ระบบสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์

SMARTCARD SYSTEM IN COMPUTER ROOM

โดย

นายกฤษดา ธาตรีมนตรีชัย

นางสาวปัทมา ศิรลัมภามาศ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2549

SMARTCARD SYSTEM IN COMPUTER ROOM

BY

MR. KRISSADA TATRIMONTRICHAI

MS. PATTAMA SIRALAMPAMAS

A PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENT FOR THE DEGREE OF

BACHELOR IN DEPARTMENT OF INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUE OF TECHNOLOGY LARDKRABANG

หัวข้อปริญญานิพนธ์	ระบบสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์
ชื่อนักศึกษา	นายกฤษดา ธาตรีมนตรีชัย รหัสนักศึกษา 46012146
	นางสาวปัทมา ศิรลัมภามาศ รหัสนักศึกษา 46012179
อาจารย์ที่ปรึกษา	ผศ. อุทัย ศรีธีระวิโรจน์
	อาจารย์สรพงษ์ วชิรรัตนพรกุล
ระดับการศึกษา	ปริญญาตรี วิศวกรรมศาสตรบัณฑิต
	สาขาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2549

ปริญญานิพนธ์ฉบับนี้ได้รับความเห็นชอบจากอาจารย์ที่ปรึกษาเป็นที่เรียบร้อยแล้ว

.....

(ผศ. อุทัย ศรีธีระวิโรจน์)
อาจารย์ผู้ควบคุมปริญญานิพนธ์

.....

(อาจารย์สรพงษ์ วชิรรัตนพรกุล)
อาจารย์ผู้ควบคุมปริญญานิพนธ์

หัวข้อปริญญานิพนธ์	ระบบสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์
ชื่อนักศึกษา	นายกฤษดา ธาตรีมนตรีชัย รหัสนักศึกษา 46012146
	นางสาวปัทมา ศิรลัมภามาศ รหัสนักศึกษา 46012179
อาจารย์ที่ปรึกษา	ผศ. อุทัย ศรีธีระวิโรจน์
	อาจารย์สรพงษ์ วชิรรัตนพรกุล
ระดับการศึกษา	ปริญญาตรี วิศวกรรมศาสตรบัณฑิต
	สาขาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2549

บทคัดย่อ

โครงงานนี้มีจุดประสงค์เพื่อควบคุมและจัดการการใช้งานคอมพิวเตอร์ของนักศึกษาในห้องคอมพิวเตอร์ของภาควิชาวิศวกรรมสารสนเทศ โดยใช้ระบบทำการตรวจสอบและยืนยันสถานะของผู้ใช้จากบัตรสมาร์ทการ์ด อาทิ การล็อกอิน เวลาเข้าใช้เครื่องคอมพิวเตอร์ เวลาเลิกใช้เครื่องคอมพิวเตอร์ และระบบจะทำการรวบรวมข้อมูล สถิติการใช้งานของนักศึกษาในแต่ละชั้นปี เพื่อจัดทำเป็นรายงานแสดง

Project Title	Smartcard System in computer room for using
Student	Mr. Krisada Tatrimontrichai ID. 46012146
	Ms. Pattama Siralampamas ID. 46012179
Advisor	Asst. Prof Uthai Sritheravirough
	Mr. Sorrapong Wachirarattanapornkut
Graduate Level	Bachelor Degree of Information Engineering
Department	Information Engineering
Academic Year	2006

Abstract

This project purposes for control and manage computer using in a computer room at Information Engineering department. The system will check and confirm status from user's smartcard such as authentication, time of using, include admin control. The system will collect using data and store to statistic of computer using for providing

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จขึ้นได้นั้น ขอกราบขอบพระคุณ อาจารย์อุทัย ศรีธีระวิโรจน์ และอาจารย์สรพงษ์ วชิรรัตนพรกุล อาจารย์ที่ปรึกษาปริญญานิพนธ์ที่คอยให้คำปรึกษาและแนวคิดต่างๆในการทำโครงงานนี้ รวมทั้งดูแลตรวจทานจนกระทั่งสำเร็จเป็นปริญญานิพนธ์ฉบับนี้ขึ้น

ขอกราบขอบพระคุณอาจารย์ทุกๆท่าน ที่เคยสั่งสอนและให้คำแนะนำตลอดมา รวมถึงเพื่อนๆทุกคนที่คอยช่วยเหลือ ให้คำปรึกษาต่างๆและเป็นกำลังใจให้

ท้ายที่สุด คณะผู้จัดทำขอขอบคุณบิดามารดา บุคคลที่มีความสำคัญที่สุดที่คอยให้การสนับสนุนในทุกด้านและคอยให้กำลังใจตลอดเวลา และทำให้ผู้จัดทำมีวันนี้ได้ จึงกราบขอบคุณมา ณ ที่นี้

คณะผู้จัดทำ

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญรูปภาพ

สารบัญรูปภาพ (ต่อ)

หน้า

สารบัญตาราง

บทที่1
บทนำ

1.1 แนวคิดเริ่มต้นในการดำเนินการ

ในปัจจุบันเทคโนโลยีสมาร์ทการ์ดมีการใช้งานอย่างแพร่หลาย และมีแนวโน้มว่าจะมีการพัฒนาเพิ่มขึ้น เนื่องจากเทคโนโลยีสมาร์ทการ์ดจะช่วยอำนวยความสะดวกให้กับผู้ใช้งานได้อย่างมาก รวมถึงมีการเก็บข้อมูลที่รวดเร็วและปลอดภัย โดยมีการนำไปใช้งานหลายชนิด อาทิ เช่น บัตรประจำตัวประชาชนอัจฉริยะ(Smartcard ID), บัตรโทรศัพท์ติดต่อข้ามประเทศ แต่ปัญหาสำคัญคือเทคโนโลยีที่จะรองรับการใช้งานจากบัตรสมาร์ทการ์ดที่ยังมีไม่มากพอเมื่อเปรียบเทียบกับประเทศอื่นๆ โดยแนวความคิดนี้ทำให้ผู้จัดทำ เลือกที่จะให้ความสำคัญกับเทคโนโลยีที่จะรองรับกับการใช้งานบัตรสมาร์ทการ์ด โดยได้เลือกระบบที่ไม่ใหญ่จนเกินไปและสามารถนำไปใช้ประโยชน์ได้ในอนาคต จึงเกิดเป็นระบบสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์ขึ้น

1.2 วัตถุประสงค์ของโครงงาน

1. เพื่อเพิ่มความสะดวกในการเข้าใช้คอมพิวเตอร์ของห้องคอมพิวเตอร์ในสถานศึกษา รวมถึงการเก็บรวบรวมข้อมูลด้านสถิติการใช้คอมพิวเตอร์ของผู้ใช้
2. เพื่อง่ายต่อการจัดการระบบของผู้ดูแลระบบ โดยระบบจะช่วยอำนวยความสะดวกและสามารถสั่งปิดการใช้งานคอมพิวเตอร์เมื่อหมดเวลาให้บริการได้

1.3 ขอบเขตของโครงงาน

1. ออกแบบให้ภายในสมาร์ทการ์ดสามารถระบุข้อมูลส่วนตัวของผู้ใช้ รหัสผ่าน เพื่อใช้ในการใช้งานคอมพิวเตอร์
2. เขียนโปรแกรมให้คอมพิวเตอร์สามารถยืนยันการใช้งานของผู้ใช้ เช่น ข้อมูลส่วนตัว เวลาที่ใช้ และข้อมูลการใช้งาน โดยจะส่งไปให้คอมพิวเตอร์ฝ่ายผู้ดูแล
3. ผู้ดูแลระบบสามารถสั่งปิดการใช้งานของเครื่องคอมพิวเตอร์ได้เมื่อหมดเวลาให้บริการการใช้งานคอมพิวเตอร์
4. ออกแบบระบบจัดเก็บข้อมูลการใช้งานคอมพิวเตอร์เพื่อแสดงเป็นรายงานสถิติ

1.4 ขั้นตอนการดำเนินการ

1. ศึกษาและรวบรวมข้อมูล
2. จัดซื้ออุปกรณ์
3. ออกแบบโปรแกรมที่ใช้ควบคุมการทำงานของเครื่องอ่าน-เขียนสมาร์ทการ์ด
4. ออกแบบโปรแกรมติดต่อระหว่างผู้ใช้ ซึ่งโปรแกรมจะยืนยันสถานะ และส่งข้อมูลไปให้ผู้ดูแลระบบ
5. ทำการทดลองโครงงานและปรับปรุงข้อบกพร่อง

การดำเนินโครงงาน	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.
1. กำหนดขอบเขตและรูปแบบของโครงงาน	←	→						
2. ศึกษาและรวบรวมข้อมูล		←	→					
3. ออกแบบโปรแกรมที่ใช้ควบคุมการทำงานของเครื่องอ่าน-เขียนสมาร์ทการ์ด		←	→	→				
4. ออกแบบโปรแกรมติดต่อระหว่างผู้ใช้ ซึ่งโปรแกรมจะยืนยันสถานะ และส่งข้อมูลไปให้ผู้ดูแลระบบ				←	→			
5. ออกแบบโปรแกรมที่ใช้ในการสั่งปิดคอมพิวเตอร์เมื่อหมดเวลาให้บริการ						←	→	
6. ทำการทดลองโครงงานและปรับปรุงข้อบกพร่อง							←	→

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถดูแล จัดการการใช้คอมพิวเตอร์ระหว่างผู้ใช้และผู้ดูแลระบบให้สะดวก และปลอดภัยยิ่งขึ้น
2. สมาร์ทการ์ดมีแนวโน้มจะพัฒนาอย่างรวดเร็ว ดังนั้นจะเป็นประโยชน์สำหรับการพัฒนาระบบต่อในอนาคตอย่างมาก

1.6 เนื้อหาของโครงงาน

ในโครงงานนี้จะประกอบไปด้วยเนื้อหาทั้งหมด 5 บท อันได้แก่ บทที่ 1 กล่าวถึง แนวคิดและที่มาของโครงงาน ระบบสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์

ในบทที่ 2 กล่าวถึง ทฤษฎีที่เกี่ยวข้องกับโครงงาน มาตรฐานของบัตรสมาร์ทการ์ด ต่อมาในบทที่ 3 เป็นขั้นตอนของการออกแบบระบบ และส่วนโปรแกรมซอฟท์แวร์ และเนื้อหาของ บทที่ 4 จะเป็นส่วนผลการทดลอง 3 ส่วน คือ ส่วนติดต่อกับนักศึกษา, ส่วนติดต่อกับผู้ดูแลระบบ และส่วนติดต่อกับเครื่องอ่าน-เขียน และบัตรสมาร์ทการ์ด

โดยในบทสุดท้าย บทที่ 5 จะกล่าวถึงบทสรุปและสิ่งที่ได้ทำโครงงานในปีการศึกษา 2549 ปัญหาในการทำโครงงาน รวมถึงแนวทางพัฒนาระบบต่อไปในอนาคต

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 สมาร์ทการ์ดคืออะไร

สมาร์ทการ์ด(Smartcard) คือ บัตรพลาสติกที่มีชิปไอซี(Integrated circuit) ติดหรือฝังอยู่ในตัวบัตรพลาสติกตามมาตรฐาน ISO(International Standard Organization) เพื่อใช้ในการเก็บข้อมูลและประมวลผลภายในตัวเองโดยวิธีการเข้ารหัสลับตามมาตรฐาน DES Algorithm(Data Encryption Standard) เพื่อให้ระบบมีการจัดการด้านความปลอดภัยที่สูงขึ้น ด้วยคุณสมบัติสำคัญประการหนึ่งที่ทำให้สมาร์ทการ์ดไม่ต้องอาศัยติดต่อสื่อสารกับระบบหลัก(Font End) นั้นก็คือสมาร์ทการ์ดไม่จำเป็นต้องมีการติดต่อสื่อสารกับศูนย์กลางข้อมูลเหมือนบัตรแถบแม่เหล็ก(Off-line) ทำให้ประหยัดในเรื่องระบบสื่อสารไปได้มาก

2.2 ประวัติความเป็นมาของสมาร์ทการ์ด

ปี ค.ศ. 1968 สมาร์ทการ์ดเกิดขึ้นครั้งแรกโดยชาวเยอรมัน Jurgen Dethloff และ Helmut Grotupp เป็นผู้คิดค้น แต่ผู้ที่ได้มาซึ่งสิทธิบัตรกลับเป็นชาวญี่ปุ่น Kunitaka Arimura

ปี ค.ศ. 1970 ได้มีการจดสิทธิบัตรในชื่อสมาร์ทการ์ดโดยชาวฝรั่งเศส Roland Moreno

ปี ค.ศ. 1974 สมาร์ทการ์ดในระยะแรกยังทำงานได้ไม่สมบูรณ์นัก เพราะสมาร์ทการ์ดรุ่นแรกๆ ยังมีปัญหาทางเทคนิคเล็กๆ น้อยๆ ซึ่งแม้ว่าสมาร์ทการ์ดจะถือกำเนิดในยุโรป แต่ในระยะแรกสมาร์ทการ์ดกลับไม่ได้รับความสนใจเท่าที่ควร

ปี ค.ศ. 1984 บริษัท French PTT(Postal and Telecommunication Services) ได้นำสมาร์ทการ์ดมาใช้งานในบัตรโทรศัพท์ เพื่อป้องกันการโกงค่าโทรศัพท์ ซึ่งในครั้งนั้นถือว่าเป็นโครงการนำร่องการนำบัตรแถบแม่เหล็กบัตรแถบแสง(Optical Storage) และสมาร์ทการ์ดมาทำการทดลองใช้งานเปรียบเทียบกัน ซึ่งแน่นอนว่าสมาร์ทการ์ดได้พิสูจน์ให้เห็นคุณลักษณะที่เหนือกว่าบัตรชนิดอื่นทั้งในเรื่องของความทนทาน ความปลอดภัย ความสวยงาม เป็นผลให้สมาร์ทการ์ดในรูปของบัตรโทรศัพท์มีการนำไปใช้ถึง 60 ล้านใบ (เฉพาะประเทศฝรั่งเศส) และตอกย้ำความสำเร็จอีกกว่า 100 ล้านใบจาก 50 ประเทศทั่วโลกในปี 1997 แต่ถึงอย่างไรสมาร์ทการ์ดก็ยังเป็นเพียงบัตรโทรศัพท์ การนำสมาร์ทการ์ดมาใช้ทางด้านการเงินธนาคารกลับเป็นไปอย่างเชื่องช้า เนื่องจากบัตรที่เกี่ยวข้องกับระบบการเงินการธนาคารมีความยุ่งยากมากกว่าบัตรโทรศัพท์

ปี ค.ศ. 1960 เทคโนโลยีการประมวลผลเพื่อการเข้ารหัสลับข้อมูลของฮาร์ดแวร์และซอฟท์แวร์มีความพร้อมมากขึ้น จึงมีการนำมาใช้ในการเข้ารหัสลับข้อมูลในสมาร์ทการ์ด ซึ่งแต่เดิมนั้นการเข้ารหัสลับจะมีการใช้งานเฉพาะในหน่วยงานทหาร หรือหน่วยงานราชการลับเท่านั้น ด้วยเหตุนี้ทำให้สมาร์ทการ์ดสามารถทำการเข้ารหัสลับ-ถอดรหัสลับข้อมูลได้ภายในบัตร ทำให้การใช้สมาร์ทการ์ดมีความปลอดภัยสูงขึ้นจนสามารถนำมาใช้เป็นบัตรเครดิต หรือบัตรเงินสดได้อย่างสมบูรณ์แบบ

ปี ค.ศ. 1984 ธนาคารในฝรั่งเศสได้นำสมาร์ทการ์ดมาใช้เป็นบัตรเครดิตเป็นครั้งแรก ในระยะแรกนั้นต้องประสบกับปัญหามากมาย เกี่ยวกับการเข้ากันได้ของบัตรต่างธนาคาร ซึ่งต้องใช้เวลาถึง 10 ปีที่จะทำให้เข้ากันได้ทั้งหมด เป็นเหตุให้มีการรวมกันของ Europay, VISA และ MASTER เพื่อกำหนดมาตรฐานแก่บัตรเครดิตการ์ด ในรูปของสมาร์ทการ์ดให้มีมาตรฐานเดียวกันทุกธนาคารในชื่อของมาตรฐาน EMV(Europay, MASTER,VISA) โดยอ้างอิงกับมาตรฐาน ISO7816 เป็นหลัก ทำให้มีผู้ที่ต้องการพัฒนาแอพพลิเคชั่นเครดิตหรือเดบิตบนสมาร์ทการ์ด ต้องทำตามข้อกำหนดของมาตรฐาน EMV เท่านั้น

2.3 ส่วนประกอบและโครงสร้างของสมาร์ทการ์ด

2.3.1 ตัวบัตรพลาสติก

สมาร์ทการ์ดเป็นชิปไอซีขนาดเล็กที่ถูกสร้างขึ้นเช่นเดียวกับชิ้นส่วนอิเล็กทรอนิกส์อื่นๆ ที่สร้างจากสารกึ่งตัวนำ แล้วนำมาติดลงบนหน้าสัมผัส และทำการฝังลงในเนื้อบัตรพลาสติก โดยพลาสติกที่นิยมนำมาทำเป็นตัวบัตรจะใช้พลาสติก 4 ชนิด ได้แก่ PVC(Polyvinyl Choloride), ABS (Acrylonitrile Butadiene Styrene), PC(Polycarbonate) และ PET(Polyethylene Terephthalate) ในประเทศไทยจะใช้บัตรพลาสติก PVC มากเป็นส่วนใหญ่ ส่วนอันดับสองเป็นบัตรพลาสติกชนิด ABS โดยบัตรพลาสติกชนิด PVC มักนำมาใช้เป็นบัตรเอทีเอ็ม บัตรเครดิต-เดบิต บัตรประจำตัวประชาชน เป็นต้น

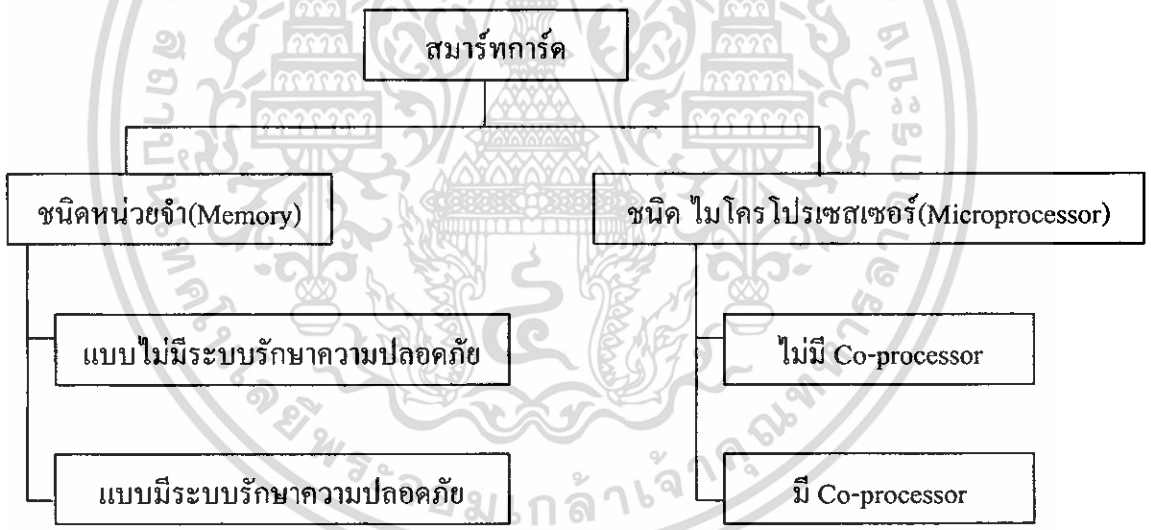
2.3.2 หน้าสัมผัสและชิปสมาร์ทการ์ด (Smart card Module)

สมาร์ทการ์ดโมดู หรือหน้าสัมผัสและชิปสมาร์ทการ์ด คือส่วนที่แสดงความเป็นตัวตนของสมาร์ทการ์ดที่ชัดเจนที่สุด ดังนั้นการที่จะระบุว่าบัตรใบใดเป็นบัตรสมาร์ทการ์ดนั้น ต้องดูที่หลักการทำงานและลูกเล่นของบัตรเป็นหลัก อันต้องใช้ประสบการณ์ที่เกี่ยวกับสมาร์ทการ์ดพอสมควร

ในการผลิตสมาร์ทการ์ดโมดู ส่วนที่เป็นหน้าสัมผัสของบัตรสมาร์ทการ์ดจะประกอบด้วยโลหะหลายชิ้นประกอบกัน แต่ละส่วนจะถูกยึดด้วยแถบฟิล์มบางๆ ทางด้านหลังของหน้าสัมผัสเพื่อให้คงรูปอยู่ได้ แถบฟิล์มตัวนี้จะมีการเจาะช่องเล็กๆ สำหรับการเชื่อมต่อสายนำสัญญาณกับชิปสมาร์ทการ์ดกับหน้าสัมผัส หลังจากวางชิปสมาร์ทการ์ดลงในตำแหน่งที่ต้องการและเชื่อมต่อสายนำสัญญาณจากชิปสมาร์ทการ์ดเข้ากับหน้าสัมผัสเรียบร้อยแล้ว ขั้นตอนสุดท้ายจะเป็นการผนึกชิปสมาร์ทการ์ดเพื่อป้องกันตัวชิป และสายนำสัญญาณต่างๆ จากสิ่งแวดล้อมภายนอก (เป็นการทดสอบขั้นต้น) ส่วนขั้นตอนที่เหลือจะเป็นการนำหน้าสัมผัสและชิปใส่ลงในบัตรพลาสติก และทดสอบการทำงานชิปขั้นสุดท้าย

2.4 ชนิดของสมาร์ทการ์ด

การแบ่งชนิดของสมาร์ทการ์ดสามารถแบ่งได้ ดังรูปที่ 2.1



รูปที่ 2.1 การแบ่งสมาร์ทการ์ดตามชนิดของหน่วยความจำ

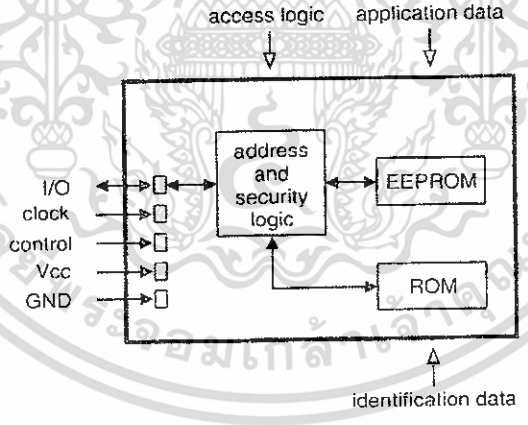
จากรูปที่ 2.1 จะเห็นได้ว่าเราสามารถแบ่งสมาร์ทการ์ดจากโครงสร้างภายในได้ 2 ชนิดคือ สมาร์ทการ์ดชนิดหน่วยความจำ(Memory Card) สมาร์ทการ์ดชนิดไมโครโปรเซสเซอร์(Processor Card) โดยชิปทั้งสองแบบจะมีหน้าสัมผัสเหมือนกัน แต่สัญญาณที่ป้อนให้แก่หน้าสัมผัสบางหน้าสัมผัส จะไม่มีการใช้งานสมาร์ทการ์ดต่างชนิดกัน เช่น แรงดันไฟฟ้าสำหรับการเขียนข้อมูลลงในชิป(Vpp) จะมีใช้ในสมาร์ทการ์ดชนิดหน่วยความจำเท่านั้น, สัญญาณนาฬิกาสำหรับป้อนให้ชิป

ทำงาน(CLK) ต้องป้อนให้กับชิปเหมือนกัน สำหรับสัญญาณนาฬิกา(CLK) ที่ป้อนให้ชิปสมาร์ทการ์ดเป็นสัญญาณนาฬิกาภายนอกที่ป้อนให้ชิปทำงานได้ เพราะภายในชิปสมาร์ทการ์ดไม่มีวงจรสำหรับสร้างสัญญาณนาฬิกา แต่หน้าสัมผัส I/O จะมีการรับ-ส่งข้อมูลที่แตกต่างกันในเรื่องจองความถี่ และวิธีการควบคุมจังหวะการรับ-ส่งของข้อมูลแต่ละบิต

ในการแบ่งสมาร์ทการ์ดออกเป็น 2 ชนิด ตามชนิดของวงจรภายในดังที่กล่าวมา อาจแบ่งได้อีกลักษณะคือ แบ่งตามความถี่ในการรับ-ส่งข้อมูลผ่านหน้าสัมผัส I/O ของสมาร์ทการ์ด ดังที่กล่าวไปแล้ว ซึ่งสามารถแบ่งได้ดังนี้

2.4.1 การ์ดหน่วยความจำ (Memory Card)

สมาร์ทการ์ดชนิดหน่วยความจำ (Memory) หรืออีกชื่อหนึ่งคือ Synchronous การ์ดประเภทนี้จะมีหน่วยความจำเพียงอย่างเดียวไม่มีซีพียู เมื่อมีการรับ-ส่งข้อมูลข้อมูลแต่ละบิตที่ส่งให้แก่ชิปจะต้องสัมพันธ์กับสัญญาณนาฬิกา สมาร์ทการ์ดชนิดนี้จะประกอบด้วยโครงสร้างในส่วนวงจรสำหรับการติดต่อสื่อสารภายนอก หน่วยความจำข้อมูล และหน่วยความจำสำหรับเก็บชุดคำสั่งของสมาร์ทการ์ด ดังรูปที่ 2.2



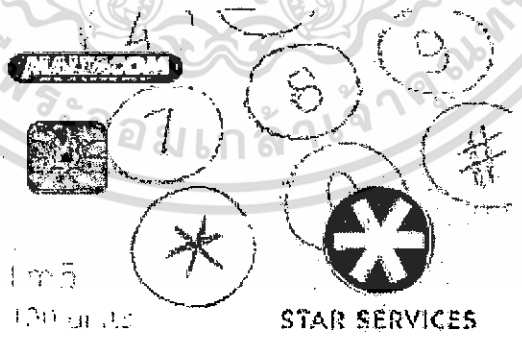
รูปที่ 2.2 โครงสร้างภายในชิปสมาร์ทการ์ดชนิดหน่วยความจำ

สมาร์ทการ์ดที่เป็นพื้นฐานของสมาร์ทการ์ดในปัจจุบัน ก็คือสมาร์ทการ์ดชนิด Free Access Memory สมาร์ทการ์ดชนิดนี้เปิดโอกาสให้อ่านหรือเขียนข้อมูลในแอดเดรสใดๆ ก็ได้ตามชื่อของสมาร์ทการ์ดชนิดนี้ ไม่มีการป้องกันข้อมูลใดๆ ภายในสมาร์ทการ์ด ซึ่งแน่นอนว่ามีความปลอดภัยต่ำที่สุด ถึงกระนั้นการอ่านข้อมูลก็ไม่ใช่เรื่องง่ายนักเมื่อมีการออกแบบหน่วยความจำข้อมูลให้มีการสลับตำแหน่งของบิตข้อมูล โดยมีวงจรควบคุมการสลับตำแหน่งของบิตเป็นส่วนป้องกันข้อมูลอีก

ต่อหนึ่ง ดังนั้นการอ่านข้อมูลออกแบบธรรมดาจะไม่ได้ข้อมูลที่ถูกต้องหากไม่ติดต่อกับวงจรควบคุมการสลับตำแหน่งของบิตโดยตรง

นอกจากนี้สมาร์ทการ์ดชนิดหน่วยความจำแบบธรรมดา ยังมีการใส่วงจรกำหนดเงื่อนไขการอ่าน-เขียนข้อมูลลงไปด้วย ทำให้สามารถกำหนดเงื่อนไขการอ่าน-เขียนข้อมูลได้ทุกไบต์ โดยสมาร์ทการ์ดที่มีวงจรป้องกันการอ่าน- เขียนชนิดนี้ถูกเรียกว่า PIN Protect Memory เนื่องจากการเข้าถึงข้อมูลจะต้องแสดงรหัสผ่านให้บัตรทราบก่อนจึงจะสามารถเข้าถึงข้อมูลได้ วงจรกำหนดเงื่อนไขการอ่าน-เขียนข้อมูลจะมีบิตพิเศษที่มีชื่อว่า Bin Protect ซึ่งเป็นข้อมูลที่ฝากไว้กับข้อมูลให้เป็นบิตที่ 9 แต่ไม่สามารถแก้ไขได้ด้วยคำสั่งเขียนข้อมูลธรรมดา เพราะ Bit Protect ไม่ได้เป็นส่วนหนึ่งของข้อมูลจริงๆ ในการแก้ไข Bit Protect นี้จะสามารถทำการเปลี่ยนแปลงได้เพียงครั้งเดียวด้วยคำสั่งเฉพาะเท่านั้น เช่น หากต้องการบังคับไม่ให้ข้อมูลไบต์ใดไม่สามารถแก้ไขได้ก็ให้ทำการเคลียร์บิตที่ 9 ของข้อมูลไบต์นั้นๆ แต่สำหรับรหัสผ่านในการเข้าถึงข้อมูลสามารถเปลี่ยนแปลงได้ แต่ต้องแสดงรหัสผ่านชุดเก่าให้บัตรได้ทราบเสียก่อนจึงจะสามารถเปลี่ยนแปลงรหัสผ่านได้

สมาร์ทการ์ดอีกชนิดหนึ่งที่มีใช้เป็นบัตรโทรศัพท์ในประเทศไทยนั้นคือ การ์ดหน่วยความจำชนิด Token ภายในสมาร์ทการ์ดชนิดนี้ จะมีการเก็บข้อมูลในลักษณะจำนวนนับ (Counter) ซึ่งจำนวนนับนี้จะเป็นตัวเลขแทนมูลค่าของเงินที่ระบุบนบัตร การนับเลขเป็นการนับถอยหลังเพื่อเห็นการนับมูลค่าที่คงเหลือในบัตร หมายความว่าหากใช้บัตรในการโทรศัพท์ไปเรื่อยๆ มูลค่าในบัตรก็จะถูกลดลงตามไปด้วยเช่นกัน ในการเข้าถึงข้อมูลของสมาร์ทการ์ดชนิดนี้ต้องมีการแสดงรหัสผ่านให้บัตรทราบเหมือนกับการ์ดหน่วยความจำ ชนิด PIN Protect แต่ไม่มี Bit Protect เท่านั้นเอง



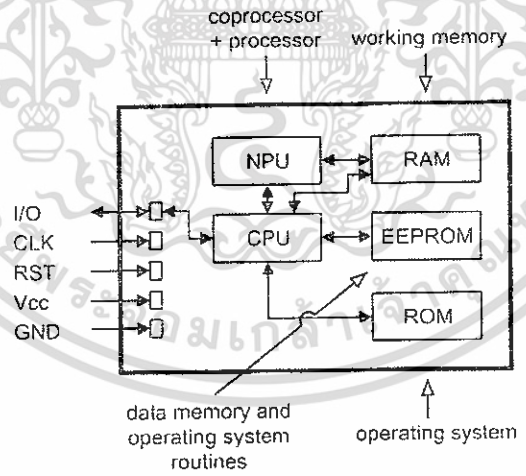
รูปที่ 2.3 บัตรสมาร์ทการ์ดที่เป็นบัตรโทรศัพท์

สมาร์ทการ์ดชนิดหน่วยความจำเป็นสมาร์ทการ์ดพื้นฐานของสมาร์ทการ์ดรุ่นใหม่ๆ ในปัจจุบัน ด้วยโครงสร้างและการทำงานที่ง่ายต่อการทำความเข้าใจ ราคาถูก สามารถเก็บข้อมูลได้

จำนวนมาก และความเร็วในการทำงานของชิปไม่สูงนัก จึงทำให้สมาร์ทการ์ดชนิดนี้เหมาะที่จะนำมาประยุกต์ใช้กับงานที่ข้อมูลไม่ค่อยสำคัญมากนัก เช่น บัตรลงเวลาทำงาน บัตรผ่านประตู บัตรโทรศัพท์ ฯลฯ ปัจจุบันสมาร์ทการ์ดชนิดหน่วยความจำ มีขนากหน่วยความจำสูงสุดถึง 64 กิโลไบต์ และอีกไม่นานนักเราจะได้เห็นสมาร์ทการ์ดที่มีขนาดหน่วยความจำข้อมูลถึง 128 กิโลไบต์

2.4.2 การ์ดชนิดโปรเซสเซอร์ (Processor card)

สมาร์ทการ์ดชนิดโปรเซสเซอร์ หรือเรียกอีกชื่อหนึ่งว่า Asynchronous card สมาร์ทการ์ดนี้ได้รับการปรับปรุงจากสมาร์ทการ์ดชนิดหน่วยความจำ โดยใช้เทคโนโลยีไมโครโปรเซสเซอร์เพื่อให้ชิปสามารถประมวลผลข้อมูลและยังเพิ่มความปลอดภัยให้กับข้อมูล ในการที่ใส่ไมโครโปรเซสเซอร์ลงไปในชิปทำให้จะต้องเพิ่มในส่วนขอหน่วยความจำสำหรับจัดเก็บระบบปฏิบัติการของไมโครโปรเซสเซอร์ และหน่วยความจำชั่วคราวสำหรับการประมวลผลข้อมูล นอกจากนี้ยังมีการใส่ชิปประมวลผลทางคณิตศาสตร์เพื่อใช้ในการประมวลผลข้อมูลด้วยอัลกอริทึมสำหรับเข้า-ออกรหัส ด้วยเหตุนี้จึงทำให้สมาร์ทการ์ดชนิดนี้มีการทำงานได้อย่างรวดเร็วมากกว่าสมาร์ทการ์ดชนิดหน่วยความจำ ดังรูปที่ 2.4



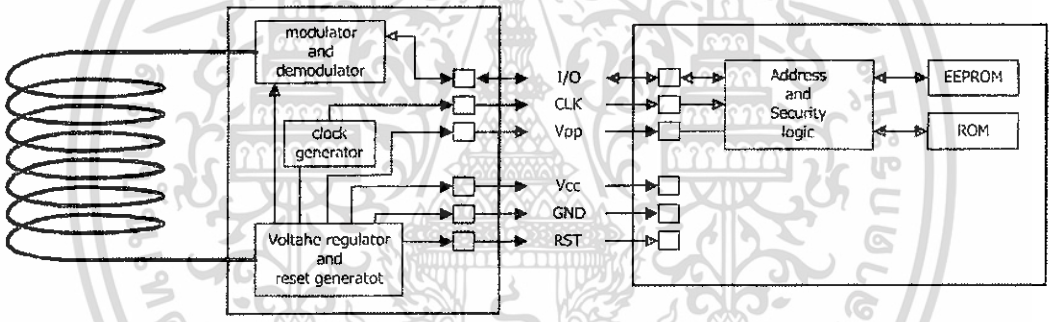
รูปที่ 2.4 โครงสร้างภายในชิปสมาร์ทการ์ดชนิดโปรเซสเซอร์

ในการรับส่งข้อมูลให้กับสมาร์ทการ์ดชนิดนี้ จะใช้หน้าสัมผัสเดียวกับสมาร์ทการ์ดชนิดหน่วยความจำ โดยสัญญาณนาฬิกาที่ป้อนจะถูกให้เป็นสัญญาณนาฬิกาให้แก่โปรเซสเซอร์ภายในสมาร์ทการ์ด ข้อมูลที่รับส่งจึงไม่จำเป็นต้องสัมพันธ์กับสัญญาณนาฬิกาที่ป้อนให้กับชิป เพียงกำหนดอัตราการรับ-ส่งข้อมูลเป็น 9600 บิตต่อวินาที ก็สมารถติดต่อกับโปรเซสเซอร์ของชิปได้แต่

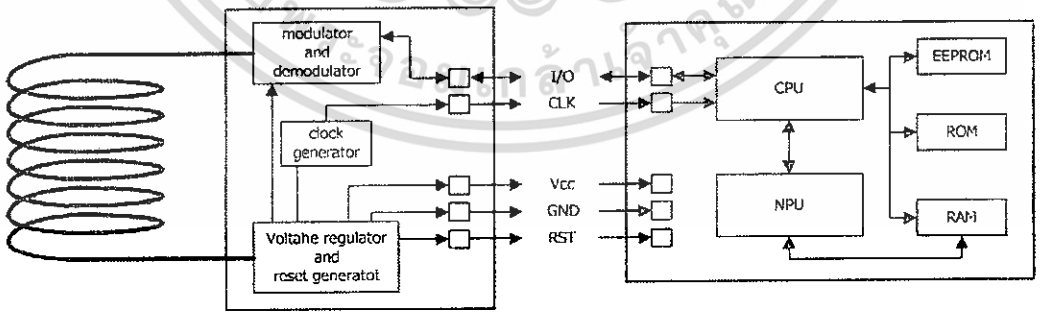
การเข้าถึงข้อมูลจะไม่สามารถทำเหมือนสมาร์ทการ์ดชนิดหน่วยความจำ การเข้าถึงข้อมูลต้องกระทำผ่านโปรเซสเซอร์ของสมาร์ทการ์ดเท่านั้น ไม่ว่าจะเป็นการอ่านหรือเขียนข้อมูลก็ตาม เพราะหน่วยความจำจะอยู่ภายในความควบคุมของโปรเซสเซอร์เพียงอย่างเดียว ข้อดีอย่างหนึ่งที่ไม่สามารถติดต่อกับหน่วยความจำในชิปได้โดยตรงก็คือ การลอบเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตแทบเป็นไปไม่ได้ ยกเว้นมีความบกพร่องในการกำหนดเงื่อนไขในการเข้าถึงข้อมูลที่เป็นความลับ

2.4.3 การ์ดชนิดแบบไม่มีสัมผัส (Contactless Card)

สมาร์ทการ์ดแบบ Contactless ไม่ใช้หน้าสัมผัสในการเข้าถึงข้อมูล ระบบสมาร์ทการ์ดแบบนี้เป็นระบบที่ทันสมัยที่สุดก็ว่าได้ สมาร์ทการ์ดชนิดนี้ใช้เทคโนโลยีการสื่อสารผ่านคลื่นวิทยุที่ความถี่ 13.56 เมกกะเฮิรตซ์โดยใช้การมอดูเลตข้อมูลและส่งให้กับชิปสมาร์ทการ์ดโดยจะมีเสารับ-ส่งสัญญาณที่เป็นขดลวดขนาดเล็กที่ฝังอยู่ในเนื้อบัตร ดังรูปที่ 2.5



ก. สมาร์ทการ์ดชนิดหน่วยความจำ แบบ Contactless



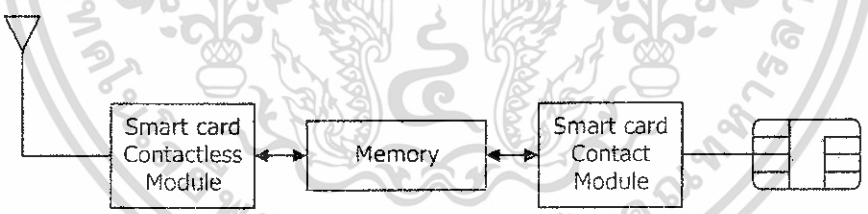
ข. สมาร์ทการ์ดชนิดโปรเซสเซอร์ แบบ Contactless

รูปที่ 2.5 โครงสร้างภายในชิปสมาร์ทการ์ดชนิด Contactless

ซึ่งในส่วนการรับสัญญาณคลื่นวิทยุจะแบ่งออกเป็น 2 ส่วนคือส่วนแรกเป็นตัวแปลงกระแสไฟฟ้าให้กับชิปและมีวงจรสร้างสัญญาณนาฬิกาให้ทำงานได้ และอีกส่วนจะถูกดิมอดูเลต เอาข้อมูลจากคลื่นวิทยุและส่งต่อให้กับชิปสมาร์ทการ์ด ในส่วนการส่งข้อมูลกลับนั้นจะอาศัยการใช้กระแสไฟฟ้าจากคลื่นวิทยุมาทำการมอดูเลต ข้อมูลและส่งกลับไปยังเสารับ-ส่งสัญญาณภายในเนื้อบัตร ดังนั้นการออกแบบสมาร์ทการ์ดแบบนี้จึงต้องใช้กระแสไฟต่ำที่สุดเท่าที่จะน้อยได้ ไม่งั้นจะไม่เพียงพอในการทำงานของการ์ด ถ้ามองดูที่สมาร์ทการ์ดประเภทนี้แล้วเราไม่อาจบอกได้ว่าเป็นสมาร์ทการ์ดแบบ Contactless เพราะรูปร่างภายนอกเหมือนบัตรพลาสติกใบหนึ่ง จะพบบ่อยในการใช้งานประเภทอาคารจอดรถ เพราะว่าสามารถอ่านข้อมูลได้อย่างรวดเร็ว หรือจะพบว่านิยมใช้เป็น Security Card

2.4.4 การ์ดชนิดลูกผสม (Com-Bi Card)

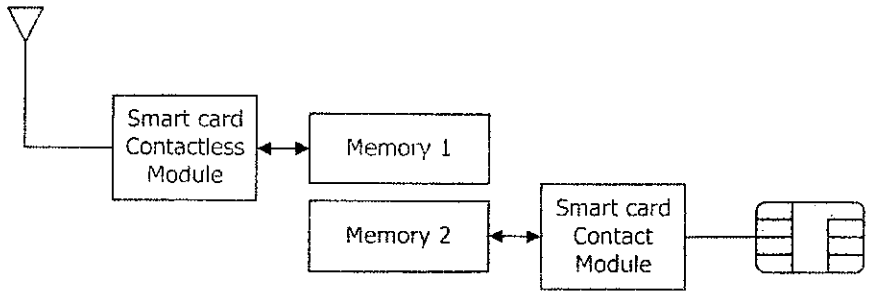
สมาร์ทการ์ดชนิดนี้เป็นการรวมเอาสมาร์ทการ์ดแบบที่หน้าสัมผัสกับสมาร์ทการ์ดแบบไม่มีหน้าสัมผัส เข้าด้วยกันสมาร์ทการ์ดชนิดนี้จะใช้หน่วยความจำข้อมูลร่วมกันเพื่อใช้กับรายการที่ต้องการความปลอดภัย สามารถทำได้โดยผ่านหน้าสัมผัสที่มีไมโครโปรเซสเซอร์ควบคุมอยู่และยังสามารถทำงานทั่วไปผ่านทางคลื่นวิทยุ ดังรูปที่ 2.6



รูปที่ 2.6 โครงสร้างภายในสมาร์ทการ์ดชนิด Com-Bi Card

2.4.5 การ์ดชนิดไฮบริด (Hybrid Card)

สมาร์ทการ์ดชนิดนี้มีลักษณะโครงสร้างเหมือนการ์ดประเภท Com-Bi Card แต่จะแตกต่างกันที่หน่วยความจำข้อมูล โดยหน่วยความจำระหว่างมีหน้าสัมผัสและไม่มีหน้าสัมผัสจะถูกแยกออกจากกันอย่างสิ้นเชิง เพื่อความสะดวกในการใช้งาน โดยในปัจจุบัน Hybrid cards จะหมายถึงบัตรที่มีการรวมคุณสมบัติการใช้งานตั้งแต่สองอย่างขึ้นไปเช่น การ์ดที่มีทั้งแถบแม่เหล็กและชิปสมาร์ทการ์ด, บัตรสมาร์ทการ์ดที่มีหน้าสัมผัสและไม่มีหน้าสัมผัส ดังรูปที่ 2.7



รูปที่ 2.7 โครงสร้างภายในสมาร์ทการ์ดชนิด Hybrid cards

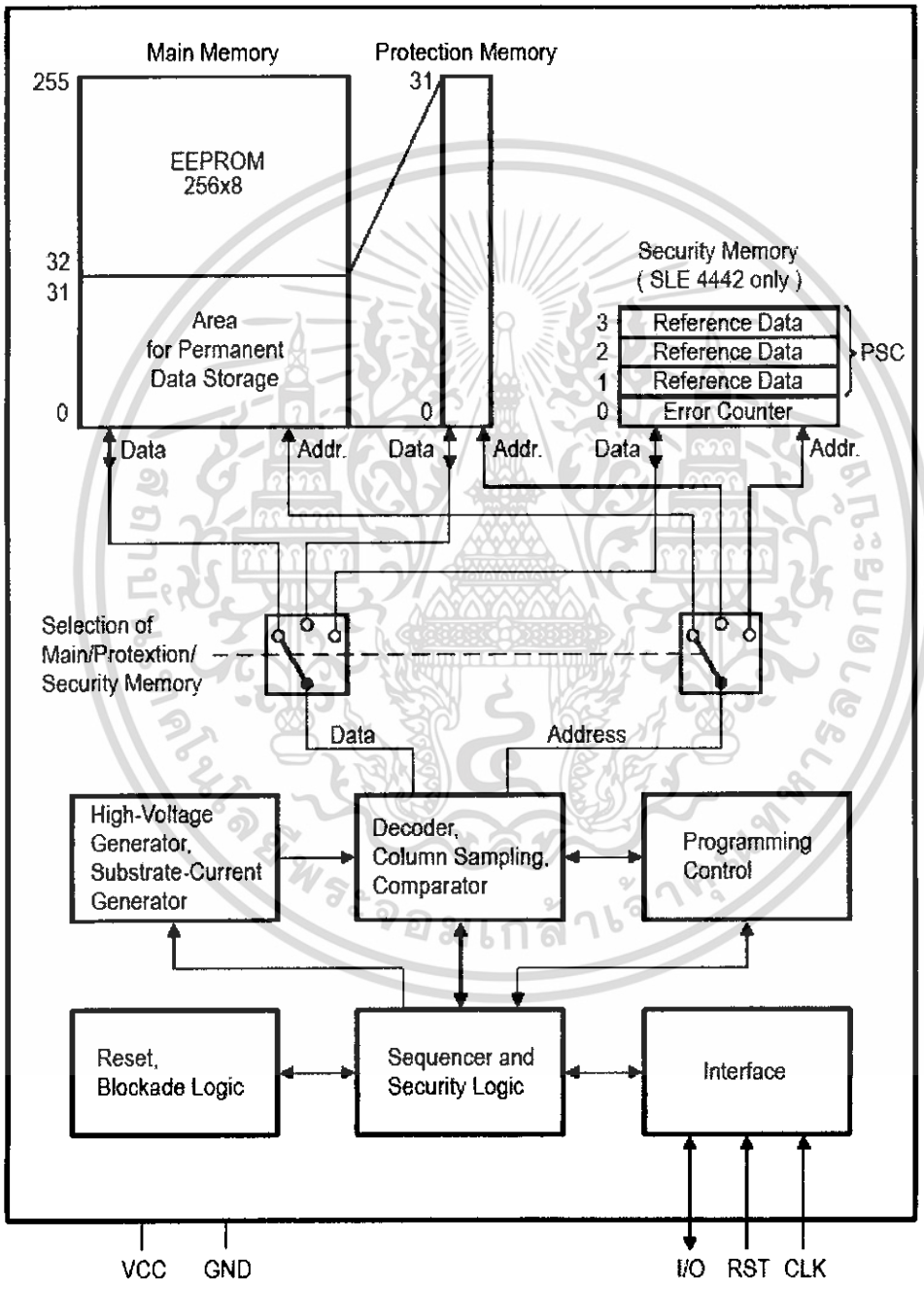
2.5 การ์ดที่มีระบบป้องกันข้อมูล

การ์ดที่มีระบบป้องกันความปลอดภัยข้อมูล คือ สมาร์ทการ์ดที่การอ่านข้อมูลสามารถทำได้อย่างอิสระ แต่การเขียนข้อมูลจะไม่สามารถทำได้หากไม่มีรหัสผ่านที่ถูกต้อง วิธีการในลักษณะนี้ช่วยให้ข้อมูลภายในสมาร์ทการ์ดได้รับการปกป้องและมีความน่าเชื่อถือ รูปแบบการสื่อสารข้อมูลของสมาร์ทการ์ดชนิดนี้เป็นการสื่อสารข้อมูลแบบซิงโครนัส(Synchronous) ตามมาตรฐาน ISO7816 ซึ่งรูปแบบคำสั่งจะแตกต่างกันไปในผู้ผลิตแต่ละราย โดยในโครงงานนี้เลือกใช้บอร์ดTSM-256 ซึ่งเป็นบอร์ดที่ใช้เพื่อการอ่านและเขียนข้อมูลกับบัตรสมาร์ทการ์ด เบอร์ SLE4442 รับคำสั่งติดต่อสื่อสารผ่านทาง RS-232 หรือ RS-485 โดย RS-232 สามารถต่อพ่วงกันเป็น Network ได้สูงสุดถึง 8 บอร์ด เลือกใช้ค่าความเร็วการสื่อสารได้ตั้งแต่ 2400-19200 ชุดคำสั่งที่ใช้งานเป็นแบบ ASCII สะดวกใช้งานง่าย สามารถเขียนข้อมูลถาวรลงไปในบัตรได้ มีระบบตรวจสอบค่า PSC พร้อม Error Counter ใช้ความปลอดภัยกับข้อมูลสูง ประยุกต์ใช้ต่อเข้ากับ MCU ได้โดยตรงด้วยจุดต่อแบบ TTL Level Socket ที่ใช้เสียบบัตรคุณภาพดีเสียบ ค้างไว้ได้แน่นแต่ดึงออกง่าย TSM-256 บอร์ดที่เหมาะกับการประยุกต์ใช้งานที่ต้องการให้ความปลอดภัยของข้อมูลสูงของบัตรสมาร์ทการ์ด

2.5.1 คุณสมบัติทั่วไปของสมาร์ทการ์ดเบอร์ SLE4442

สมาร์ทการ์ด เบอร์ SLE4442 มีหน่วยความจำแบบ EEprom ขนาด 256 ไบต์ โดยแบ่งเป็น Protectable Data Memory 32 ไบต์ และ Unprotected Data Memory 224 ไบต์ สามารถอ่านและเขียนได้ 100,000 ครั้ง เก็บข้อมูลได้นานถึง 10 ปี ส่วนที่เป็น Protectable Data Memory นั้นสามารถเขียนข้อมูลถาวรไว้โดยจะลบหรือแก้ไขเปลี่ยนแปลงไม่ได้อีกเลยและในส่วนนี้ได้ถูกเขียนข้อมูลถาวรไว้แล้ว 12 ไบต์ ตามมาตรฐาน ISO7816 นอกจากนี้ SLE4442 ยังมี PSC(Programmable Security Code) 3 ไบต์ เพื่อใช้ในการตรวจสอบค่าให้ตรงกับค่า PSC ที่มีในบัตรก่อนจึงจะเขียนข้อมูลลงในบัตรได้ และ EC(Error Counter) เพื่อใช้ในการนับจำนวนครั้งที่ทำการตรวจสอบ Verity ค่า PSC โดยถ้าทำ

การตรวจสอบ Verity ค่า PSC ไม่ถูกต้องถึง 3 ครั้ง บัตรนี้จะเขียนข้อมูลไม่ได้อีกเลยทันที การนับ Error Counter นี้จะถูก Reset เมื่อไดทำการ Verity ค่า PSC ได้ถูกต้อง ค่า PSC มาตรฐานของบัตรใหม่ที่ผลิตจากโรงงานคือ FFFFFF

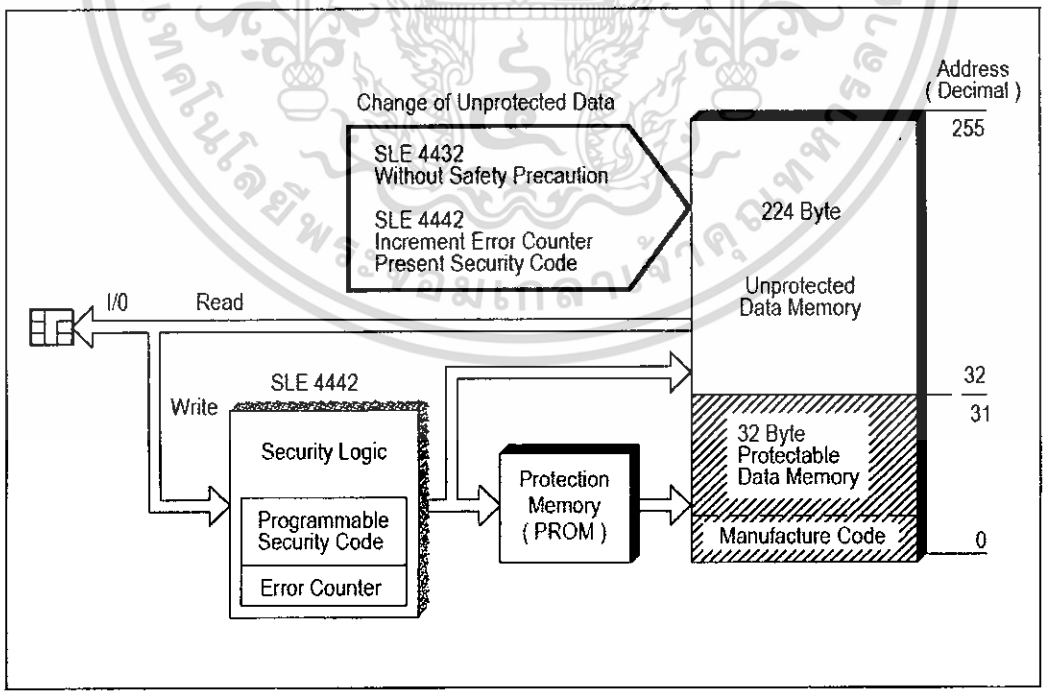


รูปที่ 2.8 บล็อกไดอะแกรมแสดงโครงสร้างภายในของ SLE4442

จากรูปที่ 2.8 จะเห็นได้ว่าหน่วยความจำขนาด 256 ไบต์ ที่อยู่ภายในสมาร์ทการ์ดเบอร์ SLE4442 จะถูกแบ่งออกเป็น 2 ส่วนด้วยกัน ได้แก่ ข้อมูลในช่วง 32 ไบต์แรกซึ่งเป็นพื้นที่ที่มีระบบป้องกันการเขียนข้อมูลทับ และหน่วยความจำส่วนถัดมาซึ่งเป็นอีอีพรอม(EEPROM) ที่สามารถทั้งเขียนและอ่านได้ กลไกในการปกป้องข้อมูลของสมาร์ทการ์ดเบอร์ SLE4442 มาจากส่วนที่เป็นหน่วยความจำปลอดภัย(Security Memory) ที่ได้รับการปกป้องโดยข้อมูลสำคัญ 2 ส่วน คือ

- ข้อมูลอ้างอิง(Reference Data หรือ PSC) เป็นข้อมูลขนาด 3 ไบต์ ที่เก็บค่าของรหัสผ่านสำหรับการเข้าไปแก้ไขข้อมูลในหน่วยความจำเอาไว้ (รหัส PSC ไม่สามารถถูกอ่านออกมาได้) รหัส PSC จะถูกกำหนดเป็นค่าหนึ่งมาโดยผู้ผลิตก่อนซึ่งสามารถจะมาปรับเปลี่ยนเองได้ในภายหลังเมื่อใช้งาน

- ไบต์แสดงความผิดพลาด(Error Counter Byte) เป็นข้อมูลที่บอกถึงจำนวนครั้งที่ป้อนรหัส PSC ผิด ซึ่งถูกกำหนดเอาไว้ตายตัวว่าจะผิดได้ไม่เกิน 3 ครั้ง หากเกินกว่านั้นการ์ดจะล็อกตัวเองอย่างถาวรทันที และไม่มีทางปลดล็อกได้ แม้ว่าจะป้อนรหัส PSC ที่ถูกต้องไปแล้วก็ตาม การเขียนข้อมูลยังหน่วยความจำก็จะไม่สามารถทำได้อีกต่อไป แต่ยังคงอ่านข้อมูลออกมาได้ตามปกติ การป้อนรหัส PSC ผิดแต่ละครั้ง Error Counter จะถูกลดลง 1 ค่าทันที ถ้าหากค่า Error Counter ถูกลดลงจนมีค่าเป็น 0 เมื่อไรก็แสดงว่าการ์ดได้ถูกล็อกไปเรียบร้อยแล้ว (ในกรณีที่ป้อนรหัสถูกในครั้งที่ 3 ค่าของ Error Counter จะถูกรีเซตกลับไปเป็น 3 ครั้งเหมือนอย่างตอนแรกเริ่ม)



รูปที่ 2.9 บล็อกไดอะแกรมแสดงภาพรวมของการ์ดที่มีระบบป้องกันข้อมูล

จากรูปที่ 2.9 จะเห็นได้ว่าการอ่านข้อมูลจากหน่วยความจำนั้น เราสามารถจะอ่านข้อมูลออกมาได้โดยไม่ต้องผ่านขั้นตอนของการป้อนรหัส PSC แต่สำหรับการเขียนข้อมูลแล้วเราจะต้องป้อนรหัส PSC ที่ถูกต้องเสียก่อน เพื่อเปิดลอจิกในการเขียนข้อมูลลงยังหน่วยความจำ นอกจากนั้นก็จะเห็นได้ว่าข้อมูล 4 ไบต์แรก เป็นข้อมูลของผู้ผลิตหรือ Manufacturer Code โดยพื้นที่ส่วนนี้ใช้เก็บข้อมูลของ ATR โดยความหมายของข้อมูลที่อยู่ในพื้นที่ส่วนนี้แต่ละไบต์จะถูกกำหนดโดยผู้ผลิตการ์ดแต่ละราย

2.5.2 รูปแบบการสื่อสารข้อมูลของสมาร์ทการ์ดเบอร์ SLE4442

รูปแบบ การสื่อสารข้อมูลของสมาร์ทการ์ดเบอร์ SLE4442 เป็นการรับส่งข้อมูลระหว่างเครื่องอ่านและสมาร์ทการ์ดแบบ 2 ทิศทาง (ข้อมูลบนสาย I/O จะถูกอ่านค่าที่ขอบขาลงของสัญญาณนาฬิกา) โดยรูปแบบการสื่อสารนี้ประกอบด้วย 4 โหมดการทำงาน ได้แก่

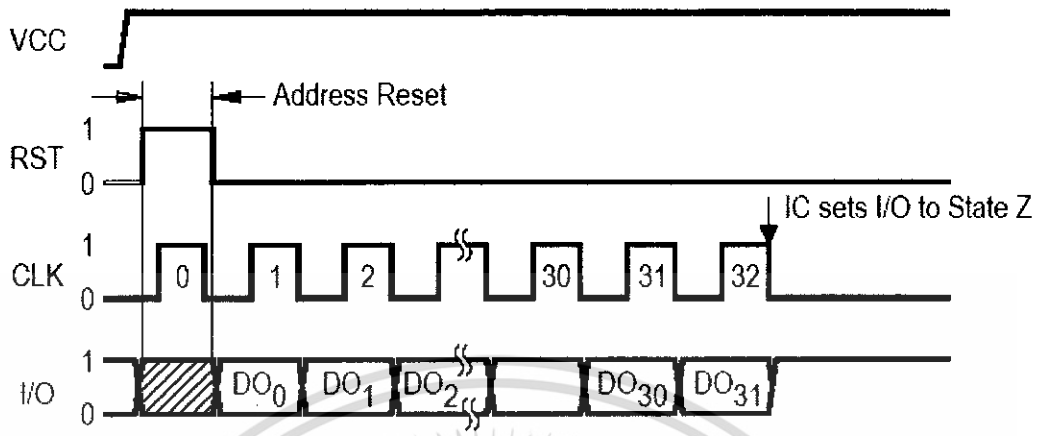
- การรีเซตและการตอบรับการรีเซตด้วย ATR(Answer To Reset)
- โหมดการส่งคำสั่ง(Command Mode)
- โหมดการอ่านข้อมูล(Outgoing Data Mode)
- โหมดการดำเนินการ(Processing Mode)

2.5.2.1 การรีเซตและการตอบรับการรีเซตด้วย ATR (Answer To Reset)

การอินเตอร์เฟสเข้ากับ Security Memory Card ทั่วๆ ไปจะสอดคล้องกับมาตรฐานในการอินเตอร์เฟสเมื่อรีเซตการทำงานของการ์ดจะทำให้การ์ดมีการตอบรับการรีเซตด้วยข้อมูล ATR สำหรับข้อมูล ATR ที่ตอบกลับมาจากสมาร์ทการ์ดเบอร์ SLE4442 จะประกอบด้วยข้อมูล 4 ไบต์ การอ่านข้อมูลที่ว่านี้สามารถทำได้โดยอ้างอิงจากสัญญาณในรูปที่ 2.10

ตารางที่ 2.1 ลักษณะของข้อมูลที่ได้จากการตอบรับการรีเซต

Answer-to-Reset (Hex)	Byte 1	Byte 2	Byte 3	Byte 4
	$DO_7 \ldots DO_0$	$DO_{15} \ldots DO_8$	$DO_{23} \ldots DO_{16}$	$DO_{31} \ldots DO_{24}$

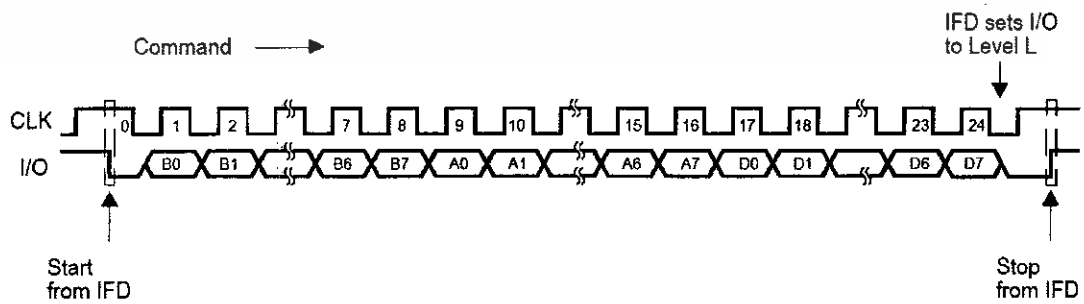


รูปที่ 2.10 สัญญาณของการรีเซตและการตอบรับการรีเซตด้วย ATR

โดยหลังจากที่ขา RST เป็นลอจิคต่ำ เมื่อมีสัญญาณนาฬิกาถูกต่อเข้าไป จะทำให้เกิดสัญญาเอาท์พุตของสมาร์ทการ์ดขึ้นที่ขา I/O ซึ่งก็คือ สัญญาณตอบรับการรีเซตนั้นเอง หลังจากที่ครบ 4 ไบต์แล้ว ที่ขา I/O จะเปลี่ยนเป็นลอจิกสูงเพื่อเป็นการบอกถึงการสิ้นสุดการรีเซต

2.5.2.2 โหมดการส่งคำสั่ง (Command Mode)

การส่งคำสั่งไปยังสมาร์ทการ์ดหรือการทำงานในโหมดการส่งคำสั่ง (Command Mode) ก็คือกระบวนการต่อเนื่องหลังจากการ์ดถูกรีเซตไปเรียบร้อยแล้ว โดยการ์ดจะรอรับคำสั่งที่ส่งมาจากเครื่องอ่านซึ่งมีรูปแบบเป็นข้อมูลมีความยาว 3 ไบต์ โครงสร้างของข้อมูลดังกล่าวประกอบด้วยคำสั่ง (Command), แอดเดรส(Address) และข้อมูล(Data) โดยคำสั่งทั้งหมดที่สมาร์ทการ์ดเบอร์ SLE4442 รองรับถูกแสดงดังตารางที่ 2.2 ส่วนรูปสัญญาณที่เกิดขึ้นระหว่างการทำงานของโหมดการส่งคำสั่งจะเป็นดังรูปที่ 2.11



รูปที่ 2.11 สัญญาณของการส่งคำสั่งไปยังการ์ด

ตารางที่ 2.2 โครงสร้างและความหมายของชุดคำสั่งที่สมาร์ทการ์ดเบอร์ SLE4442 รองรับ

Byte 1 Control								Byte 2 Address	Byte 3 Data	Operation	Mode
B7	B6	B5	B4	B3	B2	B1	B0	A7-A0	D7-D0		
0	0	1	1	0	0	0	0	address	no effect	READ MAIN MEMORY	outgoing data
0	0	1	1	1	0	0	0	address	input data	UPDATE MAIN MEMORY	processing
0	0	1	1	0	1	0	0	no effect	no effect	READ PROTECTION MEMORY	outgoing data
0	0	1	1	1	1	0	0	address	input data	WRITE PROTECTION MEMORY	processing
0	0	1	1	0	0	0	1	no effect	no effect	READ SECURITY MEMORY	outgoing data
0	0	1	1	1	0	0	1	address	input data	UPDATE SECURITY MEMORY	processing
0	0	1	1	0	0	1	1	address	input data	COMPARE VERIFICATION DATA	processing

ตารางที่ 2.3 รูปแบบและส่วนประกอบของคำสั่ง

MSB			Control				LSB	MSB			Address				LSB	MSB			Data				LSB
B7	B6	B5	B4	B3	B2	B1	B0	A7	A6	A5	A4	A3	A2	A1	A0	D7	D6	D5	D4	D3	D2	D1	D0

จะเห็นได้ว่าการส่งข้อมูลแต่ละครั้งจะต้องมีการส่งสภาวะเริ่มต้นและสภาวะสิ้นสุดกำกับไปกับตัวข้อมูลด้วย โดยสภาวะเริ่มต้นก็คือการเปลี่ยนระดับจากลอจิกค่าสูงเป็นค่าต่ำที่ขา I/O ในขณะที่ระดับลอจิกที่ขา CLK เป็นค่าสูง ส่วนสภาวะสิ้นสุดก็คือการเปลี่ยนแปลงระดับจากลอจิกค่าต่ำเป็นสูงที่ขา I/O ในขณะที่ขา CLK เป็นค่าสูง

- การอ่านข้อมูลจากหน่วยความจำหลัก (Read Main Memory)

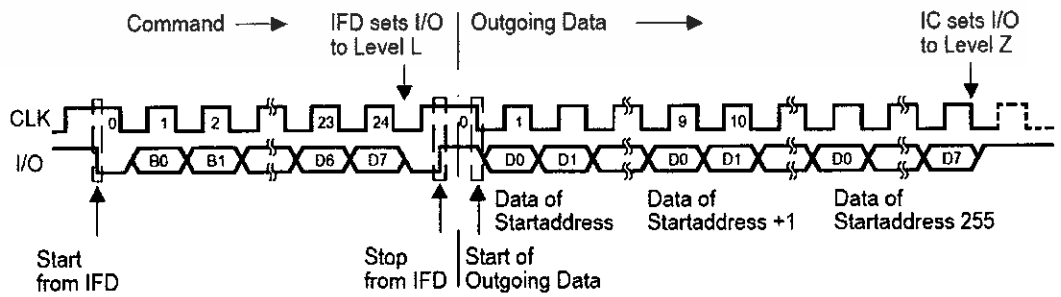
คือ คำสั่งที่ใช้ในการอ่านข้อมูลทั้งหมดออกมาจากหน่วยความจำของการ์ด ทั้งจากพื้นที่ส่วนที่ได้รับการป้องกัน(หน่วยความจำ 32 ไบต์แรก) และส่วนที่ไม่ได้รับการป้องกัน (หน่วยความจำ 224 ไบต์หลัง) โดยจะเป็นการอ่านค่าโดยเริ่มต้นจากแอดเดรสที่ส่งไปจนถึงแอดเดรสสุดท้าย (0FFH) ของพื้นที่หน่วยความจำ

ตารางที่ 2.4 ลักษณะหน่วยความจำ และรูปแบบคำสั่งในการอ่านข้อมูลจากหน่วยความจำหลัก

Address (decimal)	Main Memory	Protection Memory	Security Memory (only SLE 4442)
255	Data Byte 255 (D7 ...D0)	-	-
:	:	-	-
32	Data Byte 32 (D7 ...D0)	-	-
31	Data Byte 31 (D7 ...D0)	Protection Bit 31 (D31)	-
:	:	:	-
3	Data Byte 3 (D7 ...D0)	Protection Bit 3 (D3)	Reference Data Byte 3 (D7 ...D0)
2	Data Byte 2 (D7 ...D0)	Protection Bit 2 (D2)	Reference Data Byte 3 (D7...D0)
1	Data Byte 1 (D7 ...D0)	Protection Bit 1 (D1)	Reference Data Byte 3 (D7...D0)
0	Data Byte 0 (D7 ...D0)	Protection Bit 0 (D0)	Error Counter

Command: READ MAIN MEMORY

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ...D0
Binary	0	0	1	1	0	0	0	0	Address	No effect
Hexadecimal	30_H								OO_H ...FF_H	No effect



รูปที่ 2.12 สัญญาณของการอ่านข้อมูลจากหน่วยความจำหลัก

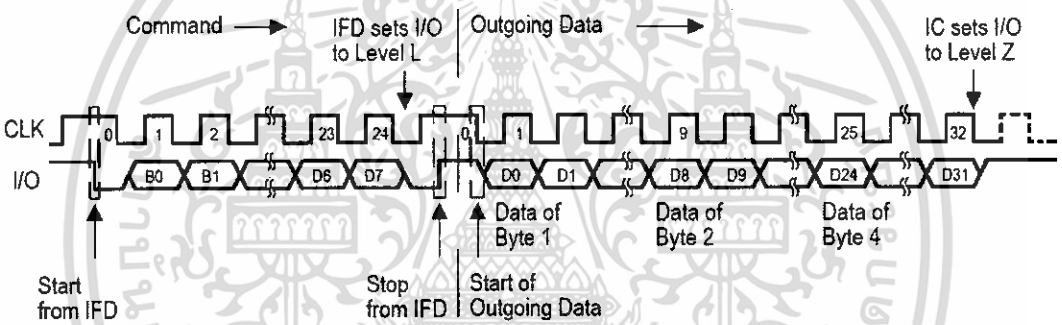
- การอ่านข้อมูลจากหน่วยความจำที่มีการป้องกัน (Read Protection Memory)

คือ คำสั่งที่ใช้ในการอ่านข้อมูลทั้งหมดออกมาจากหน่วยความจำ 32 ไบต์แรก

ตารางที่ 2.5 รูปแบบคำสั่งในการอ่านข้อมูลจากหน่วยความจำที่มีการป้องกัน

Command: READ PROTECTION MEMORY

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ... D0
Binary	0	0	1	1	0	1	0	0	No effect	No effect
Hexadecimal	34_H								No effect	No effect



รูปที่ 2.13 สัญญาณคำสั่งในการอ่านข้อมูลจากหน่วยความจำที่มีการป้องกัน

- การเขียนข้อมูลลงในหน่วยความจำหลัก (Update Main Memory)

คือ คำสั่งที่ใช้ในการเขียนข้อมูลแอดเดรสใดๆ ของหน่วยความจำทั้ง 256 ไบต์ ในกรณีที่ใช้คำสั่งนี้ในการเขียนข้อมูลลงยังหน่วยความจำ 32 ไบต์แรก ข้อมูลยังคงแก้ไขเปลี่ยนแปลงได้ภายหลัง

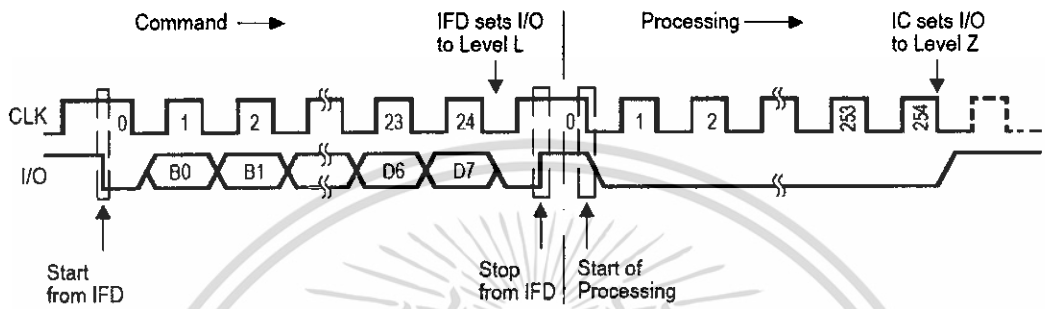
ตารางที่ 2.6 รูปแบบคำสั่งในการเขียนข้อมูลลงในหน่วยความจำหลัก

Command: UPDATE MAIN MEMORY

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ...D0
Binary	0	0	1	1	1	0	0	0	Address	Input data
Hexadecimal	38_H								OO_H ...FF_H	Input data

สำหรับการเขียนข้อมูลจะประกอบด้วย 3 เงื่อนไข คือ

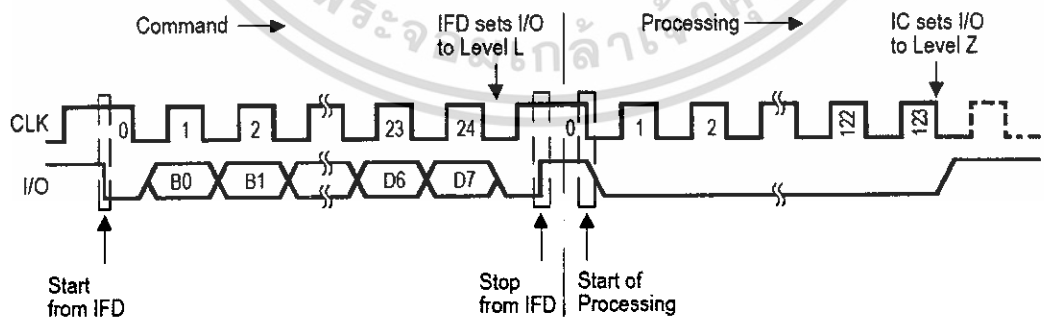
- การลบข้อมูลที่แอดเดรสของหน่วยความจำที่กำหนด ให้เป็น 0FFH แล้วทำการเขียนข้อมูลซ้ำลงยังแอดเดรสเดิม กระบวนการนี้ต้องใช้เวลา 5 มิลลิวินาที หรือเท่ากับสัญญาณนาฬิกา 255 ลูก



รูปที่ 2.14 สัญญาณของการเขียนข้อมูลลงในหน่วยความจำหลัก แบบการลบข้อมูลแล้วเขียนข้อมูลซ้ำ

- การเขียนข้อมูลที่แอดเดรสของหน่วยความจำที่กำหนดโดยไม่ต้องลบข้อมูลออก สำหรับกรณีแอดเดรสดังกล่าวจะต้องเป็นที่ว่าง (มีค่าข้อมูลเป็น 0FFH) อยู่ก่อนหน้านี้แล้วเท่านั้น กระบวนการนี้จะใช้เวลา 2.5 มิลลิวินาที หรือเท่ากับสัญญาณนาฬิกา 124 ลูก

- การลบข้อมูลที่แอดเดรสของหน่วยความจำที่กำหนด (ให้มีค่าข้อมูล 0FFH) โดยไม่มีการเขียนข้อมูลต่อ สำหรับกระบวนการนี้ใช้เวลา 2.5 มิลลิวินาที หรือเท่ากับสัญญาณนาฬิกา 124 ลูก



รูปที่ 2.15 สัญญาณของการเขียนข้อมูลลงในหน่วยความจำหลัก แบบการลบหรือเขียนข้อมูล (อย่างใดอย่างหนึ่ง)

- การเขียนข้อมูลลงในหน่วยความจำที่มีการป้องกัน (Write Protection Memory)

คือ การเขียนข้อมูลลงยังแอดเดรสของหน่วยความจำใดๆ ใน 32 ไบต์แรก คำสั่งนี้มีเงื่อนไขว่าข้อมูลที่เขียนลงไปจะถูกเขียนลงยังแอดเดรสของหน่วยความจำที่กำหนดอย่างถาวร ไม่สามารถแก้ไขเปลี่ยนแปลงอะไรได้อีก สำหรับรูปสัญญาณของกระบวนการนี้อ้างอิงได้จากรูปสัญญาณของการเขียนข้อมูลลงในหน่วยความจำหลัก (Update Main Memory)

ตารางที่ 2.7 รูปแบบคำสั่งในการเขียนข้อมูลลงในหน่วยความจำที่มีการป้องกัน

Command: WRITE PROTECTION MEMMORY

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ...D0
Binary	0	0	1	1	1	1	0	0	Address	Input data
Hexadecimal	$3C_H$								OO_H ...$1F_H$	Input data

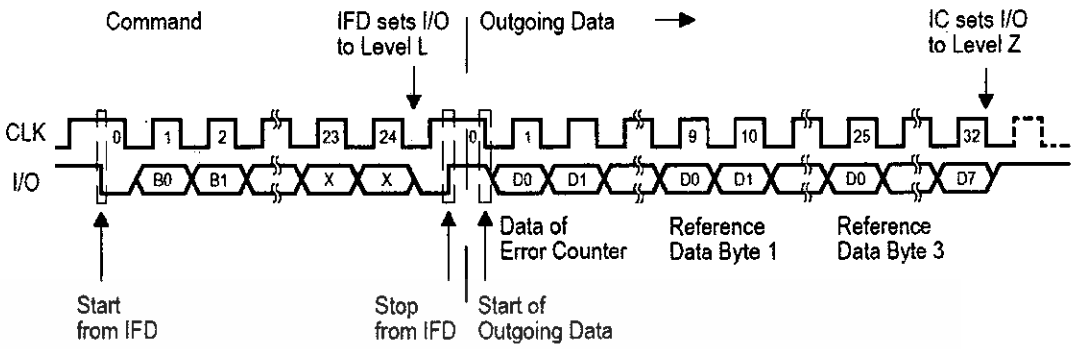
- การอ่านข้อมูลจากหน่วยความจำปลอดภัย (Read Security Memory)

คือ การอ่านค่าของ Error Counter เพื่อตรวจสอบว่าการ์ดใบนั้นๆ ได้ถูกล็อกไปแล้วหรือยัง โดยค่าภายในบิต D2, D1 และD0 ของ Error Counter จะเป็นส่วนที่บอกถึงสถานะของการ์ดใบนั้นๆ หากค่าของบิต D2, D1 และD0 เป็น 0 ทั้งหมด ก็แสดงว่าการ์ดได้ถูกล็อกไปแล้ว ซึ่งจะไม่สามารถแก้ไขอะไรได้และไม่สามารถเขียนข้อมูลลงยังการ์ดนั้นได้อีกต่อไป (แต่ว่าการอ่านข้อมูลในการ์ดจะยังคงทำได้ตามปกติ)

ตารางที่ 2.8 รูปแบบคำสั่งในการอ่านข้อมูลจากหน่วยความจำปลอดภัย

Command: READ SECURITY MEMORY

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ...D0
Binary	0	0	1	1	0	0	0	1	No effect	No effect
Hexadecimal	31_H								No effect	No effect



รูปที่ 2.16 สัญญาณของการอ่านข้อมูลจากหน่วยความจำปลอดภัย

- การเขียนข้อมูลลงในหน่วยความจำปลอดภัย

คือ การเข้าไปแก้ไขข้อมูลของรหัส PSC ภายในการ์ดหรืออาจกล่าวได้ว่าเป็นการเข้าไปเปลี่ยนรหัสป้องกันของการ์ดนั้นเอง คำสั่งจะถูกกระทำต่อเมื่อมีการส่งรหัส PSC ที่ถูกต้องไปยังการ์ดเสียก่อน โดยในกรณีที่ป้อนรหัสผิด ค่าของ D2, D1 และD0 ใน Error Counter จะค่อย ๆ ถูกเปลี่ยนจากค่า "1" เป็น "0" ไล่ไปทีละบิตตามจำนวนครั้งที่ป้อนผิด หากทั้งหมดกลายเป็นศูนย์

ตารางที่ 2.9 รูปแบบคำสั่งในการเขียนข้อมูลลงในหน่วยความจำปลอดภัย

Command: UPDATE SECURITY MEMORY

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ...D0
Binary	0	0	1	1	1	0	0	1	Address	Input data
Hexadecimal	39_H								OO_HO3_H	Input data

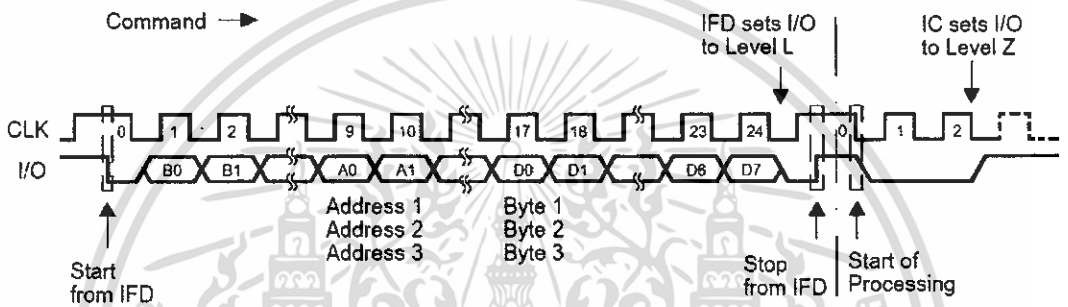
- การเปรียบเทียบและพิสูจน์ข้อมูล (Compare Verification Data)

คือ การสั่งให้การทำการเปรียบเทียบรหัส PSC กับรหัสผ่านที่เราได้ส่งไปยังการ์ด ในการเปรียบเทียบที่ว่านี้ ข้อมูลที่การ์ดจะส่งกลับมาคือค่าของ Error Counter ที่จะบอกว่ารหัสที่เราป้อนนั้นถูกต้องหรือไม่ และยังเหลือโอกาสพลาดอีกกี่ครั้งเท่านั้น (โดยเราจะไม่สามารถเข้าไปอ่าน PSC ของการ์ดออกมาได้)

ตารางที่ 2.10 รูปแบบคำสั่งในการเปรียบเทียบและพิสูจน์ข้อมูล

Command: COMPARE VERIFICATION DATA

	Control								Address	Data
	B7	B6	B5	B4	B3	B2	B1	B0	A7 ...A0	D7 ...D0
Binary	0	0	1	1	0	0	1	1	Address	Input data
Hexadecimal	33_H								OO_HO3_H	Input data



รูปที่ 2.17 สัญญาณของการเปรียบเทียบ และพิสูจน์ข้อมูล

- การเปรียบเทียบค่า PSC

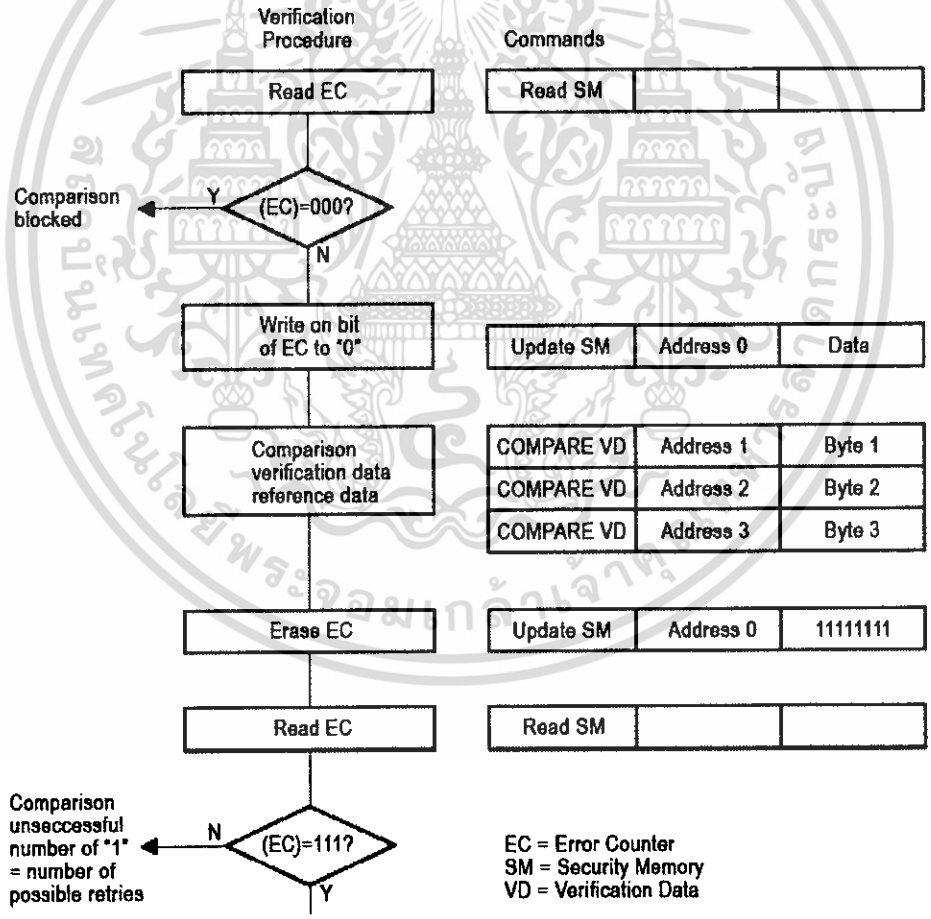
ในสมาร์ทการ์ดเบอร์ SLE4442 ผลลัพธ์ที่ได้จากการเปรียบเทียบค่า PSC ที่ถูกเก็บอยู่ในหน่วยความจำที่มีระบบรักษาความปลอดภัยต้องถูกต้อง เพื่อที่จะสามารถทำการเปลี่ยนแปลงหรือแก้ไขข้อมูล เมื่อเราทำการป้อนรหัส PSC ผิดนั้นจะเป็นผลทำให้บิตถูกเปลี่ยนจากลอจิกสูงไปสู่ลอจิกต่ำ ซึ่งไม่สามารถเปลี่ยนกลับเป็นลอจิกสูงได้ ถ้าป้อน PSC ผิด 3 ครั้ง จะทำให้บิตถูกเปลี่ยนครบ 3 ครั้ง ซึ่งจะมีผลทำให้บัตรสมาร์ทการ์ดใบนั้นไม่สามารถลบ และเขียนข้อมูลได้อีก แต่ยังคงอ่านข้อมูลได้ตามปกติ

ตารางที่ 2.11 รูปแบบคำสั่ง PSC ในการเข้าถึงหน่วยความจำแบบต่างๆ

Command	Control	Address	Data	Remark
	B7...B0	A7...A0	D7...D0	
Read Security Memory	31H	No effect	No effect	Check Error Counter
Update Security Memory	39H	00H	Input Data	Write free bit in Error Counter input data: 0000 0ddd binary

ตารางที่ 2.11 แสดงรูปแบบคำสั่ง PSC ในการเข้าถึงหน่วยความจำแบบต่างๆ (ต่อ)

Command	Control	Address	Data	Remark
	B7...B0	A7...A0	D7...D0	
Compare Verification Data	33H	01H	Input Data	Reference Data Byte 1
Compare Verification Data	33H	02H	Input Data	Reference Data Byte 1
Compare Verification Data	33H	03H	Input Data	Reference Data Byte 1
Update Security Memory	39H	00H	FFH	Erase Error Counter
Read Security Memory	31H	No effect	No effect	Check Error Counter



รูปที่ 2.18 กระบวนการเปรียบเทียบรหัสผ่านกับรหัส PSC

2.5.2.3 โหมดการอ่านข้อมูล (Outgoing Data Mode)

โหมดการทำงานนี้จะเกิดขึ้นหลังจากที่มีการส่งคำสั่งในกลุ่มของการขออ่านข้อมูล (เช่น Read Main Memory, Read Protection Memory และ Read Security Memory) ไปยังสมาร์ทการ์ดเพื่ออ่านข้อมูลจากพื้นที่ใดๆ ในหน่วยความจำ หลังจากที่ได้รับคำสั่งดังกล่าวสมาร์ทการ์ดจะส่งข้อมูลที่ถูกร้องขอกลับมายังเครื่องอ่าน ซึ่งก็เท่ากับว่าเครื่องอ่านจะสามารถอ่านข้อมูลที่ต้องการออกมาได้สำเร็จจากโหมดการทำงานนี้

2.5.2.4 โหมดการดำเนินการ (Processing Mode)

โหมดดำเนินการจะเกิดขึ้นหลังจากที่มีการส่งคำสั่งในกลุ่มของการขอเขียนหรือลบข้อมูลออกจากพื้นที่ใดๆ ในหน่วยความจำ (เช่น Update Main Memory, Write Protection Memory, Update Security Memory และ Compare Verification Data) โดยหลังจากที่ได้รับคำสั่งดังกล่าว สมาร์ทการ์ดจะเริ่มดำเนินกระบวนการตามที่ได้รับคำสั่งมาในโหมดการทำงานนี้ข้อมูลจากขา I/O จะไม่ถูกนำมาใช้ร่วมในการทำงานเลย (โดยจะมีสถานะเป็นลอจิกต่ำตลอดทั้งช่วง)

2.6 มาตรฐานที่เกี่ยวข้องกับสมาร์ทการ์ด

มาตรฐานของสมาร์ทการ์ดมีทั้งหมด 2 มาตรฐานด้วยกัน คือ

1. ISO 7816
2. AFNOR (แตกต่างกันตรงที่การจัดเรียงลำดับของขาสัญญาณและตำแหน่งของขาสัญญาณ) เนื่องจากในปัจจุบันสมาร์ทการ์ดแทบจะทั้งหมดใช้มาตรฐาน ISO 7816 ดังนั้นจะกล่าวเฉพาะมาตรฐานนี้เท่านั้น

2.6.1 มาตรฐาน ISO7816

เป็นการกำหนดในเรื่องของคุณลักษณะของบัตรพลาสติกที่จะมาทำเป็นสมาร์ทการ์ด โดยมีหัวข้อย่อยได้ดังนี้

- มาตรฐาน ISO7816-1เป็นมาตรฐานที่กำหนดด้วยเรื่องคุณสมบัติทางกายภาพเบื้องต้นของสมาร์ทการ์ด

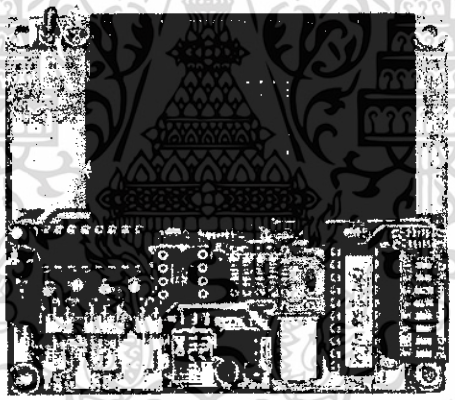
- มาตรฐาน ISO7816-2 เป็นมาตรฐานที่กำหนดขนาดของหน้าสัมผัส และตำแหน่งของหน้าสัมผัสชิปสมาร์ทการ์ดบนบัตร ประกอบด้วย

  - ขนาดของหน้าสัมผัสของชิปสมาร์ทการ์ด
  - ตำแหน่งของหน้าสัมผัสบนบัตร

- มาตรฐาน ISO7816-3 เป็นมาตรฐานที่กำหนดคุณสมบัติทางไฟฟ้าและโปรโตคอลที่ใช้ในการสื่อสารกับชิปสมาร์ทการ์ด

2.7 บอร์ด TSM-256 ของบริษัทSILA

TSM-256 เป็นบอร์ดที่ใช้เพื่อการอ่านและเขียนข้อมูลกับบัตรสมาร์ทการ์ดเบอร์ SLE4442 รับคำสั่งติดต่อสื่อสารผ่านทาง RS-232 หรือ RS-485 โดย RS-232 สามารถต่อพ่วงกันเป็น Network ได้สูงสุดถึง 8 บอร์ด เลือกใช้ค่าความเร็วการสื่อสารได้ตั้งแต่ 2400-19200 ชุดคำสั่งที่ใช้งานเป็นแบบ ASCII สะดวกใช้งานง่าย สามารถเขียนข้อมูลถาวรลงไปในบัตรได้ มีระบบตรวจสอบค่า PSC พร้อม Error Counter ใช้ความปลอดภัยกับข้อมูลสูง ประยุกต์ใช้ต่อเข้ากับ MCU ได้โดยตรงด้วยจุดต่อแบบ TTL Level Socket ที่ใช้เสียบบัตรคุณภาพดีเสียบ ค้างไว้ได้แน่นแต่ดึงออกง่าย TSM256 บอร์ดที่เหมาะกับการประยุกต์ใช้งานที่ต้องการให้ความปลอดภัยของข้อมูลสูงของบัตรสมาร์ทการ์ด



รูปที่ 2.19 บอร์ด TSM-256

2.7.1 คุณสมบัติทั่วไปของบอร์ด TSM-256

- ทำงานด้วยไมโครอนโทรลเลอร์เบอร์ 89C4051
- เขียนและอ่านบัตรสมาร์ทการ์ดเบอร์ SLE4442 ของบริษัท SIEMENS ตามมาตราฐาน ISO 7816
- รับคำสั่งจากเครื่องคอมพิวเตอร์ PC เพื่อเขียนและอ่านข้อมูลบัตรสมาร์ทการ์ดได้ โดยผ่านพอร์ทสื่อสารอนุกรม RS-232 (MAX232) มีสายเชื่อมต่อให้พร้อมหรือจะประยุกต์ต่อกับ MCU ได้โดยตรงด้วยจุดต่อ RS-232 แบบ TTL Level คุณสมบัติการสื่อสารคือ Parity=None, Data=8, StopBit=1 กำหนด Baudrate ได้ตั้งแต่ 2400-19200 ค่า

- มีระบบการสื่อสารแบบ Network สามารถเชื่อมต่อกันได้สูงสุด 8 บอร์ดด้วยพอร์ทสื่อสารอนุกรม RS232 (75176 เป็น OPTION) ส่งสัญญาณได้ไกลถึง 1.2 k.m. รับคำสั่งติดต่อสื่อสารกับคอมพิวเตอร์ได้ด้วยการแปลงสัญญาณ RS-232 จาก PC เป็น RS-485 ก่อนด้วย CON-485 ของศิลา

- DIP-SWITCH 8 หลักใช้สำหรับตั้งค่าความเร็วการสื่อสารและตั้งค่า Address กรณีที่ใช้ระบบการสื่อสารแบบ Network

- จัมพ์เปอร์ใช้ปรับเลือกว่าจะใช้ RS-232 แบบ TTL Level หรือใช้กับ RS-232 ที่ต่อเข้ากับ PC

- ขั้วต่อสีขาว 3 Pin สำหรับ RS-232 และขั้วต่อสีขาว 2 Pin สำหรับ RS-485

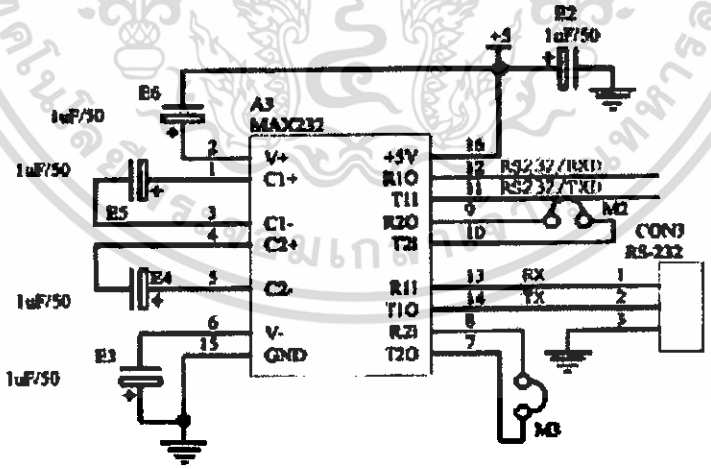
- มี LEDg แสดง POWER (สีแดง), TX (สีแดง), RX (สีเขียว) รวมทั้ง LED (สีเขียว) แสดงสถานะการทำงาน

- ใช้ไฟเลี้ยง 5 VDC โดยต่อเข้ากับขั้วต่อสีขาว 2 Pin

2.7.2 ส่วนประกอบภายในของบอร์ด TSM-256

จะประกอบด้วยวงจรดังต่อไปนี้

2.7.2.1 ไอซี MAX232



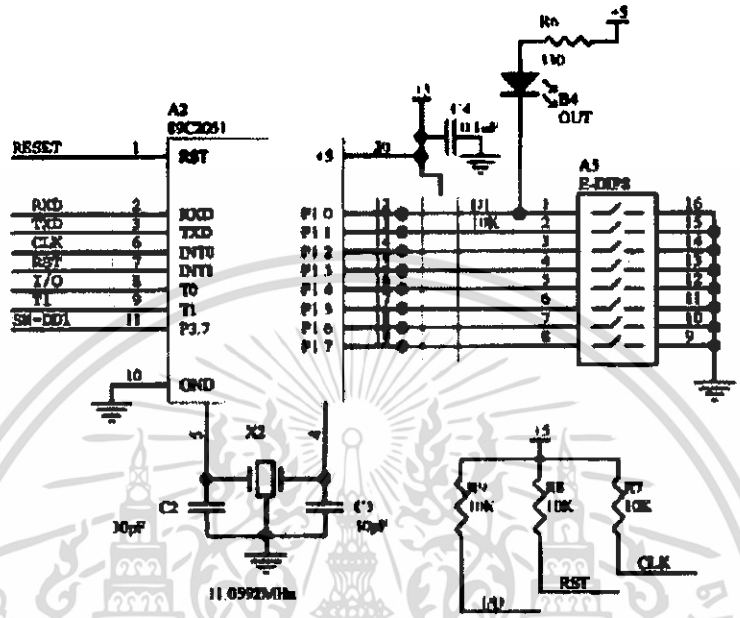
รูปที่ 2.20 วงจรไอซีMAX232

ไอซี MAX232 เป็นไอซีที่แปลงระดับสัญญาณจากระดับ TTL ไปเป็นระดับของ RS-232 และในทำนองเดียวกันก็รับระดับสัญญาณจาก RS-232เพื่อแปลงเป็นระดับสัญญาณจากระดับ TTLให้กับไมโครคอนโทรลเลอร์ โดยหน้าที่การทำงานของขาต่างๆ บนไอซี MAX232 ดังตารางที่ 2.12

ตารางที่ 2.12 แสดงหน้าที่การทำงานของขาต่างๆ ของไอซี MAX232

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	C1+	จ่ายไฟเข้าขาบวกของตัวเก็บประจุC1
2	V+	ขาไฟบวก
3	C1-	จ่ายไฟเข้าขาลบของตัวเก็บประจุC1
4	C2+	จ่ายไฟเข้าขาบวกของตัวเก็บประจุฉC2
5	C2-	จ่ายไฟเข้าขาลบของตัวเก็บประจุC2
6	V-	ขาไฟลบ
7	T20	ส่งสัญญาณที่แปลงเป็นอนุกรมแล้วส่งยังคอมพิวเตอร์
8	R2I	รับสัญญาณอนุกรมจากคอมพิวเตอร์ไปเป็น Parallel
9	R20	ส่งสัญญาณที่แปลงเป็น Parallel ไปยังสมาร์ทการ์ด
10	T2I	รับสัญญาณ Parallel จากสมาร์ทการ์ดไปเป็นสัญญาณอนุกรม
11	T1	รับสัญญาณ Parallel จากสมาร์ทการ์ดไปเป็นสัญญาณอนุกรม
12	R10	ส่งสัญญาณที่แปลงเป็น Parallel ไปยังสมาร์ทการ์ด
13	R1I	รับสัญญาณอนุกรมจากคอมพิวเตอร์แปลงเป็น Parallel
14	T10	ส่งสัญญาณที่แปลงเป็นอนุกรมไปยังคอมพิวเตอร์
15	GND	เป็นขากราวด์สำหรับต่อกับกราวด์ของระบบใช้สำหรับต่อ
16	+5V	ไฟเลี้ยง 5 V

2.7.2.2 ไมโครคอนโทรลเลอร์89C2051



รูปที่ 2.21วงจรไมโครคอนโทรลเลอร์89C2051

ไมโครคอนโทรลเลอร์ 89C2051 เป็นส่วนที่สำคัญที่ใช้ในการควบคุมการทำงานคือจะรับข้อมูลจากคอมพิวเตอร์ และแสดงค่าออกทาง LEDโดยหน้าที่การทำงานของขาต่างๆ บนไมโครคอนโทรลเลอร์89C2051 ดังตารางที่ 2.13

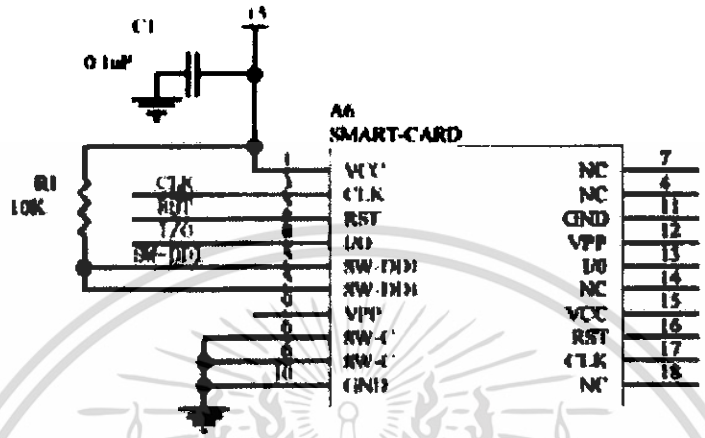
ตารางที่ 2.13 แสดงหน้าที่การทำงานของขาต่างๆ ของไมโครคอนโทรลเลอร์89C2051

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	RST	ใช้ในการรีเซตการทำงานของไมโครคอนโทรลเลอร์
2	RXD	ใช้เป็นขาอินพุตสำหรับรับข้อมูลจากการสื่อสารแบบอนุกรม
3	TXD	ใช้เป็นขาอินพุตสำหรับส่งข้อมูลจากการสื่อสารแบบอนุกรม
6	INT0	ใช้เป็นขาอินพุตสำหรับรับสัญญาณอินเตอร์รัปต์จากภายนอกช่องที่ 0
7	INT1	ใช้เป็นขาอินพุตสำหรับรับสัญญาณอินเตอร์รัปต์จากภายนอกช่องที่ 1
8	TO	ใช้เป็นขาอินพุตสำหรับรับสัญญาณไทเมอร์จากภายนอกช่อง

ตารางที่ 2.13 แสดงหน้าที่การทำงานของขาต่างๆ ของไมโครคอนโทรลเลอร์89C2051 (ต่อ)

ขาพอร์ท	สัญลักษณ์	การใช้งาน
9	T1	ที่ 0 ใช้เป็นขาอินพุตสำหรับรับสัญญาณไทเมอร์จากภายนอกช่องที่ 1
10	GND	เป็นขากราวด์สำหรับต่อกับกราวด์ของระบบ
11	P3.7	ใช้เป็นขาสัญญาณควบคุมการอ่านข้อมูลจากหน่วยความจำภายนอก
12	P1.0	เป็นขาอินพุตสำหรับนับค่าของไทม์เมอร์2
13	P1.1	เป็นขาอินพุตทริกเกอร์ของไทม์เมอร์ 2
14	P1.2	เป็นขาสำหรับเชื่อมต่อแบบ SPI เพื่อทำการติดต่อโปรแกรมข้อมูลในระบบ
15	P1.3	เป็นขาสำหรับเชื่อมต่อแบบ SPI เพื่อทำการติดต่อโปรแกรมข้อมูลในระบบ
16	P1.4	เป็นขาสำหรับเชื่อมต่อแบบ SPI เพื่อทำการติดต่อโปรแกรมข้อมูลในระบบ
17	P1.5	เป็นขาสำหรับเชื่อมต่อแบบ SPI เพื่อทำการติดต่อโปรแกรมข้อมูลในระบบ
18	P1.6	เป็นขาสำหรับเชื่อมต่อแบบ SPI เพื่อทำการติดต่อโปรแกรมข้อมูลในระบบ
19	P1.7	เป็นขาสำหรับเชื่อมต่อแบบ SPI เพื่อทำการติดต่อโปรแกรมข้อมูลในระบบ
20	+5	ใช้สำหรับต่อไฟเลี้ยง +5 V

2.7.2.3 วงจร SMART-CARD



รูปที่ 2.22 วงจร SMART-CARD

เป็นส่วนในการอ่าน-เขียนสมาร์ทการ์ดโดยหน้าที่การทำงานของขาต่างๆบน SMART-CARD ดังตารางที่ 2.14

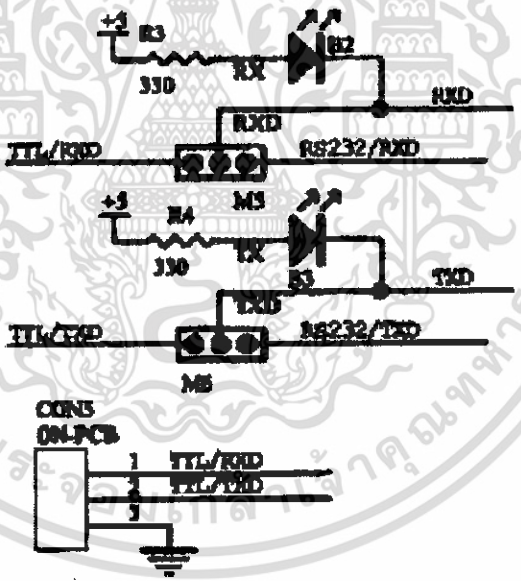
ตารางที่ 2.14 แสดงหน้าที่การทำงานของขาต่างๆ ของ SMART-CARD

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	VCC	แหล่งจ่ายกระแสไฟฟ้า
2	RST	สัญญาณรีเซต
3	CLK	สัญญาณนาฬิกา
4	NC	Not Connected
5	SW-DD1	ต่อไฟ +5 V
6	SW-C	ต่อกราวด์
7	NC	Not Connected
8	I/O	Input-Output สำหรับรับส่งข้อมูล
9	VPP	ใช้วัดกระแสแรงดันไฟฟ้า
10	GND	ขากราวด์
11	GND	ขากราวด์
12	VPP	ใช้วัดกระแสแรงดันไฟฟ้า

ตารางที่ 2.14 แสดงหน้าที่การทำงานของขาต่างๆ ของSMART-CARD (ต่อ)

ขาพอร์ท	สัญลักษณ์	การใช้งาน
13	I/O	Input-Output สำหรับรับส่งข้อมูล
14	NC	Not Connected
15	VCC	แหล่งจ่ายกระแสไฟฟ้า
16	RST	สัญญาณรีเซต
17	CLK	สัญญาณนาฬิกา
18	NC	Not Connected

2.7.2.4 วงจร LED



รูปที่ 2.23 วงจร LED

LED จะแสดงสภาวะการรบ-ส่ง (RX,TX)โดยหน้าที่การทำงานของขาต่างๆ บน LED ดังตารางที่ 2.15

ตารางที่ 2.15 แสดงหน้าที่การทำงานของขาต่างๆ ของ LED

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	TTL/RXD	ขาที่รับสัญญาณแบบขนาน
2	TTL/TXD	ขาที่ส่งสัญญาณแบบขนาน
3	GND	ขากราวด์

2.7.2.5 ไอซี DS1833

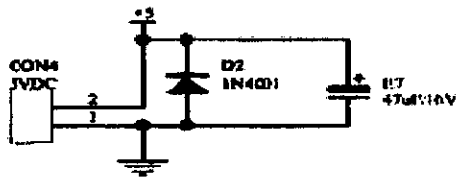
รูปที่ 2.24 ไอซี DS1833

โดยหน้าที่การทำงานของขาต่างๆ บนไอซี DS1833 ดังตารางที่ 2.16

ตารางที่ 2.16 แสดงหน้าที่การทำงานของขาต่างๆ ของไอซี DS1833

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	-	ต่อกราวด์
2	RES	ใช้ในการรีเซตการทำงาน
3	+	ต่อไฟ +5 V

2.7.2.6 ไดโอด1N4004



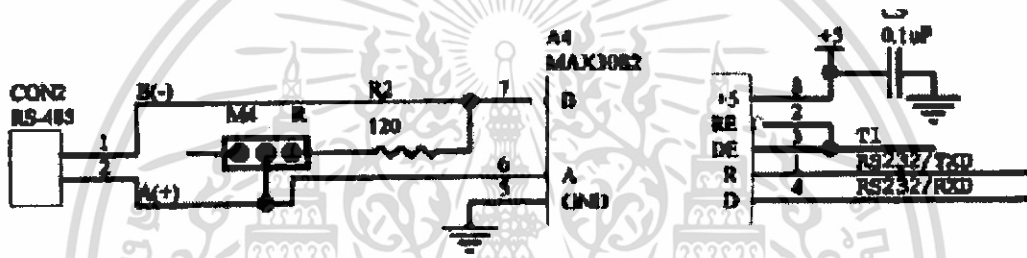
รูปที่ 2.25 ไดโอด 1N4004

โดยหน้าที่การทำงานของขาต่างๆ บนไดโอด 1N4004 ดังตารางที่ 2.17

ตารางที่ 2.17 แสดงหน้าที่การทำงานของขาต่างๆ ของไดโอด 1N4004

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	GND	ต่อกราวด์
2	+	ต่อไฟ +5 V และชาร์จ C 47uF16V

2.7.2.7 ไอซี MAX3082



รูปที่ 2.26 วงจรไอซี MAX3082

จะเป็นส่วนควบคุมทิศทางการรับส่ง "1" = TX, "0" = RX ซึ่งจะมีLEDไว้สำหรับแสดงผล โดยหน้าที่การทำงานของขาต่างๆ บนไอซีMAX3082 แสดงดังตารางที่ 2.18

ตารางที่ 2.18 แสดงหน้าที่การทำงานของขาต่างๆ ของไอซี MAX3082

ขาพอร์ท	สัญลักษณ์	การใช้งาน
1	R	Receiver Output Voltage
2	RE	Control Input Voltage
3	DE	Control Input Voltage
4	D	Driver Input Voltage
5	GND	ขากราวด์สำหรับต่อกับกราวด์ของระบบ
6	A	Receiver Input Voltage
7	B	Receiver Input Voltage
8	+5	ใช้สำหรับต่อไฟเลี้ยง +5 V

2.7.3 ชุดคำสั่งควบคุม TSM-256

TSM-256 มีคำสั่งในการติดต่อสั่งงานควบคุมทั้งหมด 8 คำสั่ง รูปแบบเป็นรหัส ASCII ทั้งหมด โดยมีลักษณะดังนี้

:ACXX...X<CR>	กรณีตั้ง DIP-SW.5 เป็น ON (NETWORK)
:CXX...X<CR>	กรณีตั้ง DIP-SW.5 เป็น OFF

: คือ รหัสนำของคำสั่ง (3AH)

A คือ Address ของบอร์ดตั้งแต่ 0-7

C คือ รหัสคำสั่งตั้งแต่ 0-7

XX...X คือ ข้อมูลติดตามของแต่ละคำสั่งซึ่งอาจจะมีหรือไม่ก็ได้รวมมีความยาวตามกำหนดแต่ละคำสั่ง

<CR> คือ รหัสลงท้ายของแต่ละคำสั่ง (0DH)

โดยเมื่อ TSM-256 รับคำสั่งก็จะทำงานตามคำสั่งทันที

2.7.3.1 คำสั่ง CHECK

:0<CR> / :A0<CR> (กรณีที่ต่อแบบ NETWORK) โดยเมื่อ TSM-256 ได้รับคำสั่งนี้จะส่งข้อความแสดงชื่อสินค้าและ Version ของสินค่ากลับมาดังนี้ TSM-256 V1.0<CR>

2.7.3.2 คำสั่ง STATUS

:1<CR> / :A1<CR> (กรณีที่ต่อแบบ NETWORK) คำสั่งนี้ TSM-256 จะทำการตรวจสอบว่ามีบัตรเสียบอยู่บนบอร์ดหรือไม่ หากไม่มีบัตรยู่บนบอร์ดจะส่งข้อมูลกลับมาดังนี้คือ ER<CR> หากมีบัตรเสียบอยู่บนบอร์ดจะส่งข้อมูลแสดง Manufacturer Code (4 ไบต์) กลับมาดังนี้ XXXXXXXX<CR> เช่น เมื่อเสียบบัตรสมาร์ทการ์ดเบอร์ SLE4442 อยู่ TSM-256 จะส่ง Manufacturer Code กลับมาคือ A2131091<CR>

2.7.3.3 คำสั่ง Read Data

:2BB<CR> / :A2BB<CR> (กรณีที่ต่อแบบ NETWORK) เป็นคำสั่งที่ใช้ในการอ่านข้อมูลของบัตรออกมาแสดงเป็นจำนวน 16 Bytes โดยผู้ใช้ต้องกำหนดตำแหน่ง Address เริ่มต้น (เป็นเลขฐานสิบหก) BBH ด้วยทุกครั้ง ข้อมูลที่ส่งกลับมามีลักษณะดังนี้ XXXXXXXX_ _ _ _XX<CR>

เช่น เมื่อคำสั่ง :221<CR> TSM-256 เมื่อได้รับคำสั่งจะเริ่มอ่านข้อมูลในตำแหน่ง Address 21H ไปจนถึงข้อมูลในตำแหน่ง Address 30H หากไม่ได้เสียบบัตรบนบอร์ดหรือไม่ใช่บัตรสมาร์ทการ์ดเบอร์ SLE4442 จะไม่สามารถอ่านข้อมูลออกได้และเบอร์ TSM-256 จะส่งคำว่า ER<CR>กลับมา

2.7.3.4 คำสั่ง Write Data

:3BBXXXX_ _XX<CR> / :A3BBXXXX_ _ XX<CR> (กรณีที่ต่อแบบ NETWORK) คำสั่งนี้ใช้ในการเขียนข้อมูลลงในบัตรสมาร์ทการ์ด สามารถเขียนข้อมูลความยาวสูงสุดได้ครั้งละ 16 Bytes เริ่มเขียนข้อมูลลงในที่ตำแหน่ง Address เริ่มต้น BBH ที่กำหนดไว้จนถึงตำแหน่ง Address ของข้อมูล Byte สุดท้าย เมื่อเขียนขอมูลลงในบัตรเรียบร้อยแล้ว TSM-256 จะส่งคำว่า OK<CR> กลับมา หากไม่สามารถเขียนข้อมูลลงในบัตรได้หรือบนบอร์ดไม่มีบัตรหรือไม่ใช่บัตรสมาร์ทการ์ดเบอร์ SLE4442 จะส่งคำว่า ER<CR> กลับมา เช่นเมื่อส่งคำสั่ง :32115151515<CR> ข้อมูลในตำแหน่ง Address 21H ไปจนถึงข้อมูลในตำแหน่ง Address 24H จะมีค่าเป็น 15H ทั้งหมด หรือเมื่อส่งคำสั่ง :30831313131<CR> ข้อมูลที่ตำแหน่ง Address 08H ไปจนถึงข้อมูลในตำแหน่ง Address 0BH จะมีค่าเป็น 31H ทั้งหมดแต่เป็นการเขียนแบบไม่ถาวรสามารถลบหรือแก้ไขเปลี่ยนแปลงได้

2.7.3.5 คำสั่ง Read Protection Memory

:4<CR> / :A4<CR> (กรณีที่ต่อแบบ NETWORK) คำสั่งนี้เป็นการอ่านค่า Bit Organization ของส่วน Protection Memory ทั้ง32Bits เรียงจาก 0-31 (ซ้ายไปขวา) โดยแต่ละ Bit จะแสดงค่าว่าตำแหน่ง Address ของส่วน Protection Memory (00H-20H) ตำแหน่งใดที่ยังสามารถเขียนข้อมูลลงไปได้ และตำแหน่งใดได้มีการเขียนข้อมูลถาวรไว้แล้ว โดยตำแหน่งที่มีการเขียนข้อมูลถาวรไว้นั้นจะมีค่าเป็น 0 ส่วนตำแหน่งที่ยังสามารถเขียนข้อมูลลงไปได้จะมีค่าเป็น 1 เช่น 00001100111111111111100000011111<CR> จะเห็นว่า Bit ในตำแหน่งที่ 0-3 เป็น 0 การแสดงว่าตำแหน่ง Address ที่ 00H-03H มีข้อมูลถาวรอยู่ไม่สามารถเขียนข้อมูลทับลงไปได้ แต่ถ้าไม่มีบัตรนี้อยู่หรือไม่ใช่บัตรสมาร์ทการ์ดเบอร์ SLE4442 จะได้รับคำว่า ER<CR> กลับมา

2.7.3.6 คำสั่ง Write Protection Memory

:5BBXXXX_XX<CR> / :A5BBXXXX_XX<CR> (กรณีที่ต่อแบบ NETWORK) คำสั่งนี้จะคล้ายกับคำสั่ง Write Data ต่างกันตรงที่เมื่อใช้คำสั่งนี้ตามหลังคำสั่งที่ 3 จะเป็นการเขียนข้อมูลถาวรลงในส่วน Protection Memory โดย BBH จะเป็นตำแหน่ง Address เริ่มต้นที่จะเขียนข้อมูลลงไปเมื่อเขียนข้อมูลเสร็จเรียบร้อยจะส่งคำว่า OK<CR> กลับมาแต่ถ้าไม่สามารถเขียนข้อมูลลงในบัตรนี้ได้

หรือบัตรไม่ใช่เบอร์ SLE4442 หรือไม่มีบัตรอยู่ก็จะส่งคำว่า ER<CR> กลับมา เช่น ถ้าต้องการเขียนข้อมูลถาวรลงในตำแหน่ง Address 08H ถึงข้อมูลในตำแหน่ง Address 0BH ให้มีค่าเป็น 31H ให้ส่งคำสั่ง :30831313131<CR> และตามหลังด้วยคำสั่ง :50831313131<CR> ให้กับ TSM-256 จะพบว่าในตำแหน่ง Address 08H ถึงข้อมูลในตำแหน่ง Address 0BH จะมีค่าเป็น 31H และไม่สามารถเปลี่ยนแปลงแก้ไขใดๆ ได้อีกเลย เมื่อส่งคำสั่ง :4<CR> ให้กับ TSM-256 เพื่ออ่านค่า BitOrganization ของส่วน Protection Memory Bit ในตำแหน่งที่ 8-11 จะมีค่าเป็น 0 ดังนี้ 00001100000001111111110000000111111<CR> แต่ใส่เพียงคำสั่งที่ 5 อย่างเดียวโดยไม่ได้ส่งคำสั่งที่ 3 ไปก่อนก็จะไม่มีผลกับการเปลี่ยนแปลงของข้อมูลใดๆ เลย

2.7.3.7 คำสั่ง Verify PSC

:6PPPPPP<CR> / :A6PPPPPP<CR> (กรณีที่ต่อแบบ NETWORK) คำสั่งนี้ใช้ในการตรวจสอบ Verify ค่า PSC (Programmable Security Code) ซึ่งเป็นรหัสขนาด 3 Bytes (PPPPPPH) โดยจะต้องทำการตรวจสอบ Verify ค่า PSC ก่อนเสมอหลังจากที่จ่ายไฟเข้าเพื่อที่จะสามารถเขียนข้อมูลลงไปในบัตรได้ด้วยการใส่ค่า PSC (PPPPPPH) ตามหลังรหัสคำสั่ง หาก Verify ค่า PSCได้ตรงกับค่าในบัตรก็ส่งคำว่า OK<CR> กลับมาแต่ถ้าไม่ถูกต้องก็จะส่งคำว่า ER<CR> กลับมา (N คือจำนวนครั้งที่ทำการ Verify ค่า PSC เช่น ถ้า Verify ค่า PSC ไม่ถูกต้องครั้งที่ 1 ก็ส่งคำว่า ER<CR> กลับมา) และจะนับเก็บค่า Error Counter (EC) ไว้จนกว่าจะถูก Reset เมื่อได้ทำการ Verify ค่า PSC ได้ถูกต้อง การตรวจสอบ Verify ค่า PSC สามารถทำได้ 3 ครั้ง ถ้าตรวจสอบ Verify ค่า PSCไม่ถูกต้องจนถึงครั้งที่ 3 (TSM-256 จะส่งคำว่า ER<CR> กลับมา) บัตรนี้จะไม่สามารถเขียนข้อมูลใดๆ ลงไปได้อีก บัตรใหม่ที่ผลิตจากโรงงานนั้นมีค่า PSC Code คือ FFFFFF การVerify หลังจากจ่ายไฟเข้าบัตรนี้ถ้าถูกต้องจะมีผลตลอดไปจนกว่าจะดึงบัตรออก ถึงแม้ว่าจะส่งคำสั่งไป Verify ค่า PSC ที่ไม่ถูกต้องอีกครั้งก็จะไม่มีผลใดๆ ทั้งสิ้นเพราะถือว่าได้ทำการ Verify ค่า PSC ถูกต้องกับค่าในบัตรไปแล้ว

2.7.3.8 คำสั่ง CHANGE PSC

:7PPPPPP<CR> / :A7PPPPPP<CR> (กรณีที่ต่อแบบ NETWORK) คำสั่งนี้ใช้ในการเปลี่ยนแปลงค่า PSC โดยข้อมูล PPPPPPH ที่ตามหลังรหัสคำสั่งจะเป็นค่า PSC Code ที่ต้องการกำหนดขึ้นมาใหม่ เมื่อ TSM-256 ได้ทำการเปลี่ยนค่าเสร็จเรียบร้อยจะส่งคำว่า OK<CR> กลับมาแต่ถ้าไม่สามารถเปลี่ยนค่าได้หรือไม่ใช้บัตรเบอร์ SLE4442 หรือไม่มีบัตรก็จะส่งคำว่า ER<CR> มาแทน

คำสั่งRead Data, คำสั่ง Read Protection Memory และคำสั่ง Verify PSCทั้ง 3 คำสั่งนี้จะต้องกระทำคำสั่ง Write Protection Memory ก่อนเสมอ คือทำการตรวจสอบ Verify ค่า PSC ให้ตรงกันกับค่า PSC ในบัตรก่อนจึงจะสามารถทำงานในคำสั่งเหล่านี้ได้

2.8 My SQL server

MySQL เป็นฐานข้อมูลแบบ open source ที่ได้รับความนิยมในการใช้งานสูงสุดโปรแกรมหนึ่งบนเครื่องให้บริการ ที่ความสามารถในการจัดการกับฐานข้อมูลด้วยภาษา SQL(Structures Query Language) อย่างมีประสิทธิภาพ มีความรวดเร็วในการทำงาน รองรับการทำงานจากผู้ใช้หลายๆ คน และหลายๆ งานได้ในขณะเดียวกัน

MySQL ถูกพัฒนาขึ้นโดย MySQL AB โดยมีลิขสิทธิ์การใช้งาน 2 แบบ นั่นคือ ผู้ดูแลระบบสามารถใช้งานซอฟแวร์ MySQL ได้โดยไม่มีค่าใช้จ่ายใดๆ ภายใต้ลิขสิทธิ์ของ GNU General Public License หรืออาจเลือกใช้แบบที่มีลิขสิทธิ์ทางการค้าของ MySQL AB ซึ่งเป็นผู้ผลิตและพัฒนาซอฟแวร์โดยตรงก็ได้

คำอธิบายเพิ่มเติมเกี่ยวกับหน้าที่ความสามารถและการทำงานของโปรแกรม MySQL มีดังต่อไปนี้

- **MySQL ถือเป็นระบบจัดการฐานข้อมูล(DataBase Management System (DBMS))**

ฐานข้อมูลมีลักษณะเป็นโครงสร้างของการเก็บรวบรวมข้อมูล การที่จะเพิ่มเติม เข้าถึงหรือประมวลผลข้อมูลที่เก็บในฐานข้อมูลจำเป็นจะต้องอาศัยระบบจัดการฐานข้อมูล ซึ่งจะทำหน้าที่เป็นตัวกลางในการจัดการกับข้อมูลในฐานข้อมูลทั้งสำหรับการใช้งานเฉพาะ และรองรับการทำงานของแอพลิเคชันอื่นๆ ที่ต้องการใช้งานข้อมูลในฐานข้อมูล เพื่อให้ได้รับความสะดวกในการจัดการกับข้อมูลจำนวนมาก MySQL ทำหน้าที่เป็นทั้งตัวฐานข้อมูลและระบบจัดการฐานข้อมูล

- **MySQL เป็นระบบจัดการฐานข้อมูลแบบ relational**

ฐานข้อมูลแบบ relational จะทำการเก็บข้อมูลทั้งหมดในรูปแบบของตารางแทนการเก็บข้อมูลทั้งหมดลงในไฟล์เพียงไฟล์เดียว ทำให้ทำงานได้รวดเร็วและมีความยืดหยุ่น นอกจากนั้น แต่ละตารางที่เก็บข้อมูลสามารถเชื่อมโยงเข้าหากันทำให้สามารถรวมหรือจัดกลุ่มข้อมูลได้ตามต้องการ โดยอาศัยภาษา SQL ที่เป็นส่วนหนึ่งของโปรแกรม MySQL ซึ่งเป็นภาษามาตรฐานในการเข้าถึงฐานข้อมูล

- **MySQL แจกจ่ายให้ใช้งานแบบ open source**

นั่นคือผู้ใช้งาน MySQL ทุกคนสามารถใช้งานและปรับแต่งการทำงานได้ตามต้องการสามารถ

ดาวน์โหลดโปรแกรม MySQL ได้จากอินเทอร์เน็ตและนำมาใช้งานโดยไม่มีค่าใช้จ่ายใด ในระบบปฏิบัติการ Red Hat Linux นั้น มีโปรแกรมที่สามารถใช้งานเป็นฐานข้อมูลให้ผู้ดูแลระบบสามารถเลือกใช้งานได้หลายโปรแกรม เช่น MySQL และ PostgreSQL ผู้ดูแลระบบสามารถเลือกติดตั้งได้ทั้งในขณะที่ติดตั้งระบบปฏิบัติการ Red Hat Linux หรือจะติดตั้งภายหลังจากที่ติดตั้งระบบปฏิบัติการก็ได้ อย่างไรก็ตามสาเหตุที่ผู้ใช้งานจำนวนสมากนิยมใช้งานโปรแกรม MySQL คือ MySQL สามารถทำงานได้อย่างรวดเร็ว น่าเชื่อถือและใช้งานง่าย นอกจากนั้น MySQL ถูกออกแบบและพัฒนาขึ้นมาเพื่อทำหน้าที่เป็นเครื่องให้บริการรองรับการจัดการกับฐานข้อมูลขนาดใหญ่ ซึ่งการพัฒนายังคงดำเนินอยู่อย่างต่อเนื่อง ส่งผลให้มีฟังก์ชันการทำงานใหม่ๆ ที่อำนวยความสะดวกแก่ผู้ใช้งานเพิ่มขึ้นอยู่ตลอดเวลา รวบไปถึงการปรับปรุงด้านความต่อเนื่อง ความเร็วในการทำงานและความปลอดภัย ทำให้ MySQL เหมาะต่อการนำไปใช้งานเพื่อเข้าถึงฐานข้อมูลบนเครือข่ายอินเทอร์เน็ต

2.9 Visual C#

ภาษา Visual C# (วิชวลซีชาร์ป) ถือเป็นภาษาที่เกิดขึ้นมาพร้อมกับแนวความคิดของการเขียนโปรแกรมในยุค .NET โดยมีแนวของภาษาเป็นแบบการเขียนโปรแกรมเชิงวัตถุสมัยใหม่ (Modern Oriented Programming) เรียกสั้นๆ ว่า Modern OOP หรืออาจจะกล่าวได้ว่า ภาษา Visual C# คือภาษาต้นแบบของการเขียนโปรแกรมใน .NET นั่นเอง โดยที่ภาษาอื่นๆ ที่เกิดขึ้นมาก่อนหน้านี้จะต้องปรับตัวเข้าหา .NET ทั้งหมด ซึ่งสามารถสังเกตได้ว่าไวยากรณ์การใช้งานของแต่ละภาษานั้นล้วนแล้วแต่ถูกปรับเปลี่ยนไปจากเวอร์ชั่นก่อนหน้านี้อย่างสิ้นเชิง

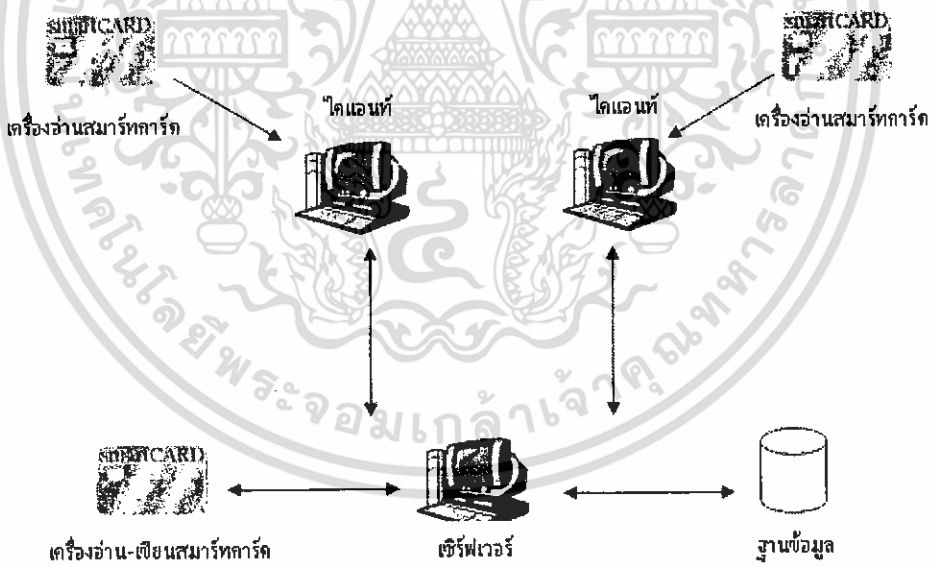
สำหรับภาษา Visual C# แล้วการเขียนโปรแกรมเชิงวัตถุ ไม่ใช่เรื่องยุ่งยากอีกต่อไป โดยที่จุดขึนของภาษา Visual C# จะอยู่ที่การอาศัยไวยากรณ์ที่ปรับปรุงมาจาก C/C++ ร่วมกับความง่ายของภาษา Visual Basic ร่วมเข้ามาเป็น Visual C#

บทที่ 3

การออกแบบ

ในโครงงานระบบสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์นี้ มีส่วนประกอบหลักๆ ที่สำคัญคือ เครื่องอ่าน-เขียนสมาร์ทการ์ด ซึ่งควบคุมการทำงานโดยไมโครคอนโทรลเลอร์ ติดต่อกับพอร์ทอนุกรมของเครื่องคอมพิวเตอร์ และจะมีการควบคุมการใช้งานทรัพยากรคอมพิวเตอร์ โดยประมวลผลจากคอมพิวเตอร์ส่งคำสั่งผ่านไปทางไมโครคอนโทรลเลอร์ ทางด้านฝั่งเซิร์ฟเวอร์หรือผู้ดูแลระบบจะสามารถกำหนดว่าผู้ใดสามารถเข้ามาใช้งานเครื่องคอมพิวเตอร์ได้ และสามารถเข้ามาตรวจสอบข้อมูลการเข้าใช้งานทรัพยากรคอมพิวเตอร์ได้

3.1 ภาพรวมของระบบ



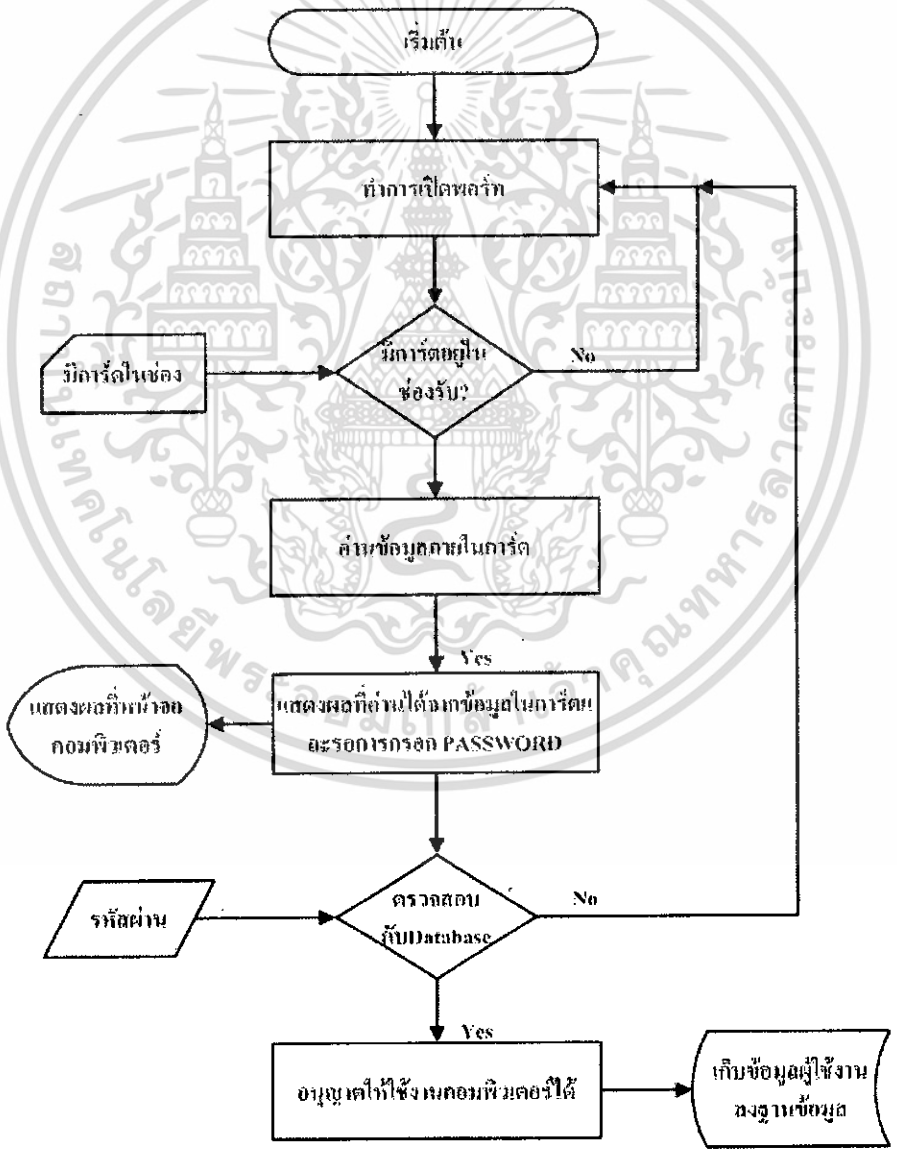
รูปที่ 3.1 ภาพรวมของระบบ

นักศึกษาทุกคนจะมีบัตรสมาร์ทการ์ดเป็นบัตรประจำตัวนักศึกษา โดยที่เครื่องคอมพิวเตอร์จะติดตั้งเครื่องอ่านข้อมูลบัตรสมาร์ทการ์ด เมื่อนักศึกษาคนใดต้องการเข้าใช้งานทรัพยากรคอมพิวเตอร์จะต้องทำการเสียบบัตรสมาร์ทการ์ด จากนั้นข้อมูลจากบัตรก็จะถูกตรวจสอบ

กับฐานข้อมูลผ่านโปรแกรมที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ เมื่อการตรวจสอบกับฐานข้อมูลถูกต้องเครื่องคอมพิวเตอร์จะอยู่ในสถานะพร้อมใช้งานและสามารถเก็บข้อมูลการเข้าใช้งานทรัพยากรคอมพิวเตอร์ นอกจากนี้ผู้ดูแลระบบยังสามารถนำข้อมูลการเข้าใช้งานทรัพยากรมาประมวลผลเพื่อตรวจดูการใช้งาน

3.2 การออกแบบทางด้านซอฟท์แวร์

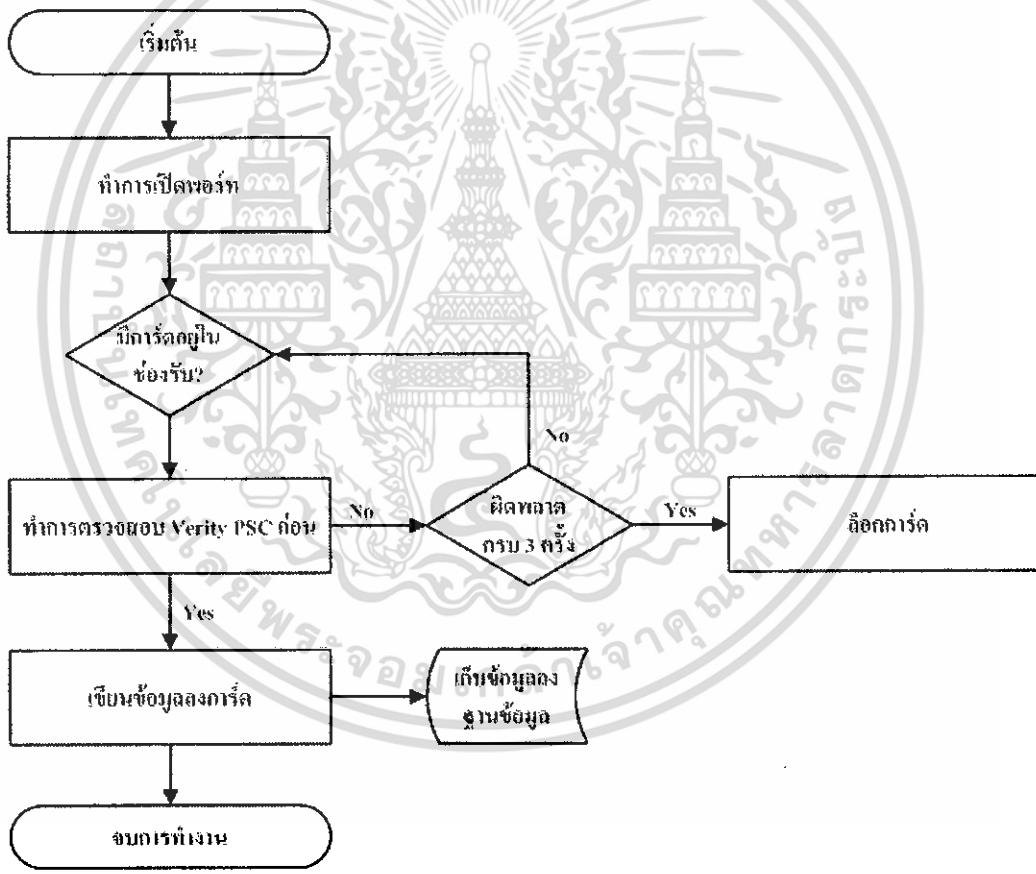
3.2.1 โปรแกรมการอนุญาตให้ใช้งานคอมพิวเตอร์



รูปที่ 3.2 โฟลวชาร์ทแสดงโปรแกรมการอนุญาตให้ใช้งานคอมพิวเตอร์

เมื่อเริ่มระบบการทำงาน คอมพิวเตอร์สั่งให้เปิดพอร์ทอ่านสมาร์ทการ์ดและเริ่มระบบการใช้งานคอมพิวเตอร์ โดยระบบจะตรวจสอบว่ามีบัตรอยู่ในช่องเสียบบัตรหรือไม่ เมื่อมีบัตรเข้ามาในช่องเสียบบัตรจะอ่านข้อมูลจากในบัตรและร้องขอรหัสผ่านโดยจะแสดงบนส่วนติดต่อผู้ใช้ เมื่อผู้ใช้มีการใส่รหัสผ่านจะนำรหัสผ่านที่ได้ไปตรวจสอบจากฐานข้อมูลว่าผู้ใช้สามารถใช้งานคอมพิวเตอร์นี้ได้หรือไม่ ถ้ามีก็ทำการอนุญาตให้ใช้งานคอมพิวเตอร์ได้ และทำการเก็บข้อมูลผู้ใช้ลงบนฐานข้อมูล

3.2.2 โปรแกรมการเขียนข้อมูลลงบัตรสมาร์ทการ์ด



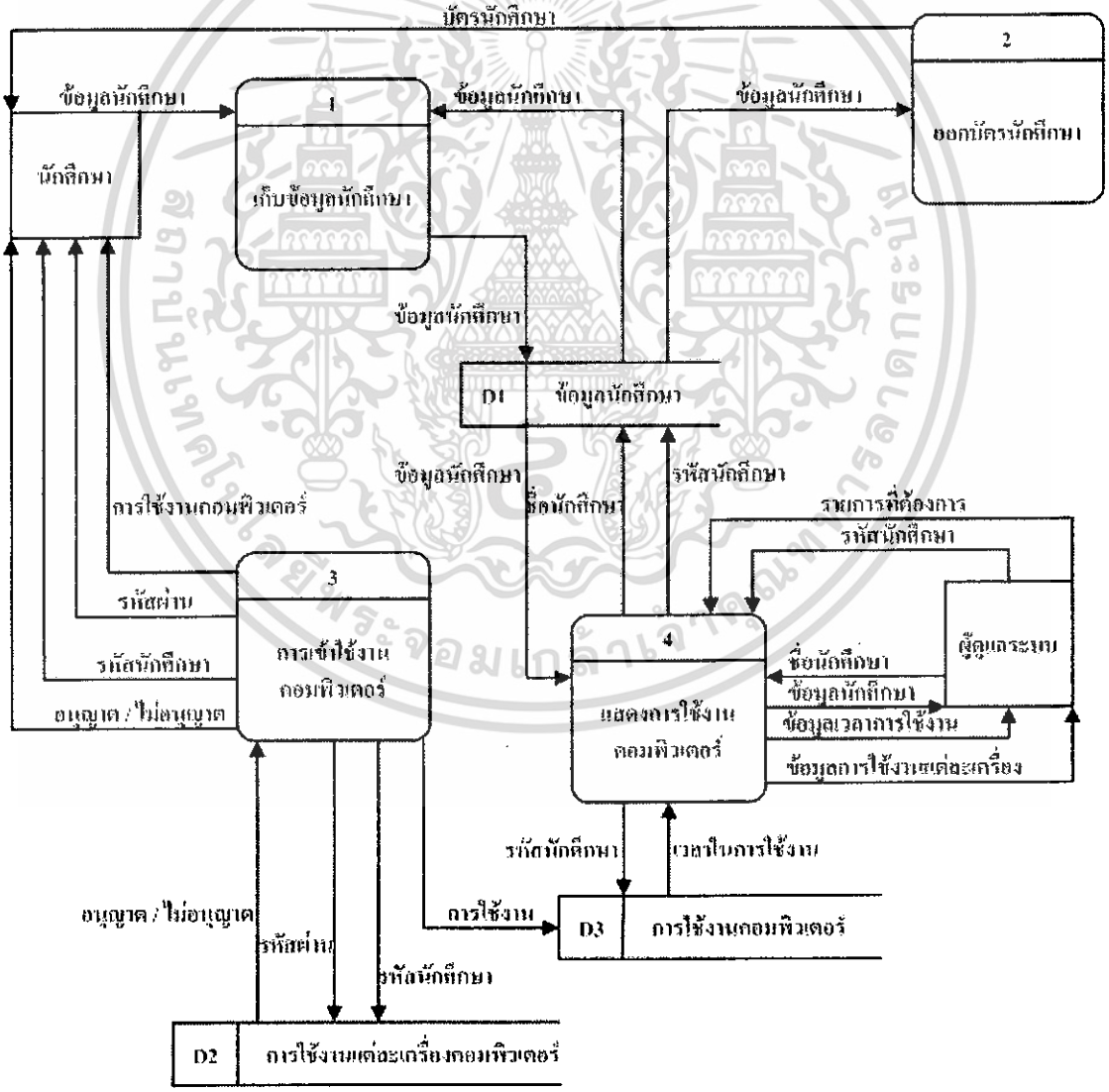
รูปที่ 3.3 โฟลว์ชาร์ทแสดงโปรแกรมการเขียนข้อมูลลงบัตรสมาร์ทการ์ด

เมื่อจ่ายไฟให้ระบบแล้วจะทำการเปิดพอร์ทจากโปรแกรม จากนั้นทำการตรวจสอบว่ามีบัตรในช่องเสียบบัตร หรือไม่ ถ้ามีจะต้องทำการใส่ค่า Programmable Security Code (PSC) ที่มีขนาด 3 ไบต์ โดยจะต้องทำการตรวจสอบ Verify PSC ก่อนการเขียนข้อมูลลงบนบัตรสมาร์ทการ์ด เสมอ

และ ค่า PSC จะสามารถใส่ได้เพียง 3 ครั้งถ้าผิดครบ 3 ครั้ง จะทำการล็อค ทำให้ไม่สามารถใช้งานบัตรใบนั้นได้อีกต่อไป โดยจะเก็บค่า Error ใน Error Counter (EC) เสร็จแล้วก็จะทำการ เขียนข้อมูลลงบนบัตรโดยมีรูปแบบ เป็นตัวเลข 8 ตัว ตามที่ผู้ดูแลระบบกำหนดให้และทำการเขียนข้อมูลลงบนบัตร และเก็บข้อมูลลงบนฐานข้อมูล

3.2.3 Dataflow diagram

สำหรับภาพรวมของระบบควบคุมการเข้าใช้งานคอมพิวเตอร์ผ่านบัตรสมาร์ทการ์ด แสดงได้ดังรูปต่อไปนี้

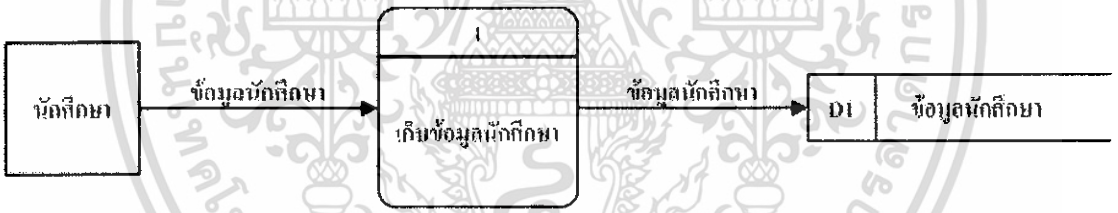


รูปที่ 3.4 ภาพรวมของโปรแกรมควบคุมการใช้งานคอมพิวเตอร์

รูปที่ 3.5 Context diagram

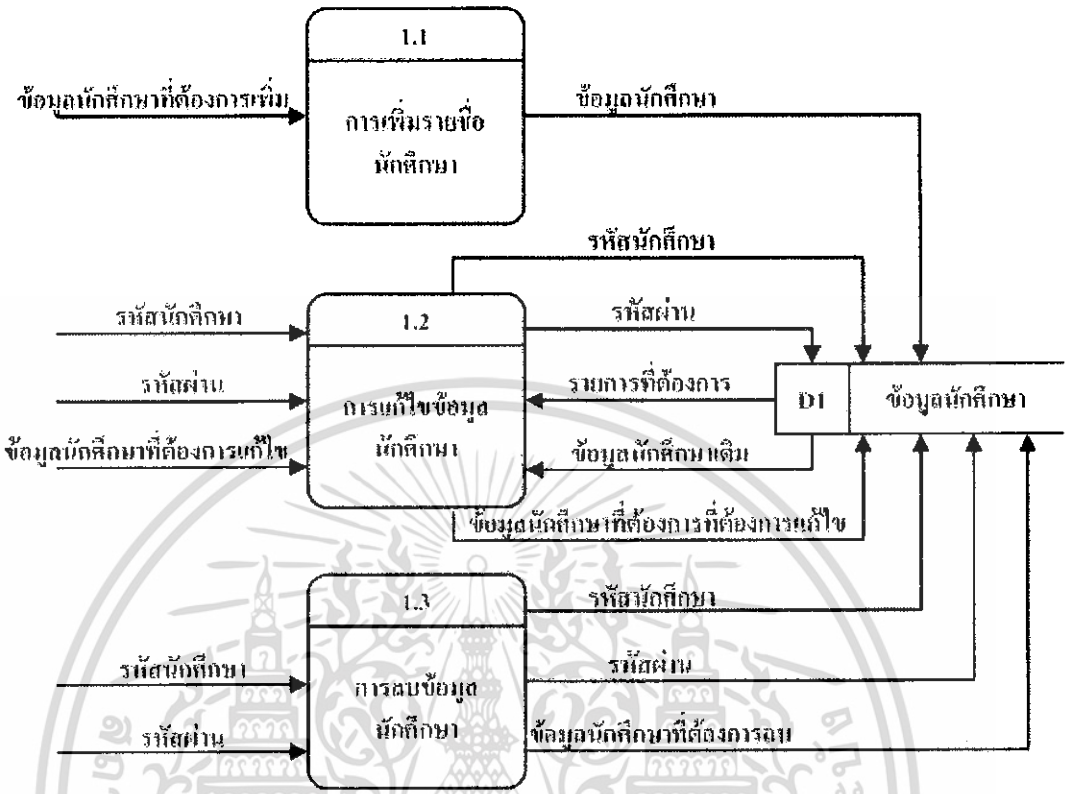
จากรูปที่ 3.5 เป็นการแสดง context diagram ของระบบประกอบด้วยนักศึกษาซึ่งเป็นผู้ให้ข้อมูลนักศึกษารวมทั้งการใช้งานคอมพิวเตอร์แก่ระบบ ส่วนทางผู้ดูแลระบบนั้นจะสามารถตรวจสอบการใช้งานคอมพิวเตอร์ที่ห้องคอมพิวเตอร์ภายในภาควิชาของนักศึกษาได้จากรหัสนักศึกษา หรือชื่อนักศึกษาที่ต้องการทราบข้อมูล โดยการทำงานจะแบ่งออกเป็น

3.2.3.1 ขั้นตอนการเก็บข้อมูลนักศึกษา



รูปที่ 3.6 ขั้นตอนการเก็บข้อมูลนักศึกษา

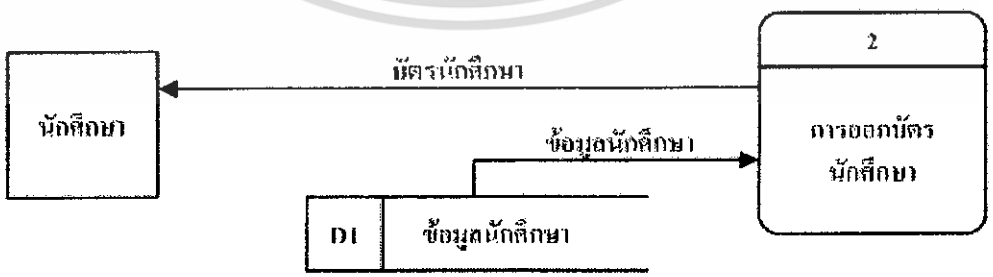
โดยรูปที่ 3.6 แสดงขั้นตอนการเก็บข้อมูลนักศึกษาโดยนักศึกษาจะเป็นผู้ให้ข้อมูลแก่ระบบ โดยที่ระบบจะนำข้อมูลที่ได้เก็บลงฐานข้อมูลนักศึกษา การเก็บข้อมูลนักศึกษานั้นสามารถแบ่งได้เป็นอีก 3 ขั้นตอนย่อยๆ ดังรูปที่ 3.7



รูปที่ 3.7 ขั้นตอนย่อยของการเก็บข้อมูลนักศึกษา

จากรูปที่ 3.7 จะเห็นว่าข้อมูลย่อยของการเก็บข้อมูลนักศึกษา คือ การเพิ่มรายชื่อนักศึกษา และการแก้ไขข้อมูลนักศึกษา การลบข้อมูลนักศึกษา

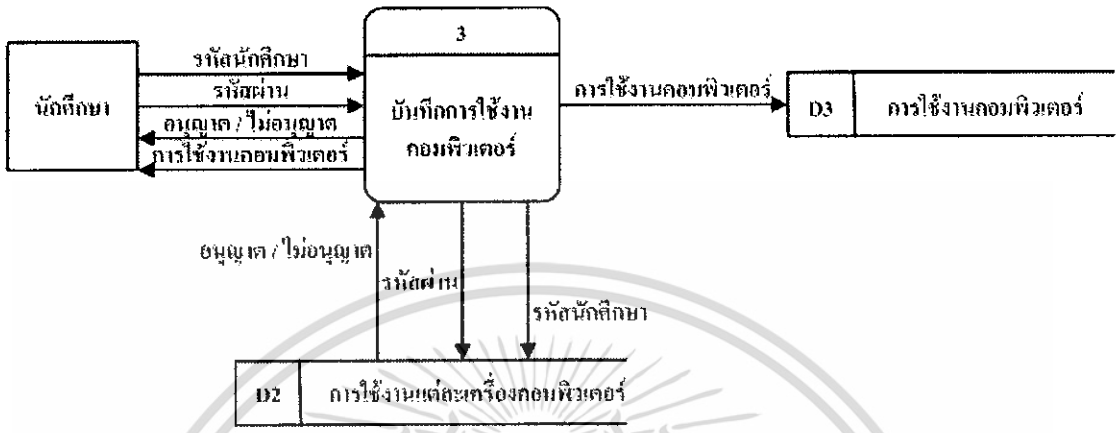
3.2.3.2 ขั้นตอนการออกบัตรนักศึกษา



รูปที่ 3.8 การออกบัตรนักศึกษา

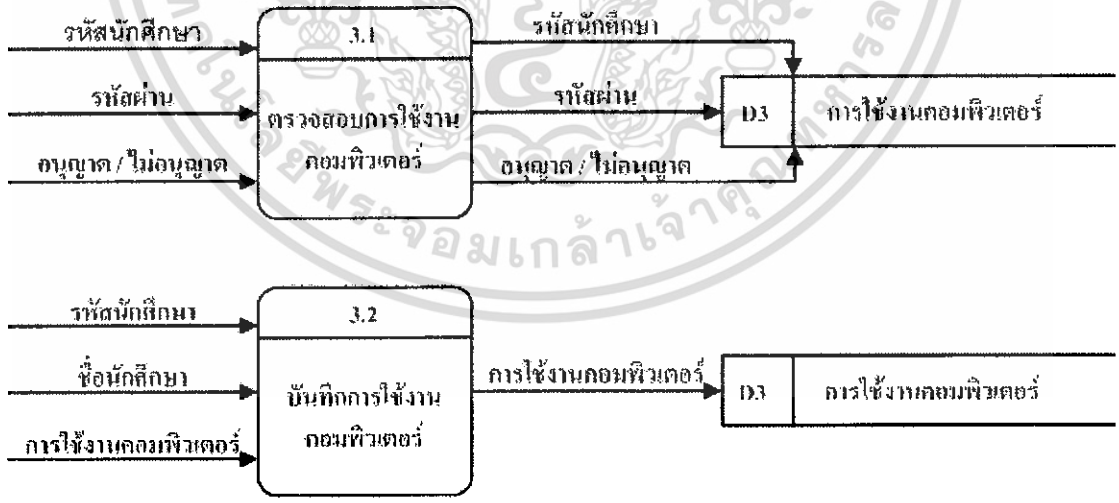
ในการออกบัตรนักศึกษา ระบบจะนำข้อมูลจากฐานข้อมูลนักศึกษามาออกบัตรนักศึกษา

3.2.3.3 ขั้นตอนบันทึกการใช้งานคอมพิวเตอร์



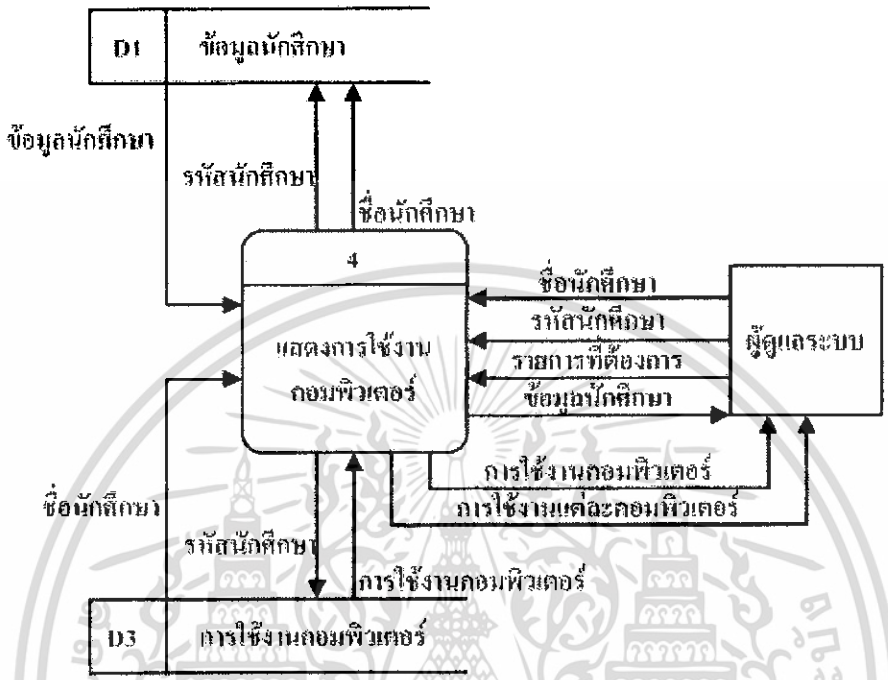
รูปที่ 3.9 ขั้นตอนบันทึกการใช้งานคอมพิวเตอร์

จากรูปที่ 3.9 จะแสดงขั้นตอนการบันทึกการใช้งานคอมพิวเตอร์ของนักศึกษา โดยแบ่งการทำงานออกเป็น 2 ขั้นตอนย่อย ดังรูปที่ 3.10 คือ จะมีการตรวจสอบสิทธิในการเข้าใช้คอมพิวเตอร์ก่อน หลังจากนั้นก็จะมีการบันทึกการใช้งานคอมพิวเตอร์ลงฐานข้อมูล



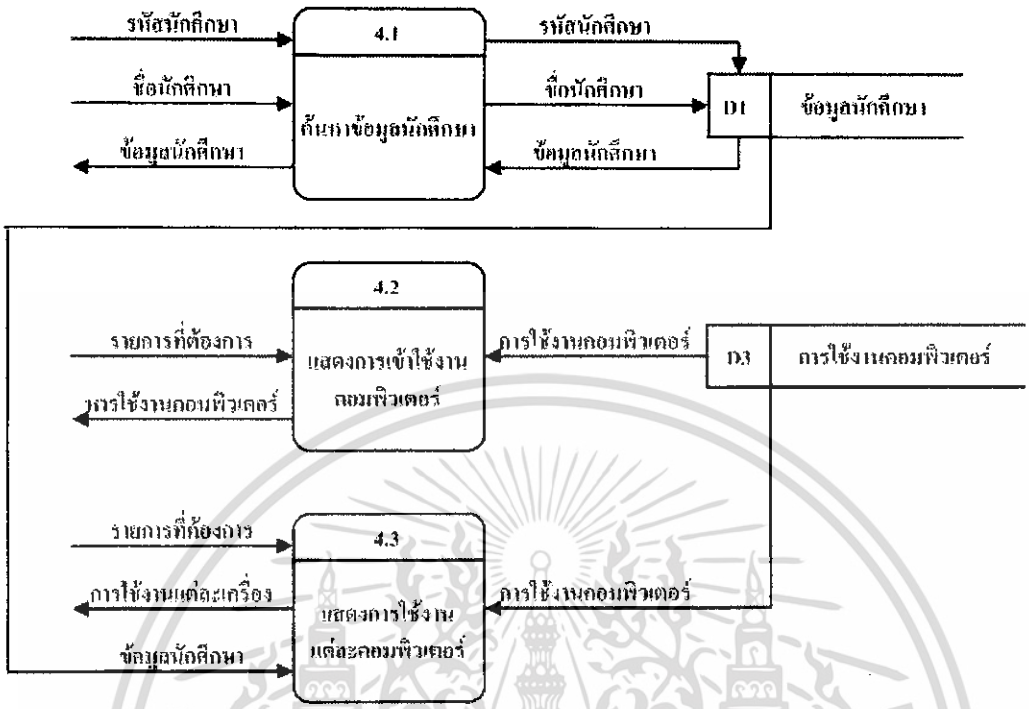
รูปที่ 3.10 ขั้นตอนย่อยของบันทึกการใช้งานคอมพิวเตอร์

3.2.3.4 ขั้นตอนแสดงการใช้งานคอมพิวเตอร์



รูปที่ 3.11 ขั้นตอนแสดงเวลาการใช้งานคอมพิวเตอร์

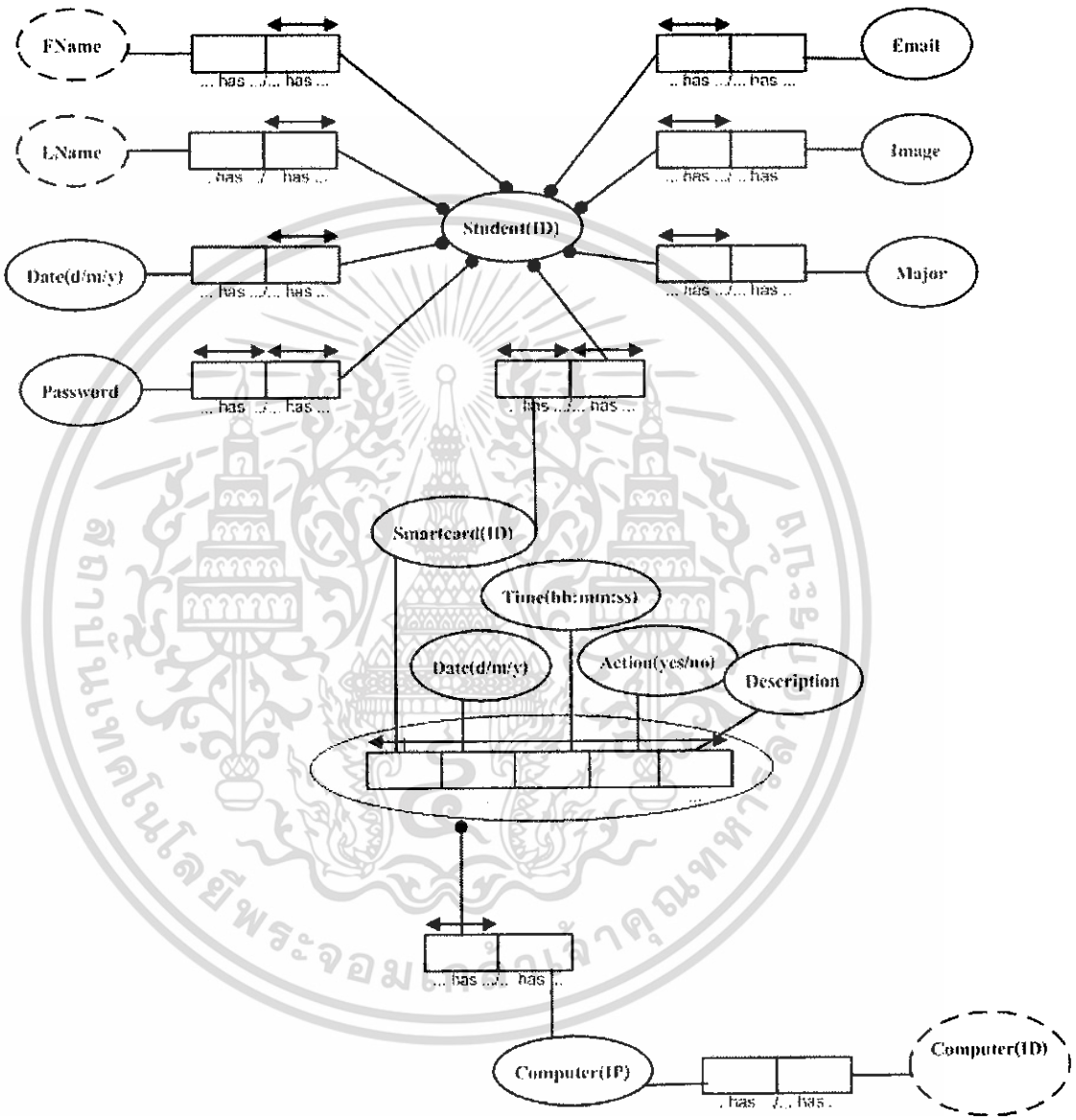
จากรูปที่ 3.11 ผู้ดูแลระบบสามารถดูบันทึกการใช้งานคอมพิวเตอร์ของนักศึกษาแต่ละคนได้ว่าได้มีการใช้งานทรัพยากรใดบ้างโดยจะแบ่งออกเป็น 3 ขั้นตอนย่อย ซึ่งแสดงได้ดังรูปที่ 3.12



รูปที่ 3.12 ขั้นตอนย่อยของการแสดงการใช้งานคอมพิวเตอร์

3.2.4 การออกแบบฐานข้อมูล

3.2.4.1 NIAM-MODEL



รูปที่ 3.13 ฐานข้อมูลของระบบ (NIAM-MODEL)

3.2.4.2 Data Dictionary

Student(ID)	Smartcard(ID)	Password	FName	LName

Date	Major	Email	image

ตารางที่ 3.1 ตารางเก็บข้อมูลนักศึกษา

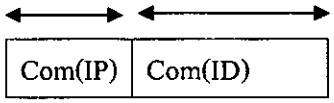
Field	Type	Description
Student(ID)	nvarchar(10)	รหัสนักศึกษา
Smartcard(ID)	nvarchar(15)	รหัสบัตรสมาร์ทการ์ด
Password	nvarchar(10)	รหัสผ่าน
FName	nvarchar(20)	ชื่อนักศึกษา
LName	nvarchar(20)	นามสกุลนักศึกษา
Date	datetime(8)	วันที่ที่มีการบันทึก
Major	nvarchar(20)	ภาควิชา
Email	nvarchar(50)	E-mailนักศึกษา
image	nvarchar(255)	รูปถ่ายนักศึกษา

Student(ID)	Date(d/m/y)	Time(hh:mm:ss)	Acton(Yes/No)	Com(IP)

Descrition

ตารางที่ 3.2 ตารางเก็บข้อมูลการใช้งานคอมพิวเตอร์

Field	Type	Description
Student(ID)	nvarchar(10)	รหัสนักศึกษา
Date(d/m/y)	Datetime(8)	วันที่ใช้งานคอมพิวเตอร์
Time(hh:mm:ss)	Datetime(8)	เวลาที่ใช้งาน
Acton(Yes/No)	Nvchar(5)	อนุญาต / ไม่อนุญาต
Com(IP)	Nvchar (10)	รหัสIP คอมพิวเตอร์
Description	Nvchar (255)	รายการที่ใช้งาน



ตารางที่ 3.3 ตารางเก็บข้อมูลคอมพิวเตอร์

Field	Type	Description
Computer(IP)	Nvchar (10)	รหัส IP คอมพิวเตอร์
Computer(ID)	Nvchar (10)	รหัสคอมพิวเตอร์

บทที่ 4

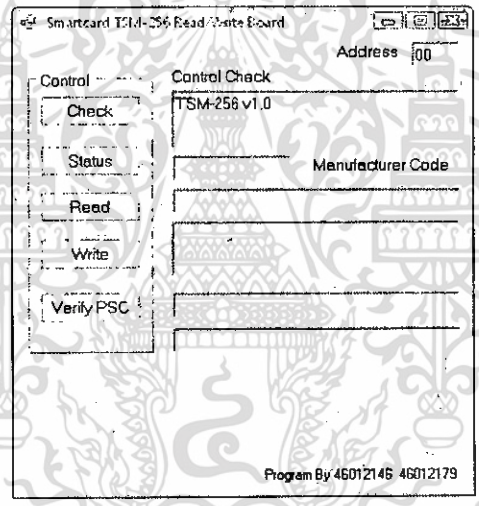
ผลการทดลอง

4.1 ขั้นตอนการทดลอง ประกอบด้วย 3 ส่วนคือ

4.1.1 ส่วนติดต่อกับเครื่องอ่านเขียน และบัตรสมาร์ทการ์ด

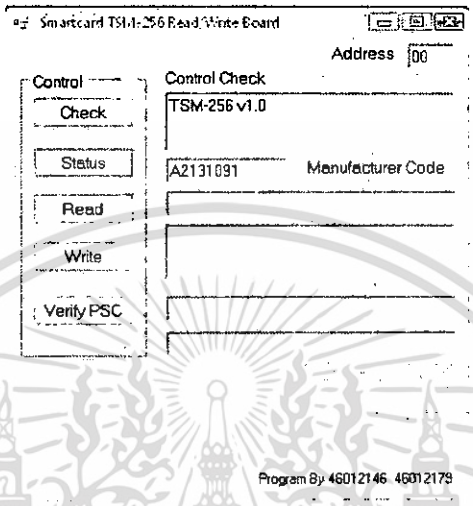
ประกอบด้วยขั้นตอนดังนี้

1. เมื่อเสียบบัตรและกดปุ่ม Check โปรแกรมจะแสดงค่า “TSM-256 V1.0” ซึ่งเป็นค่าเวอร์ชั่นของเครื่องอ่าน



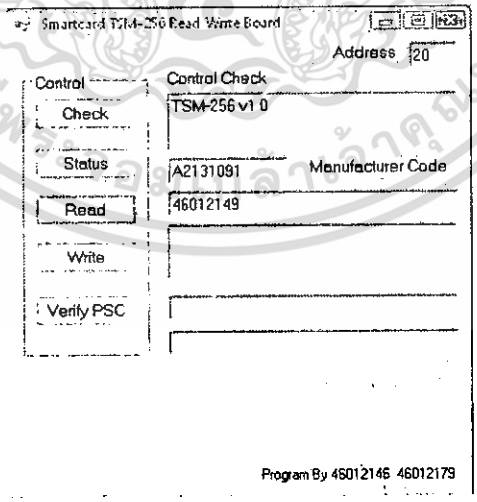
รูปที่ 4.1 ผลลัพธ์จากการกดปุ่ม Check

2. ถ้ามีบัตรเสียบอยู่และกดปุ่ม Status โปรแกรมจะแสดงค่า Manufacturer Code ซึ่งจะส่งค่ากลับมาคือ “A2131091”



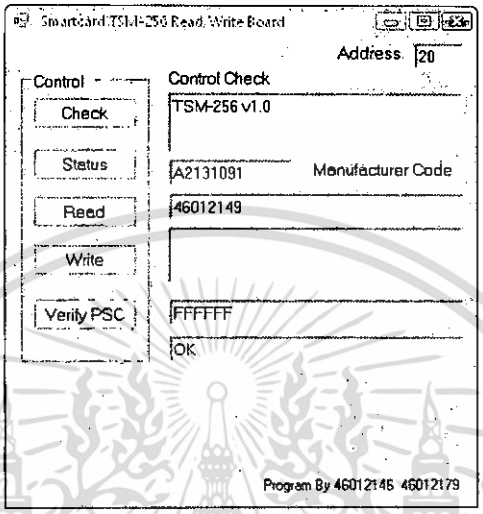
รูปที่ 4.2 ผลลัพธ์จากการกดปุ่ม Status

3. เมื่อกดปุ่ม Read และกำหนดค่า Address โดยรหัสนักศึกษาถูกกำหนดไว้ที่ Address ที่ 20 โดยจะแสดงค่ารหัสนักศึกษากลับมา



รูปที่ 4.3 รหัสนักศึกษาถูกอ่านจากบัตรสมาร์ทการ์ด

4. เมื่อกดปุ่ม Write และกำหนดค่า Address โปรแกรมจะทำการเขียนข้อมูลลงในบัตรตามที่ได้กำหนด Address ไว้ (ก่อนทำการเขียนบัตร ต้อง Verify PSC ก่อน)

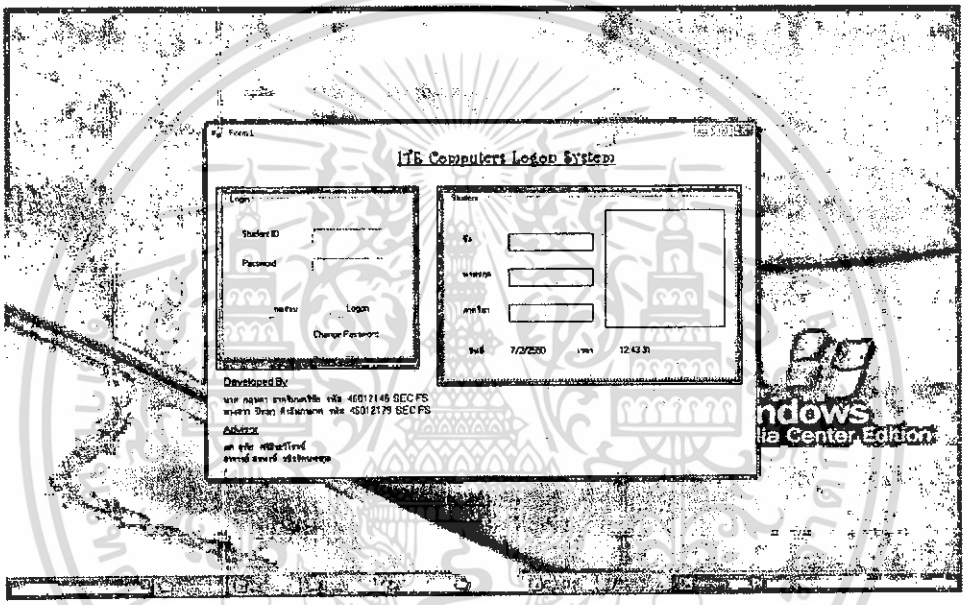


รูปที่ 4.4 การ Verify PSC และเขียนข้อมูลลงบนบัตร

4.1.2 ส่วนติดต่อกับนักศึกษา

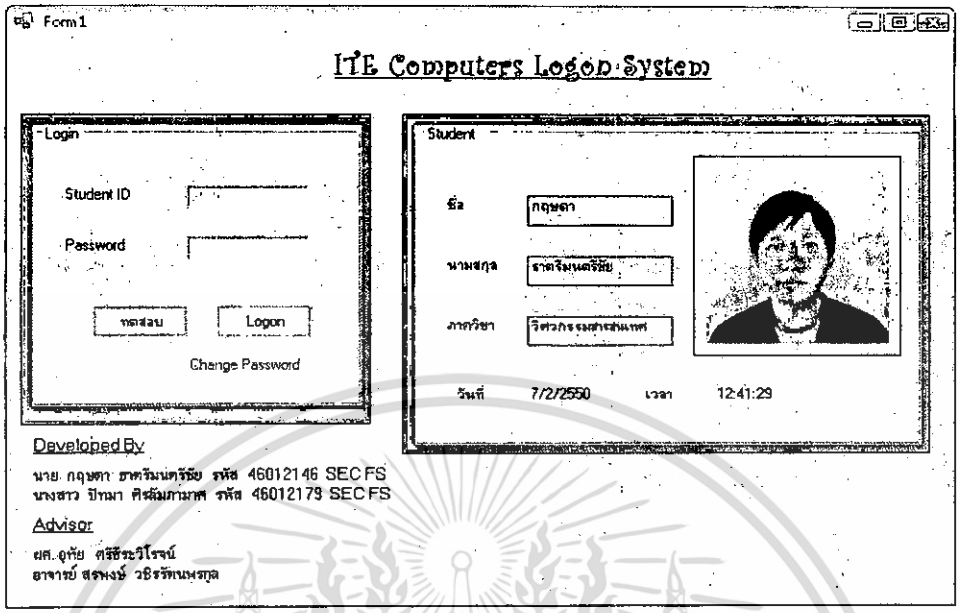
ประกอบด้วยขั้นตอนดังนี้

1. เมื่อนักศึกษาเสียบบัตรสมาร์ทการ์ด ระบบจะมีการตรวจเช็คว่ามีบัตรถูกเสียบหรือไม่ โดยใช้การอินเตอร์รัปต์ จากไทมเมอร์ ถ้ามี ระบบจะนำรหัสนักศึกษามาแสดงในช่องรหัสโดยในที่นี้นักศึกษาจะไม่สามารถคลิก Icon ต่างๆ บนหน้าจอ desktop ได้ ดังรูป 4.5



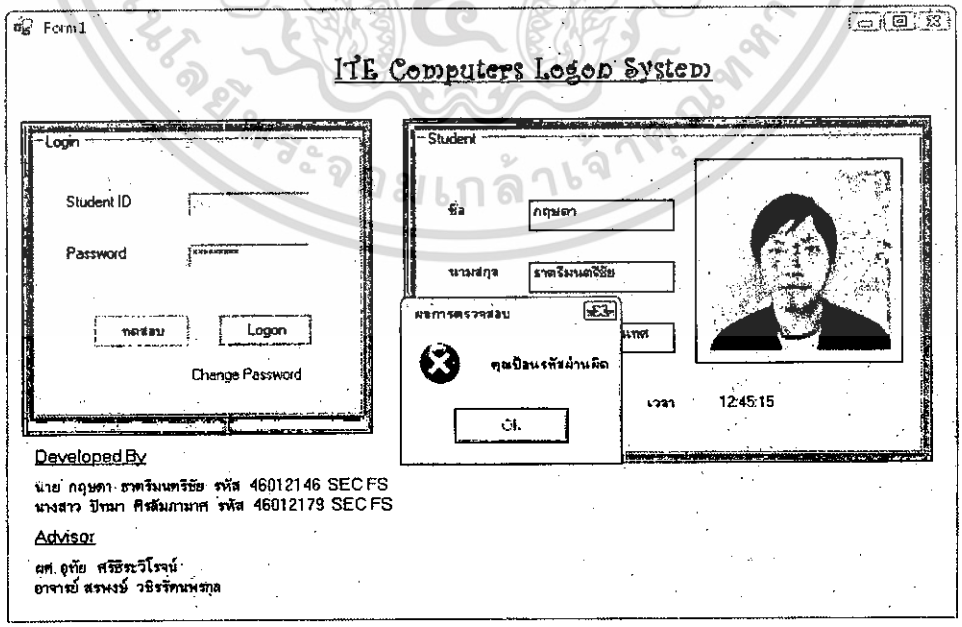
รูปที่ 4.5 หน้าต่างโปรแกรมการใช้บัตรสมาร์ทการ์ดทางฝั่งไคแอนท์

2. จากนั้นเมื่อกดปุ่มทดสอบ ระบบจะทำการดึงข้อมูลของนักศึกษาจากฐานข้อมูลโดยอ้างอิงกับค่ารหัสที่รับเข้ามา แล้วนำค่าตัวแปรที่ได้แสดงเป็นชื่อ และ นามสกุลของนักศึกษา



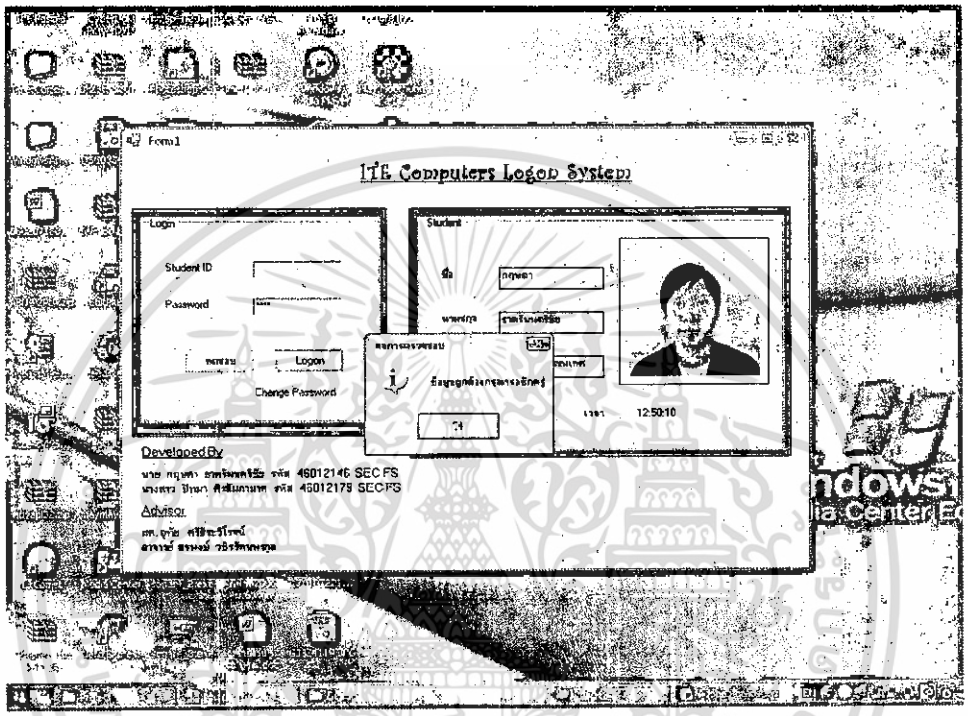
รูปที่ 4.6 ระบบดึงข้อมูลโดยอ้างอิงกับรหัสนักศึกษา

3. จากนั้นให้นักศึกษากรอกรหัสผ่าน แล้วกดปุ่ม Logon จากนั้นระบบจะทำการเปรียบเทียบรหัสผ่าน แล้วเช็คว่าตรงกันหรือไม่ถ้าไม่ตรงระบบจะให้มีการกรอกรหัสผ่านใหม่โดยแสดงข้อความว่า “คุณป้อนรหัสผ่านผิด”



รูปที่ 4.7 การป้อนรหัสผ่านผิด

4. ถ้ารหัสผ่านถูกต้องระบบจะทำการอนุญาตให้เข้าใช้คอมพิวเตอร์โดยทางหน้าจอ desktop จะสามารถใช้งานได้ตามปกติ และจะมีข้อความว่า “ข้อมูลถูกต้องกรุณารอซักครู่”

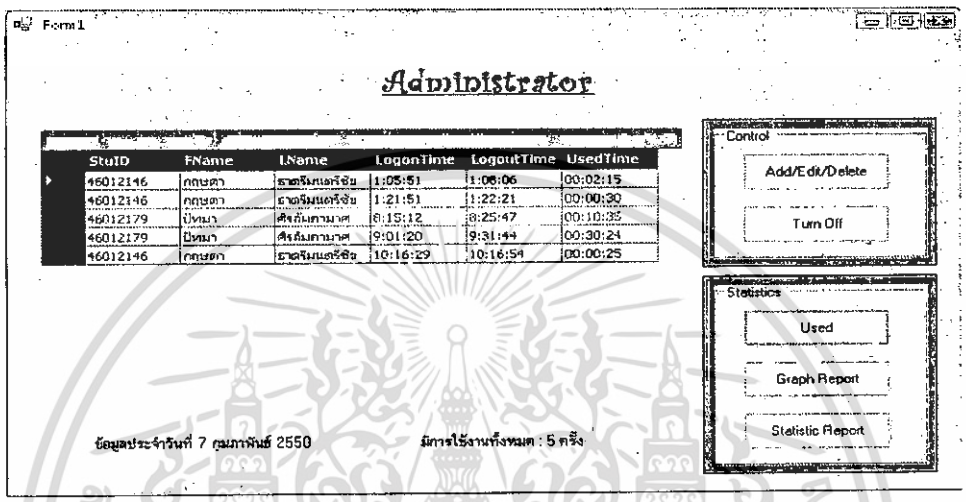


รูปที่ 4.8 ระบบเสร็จสิ้นการทำงาน

4.1.3 ส่วนติดต่อกับผู้ดูแลระบบ

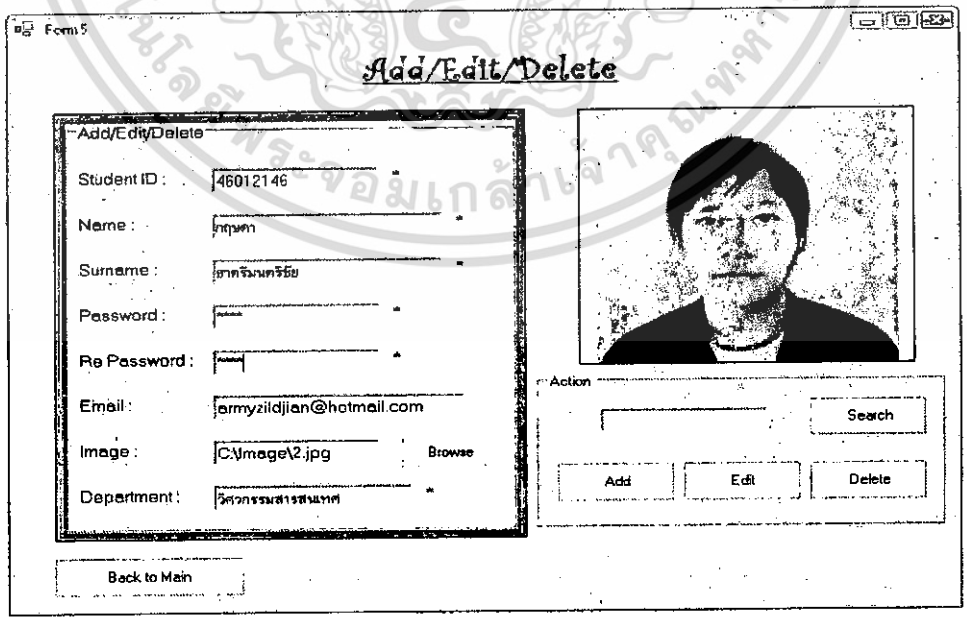
ประกอบด้วยขั้นตอนดังนี้

1. ผู้ดูแลระบบตรวจดูสถิติการใช้งานในแต่ละวัน



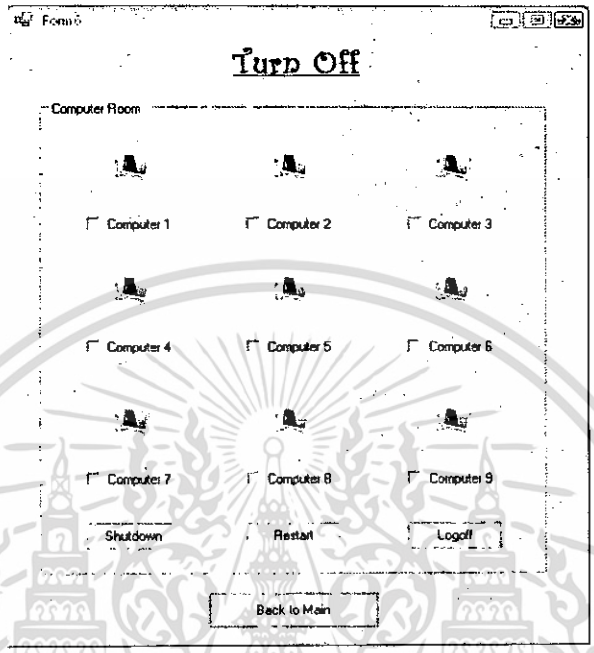
รูปที่ 4.9 ส่วนติดต่อกับผู้ดูแลระบบ

2. ผู้ดูแลระบบสามารถ Add/Edit/Delete ข้อมูลนักศึกษาได้



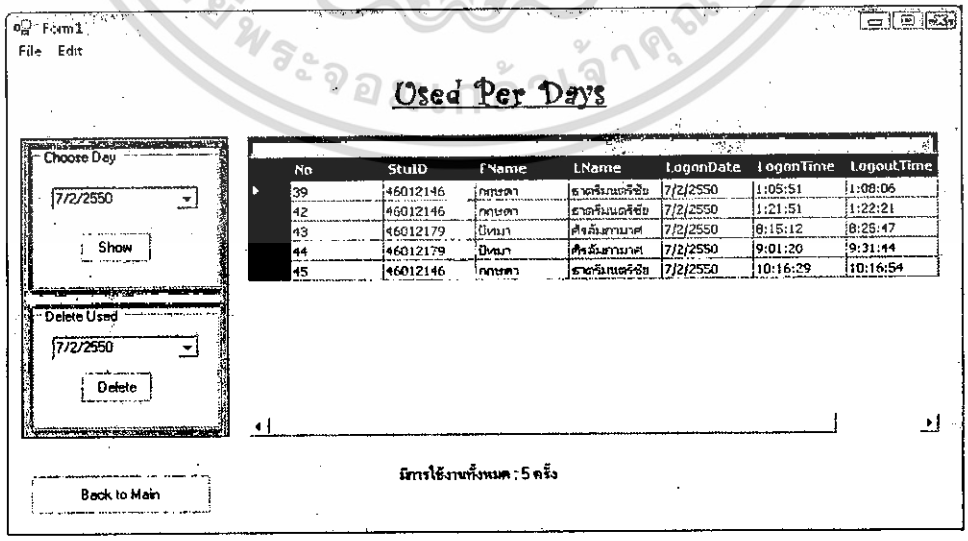
รูปที่ 4.10 ข้อมูลนักศึกษา

3. ผู้ดูแลระบบสามารถ สั่ง Shutdown/Restart/Logoff เครื่องคอมพิวเตอร์ได้



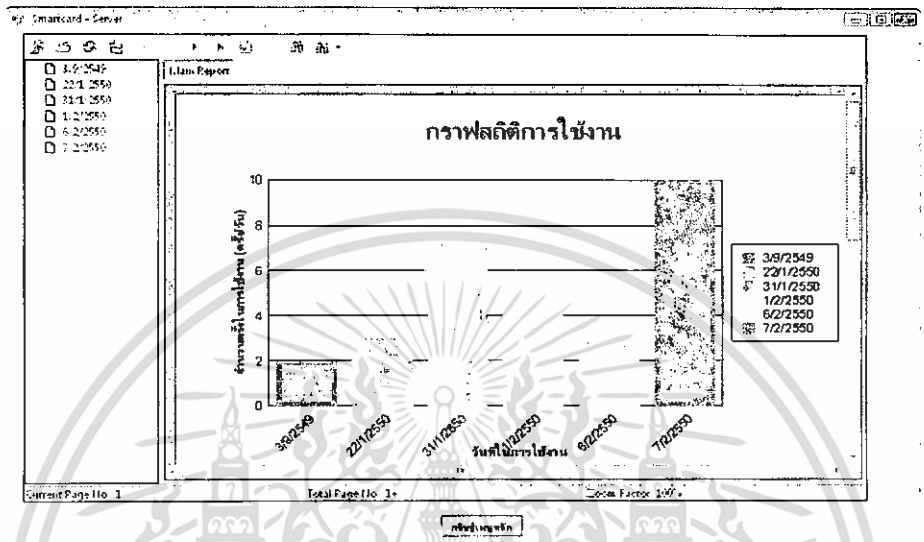
รูปที่ 4.11 การสั่งงาน Shutdown/Restart/Logoff

4. ผู้ดูแลระบบเรียกดูสถิติการใช้งานเครื่องคอมพิวเตอร์ โดยสามารถเลือกวันที่จะค้นหาและลบข้อมูลการใช้งานในวันนั้นๆ ได้



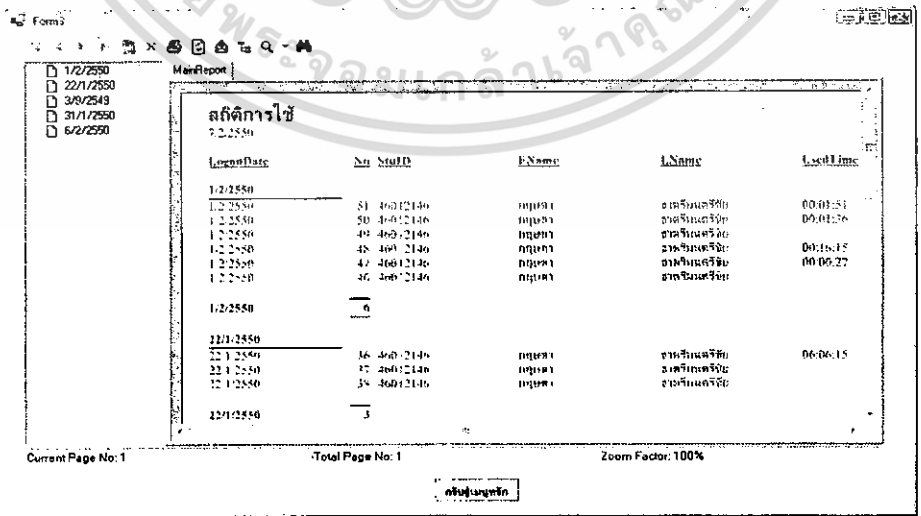
รูปที่ 4.12 สถิติการใช้งาน

5. ผู้ดูแลระบบสามารถ เรียกดูการใช้งานในรูปแบบของ Graph Report (Crystal Report) ได้



รูปที่ 4.13 สถิติการใช้งานรูปแบบของ Graph Report

6. ผู้ดูแลระบบสามารถ เรียกดูการใช้งานในรูปแบบของ Report (Crystal Report) แบบเต็ม โดยแสดงข้อมูลการใช้งานทั้งหมด



รูปที่ 4.14 สถิติการใช้งานรูปแบบของ Report

บทที่ 5
สรุปผลและแนวทางการพัฒนาต่อไป

5.1 สรุปผลโครงงาน

โครงงานในปีการศึกษานี้ ได้ทำการเขียนโปรแกรมติดต่อกับ เครื่องอ่านเขียน สมาร์ทการ์ด และโปรแกรมจัดการข้อมูลการใช้งานเพื่อรวบรวมแล้วแสดงเป็นสถิติ ด้วยรูปแบบของโปรแกรม Crystal Report โดยโปรแกรมจะอ่านค่ารหัสนักศึกษาจากบัตรสมาร์ทการ์ด เพื่อนำมาใช้ในส่วนล็อกออน โดยจะให้นักศึกษากรอกรหัสผ่านและ นำค่ารหัสผ่านไปตรวจสอบกับฐานข้อมูล แล้วแสดงผลการตรวจสอบรหัสผ่านจากนั้นจึงอนุญาตให้เข้าใช้งานคอมพิวเตอร์ได้

5.2 ปัญหาของการทำโครงงาน

ปัญหาของโครงงานนี้ คือ ผู้ทำโครงงาน ไม่มีความชำนาญในการเขียนโปรแกรมติดต่อกับส่วนฮาร์ดแวร์ ทำให้โครงงานล่าช้า เช่น โปรแกรมรับค่าจากเครื่องอ่านซึ่งต้องอ่านค่าจากในบัตรมาแสดง โดยในที่นี้ ผู้จัดทำใช้โปรแกรม Visual C# ซึ่งเป็นโปรแกรมใหม่ต่อการเขียนโปรแกรมติดต่อกับฮาร์ดแวร์ ทำให้ไม่สามารถหาข้อมูลได้เท่าที่ควร

5.3 แนวทางพัฒนาต่อไป

แนวทางในการพัฒนาโครงงานต่อไป อาจเพิ่มความสามารถของโปรแกรม เช่น การตรวจสอบการใช้งานคอมพิวเตอร์ และมีการแจ้งเตือนการใช้งานที่ไม่เหมาะสมไปยังผู้ดูแลระบบ รวมทั้งอาจทำการพัฒนาเทคโนโลยีที่จะรองรับการใช้งานสมาร์ตการ์ดที่หลากหลายมากขึ้น อาทิเช่น การใช้สมาร์ตการ์ดกับงานห้องสมุด ร้านอินเตอร์เน็ตคาเฟ่ และหอพักนักศึกษา

บรรณานุกรม

1. เลิศ แซ่ตั้ง. 2546. **เทคโนโลยีสมาร์ทการ์ด**. กรุงเทพฯ ; ซีเอ็ดยูเคชั่น.

2. อารัมภีย์ จันทร์ใย และโสรัตย์ อุนหะวราการ. 2546. **เรียนรู้และเข้าใจสมาร์ทการ์ดในภาคปฏิบัติ**. ฉบับที่ 240-246. วารสารเซมิคอนดักเตอร์อิเล็กทรอนิกส์.

3. ศุภชัย สมพานิช. 2546. **คู่มือการเขียนโปรแกรม Visual C# .NET ฉบับโปรแกรมเมอร์**. กรุงเทพฯ ; อินโฟเพรส.

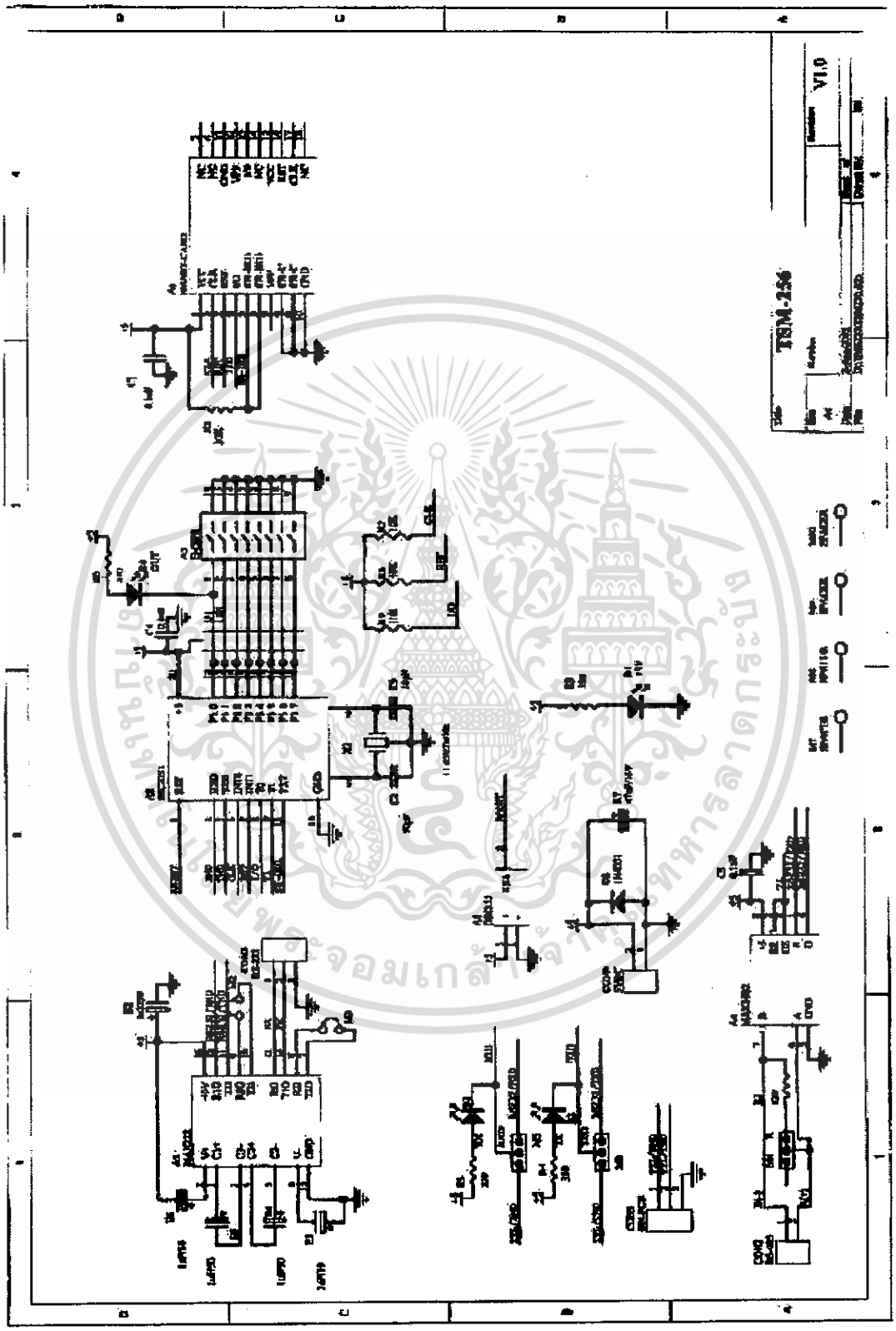
4. สงกรานต์ ทองว่าง. 2548. **My SQL ระบบฐานข้อมูลสำหรับอินเทอร์เน็ต**. กรุงเทพฯ ; ซีเอ็ดยูเคชั่น

แหล่งค้นคว้าทางอินเตอร์เน็ต

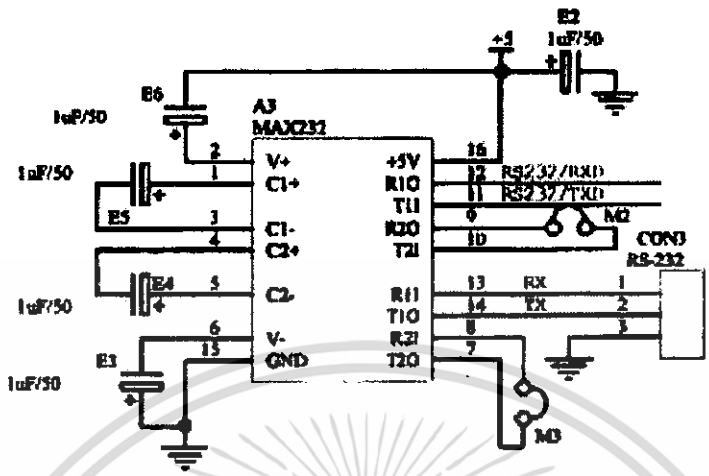
1. http://www.functionx.com/vcsharp/ เป็นแหล่งค้นคว้าข้อมูลเรื่อง Visual C#
2. http://www.mysql.com/ เป็นแหล่งค้นคว้าข้อมูลเรื่อง My SQL
3. http://www.thaisharp.net/ เป็นแหล่งค้นคว้าข้อมูลเรื่อง Visual C#
4. http://www.c-sharpcorner.com/ เป็นแหล่งค้นคว้าข้อมูลเรื่อง Visual C#
5. http://www.csharp-station.com/ เป็นแหล่งค้นคว้าข้อมูลเรื่อง Visual C#

ภาคผนวก ก.

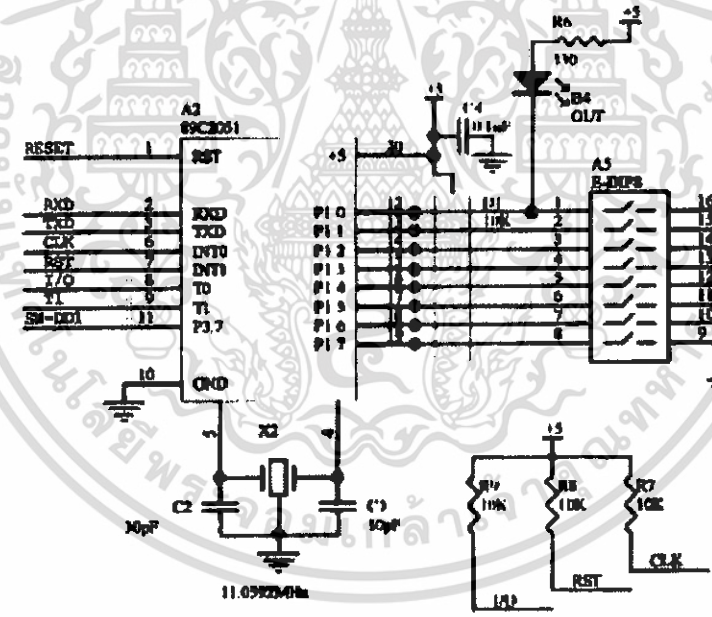
ส่วนวงจรอิเล็กทรอนิกส์ภายในเครื่องอ่านเขียนสมาร์ทการ์ด TSM-256



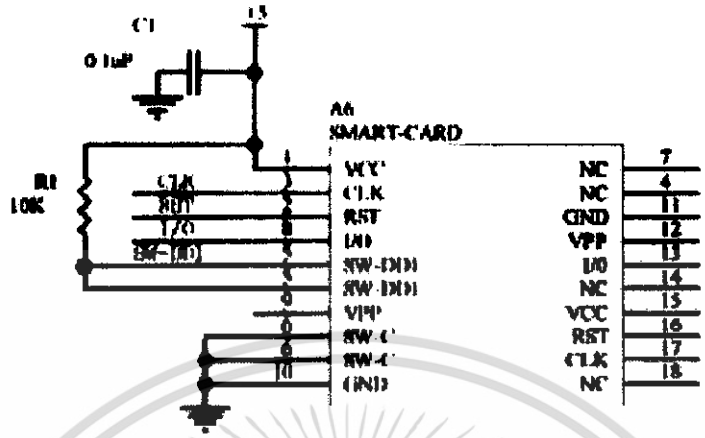
รูปที่ ก.1 วงจรบอร์ด TSM-256



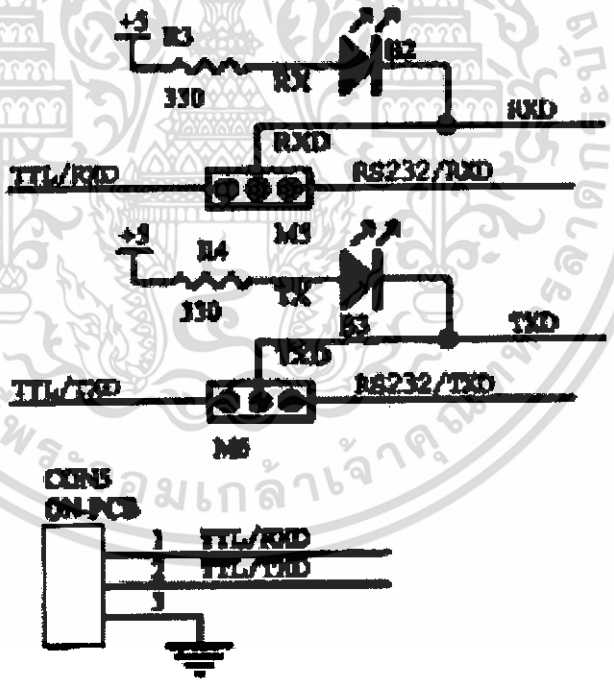
รูปที่ ก.2 ไอซีMAX232



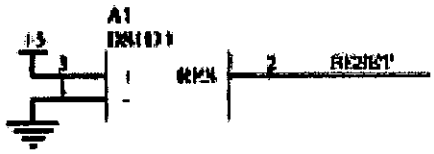
รูปที่ ก.3 ไมโครคอนโทรลเลอร์89C2051



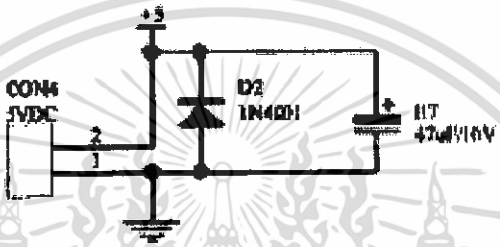
รูปที่ ก.4 SMART-CARD



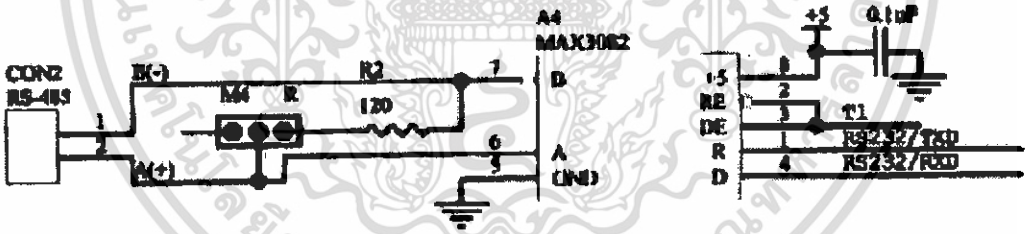
รูปที่ ก.5 LED



รูปที่ ก.6 ไอซี DS1833



รูปที่ ก.7 ไดโอด 1N4004



รูปที่ ก.8 ไอซี MAX3082

ภาคผนวก ข.

รายละเอียดตัวอุปกรณ์

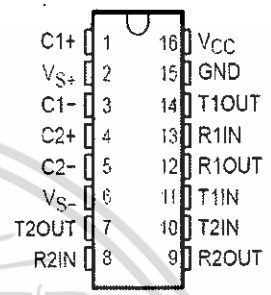
1. MAX232
2. AT89C2051
3. MAX3082

MAX232, MAX232I
DUAL EIA-232 DRIVERS/RECEIVERS

SLLS047L - FEBRUARY 1989 - REVISED MARCH 2004

- Meets or Exceeds TIA/EIA-232-F and ITU Recommendation V.28
- Operates From a Single 5-V Power Supply With 1.0-μF Charge-Pump Capacitors
- Operates Up To 120 kbit/s
- Two Drivers and Two Receivers
- ±30-V Input Levels
- Low Supply Current . . . 8 mA Typical
- ESD Protection Exceeds JESD 22
  - 2000-V Human-Body Model (A114-A)
- Upgrade With Improved ESD (15-kV HBM) and 0.1-μF Charge-Pump Capacitors is Available With the MAX202
- Applications
  - TIA/EIA-232-F, Battery-Powered Systems, Terminals, Modems, and Computers

MAX232 . . . D, DW, N, OR NS PACKAGE
MAX232I . . . D, DW, OR N PACKAGE
(TOP VIEW)



description/ordering information

The MAX232 is a dual driver/receiver that includes a capacitive voltage generator to supply TIA/EIA-232-F voltage levels from a single 5-V supply. Each receiver converts TIA/EIA-232-F inputs to 5-V TTL/CMOS levels. These receivers have a typical threshold of 1.3 V, a typical hysteresis of 0.5 V, and can accept ±30-V inputs. Each driver converts TTL/CMOS input levels into TIA/EIA-232-F levels. The driver, receiver, and voltage-generator functions are available as cells in the Texas Instruments LinASIC™ library.

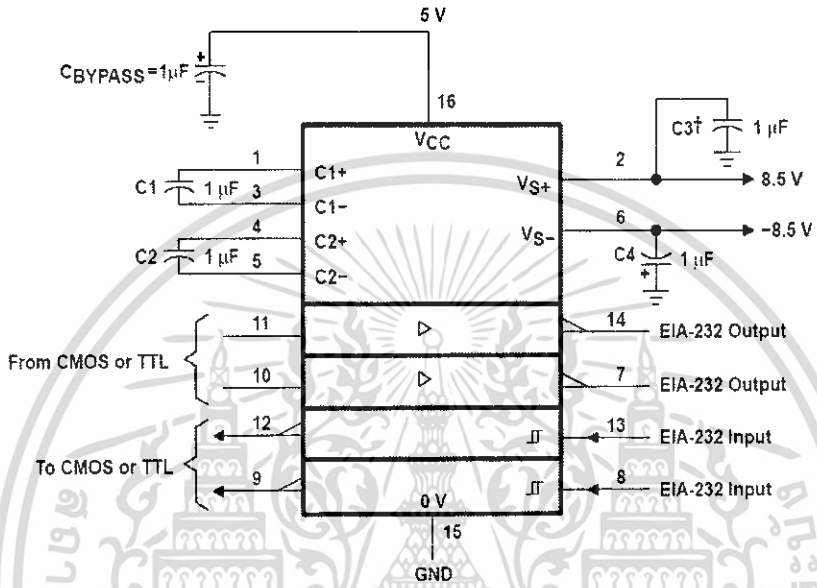
ORDERING INFORMATION

T_A	PACKAGE†		ORDERABLE PART NUMBER	TOP-SIDE MARKING
0°C to 70°C	PDIP (N)	Tube of 25	MAX232N	MAX232N
	SOIC (D)	Tube of 40	MAX232D	MAX232
		Reel of 2500	MAX232DR	
	SOIC (DW)	Tube of 40	MAX232DW	MAX232
		Reel of 2000	MAX232DWR	
	SOP (NS)	Reel of 2000	MAX232NSR	MAX232
−40°C to 85°C	PDIP (N)	Tube of 25	MAX232IN	MAX232IN
	SOIC (D)	Tube of 40	MAX232ID	MAX232I
		Reel of 2500	MAX232IDR	
	SOIC (DW)	Tube of 40	MAX232IDW	MAX232I
		Reel of 2000	MAX232IDWR	

† Package drawings, standard packing quantities, thermal data, symbolization, and PCB design guidelines are available at www.ti.com/sc/package.

รูปที่ ข.1 รายละเอียดวงจรปรับแรงดันไฟฟ้า MAX232

APPLICATION INFORMATION



†C3 can be connected to V_{CC} or GND.

NOTES: A. Resistor values shown are nominal.

B. Nonpolarized ceramic capacitors are acceptable. If polarized tantalum or electrolytic capacitors are used, they should be connected as shown. In addition to the 1-µF capacitors shown, the MAX202 can operate with 0.1-µF capacitors.

รูปที่ ข.2 การทำงานของวงจรปรับแรงดันไฟฟ้า MAX232

Features

- Compatible with MCS-51™ Products
- 2K Bytes of Reprogrammable Flash Memory
  - Endurance: 1,000 Write/Erase Cycles
- 2.7V to 6V Operating Range
- Fully Static Operation: 0 Hz to 24 MHz
- Two-level Program Memory Lock
- 128 x 8-bit Internal RAM
- 15 Programmable I/O Lines
- Two 16-bit Timer/Counters
- Six Interrupt Sources
- Programmable Serial UART Channel
- Direct LED Drive Outputs
- On-chip Analog Comparator
- Low-power Idle and Power-down Modes

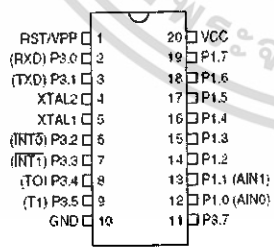
Description

The AT89C2051 is a low-voltage, high-performance CMOS 8-bit microcomputer with 2K bytes of Flash programmable and erasable read only memory (PEROM). The device is manufactured using Atmel's high-density nonvolatile memory technology and is compatible with the industry-standard MCS-51 instruction set. By combining a versatile 8-bit CPU with Flash on a monolithic chip, the Atmel AT89C2051 is a powerful microcomputer which provides a highly-flexible and cost-effective solution to many embedded control applications.

The AT89C2051 provides the following standard features: 2K bytes of Flash, 128 bytes of RAM, 15 I/O lines, two 16-bit timer/counters, a five vector two-level interrupt architecture, a full duplex serial port, a precision analog comparator, on-chip oscillator and clock circuitry. In addition, the AT89C2051 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port and interrupt system to continue functioning. The power-down mode saves the RAM contents but freezes the oscillator disabling all other chip functions until the next hardware reset.

Pin Configuration

PDIP/SOIC



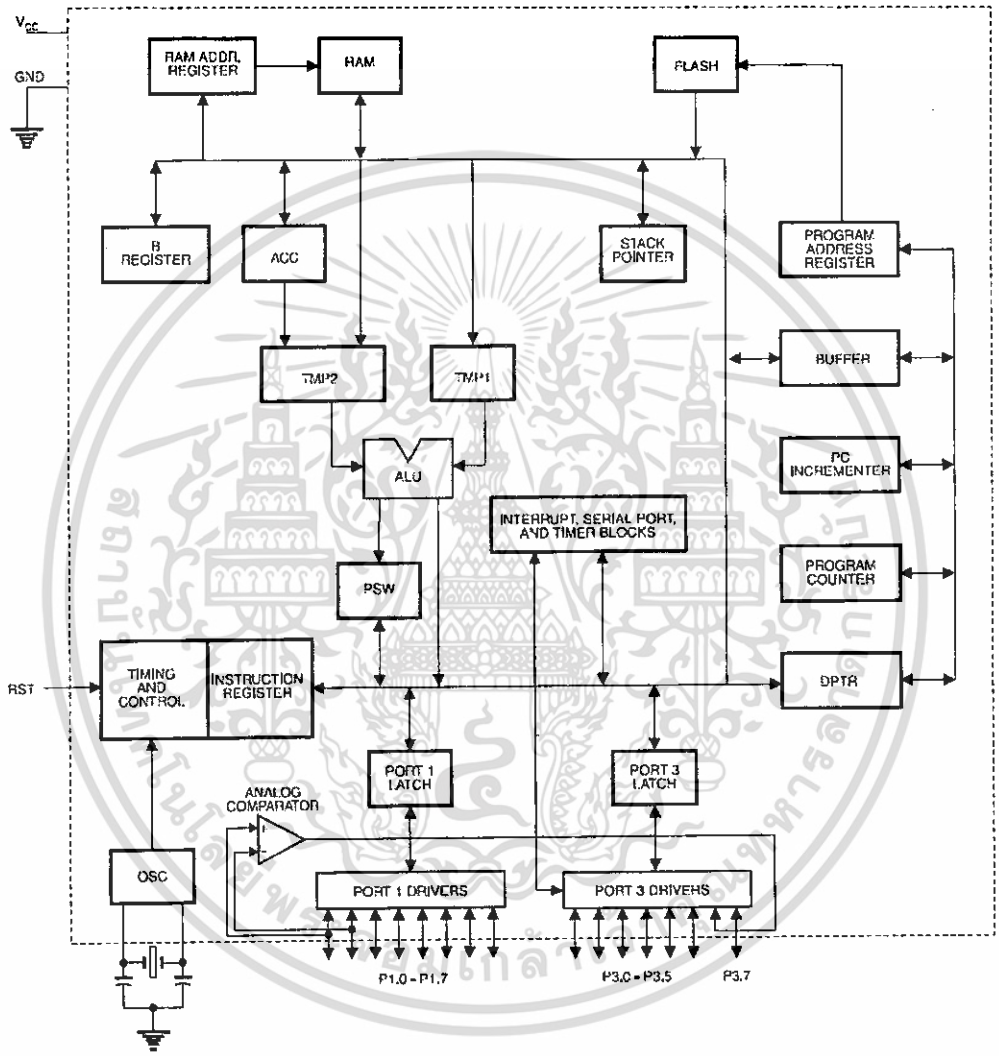
8-bit Microcontroller with 2K Bytes Flash

AT89C2051

Rev. 0368E–02/00

รูปที่ ข.3 รายละเอียดไมโครคอนโทรลเลอร์ AT89C2051

Block Diagram



รูปที่ ข.4 บล็อกไดอะแกรมไมโครคอนโทรลเลอร์ AT89C2051

Pin Description

VCC

Supply voltage.

GND

Ground.

Port 1

Port 1 is an 8-bit bi-irectional I/O port. Port pins P1.2 to P1.7 provide internal pullups. P1.0 and P1.1 require external pullups. P1.0 and P1.1 also serve as the positive input (AIN0) and the negative input (AIN1), respectively, of the on-chip precision analog comparator. The Port 1 output buffers can sink 20 mA and can drive LED displays directly. When 1s are written to Port 1 pins, they can be used as inputs. When pins P1.2 to P1.7 are used as inputs and are externally pulled low, they will source current (I_{IL}) because of the internal pullups.

Port 1 also receives code data during Flash programming and verification.

Port 3

Port 3 pins P3.0 to P3.5, P3.7 are seven bi-irectional I/O pins with internal pullups. P3.6 is hard-wired as an input to the output of the on-chip comparator and is not accessible as a general purpose I/O pin. The Port 3 output buffers can sink 20 mA. When 1s are written to Port 3 pins they are pulled high by the internal pullups and can be used as inputs. As inputs, Port 3 pins that are externally being pulled low will source current (I_{IL}) because of the pullups.

Port 3 also serves the functions of various special features of the AT89C2051 as listed below:

Port Pin	Alternate Functions
P3.0	RXD (serial input port)
P3.1	TXD (serial output port)
P3.2	$\overline{INT0}$ (external interrupt 0)
P3.3	$\overline{INT1}$ (external interrupt 1)
P3.4	T0 (timer 0 external input)
P3.5	T1 (timer 1 external input)

Port 3 also receives some control signals for Flash programming and verification.

RST

Reset input. All I/O pins are reset to 1s as soon as RST goes high. Holding the RST pin high for two machine cycles while the oscillator is running resets the device.

Each machine cycle takes 12 oscillator or clock cycles.

XTAL1

Input to the inverting oscillator amplifier and input to the internal clock operating circuit.

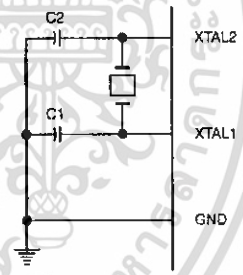
XTAL2

Output from the inverting oscillator amplifier.

Oscillator Characteristics

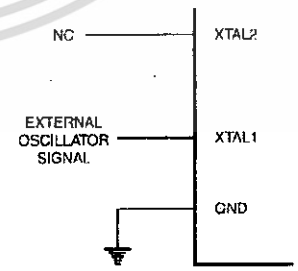
XTAL1 and XTAL2 are the input and output, respectively, of an inverting amplifier which can be configured for use as an on-chip oscillator, as shown in Figure 1. Either a quartz crystal or ceramic resonator may be used. To drive the device from an external clock source, XTAL2 should be left unconnected while XTAL1 is driven as shown in Figure 2. There are no requirements on the duty cycle of the external clock signal, since the input to the internal clocking circuitry is through a divide-by-two flip-flop, but minimum and maximum voltage high and low time specifications must be observed.

Figure 1. Oscillator Connections



Note: C1, C2 = 30 pF ± 10 pF for Crystals
= 40 pF ± 10 pF for Ceramic Resonators

Figure 2. External Clock Drive Configuration



รูปที่ ข.5 ขาของไมโครคอนโทรลเลอร์ AT89C2051

ภาคผนวก ค.
คู่มือการติดตั้งโปรแกรม

คู่มือการติดตั้งโปรแกรมสมาร์ทการ์ดสำหรับการใช้งานห้องคอมพิวเตอร์

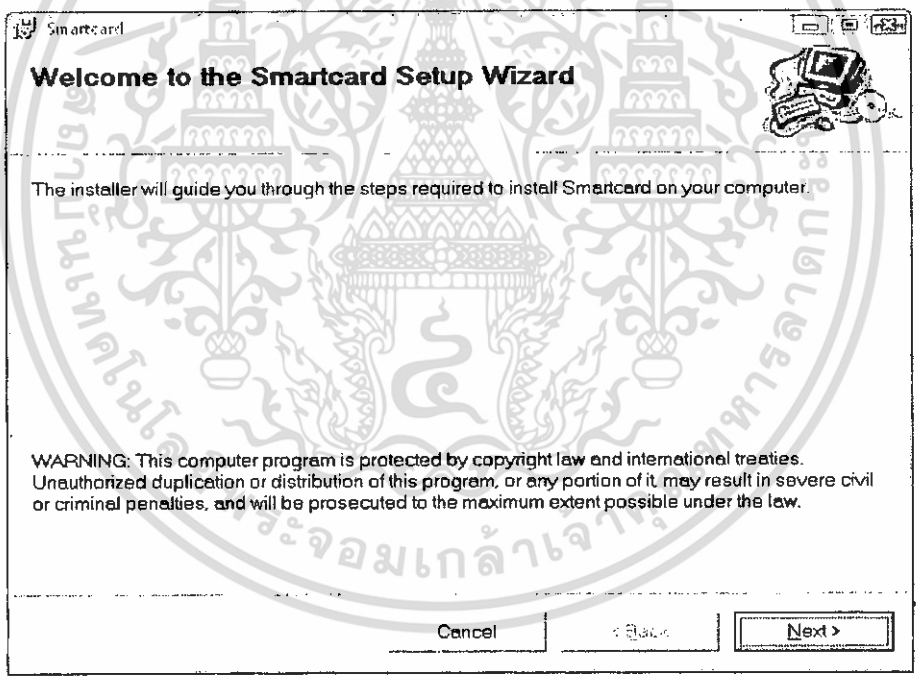
การใช้งานโปรแกรม จะประกอบด้วย 2 ส่วน คือ

1. โปรแกรมฝั่งไคแอนท์
2. โปรแกรมฝั่งเซิร์ฟเวอร์

การติดตั้งโปรแกรมการใช้งาน

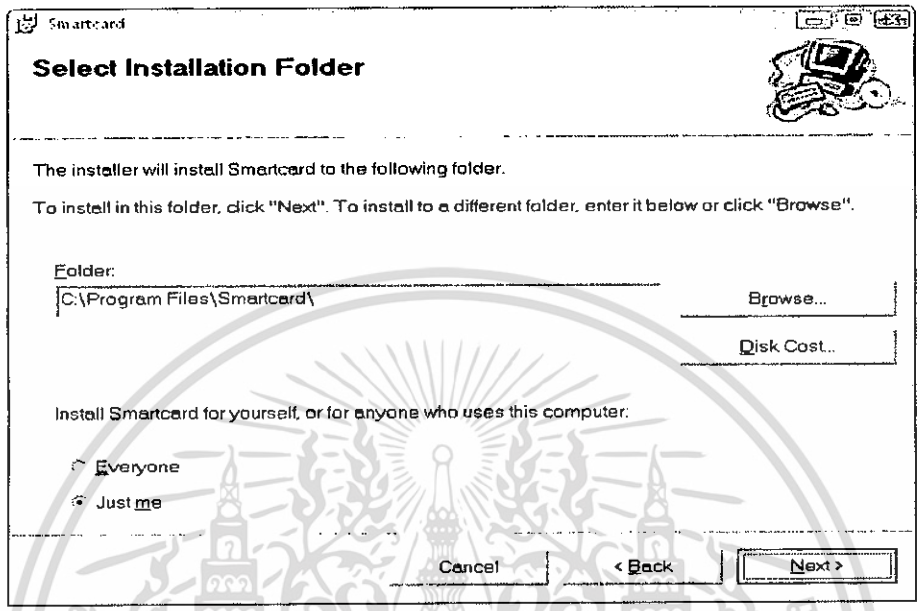
- ฝั่ง ไคแอนท์

1. เข้าไปยังโฟลเดอร์ Smartcard แล้วดับเบิ้ลคลิกเข้าไปที่ Client ทำการติดตั้งโปรแกรมโดยดับเบิ้ลคลิกที่ Setup.exe



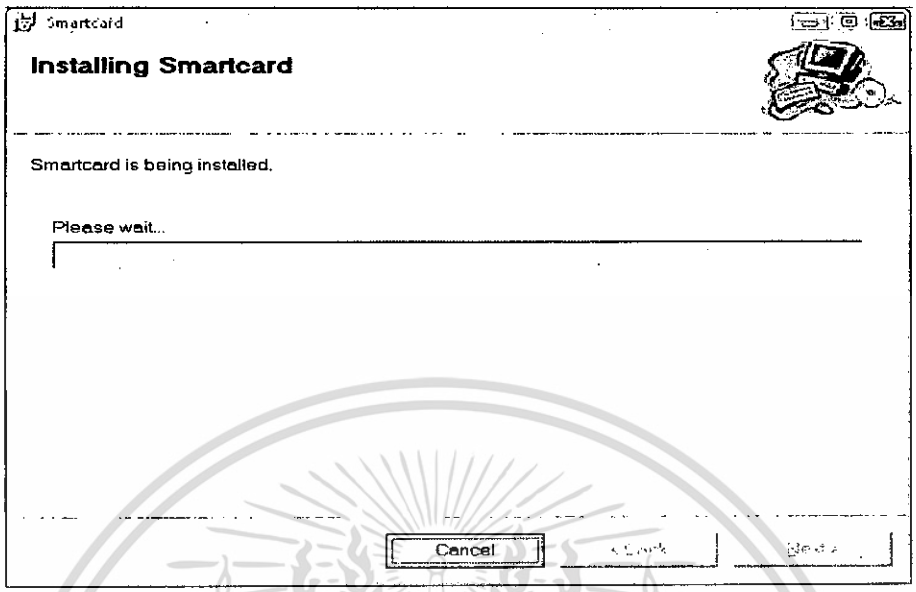
รูปที่ ค.1 หน้าต่างติดตั้งโปรแกรม

2. หลังจากดับเบิ้ลคลิกแล้วก็จะเกิดหน้าต่างให้เลือกไดเรคทอรีจากนั้น ให้คลิก Next ไปเรื่อยๆ



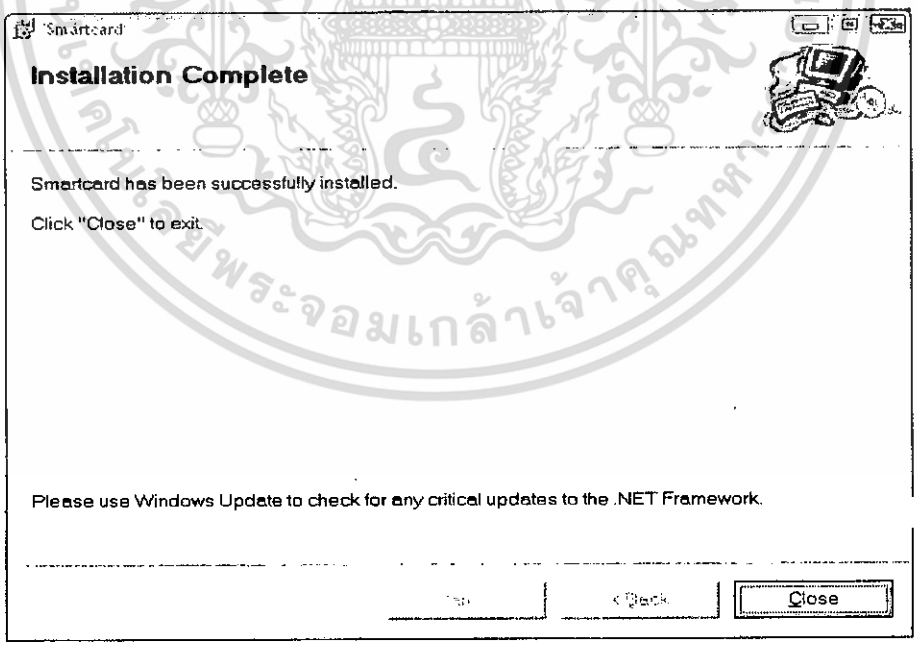
รูปที่ ค.2 หน้าต่างติดตั้งโปรแกรม (ต่อ)

รูปที่ ค.3 หน้าต่างติดตั้งโปรแกรม (ต่อ)



รูปที่ ค.4 หน้าต่างติดตั้งโปรแกรม (ต่อ)

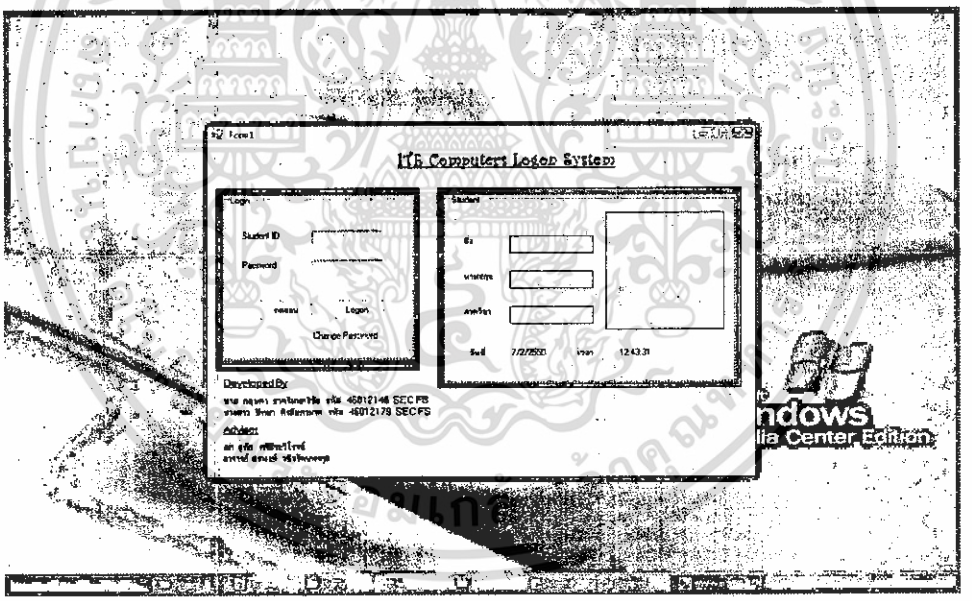
3. เมื่อเสร็จแล้วจะขึ้นหน้าจอสุดท้าย ให้กด Close เป็นอันเสร็จสิ้นการติดตั้งโปรแกรม



รูปที่ ค.5 หน้าต่างติดตั้งโปรแกรม (ต่อ)

- ฝั่ง เซิร์ฟเวอร์

1. เข้าไปที่โฟลเดอร์ Smartcard แล้วเลือก Server จากนั้นติดตั้งเช่นเดียวกับฝั่งไคแอนท์ และหลังจากติดตั้งสำเร็จสามารถเรียกใช้โปรแกรมได้ตามที่เลือกไว้ (default : C:\Smartcart\Server.exe)
2. ทำการติดตั้งฐานข้อมูล MySQL (http://dev.mysql.com/downloads/) จากนั้นทำการ Import ไฟล์ SQL ชื่อ Smartcard.sql จะเสร็จสิ้นการติดตั้งฐานข้อมูล
3. ทำการติดตั้งโปรแกรมติดต่อกับเครื่องอ่านเขียนสมาร์ทการ์ดโดยเข้าไปที่โฟลเดอร์ Smartcard แล้วเลือก Smartcard Control จากนั้นติดตั้งเช่นเดียวกัน เมื่อติดตั้งเสร็จเรียบร้อย สามารถเรียกโปรแกรมได้ตามที่เลือกไว้ (default : C:\Smartcard\Control.exe) เมื่อทำการติดตั้งโปรแกรมเสร็จเรียบร้อย เมื่อมีการเสียบบัตรสมาร์ทการ์ดจะปรากฏหน้าต่างหน้าจอคอมพิวเตอร์ดังรูป ค. 6



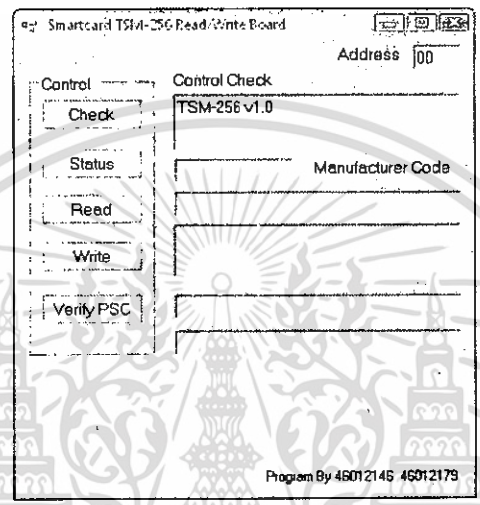
รูปที่ ค.6 หน้าต่างโปรแกรมการใช้บัตรสมาร์ทการ์ดทางฝั่งไคแอนท์

ภาคผนวก ง.
คู่มือการใช้งาน

- ส่วนติดต่อกับเครื่องอ่านเขียน และบัตรสมาร์ทการ์ด

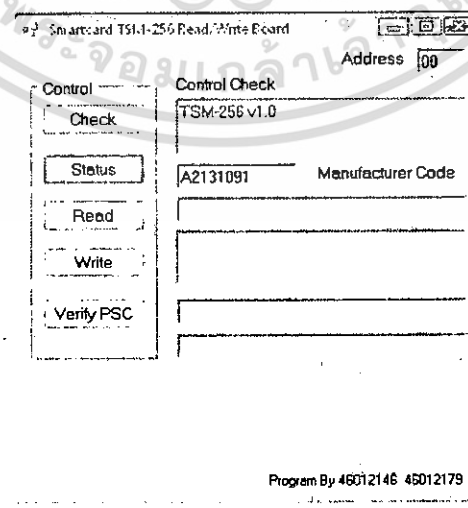
ประกอบด้วยขั้นตอนดังนี้

1. เมื่อเสียบบัตรและกดปุ่ม Check โปรแกรมจะแสดงค่า “TSM-256 V1.0” ซึ่งเป็นค่าเวอร์ชั่นของเครื่องอ่าน



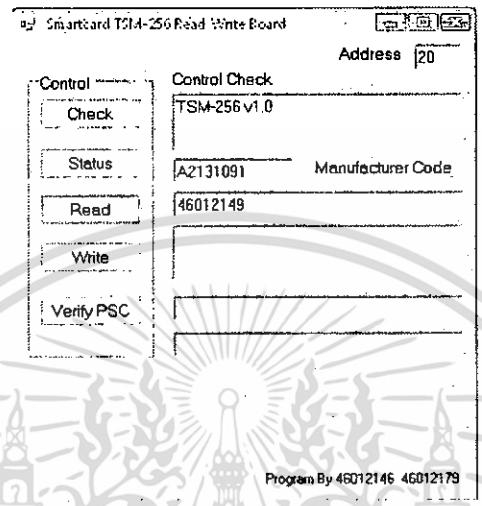
รูปที่ ง.1 ผลลัพธ์จากการกดปุ่ม Check

2. ถ้ามีบัตรเสียบอยู่และกดปุ่ม Status โปรแกรมจะแสดงค่า Manufacturer Code ซึ่งจะส่งค่ากลับมาคือ “A2131091”



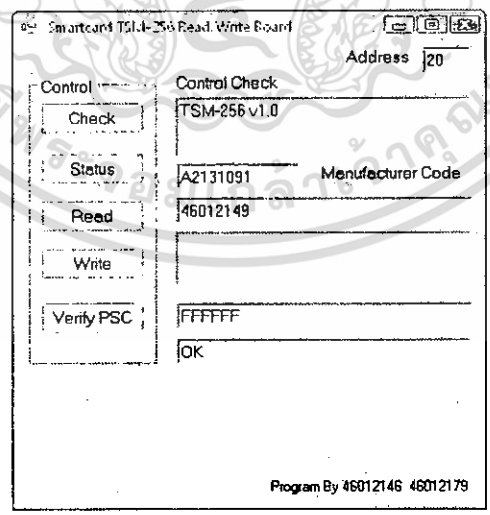
รูปที่ ง.2 ผลลัพธ์จากการกดปุ่ม Status

3. เมื่อกดปุ่ม Read และกำหนดค่า Address โดยรหัสนักศึกษาถูกกำหนดไว้ที่ Address ที่ 20 โดยจะแสดงค่ารหัสนักศึกษากลับมา



รูปที่ ง.3 รหัสนักศึกษาถูกอ่านจากบัตรสมาร์ทการ์ด

4. เมื่อกดปุ่ม Write และกำหนดค่า Address โปรแกรมจะทำการเขียนข้อมูลลงในบัตรตามที่ได้กำหนด Address ไว้ (ก่อนทำการเขียนบัตร ต้อง Verify PSC ก่อน)

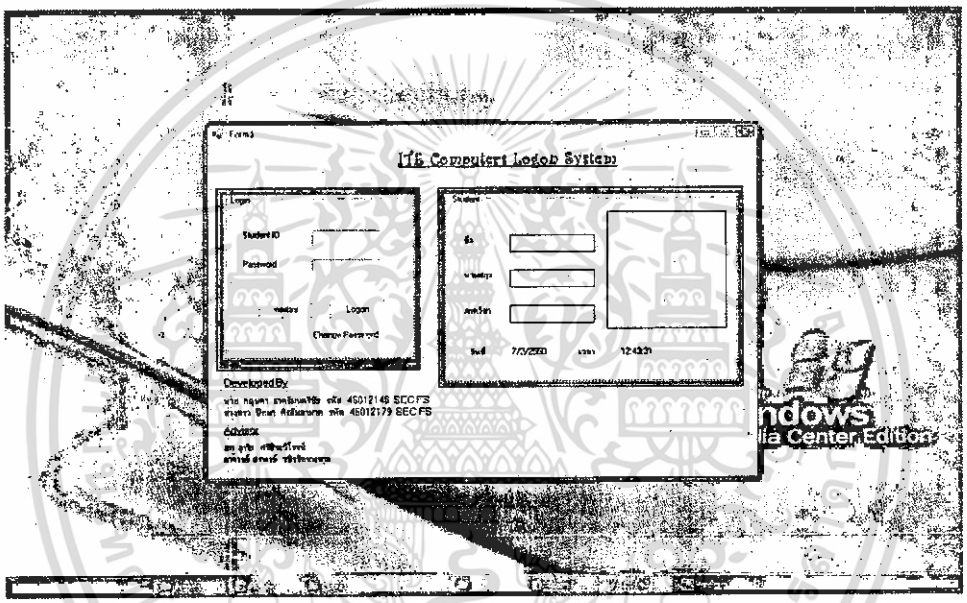


รูปที่ ง.4 การ Verify PSC และเขียนข้อมูลลงบนบัตร

- ส่วนติดต่อกับนักศึกษา

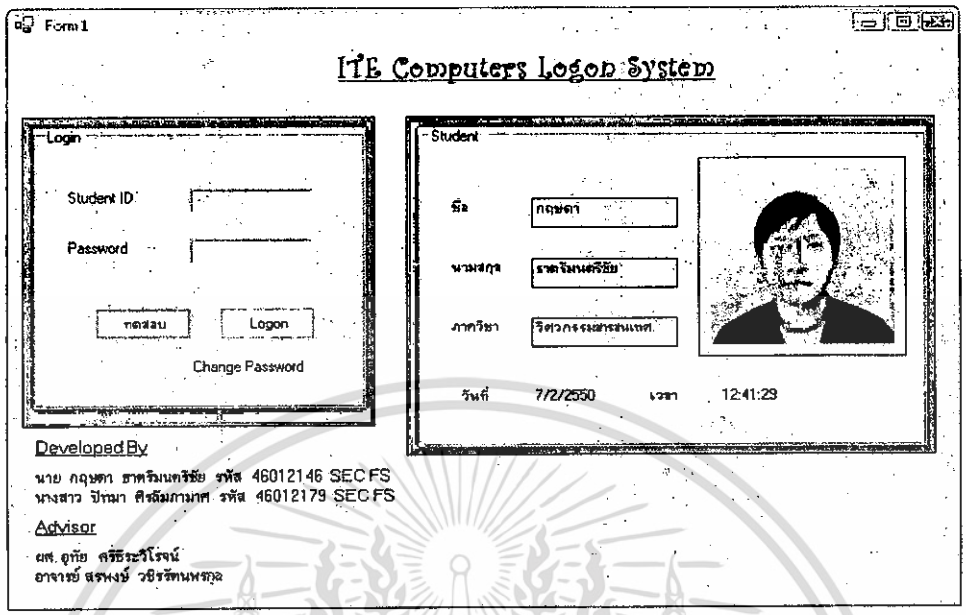
ประกอบด้วยขั้นตอนดังนี้

1. เมื่อนักศึกษาเสียบบัตรสมาร์ทการ์ด ระบบจะมีการตรวจเช็คว่ามีบัตรถูกเสียบหรือไม่ โดยใช้การอินเตอร์รัปต์ จากไทมเมอร์ ถ้ามี ระบบจะนำรหัสนักศึกษามาแสดงในช่องรหัสโดยในที่นี้นักศึกษาจะไม่สามารถคลิก Icon ต่างๆ บนหน้าจอ desktop ได้ ดังรูป ง.5



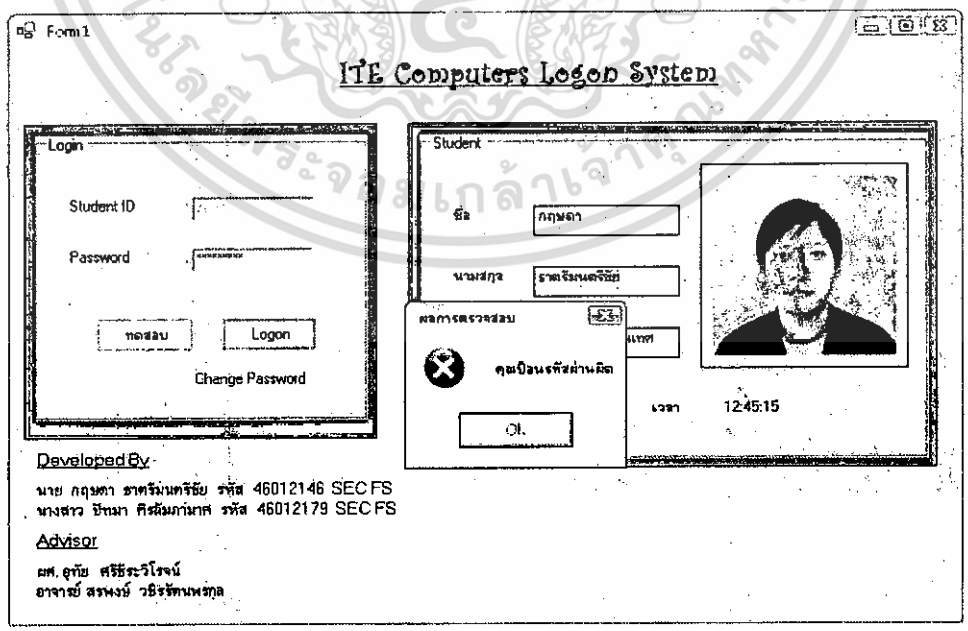
รูปที่ ง.5 หน้าต่างโปรแกรมการใช้บัตรสมาร์ทการ์ดทางฝั่งไคแอนท์

2. จากนั้นเมื่อกดปุ่มทดสอบ ระบบจะทำการดึงข้อมูลของนักศึกษาจากฐานข้อมูลโดยอ้างอิงกับค่ารหัสที่รับเข้ามา แล้วนำค่าตัวแปรที่ได้แสดงเป็นชื่อ และ นามสกุลของนักศึกษา



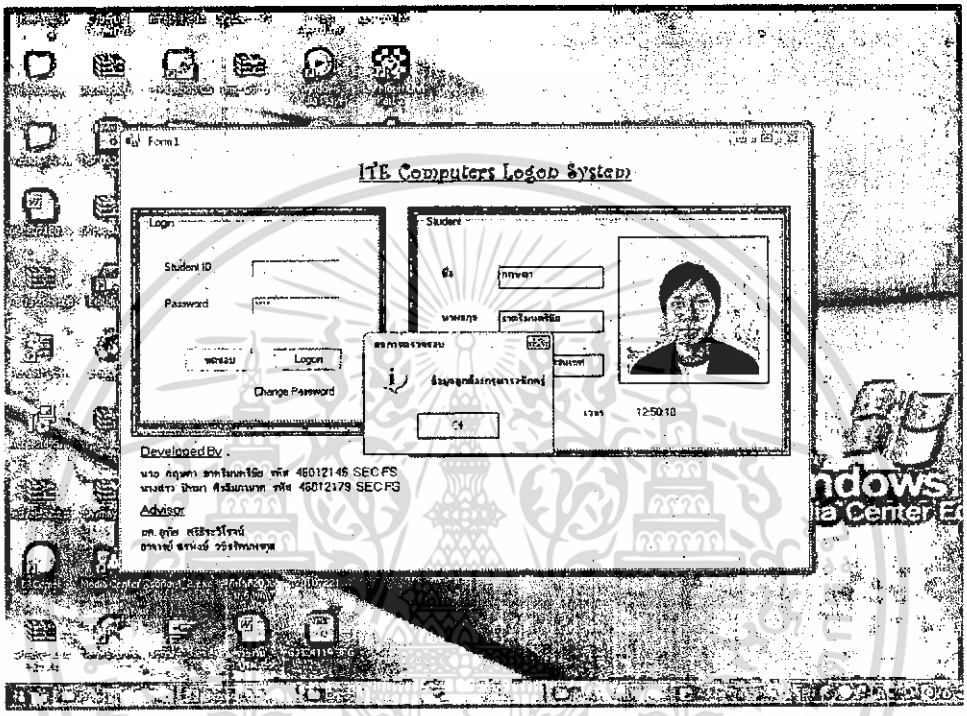
รูปที่ ง.6 ระบบดึงข้อมูลโดยอ้างอิงกับรหัสนักศึกษา

3. จากนั้นให้นักศึกษากรอกรหัสผ่าน แล้วกดปุ่ม Logon จากนั้นระบบจะทำการเปรียบเทียบรหัสผ่าน แล้วเช็คว่าตรงกันหรือไม่ถ้าไม่ตรงระบบจะให้มีการกรอกรหัสผ่านใหม่โดยแสดงข้อความว่า “คุณป้อนรหัสผ่านผิด”



รูปที่ ง.7 การป้อนรหัสผ่านผิด

4. ถ้ารหัสผ่านถูกต้องระบบจะทำการอนุญาตให้เข้าใช้คอมพิวเตอร์โดยทางหน้าจอ desktop จะสามารถใช้งานได้ตามปกติ และจะมีข้อความว่า "ข้อมูลถูกต้องกรุณารอซักครู่"

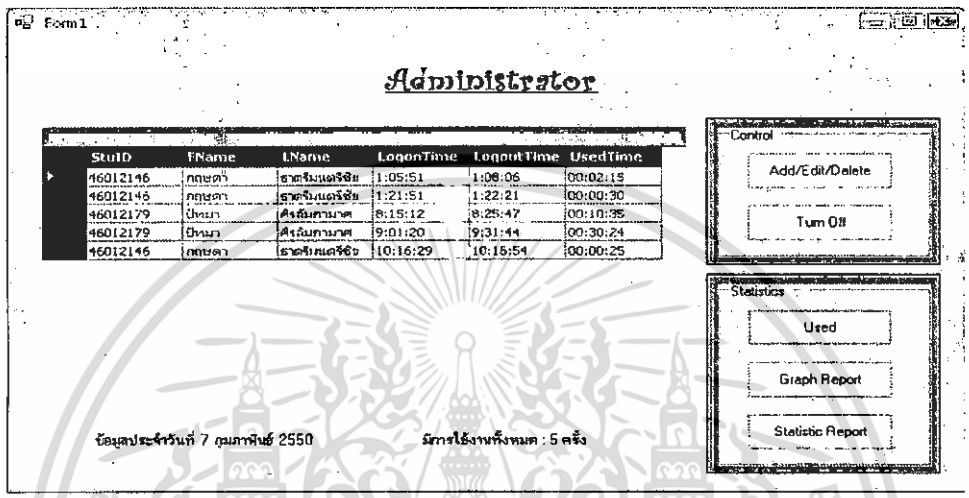


รูปที่ ง.8 ระบบเสร็จสิ้นการทำงาน

- ส่วนติดต่อกับผู้ดูแลระบบ

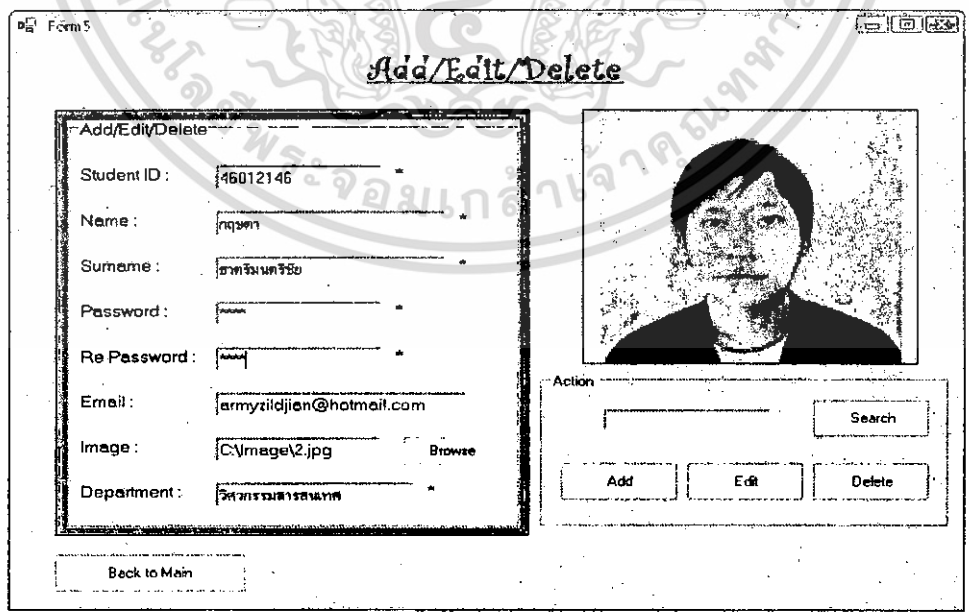
ประกอบด้วยขั้นตอนดังนี้

1. ผู้ดูแลระบบตรวจดูสถิติการใช้งานในแต่ละวัน



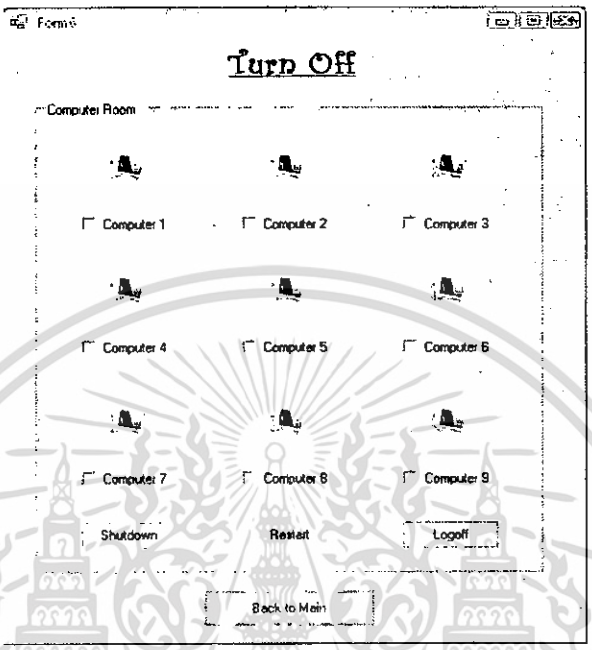
รูปที่ ง.9 ส่วนติดต่อกับผู้ดูแลระบบ

2. ผู้ดูแลระบบสามารถ Add/Edit/Delete ข้อมูลนักศึกษาได้



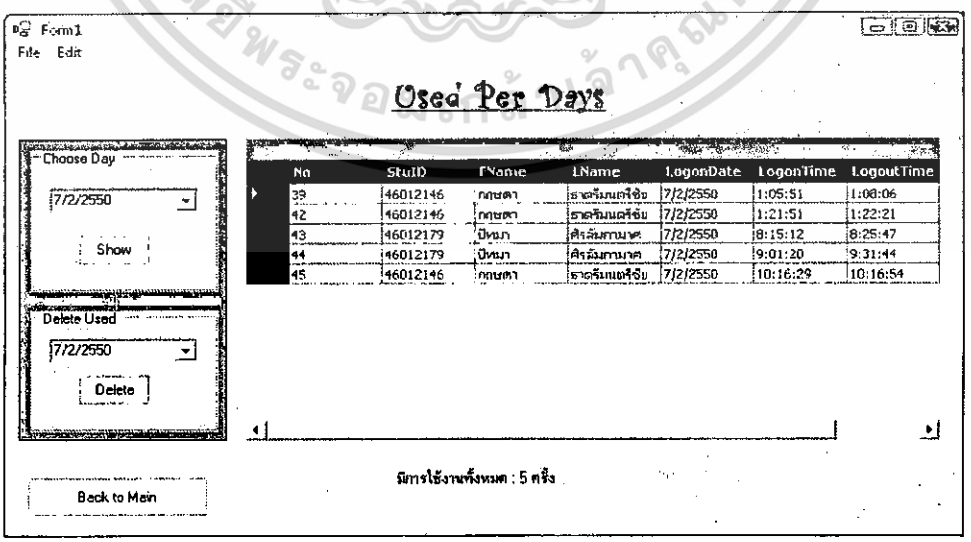
รูปที่ ง.10 ข้อมูลนักศึกษา

3. ผู้ดูแลระบบสามารถ สั่ง Shutdown/Restart/Logoff เครื่องคอมพิวเตอร์ได้



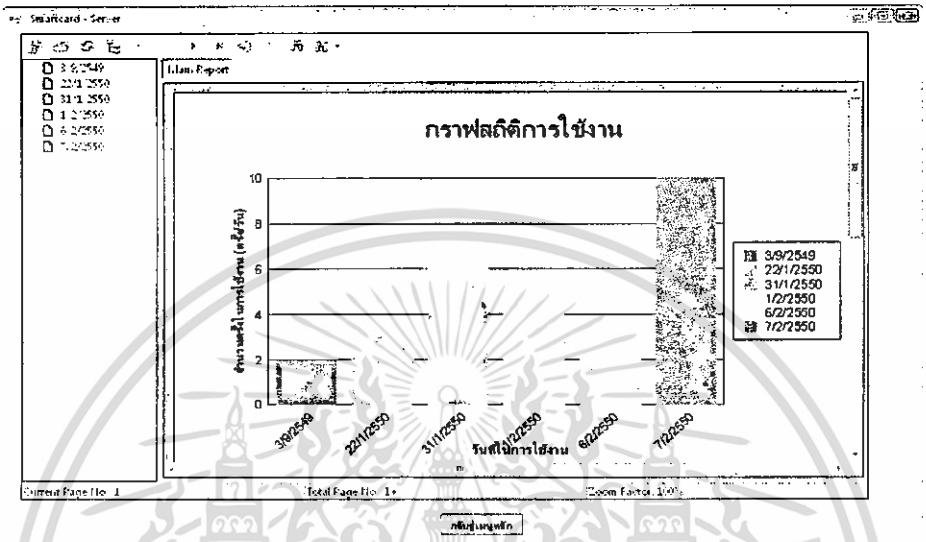
รูปที่ ง.11 การสั่งงาน Shutdown/Restart/Logoff

4. ผู้ดูแลระบบเรียกดูสถิติการใช้งานเครื่องคอมพิวเตอร์ โดยสามารถเลือกวันที่จะค้นหาและลบข้อมูลการใช้งานในวันนั้นๆ ได้



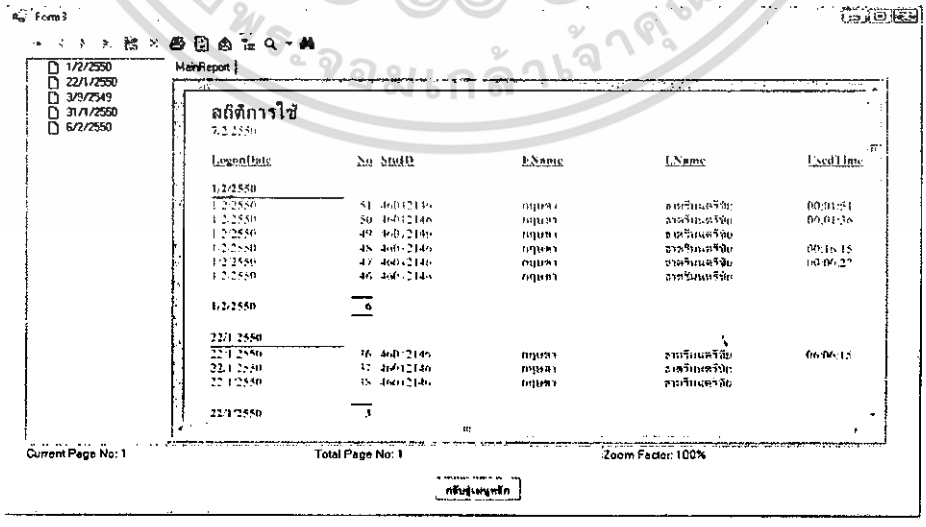
รูปที่ ง.12 สถิติการใช้งาน

5. ผู้ดูแลระบบสามารถ เรียกดูการใช้งานในรูปแบบของ Graph Report (Crystal Report) ได้



รูปที่ ง.13 สถิติการใช้งานรูปแบบของ Graph Report

6. ผู้ดูแลระบบสามารถ เรียกดูการใช้งานในรูปแบบของ Report (Crystal Report) แบบเต็ม โดยแสดงข้อมูลการใช้งานทั้งหมด



รูปที่ ง.14 สถิติการใช้งานรูปแบบของ Report