Pad hex data string to next multiple of nBlockLen bytes as per RFC 2630
    Dim nLen As Long
    Dim sPad As String
    Dim nPad As Integer
    Dim sHex As String
    Dim i As Integer
    nLen = Len(strData) \ 2
    nPad = ((nLen \ nblocklen) + 1) * nblocklen - nLen
    nPad = nPad And &HFF
    sHex = IIf(nPad < 16, "0" & Hex(nPad), Hex(nPad))
    sPad = ""
    ' Pad with # of pads (1-n)
    For i = 1 To nPad
        sPad = sPad & sHex
    Next
    PadHexString = strData & sPad

End Function

Public Function UnpadHexString(strData As String, nblocklen As Long) As String
' Strip RFC 2630-style padding from hex string
    Dim nLen As Long
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
    Dim nPad As Long
    nLen = Len(strData)
    ' Get # of padding bytes from last char hex pair
    nPad = Int("&H" & (Right(strData, 2)))
    If nPad > nblocklen Then nPad = 0    ' In case invalid
    UnpadHexString = Left(strData, nLen - nPad * 2)
End Function
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

William Stallings. 2541. **Cryptography And Network Security : principles and practice**. 2nd ed. New Jersey : Prentice - Hall, Inc.

Andrew S. Tanenbaum. 2539. **Computer Networks**. 3rd ed. New Jersey : Prentice Hall PTR.

Behrouz A. Forouzan. 2544. **Data Communications and Networking**. 2nd ed. McGraw – Hill.

วรพจน์ กรแก้ววัมนกุล และ ชัยวัฒน์ ลิ้มพรจิตรวิไล, ผู้แปล. **เรียนรู้และปฏิบัติการไมโครคอนโทรลเลอร์ MCS-51 แบบแฟลช**. กรุงเทพ ฯ : บริษัท อินโนเวตีฟ เอ็กเพอริเมนต์ จำกัด.

ธีรวัฒน์ ประกอบผล, ผศ. 2543. **ระบบคอมพิวเตอร์และภาษาแอสเซมบลี**. พิมพ์ครั้งที่ 1. กรุงเทพ ฯ : สำนักพิมพ์ สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น)

ศุภชัย สมพานิช. 2545. **สร้างระบบฐานข้อมูลด้วย Visual Basic ฉบับปรับปรุง**. กรุงเทพ ฯ : บริษัท ด่านสุทธาการพิมพ์

ณรงค์ชัย นิมิตบุญอนันต์. 2542. **Computer Security for E-Commerce**. กรุงเทพ ฯ : SUM Publishing Department

อภิชาต คงสุวรรณ และ อวิรินี นาชิน. 2542 **"ระบบรักษาความปลอดภัยภายในหมู่บ้านโดยผ่านระบบเครือข่ายคอมพิวเตอร์."** วิทยานิพนธ์วิศวกรรมศาสตร์บัณฑิต สาขาวิชาวิศวคอมพิวเตอร์, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ธีรวัฒน์ ประกอบผล, ผศ. 2537. **การพัฒนาไมโครคอนโทรลเลอร์ด้วยภาษาซี**. พิมพ์ครั้งที่ 2. กรุงเทพ ฯ : สำนักพิมพ์ สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้