บทที่ 2

ทบทวนวรรณกรรม

การศึกษาเรื่อง "ความเป็นไปได้ของระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์ของการประปานครหลวง" นั้น อาศัยแนวความคิดและทฤษฎีที่เกี่ยวข้อง ดังนี้

2.1 แนวคิดเกี่ยวกับระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์

2.2 แนวคิดด้านเทคโนโลยี SCADA

2.3 ทฤษฎีเกี่ยวข้องกับระบบเน็ตเวิร์ค (NETWORK)

2.4 ทฤษฎีที่เกี่ยวกับความคุ้มค่าในด้านการลงทุน

2.5 SWOT Analysis

2.1 แนวคิดเกี่ยวกับระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์

"ระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์" เป็นระบบแบบใหม่ที่นำมาตรวัดน้ำแบบอิเล็กทรอนิกส์มาแทนที่มาตรวัดน้ำแบบอนาลอกที่ใช้อยู่เดิม โดยตัวมาตรวัดน้ำแบบอิเล็กทรอนิกส์นี้จะมีตัวเลขบอกจำนวนยูนิตน้ำและคำนวณราคาค่าน้ำประปาตามยูนิตน้ำที่ใช้ไปในแต่ละรอบบิล ซึ่งเป็นระบบการคิดเงินแบบอิเล็กทรอนิกส์ เพื่อให้ผู้ใช้น้ำสามารถควบคุมปริมาณการใช้น้ำได้ด้วยตนเอง และเมื่อเป็นระบบแบบอัตโนมัติแล้ว จะทำให้การตัดยอดในแต่ละรอบบิลเป็นที่แน่นอนและเป็นระบบมากขึ้นกว่าแต่ก่อน โดยข้อมูลการใช้น้ำประปาของผู้ใช้น้ำต่างๆ นั้น จะถูกส่งจากมาตรวัดน้ำแบบอิเล็กทรอนิกส์ไปยังศูนย์รวบรวมข้อมูลโดยอัตโนมัติ อีกทั้งยังสามารถส่งผ่านข้อมูลค่าน้ำประปาจากศูนย์รวบรวมข้อมูลไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้น้ำโดยผ่านทาง SMS จึงทำให้เป็นการลดค่าใช้จ่ายในการจัดจ้างเจ้าหน้าที่ไปอ่านมาตรวัดน้ำ และออกใบแจ้งหนี้ไปให้ตามบ้าน รวมถึงเป็นการลดปริมาณกระดาษได้เป็นอย่างมาก เพราะผู้ใช้น้ำสามารถอ่านราคาค่าน้ำแล้วไปจ่ายเงินยังสถานที่ต่างๆ ที่การประปานครหลวงกำหนดได้

ระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์ดังกล่าวนี้ จะมีศูนย์ควบคุมระบบการจ่ายน้ำ ที่เป็นศูนย์กลางในการควบคุมและสั่งการการทำงานของระบบต่างๆ รวมทั้งสามารถควบคุมการปิด-เปิดน้ำที่ตัวมาตรวัดน้ำแบบอิเล็กทรอนิกส์ที่ติดตั้งอยู่ตามสถานที่ที่

ติดตั้งมาตรวัดน้ำนั้นไว้ เป็นการควบคุมจากระยะไกลโดยผ่านศูนย์ควบคุมระบบการจ่ายน้ำได้ ดังนั้น ระบบควบคุมการจ่ายน้ำแบบอิเล็กทรอนิกส์นี้จะช่วยให้การปิด-เปิดน้ำให้แก่ผู้ใช้น้ำ ในกรณีที่ผู้ใช้น้ำถูกระงับการใช้น้ำ และได้ไปทำการชำระเงินค่าน้ำที่ค้างชำระพร้อมทั้งค่าธรรมเนียมในการบรรจบมาตรวัดน้ำเรียบร้อยแล้ว ให้เป็นไปด้วยความรวดเร็วยิ่งขึ้น โดยข้อมูลจะถูกส่งไปยังศูนย์ควบคุมระบบการจ่ายน้ำ เจ้าหน้าที่ที่ศูนย์ควบคุมระบบการจ่ายน้ำก็จะทำการสั่งการจากศูนย์ควบคุมดังกล่าวให้ทำการเปิดการจ่ายน้ำให้แก่ผู้ใช้น้ำได้ตามปกติ โดยมิต้องรอให้เจ้าหน้าที่ไปทำการบรรจบมาตรวัดน้ำให้ยังสถานที่ที่ติดตั้งมาตรวัดน้ำนั้น จึงถือเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการให้บริการแก่ผู้ใช้น้ำได้เป็นอย่างดี

เนื่องด้วยการประปานครหลวง (2549) ได้จัดแบ่งประเภทของผู้ใช้น้ำออกเป็น 2 ประเภท ได้แก่ ประเภทที่หนึ่งคือ ที่พักอาศัย หมายรวมถึง สถานที่พักอาศัยทั้งรายเดี่ยว รายกลุ่ม และขายเหมาประเภทที่พักอาศัย วัดหรือสถานที่ที่ใช้ประกอบศาสนกิจทุกศาสนา มูลนิธิหรือองค์กรที่มีวัตถุประสงค์ในการประกอบกิจกรรมหรือบำเพ็ญประโยชน์ต่อสาธารณชนส่วนรวม โดยไม่หวังกำไร โรงเรียนทั้งของรัฐและเอกชน ที่เปิดสอนระดับอนุบาล ประถมศึกษา มัธยมศึกษา ทั้งสายสามัญและสายอาชีพ แต่ไม่เกินระดับประกาศนียบัตรวิชาชีพ (ปวช.) โรงพยาบาลของรัฐหรือสถานพยาบาลของรัฐ สถานที่ค้าขายหรือประกอบการหรือรับจ้างเพื่อช่วยเหลือครอบครัวเล็กๆ น้อยๆ ซึ่งของที่ขายราคาไม่สูงนักและมีจำนวนน้อยโดยดำเนินการเองไม่ได้จ้างหรือให้ผู้อื่นเช่าดำเนินการ ส่วนประเภทที่สองคือ หน่วยงานราชการหรือรัฐวิสาหกิจต่างๆ ธุรกิจอุตสาหกรรม และหมายรวมถึงที่นอกเหนือจากประเภทที่หนึ่ง ซึ่งทำให้มีอัตราราคาค่าน้ำที่แตกต่างกันในแต่ละประเภท โดยมาตรการในการระงับการจ่ายน้ำของการประปานครหลวงในปัจจุบัน มีดังนี้

การระงับการใช้น้ำชั่วคราว กรณีที่ผู้ใช้น้ำค้างชำระค่าน้ำประปาเป็นจำนวน 2 ฉบับ สำหรับมาตรวัดน้ำขนาดเส้นผ่าศูนย์กลางไม่เกิน 1 นิ้ว และในกรณีที่ผู้ใช้น้ำค้างชำระค่าน้ำประปาเป็นจำนวน 1 ฉบับ สำหรับมาตรวัดน้ำขนาดเส้นผ่าศูนย์กลางขนาด 1 นิ้วครึ่งขึ้นไปหรือมาตรวัดน้ำชั่วคราว โดยทางการประปานครหลวงจะทำการงดการจ่ายน้ำไปยังผู้ใช้น้ำ ด้วยวิธีการผูกลวดเป็นระยะเวลา 15 วัน หลังจากนั้นถ้าผู้ใช้น้ำยังไม่ชำระเงินภายในกำหนดระยะเวลาดังกล่าว จะถูกระงับการใช้น้ำถาวร โดยการถอดมาตรวัดน้ำออก จากนั้นผู้ใช้น้ำมีหน้าที่ที่จะต้องมาติดต่อขอกลับเป็นผู้ใช้น้ำกับทางการประปานครหลวง พร้อมทั้งชำระหนี้ที่ค้างทั้งหมดและค่าธรรมเนียมในการบรรจบมาตรวัดน้ำ โดยหากมาชำระเงินภายใน 15 วัน นับจากวันที่งดจ่ายน้ำ ต้องชำระ

ค่าธรรมเนียมดังกล่าวเป็นจำนวนเงิน 100 บาท ถ้าเกินกว่า 15 วัน แต่ไม่เกิน 30 วัน นับจากวันที่งดจ่ายน้ำ ต้องชำระค่าธรรมเนียมดังกล่าวเป็นจำนวนร้อยละ 10 ของค่าใช้จ่ายเหมาจ่ายในการติดตั้งประปาใหม่ตามขนาดมาตรวัดน้ำ ถ้าเกินกว่า 30 วัน แต่ไม่เกิน 150 วัน นับจากวันที่งดจ่ายน้ำจะต้องชำระค่าธรรมเนียมดังกล่าวเป็นจำนวนร้อยละ 25 ของค่าใช้จ่ายเหมาจ่ายในการติดตั้งประปาใหม่ตามขนาดมาตรวัดน้ำ และถ้าหากเกินกว่า 150 วัน นับจากวันที่งดจ่ายน้ำ จะต้องชำระค่าธรรมเนียมดังกล่าวเท่ากับค่าใช้จ่ายเหมาจ่ายในการติดตั้งประปาใหม่ตามขนาดมาตรวัดน้ำ

จากที่ได้กล่าวมาข้างต้น จะเห็นได้ว่าระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์นี้ ทำให้ลดค่าใช้จ่ายในการจ้างเจ้าหน้าที่หรือตัวแทนอ่านมาตรของการประปานครหลวงลง เนื่องจากระบบแบบอิเล็กทรอนิกส์ใช้การรับ-ส่งข้อมูล ผ่านศูนย์ควบคุม (Control Center) จึงไม่ต้องให้เจ้าหน้าที่หรือตัวแทนอ่านมาตรไปจดตัวเลขมาตรวัดน้ำ อีกทั้งยังเป็นการเพิ่มความสะดวกรวดเร็วในการทำการปิด-เปิดการจ่ายน้ำไปตามบ้านเรือนต่างๆ และยังเป็นการลดขั้นตอนการเก็บเงินของการประปานครหลวงลงได้อีกทางหนึ่ง เพราะเมื่อไม่มีเจ้าหน้าที่ไปเก็บเงินตามสถานที่ที่ติดตั้งมาตรวัดน้ำ ผู้ใช้น้ำก็ยังสามารถไปจ่ายเงินได้ตามสถานที่ที่กำหนด เช่น สำนักงานประปาสาขา เคาท์เตอร์เซอร์วิส และหักเงินผ่านบัญชีของธนาคารต่างๆ เป็นต้น จึงเป็นการลดโอกาสของการสูญหายของเงินค่าน้ำประปาที่เก็บมาได้จากเจ้าหน้าที่หรือตัวแทนอ่านมาตรที่รับชำระเงินโดยตรง ตามสถานที่ที่ติดตั้งมาตรวัดน้ำนั้นๆ ได้ด้วย ยิ่งไปกว่านั้นการใช้ระบบควบคุมการจ่ายน้ำและการคิดเงินแบบอิเล็กทรอนิกส์จะทำให้มีรายได้เพิ่มขึ้น เนื่องจากระบบแบบใหม่นี้จะมีความเที่ยงตรงขึ้น ทำให้การอ่านค่ามีความแม่นยำมากขึ้นกว่าระบบแบบเดิม

2.2 แนวคิดด้านเทคโนโลยี SCADA

ฐานิศ และพงษ์พิศักดิ์ (2542) ได้กล่าวว่า สกาด้า (SCADA: Supervisory Control and Data Acquisition) หมายถึงระบบที่สามารถดึงเอาสัญญาณจากตัววัดที่อยู่ในรูปของไฟฟ้าหรือพลังงานอื่นๆ มาแปลงให้อยู่ในรูปของข้อมูลที่เป็นตัวเลขเพื่อประโยชน์ต่างๆ ให้กับผู้ปฏิบัติงาน (Data Acquisition) เช่นนำไปแสดงผลบนจอภาพเพื่อการติดตามผล (Monitoring) คำนวณสรุปผลรายงานการทำงานของระบบการผลิต (Logging Report) บันทึกเก็บไว้เป็นสถิติเพื่อการวิเคราะห์ผลการผลิต เป็นต้น ขณะเดียวกันข้อมูลที่ได้สามารถนำมาคำนวณด้วยสมการทางคณิตศาสตร์ชั้นสูง เพื่อกำหนดค่าการควบคุมทางปฏิบัติที่พนักงานควบคุมไม่สามารถคิดคำนวณได้ทันการในเวลาปกติ ค่าที่คำนวณได้นี้จะถูกส่งป้อนกลับไปยังอุปกรณ์ควบคุมการผลิตเพื่อให้ควบคุมตามค่าที่คำนวณเหล่านี้ (Supervisory Control) สกาด้า เป็นระบบที่ได้รับการพัฒนาอย่างต่อเนื่องควบคู่ไปกับเทคโนโลยีคอมพิวเตอร์เป็นหัวใจในการทำงาน สกาด้าต้องประกอบด้วยอุปกรณ์หลัก 3 ประเภท ได้แก่ อุปกรณ์รับส่งสัญญาณ (I/O Device) อุปกรณ์สื่อสารข้อมูล และเครื่องคอมพิวเตอร์ โดยอุปกรณ์รับส่งสัญญาณทำหน้าที่อ่าน สัญญาณป้อนเข้า (Input) ที่ได้จากตัววัดในรูปของสัญญาณอนาลอกและแปลงให้เป็นสัญญาณดิจิตอลที่เป็นตัวเลขเพื่อส่งไปให้เครื่องคอมพิวเตอร์ ขณะเดียวกันจะมีอุปกรณ์ภาคส่งที่ทำหน้าที่ส่งสัญญาณออก (Output) จากสัญญาณแบบดิจิตอลแปลงเป็นสัญญาณอนาลอกที่ได้จากเครื่องคอมพิวเตอร์ไปยังอุปกรณ์ควบคุม ดังนั้นจะเห็นได้ว่าอุปกรณ์รับส่งสัญญาณเองก็จะมีระบบคอมพิวเตอร์อยู่ในตัวเพื่อทำหน้าที่สื่อสารสัญญาณกับเครื่องคอมพิวเตอร์ อุปกรณ์รับส่งสัญญาณที่มีใช้กันทั่วไป ได้แก่ พีแอลซี, อุปกรณ์ควบคุม (Controller), อาร์ทียู (RTU: Remote Terminal Unit) และเครื่องชั่งวัดต่างๆ ที่สามารถทำหน้าที่ดังกล่าวได้

อุปกรณ์สื่อสารเป็นส่วนสำคัญที่ทำหน้าที่รับส่งสัญญาณดิจิตอลไปให้เครื่องคอมพิวเตอร์ อุปกรณ์รับส่งสัญญาณเหล่านี้จะมีช่องต่อสำหรับสื่อสารสัญญาณกับเครื่องคอมพิวเตอร์ได้ โดยทั่วไปจะใช้แบบมาตรฐาน RS-232 และในปัจจุบันนี้อุปกรณ์รับส่งสัญญาณได้รับการพัฒนาให้สามารถสื่อสารสัญญาณระหว่างอุปกรณ์ด้วยระบบเครือข่ายข้อมูลท้องถิ่น (Local Area Network) ตามแบบมาตรฐาน RS-422 และ RS-485 โดยต่อสายสัญญาณระหว่างกันด้วยสื่อสัญญาณแบบสายขดลวดตีเกลียว (Twisted Pair Wire) จนถึงแบบสายใยแก้วนำแสง อีกทั้งมีการพัฒนาให้อุปกรณ์สามารถสื่อสารระยะไกลถึงกันได้ด้วยสื่อสัญญาณแบบผ่านทาง

สายโทรศัพท์และแบบคลื่นวิทยุ ด้วยการนำเทคโนโลยีคอมพิวเตอร์ผสมผสานกับเทคโนโลยีสื่อสารข้อมูล (Data Communication) เครื่องคอมพิวเตอร์ในระบบสกาด้า จึงสามารถรับส่งสัญญาณกับอุปกรณ์รับส่งสัญญาณจากที่ไกลๆ ได้ ในปัจจุบันจึงมักหมายรวมระบบสกาด้าและระบบการวัดระยะไกล (Telemetering) เป็นระบบเดียวกัน

ระบบ SCADA สามารถควบคุมและตรวจสอบการทำงานของระบบควบคุมที่อยู่ห่างไกลกันเช่น ต่างจังหวัดหรือต่างประเทศ โดยผ่านตัวกลางสื่อสารแบบต่าง ๆ เช่น Radio, Internet, Fiber optic, Satellite, ฯลฯ เป็นต้น

2.2.1 <u>เครือข่ายการสื่อสารสำหรับระบบ SCADA</u>

รูปแบบของการเชื่อมโยงการสื่อสารสำหรับระบบ SCADA ที่สะดวกและมีปัญหาน้อยที่สุด คือ การเชื่อมโยงแบบจุดต่อจุด (Point to Point) โดยมีการเชื่อมโยงระหว่างสองจุดเท่านั้น แต่เมื่อสถานีที่ต้องการติดต่อกันมีมากกว่าสองจุด จึงต้องทำเครือข่ายการสื่อสาร (Communication Network) ขึ้น แบ่งเป็นสองรูปแบบหลัก คือ

1. เครือข่ายสวิตช์ชิ่ง (Switching Network) ประกอบด้วยโหนด (Node) หลายๆโหนดเชื่อมโยงกันด้วยเส้นทางส่งข้อมูล ซึ่งข้อมูลจะถูกส่งจากต้นทางสู่ปลายทางโดยผ่านโหนดต่างๆของเครือข่าย โหนดจะมีหน้าที่รับส่งข้อมูลให้กับสถานีที่ใช้โหนดนั้น การเชื่อมโยงระหว่างโหนดกับสถานีจะเป็นแบบจุดต่อจุด แต่การเชื่อมโยงระหว่างโหนดกับโหนดจะเป็นแบบมัลติเพลกซ์ (Multiplex) คือ ใช้สายส่งข้อมูลร่วมกัน ข้อมูลที่ถูกส่งผ่านอาจผ่านโหนดกี่โหนดก็ได้ โดยเครือข่ายสวิตช์ชิ่งจะเลือกเส้นทางที่สะดวกและเหมาะสมให้ ตัวอย่าง เช่น เครือข่ายแพ็กเกจสวิตช์ (Package switched Network) ข้อมูลจาก A ส่งไปยัง B อาจผ่านโหนด 1 และ 2 หรือ ผ่านโหนด 1, 3 และ 2 ก็ได้ แล้วแต่เส้นทางที่เหมาะสมในขณะส่ง

2. เครือข่ายบรอดคาสต์ (Broadcast Networks) หรือเครือข่ายแพร่สัญญาณ การส่งข้อมูลจากโหนดใดโหนดหนึ่ง จะสามารถแพร่กระจายสัญญาณออกไปยังทุกโหนดในเครือข่าย และทุกโหนดจะสามารถรับข้อมูลได้เหมือนกัน เครือข่ายบรอดคาสต์ ต้องสื่อกลางในการส่งข้อมูลเพียงเส้นทางเดียว ซึ่งอาจเป็นชั้นบรรยากาศ หรือสายเคเบิลเพียงสายเดียว เช่น ในเครือข่ายวิทยุ เครือข่าย GPRS เครือข่ายดาวเทียม และเครือข่ายแบบบัส

แต่ละแบบการส่งสัญญาณติดต่อกันหลายๆ สัญญาณในเวลาเดียวกันหรือติดต่อระหว่างหลายสถานีพร้อมๆกัน ก็จะใช้เทคโนโลยีแบบต่างๆ กันตามความเหมาะสมของแต่ละระบบ เช่น การใช้ตัวพาหะคนละความถี่ ใช้เทคนิคการมัลติเพลกซ์แบบความถี่ หรือแบบมัลติเพลกซ์แบบแบ่งเวลาที่ระบุสถานีผู้ส่ง

สถานีแม่ (Master Station) ตัวสถานีแม่จะประกอบด้วย

1. PLC พร้อมหน่วยอินพุตเอาต์พุต
2. คอมพิวเตอร์
3. โต๊ะควบคุม (Control Desk) และแผงแสดงการทำงาน (Mimic Panel)

สถานีลูก (Slave Station) ตัวสถานีลูกจะประกอบด้วย

1. PLC พร้อมหน่วยอินพุตเอาต์พุต
2. อุปกรณ์ที่ต้องการควบคุม เช่น มิเตอร์ดิจิตอล อุปกรณ์วัดระดับน้ำ

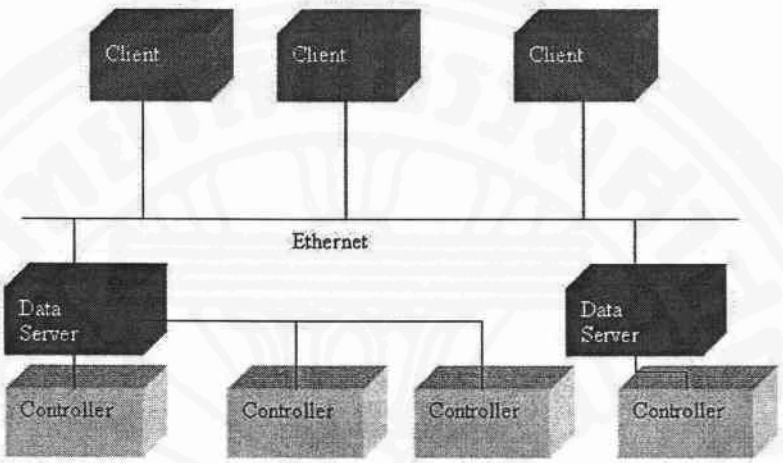
2.2.2 โครงสร้างของSCADA (Architecture)

โครงสร้างด้านฮาร์ดแวร์(Hardware Architecture)

ระบบ SCADA แบ่งตามโครงสร้างฮาร์ดแวร์ได้สองระดับคือ Client และ Data Server หรือ เรียกสั้น ๆ ว่า Server โดยที่ Client คือคอมพิวเตอร์ที่รับและส่งข้อมูลไปยัง Data Server โดยฝั่ง Client นี้จะแสดงผลการทำงานของระบบควบคุม เช่น แสดงเป็นกราฟิก กราฟแบบต่อเนื่อง หรือระบบแจ้งเตือนเมื่อเกิดเหตุการณ์ฉุกเฉินหรือต้องการแจ้งเตือน เป็นต้น ฝั่ง Client สามารถสั่งงานควบคุมไปยัง Data Server เพื่อส่งสัญญาณไปยัง PLC, DCS หรือ Controller อีกทอดหนึ่ง ส่วน Data Server จะทำหน้าที่ติดต่อกับ PLC, DCS, Controller หรือ RTU ต่าง ๆ เพื่อรับสัญญาณและส่งสัญญาณไปยัง Client และรับการร้องขอจาก Client เพื่อควบคุมอุปกรณ์ PLCและ Controller ต่าง ๆ Client และ Data Server ส่วนใหญ่ติดต่อกันผ่านระบบเครือข่าย Ethernet ดังภาพที่ 2.1

ภาพที่ 2.1

โครงสร้างแบบฮาร์ดแวร์ของระบบ SCADA



จากภาพที่ 2.1 นั้น Controller จะติดต่อกับอุปกรณ์ Field Instrument ต่าง ๆ เช่น เซ็นเซอร์ รีเลย์ เป็นต้นเพื่อนำสัญญาณมาให้กับ Data Server

ลักษณะพิเศษของ SCADA

ลักษณะพิเศษของระบบ SCADA ที่ต่างจากระบบควบคุมด้วยระบบคอมพิวเตอร์อื่น คือ ระบบ SCADA จะมีอุปกรณ์ปลายทางที่ถูกควบคุมอยู่ในตำแหน่งที่ห่างไกลจากศูนย์กลาง ระบบคอมพิวเตอร์ที่มีผู้สั่งการ โดยการส่งสัญญาณควบคุมจะถูกส่งผ่านสื่ออื่นเป็นตัวกลาง เช่น คลื่นวิทยุ microwave หรือระบบสื่อสารดาวเทียม

Realtime Database Servers

เป็นระบบฐานข้อมูลที่ใช้จัดการและเก็บค่าของกระบวนการ ณ เวลาปัจจุบันในขณะใดๆ ค่า realtime จะเปลี่ยนแปลงไปตามสภาพของกระบวนการที่เปลี่ยนแปลงไปตามเวลา ค่าของกระบวนการจะถูกตรวจจับ (monitor & scan) โดย RTU (Remote Termination Unit) จากนั้นข้อมูล ค่า realtime จะถูกประมวลนำมาแสดงผลบน MMI (Man-Machine Interface) เพื่อให้โอเปอเรเตอร์ รู้ถึงสภาพของกระบวนการ ณ ขณะนั้นๆ ค่า realtime ทุกๆ ค่าจะถูก update ได้ไม่เกินทุกๆ 2 วินาที

2.2.3 หน้าที่การทำงาน (Functionality)

ระบบแสดงกราฟสัญญาณแบบต่อเนื่อง(Trending)

Trending เป็นความสามารถในการพล็อตกราฟต่อเนื่องกันไปบนจอภาพเพื่อแสดงค่าสัญญาณจาก Data Server โดยอาจจะสามารถพล็อตสัญญาณได้หลายสัญญาณเช่น 8 – 24 สัญญาณ พร้อมกันในหน้าต่างเดียว เพื่อให้สามารถเปรียบเทียบสัญญาณที่พล็อตได้ และไม่จำกัดว่าจะสร้างหน้าต่างพล็อตจำนวนเท่าใด

Trending อาจมีความสามารถในการ ซูมสัญญาณที่พล็อต และหยุดการพล็อตเพื่อเลื่อนดูค่าที่ พล็อตในแต่ละช่วงเวลาได้ด้วยตัวของผู้ใช้งานเอง นอกจากนั้นการพล็อตอาจสามารถเลือกได้ว่าจะให้เป็นการพล็อตแบบใดเช่น Time plot, Logarithmic plot, Strip Chart, Bar Chart, Circular, X-Y plot เป็นต้น นอกจากนั้นบางผู้ผลิตยังสามารถนำค่า Historian หรือข้อมูลสัญญาณที่เก็บไว้ในฐานข้อมูลออกมาพล็อต ได้อีกด้วย

โดย Trending Module นี้อาจเป็นแบบ ActiveX Control คือสามารถนำไปใช้งานในแอปลิเคชั่นอื่นที่สนับสนุนการนำเข้า ActiveX ได้

ระบบแจ้งเตือน (Alarm)

SCADA Software ส่วนใหญ่มีระบบแจ้งเตือนโดย Alarm Display จะรับสัญญาณมาจาก Alarm DB ในฝั่ง SCADA Server โดย Alarm DB สามารถที่จะทำการกำหนดคอนฟิกูเรชั่นว่าจะนำสัญญาณตัวใดมาเป็นตัวพารามิเตอร์ในการแจ้งเตือนบ้าง และมีการแบ่งระดับของ Priority, Limit อย่างไร เป็นต้น

ระบบแจ้งเตือนยังสามารถที่จะเก็บข้อมูลการแจ้งเตือนไว้ในฐานข้อมูลประเภทต่าง ๆ ได้เช่น MS SQL Server, MS Access, Oracle, MS Excel เป็นต้น และบางยี่ห้อสามารถแสดงออกมาเป็นรายงานในรูปแบบตารางหรือ แผนภูมิได้อีกด้วย

การทำงานแบบ Automation

เป็นความสามารถที่ SCADA ทำหน้าที่ต่าง ๆ ตามที่กำหนด เช่น ส่งอีเมล์ แสดงข้อความแบบ Instance Messageบนหน้าจอ เปิดไปยังหน้าจออื่น ๆ เก็บข้อมูลลงฐานข้อมูล เปิดโปรแกรม หรือรันคำสั่งสคริปต์ เป็นต้น ตามสัญญาณที่ได้รับจาก Data Server และข้อกำหนดที่สร้างขึ้น

2.2.4 <u>ความรู้ความเข้าใจในหลักการของระบบโทรมาตร</u>

ระบบโทรมาตรหรือระบบ SCADA (Supervisory Control And Data Acquisition) เป็นระบบที่ใช้ในการรวบรวมและจัดการข้อมูล แสดงผลของการทำงานการตรวจวัดรับ-ส่งข้อมูล และควบคุมการทำงานของอุปกรณ์ โดยเฉพาะกับอุปกรณ์ที่อยู่ห่างไกลออกไปจากศูนย์ควบคุม และไม่มีเจ้าหน้าที่ปฏิบัติงานที่สถานีนั้นๆ (UnMan Station)

เนื่องจากระบบ SCADA เป็นระบบควบคุมและแสดงผลข้อมูลระยะไกล ซึ่งอาศัยโครงข่ายการสื่อสารและอุปกรณ์สื่อสารต่างๆ ในการติดต่อระหว่างศูนย์ควบคุม (สถานีหลัก) และสถานีสนามที่ทำการตรวจวัดข้อมูลที่ต้องการ ดังนั้นระบบโครงข่ายการสื่อสารจึงมีความสำคัญต่อการทำงานของระบบเป็นอย่างยิ่ง และจะต้องมีความเชื่อถือได้สูงมาก เพื่อให้ศูนย์ควบคุมสามารถติดตามสถานะต่างๆที่เกิดขึ้น และควบคุมอุปกรณ์ที่ติดตั้งอยู่ที่สถานีสนามได้ตลอดเวลา อย่างถูกต้องและต่อเนื่อง ตัวอย่างในการนำระบบ SCADA มาใช้งานเช่น การตรวจวัดการสูบจ่ายน้ำมันที่สถานีสูบจ่าย การตรวจวัดข้อมูลทางอุตุ-อุทกระยะไกล ซึ่งในงานของกรมชลประทาน ได้ทำการติดตั้งระบบดังกล่าวนี้ที่โครงการระบบโทรมาตรเขื่อนป่าสักชลสิทธิ์ และโครงการระบบโทรมาตรลุ่มน้ำท่าตะเภา จังหวัดชุมพร เป็นต้น

จากที่กล่าวไว้แล้วว่าระบบ SCADA เป็นระบบที่ใช้ในการควบคุม และแสดงผลข้อมูลในระยะไกล ดังนั้น ระบบ SCADA จึงทำหน้าที่เป็นหลายระดับ โดยศูนย์ควบคุม (สถานีหลัก) จะทำหน้าที่ในการส่งคำสั่งในการควบคุมไปที่หน่วยควบคุมระยะไกล (Remote Terminal Unit : RTU) ที่ติดตั้งอยู่ที่สถานีสนามของระบบ เพื่อให้ RTU ทำหน้าที่ในการควบคุมการทำงานของอุปกรณ์และประมวลผลข้อมูลที่สถานีสนามก่อนที่จะส่งรายงานไปยังศูนย์ควบคุม

การกำหนดให้สถานีสนาม (RTU) ทำการประมวลผลข้อมูลตามกระบวนการในการควบคุมหรือผลที่ได้จากการตรวจวัดให้เสร็จสิ้นแล้วจึงส่งข้อมูลหรือรายงานการประมวลผลไปยังศูนย์ควบคุม เป็นปัจจัยสำคัญและเป็นข้อได้เปรียบในการออกแบบระบบ SCADA (หรือระบบโทรมาตร) เนื่องจากการสื่อสารข้อมูลทางไกล โดยใช้สื่อ (Media) ประเภทใดก็ตาม จะมีข้อจำกัดในตัวเองในการรับ - ส่งข้อมูลที่มีปริมาณมากและมีระยะห่างไกล แม้ว่าการคำนวณออกแบบได้ดำเนินการให้มีความมั่นคงสูงอยู่แล้วก็ตาม ดังนั้น การออกแบบเพื่อลดปริมาณข้อมูล โดยให้ RTU ทำหน้าที่ในการควบคุมอุปกรณ์หรือประมวลผลข้อมูลในการตรวจวัดด้วยตัวเอง และศูนย์ควบคุม

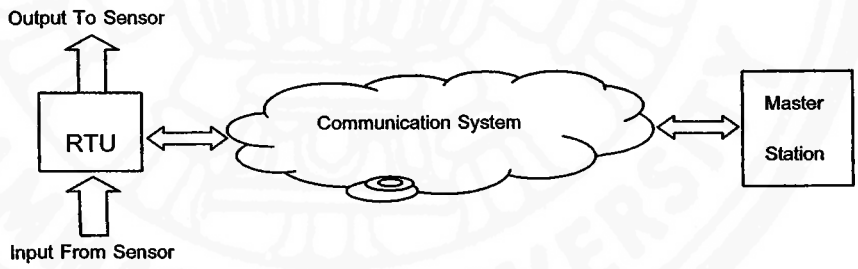
(สถานีหลัก) ทำหน้าที่เพียงส่งคำสั่งไปที่ RTU ให้ดำเนินการเท่านั้น จะทำให้ระบบ SCADA สามารถทำงานได้อย่างมีประสิทธิภาพและมีความน่าเชื่อถือ

ส่วนประกอบหลัก ๆ ของระบบ SCADA ดังแสดงในภาพที่ 2.2

- Remote Terminal Unit (หน่วยควบคุมระยะไกล)
- Communication System (ระบบสื่อสาร)
- Master Station (สถานีหลัก หรือศูนย์ควบคุม)

ภาพที่ 2.2

ส่วนประกอบหลักของระบบ SCADA



2.2.4.1 <u>หน่วยควบคุมระยะไกล (Remote Terminal Unit)</u>

Remote Terminal Unit (RTU) เป็นส่วนหนึ่งของระบบ SCADA ที่ถูกติดตั้งอยู่ที่สถานีสนามหรือสถานีตรวจวัดข้อมูล โดย RTU ในระบบ SCADA จะถูกต่อกับเครื่องมือวัดข้อมูลที่ต้องการตรวจวัด และรวบรวมข้อมูลที่สถานีสนาม (Local Station) ทั้งข้อมูลที่เป็นค่าต่อเนื่อง (Analog) หรือข้อมูลสถานะ (Digital) โดยต่ออุปกรณ์ตรวจวัดข้อมูลเข้ากับส่วน Input Unit ของ RTU แล้วนำเอาค่าที่ทำการตรวจวัดได้มาทำการประมวลผลและส่งกลับไปแสดงผลที่ศูนย์ควบคุมโดยผ่านระบบสื่อสาร

นอกจากนั้น RTU ยังจะต้องรับคำสั่งในการควบคุมอุปกรณ์จากศูนย์ควบคุม โดยต่ออุปกรณ์ที่ต้องการควบคุมเข้ากับส่วน Output Unit ของ RTU ซึ่งในการควบคุมต่าง ๆ ไม่ว่าจะเป็นการควบคุมการตรวจวัดข้อมูล หรือเป็นคำสั่งจากศูนย์ควบคุม จะต้องสร้างโปรแกรมในการติดต่อกับส่วน Input Unit เพื่ออ่านค่าที่ตรวจวัดได้และทำการประมวลผลค่านั้นให้ออกมาในรูปที่ต้องการโดยมีข้อกำหนดในการติดต่อสื่อสารระหว่างสถานีสนามกับศูนย์ควบคุม หรือสถานีสนามกับสถานีสนาม (Alternative Route) หรือผ่านสถานีทวนสัญญาณ โดยผ่านช่องสัญญาณในการสื่อสาร (Communication Port) ของ CPU ซึ่งโปรแกรมจะถูกเก็บลงใน Central Processing Unit (CPU) ของ RTU

ส่วนประกอบหลักของ RTU ที่สำคัญมีอยู่ 3 ส่วนดังต่อไปนี้

1) Central Processing Unit (CPU) ของ RTU หน้าที่หลัก คือ

- ทำหน้าที่ในการประมวลผลสัญญาณที่รับมาจาก Field Instrument โดยสัญญาณที่ได้รับมาจาก Field Instrument จะถูกต่อเข้ากับ I/O Module ตามมาตรฐานสัญญาณต่างๆ เช่น สัญญาณ Analog 4 – 20 mA. หรือสัญญาณ Digital On – Off โดยเมื่อ CPU รับสัญญาณจาก Module ที่ต่อผ่าน I/O Bus แล้วจะทำการประมวลผลโดยสัญญาณ Analog จะถูกแปลงเป็นค่า Digital โดยใช้ Analog to Digital Converter แล้วนำไปประมวลผลต่อไป

- ทำหน้าที่ในการประมวลผลข้อมูลต่างๆที่ได้รับจาก I/O Module เพื่อที่จะส่งข้อมูลให้กับศูนย์ควบคุม และทำหน้าที่แปลงคำสั่งจากศูนย์ควบคุมเพื่อใช้ในการควบคุมอุปกรณ์ต่าง ๆ ที่ติดตั้งอยู่ที่สถานีสนาม

- ทำหน้าที่ในการควบคุมระบบการสื่อสารระหว่าง RTU กับศูนย์ควบคุม โดยผ่าน Port ในการสื่อสาร ซึ่ง Port ที่ใช้ในการสื่อสารนั้นจะขึ้นอยู่กับสื่อที่ใช้เช่น สายสัญญาณต่าง ๆ Microwave GPRS ดาวเทียม หรือ วิทยุสื่อสาร

2) Input / Output Module (I/O Module) ทำหน้าที่ในการรับ - ส่งสัญญาณจาก CPU เพื่อส่งไปควบคุม หรืออ่านค่าจากอุปกรณ์เครื่องมือวัดต่างๆ ซึ่งสามารถแบ่ง Module ออกเป็น 4 ชนิดดังต่อไปนี้

- Analog Input Module เป็น Module ที่รับสัญญาณ Analog ที่เป็นสัญญาณไฟฟ้า 4 - 20 mA. หรือ 0 - 5 Volts ซึ่งเป็นมาตรฐานทางอุตสาหกรรมจากอุปกรณ์วัดค่าต่างๆ

- Digital Input Module เป็น Module ที่รับสัญญาณ Digital 0 หรือ 1 ตามลักษณะ Close or Open Switch

- Analog Output Module เป็น Module ที่ส่งสัญญาณ Analog ที่เป็นสัญญาณไฟฟ้า 4 - 20 mA. หรือ 0 - 5 Volts ซึ่งเป็นมาตรฐานทางอุตสาหกรรม

- Digital Output Module เป็น Module ที่ส่งสัญญาณ Digital 0 หรือ 1 ตามลักษณะ Close or Open Switch

ในการนำเอา RTU ไปต่อร่วมกับอุปกรณ์เครื่องมือวัดต่างๆ ได้อย่างถูกต้องจะต้องต่อ Input / Output Module ของ RTU ให้ถูกต้องตรงกับลักษณะของสัญญาณที่ทำการรับหรือส่งระหว่าง Input / Output Module ของ RTU กับอุปกรณ์เครื่องมือหรืออุปกรณ์ที่ใช้ในการควบคุมในกระบวนการต่างๆ ซึ่งจะขึ้นอยู่กับลักษณะสัญญาณ Analog หรือ Digital ตารางที่ 1 ลักษณะสัญญาณที่จะติดต่อกันระหว่าง Input / Output Module ของ RTU กับ Sensors ต่าง ๆ และได้แสดงลักษณะการต่ออุปกรณ์เครื่องมือวัดข้อมูล (Sensor) ตามภาพที่ 2.3

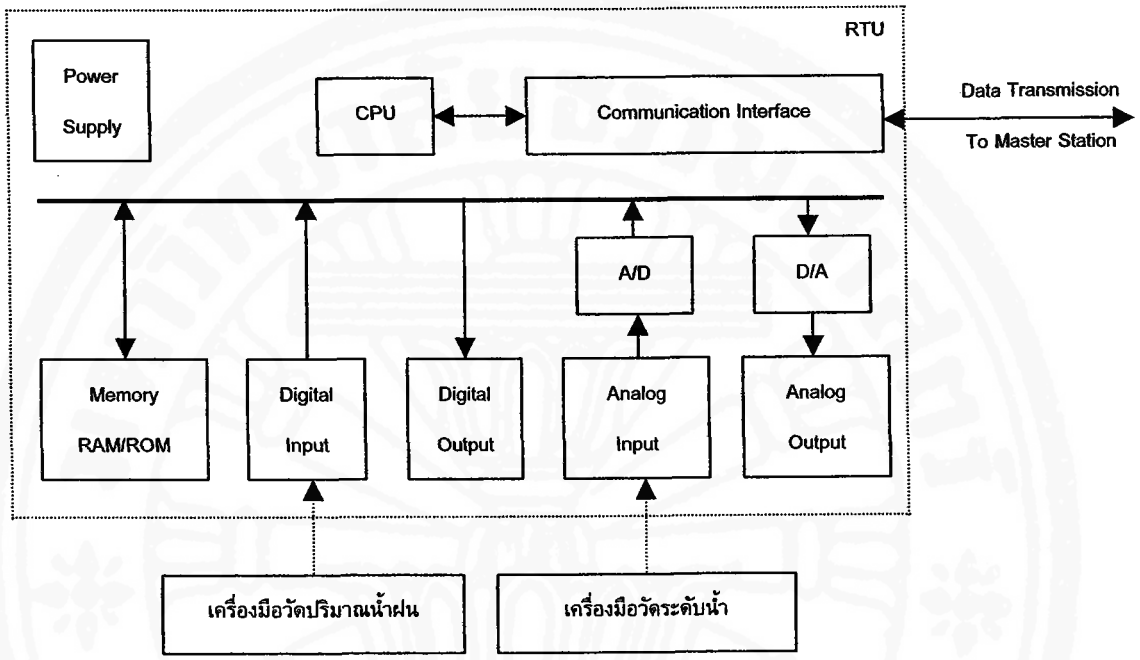
ตารางที่ 2.1

ลักษณะสัญญาณที่จะติดต่อกันระหว่าง Input / Output Module กับ Sensors

Input / Output Module	Sensors
Analog Input	เครื่องมือวัด (4 – 20 mA)
Digital Input	เครื่องมือวัดสถานะ (On-Off)
Analog Output	อุปกรณ์ควบคุม (4 – 20 mA)
Digital Output	อุปกรณ์ควบคุมสถานะ (On-Off)

ภาพที่ 2.3

การเชื่อมต่อระหว่าง RTU กับเครื่องมือวัดต่างๆ



3) Communication Port ทำหน้าที่เป็นช่องทางในการสื่อสารข้อมูลระหว่าง RTU กับศูนย์ควบคุมหรือ RTU ด้วยกัน และสามารถใช้ช่องทาง (Port) ในการสื่อสารมากกว่า 1 Port โดยจะต้องกำหนดชนิดของช่องทางในการสื่อสารและรวมถึงการกำหนดสื่อที่ใช้ด้วย เช่น วิทยุสื่อสาร ดาวเทียม Microwave เป็นต้น

2.2.4.2 ระบบสื่อสาร (Communication System)

Communication System ระบบการสื่อสารของระบบ SCADA ทำหน้าที่ในการสื่อสารเพื่อรับ-ส่งข้อมูลหรือคำสั่งระหว่าง RTU กับ RTU หรือระหว่าง RTU กับศูนย์ควบคุมซึ่งระบบสื่อสารของระบบ SCADA สามารถที่จะใช้สื่อ (Media) ต่าง ๆ ในการสื่อสารเช่น วิทยุ Microwave ดาวเทียม ข่ายสายโทรศัพท์ หรือ สายสัญญาณ (RS-232, RS-485) เป็นต้น การพิจารณาเลือกใช้สื่อ (Media) จะต้องคำนึงถึงจำนวนข้อมูล ระยะทางที่ใช้ในการสื่อสาร รวมไปถึงภูมิประเทศและค่าใช้จ่าย

ในหลักการทั่วไปของการสื่อสารข้อมูลของระบบ SCADA สามารถทำได้ 2 แบบคือ

- Time Mode คือการรับ – ส่งข้อมูลตามเวลาที่ผู้ใช้งานกำหนด เช่น กำหนดช่วงเวลาการรับ - ส่งข้อมูล ทุก ๆ 15 ,30 นาที หรือ 1 ชั่วโมง หรือสามารถที่จะกำหนด ณ เวลาใด ๆ เช่น ทุกๆ 7:00 น. ของทุกๆ วัน เป็นต้น

- Event Mode หมายถึงการรับ – ส่งข้อมูลเมื่อมีเหตุการณ์ผิดปรกติ หรือเหตุการณ์ที่ต้องให้ความสนใจเป็นพิเศษ เกิดขึ้นโดย RTU จะเป็นผู้ส่งข้อมูลให้กับสถานีหลักโดยไม่ต้องรอให้ถึงเวลาที่สถานีหลักเรียกถามข้อมูล

ระบบสื่อสารที่ใช้ในระบบ SCADA จะต้องคำนึงถึงความความเร็วและจำนวนข้อมูลที่ส่งผ่านสื่อ ซึ่งโดยปกติแล้วความเร็วที่ใช้ในการสื่อสารข้อมูลของระบบ SCADA จะอยู่ในระดับปานกลาง คือมี Baud rate จะอยู่ที่ประมาณ 300 – 2400 Bit/Sec. และเป็นระบบสื่อสารจะต้องมีความเชื่อถือได้อย่างสูง และในระบบจะต้องสามารถใช้สื่อได้หลายสื่อร่วมกัน เช่น วิทยุสื่อสาร ดาวเทียม GPRS Microwave และ สายสัญญาณ (RS-232 RS-485 เป็นต้น) โดยข้อมูลที่ส่งผ่านระบบสื่อสารเป็นได้ทั้งข้อมูลที่ตรวจวัด ข้อมูลที่ได้ทำการประมวลผล หรือเป็นคำสั่งในการควบคุมการทำงานของอุปกรณ์ เป็นต้น

สำหรับโปรโตคอลที่ใช้ในการสื่อสารข้อมูลระหว่าง RTU กับ RTU และ RTU กับ Control Center ที่เป็นรูปแบบที่กำหนดโดย OSI (Open Systems Interconnection) ประกอบไปด้วย 7 Layers ดังต่อไปนี้

- Physical Layer
- Link Layer
- Network Layer
- Transportation Layer
- Session Layer
- Presentation Layer
- Application Layer

2.2.4.3 สถานีหลัก (Master Station) หรือศูนย์ควบคุม (Control Center)

Master Station ทำหน้าที่ในการรวบรวมและจัดการข้อมูล รวมไปถึงการควบคุมระบบทั้งหมดเพื่อนำเอาข้อมูลจาก RTU ทุกตัวในระบบมาทำการประมวลผลเพื่อให้สามารถที่จะควบคุมกระบวนการต่างๆ หรือแสดงผลข้อมูลของ RTU แต่ละตัวให้เป็นไปตามที่ต้องการ นอกจากนั้น Master Station ยังจะต้องทำหน้าที่จัดการระบบการสื่อสารของระบบ SCADA เพื่อนำเอาข้อมูลจาก RTU มาทำการประมวลผลตามเวลาที่กำหนด (Time Mode) โดยศูนย์ควบคุมจะทำหน้าที่ในการจัดลำดับในการเรียกถามข้อมูลจาก RTU แต่ละตัว (Polling) หรือทำหน้าที่ในการรอรับข้อมูลที่อาจจะเกิดขึ้นเนื่องจากความผิดปรกติบางอย่างที่ RTU ซึ่งเป็นการรายงานทันทีที่เกิดเหตุการณ์ขึ้น (Event Mode) โดยไม่ต้องรอให้ Master Station เรียกถามข้อมูล

ในปัจจุบันระบบ SCADA ได้นำเอาระบบ Computer เข้ามาใช้และเนื่องจากผู้ผลิตระบบ SCADA อาจจะไม่ได้ผลิต Computer และผู้ผลิต Computer ก็อาจจะไม่ได้ผลิตระบบ SCADA ดังนั้นในการที่จะนำเอาข้อมูลต่างๆจาก RTU แต่ละตัวในระบบมาแสดงผลข้อมูลหรือทำรายงานโดยใช้ระบบ Computer นั้นจะต้องทำการแปลงโปรโตคอลของระบบ SCADA ให้เป็นโปรโตคอลมาตรฐานที่สามารถที่จะติดต่อกับ Computer ได้ดังนั้นจึงสามารถแบ่ง Master Station ออกเป็น 2 ส่วนคือ

- Field Interface Unit (FIU) ทำหน้าที่เป็น Gateway ซึ่งทำหน้าที่ในการแปลงโปรโตคอลซึ่งในที่นี้ใช้ MODBUS โปรโตคอลซึ่งเป็นโปรโตคอลมาตรฐานที่ใช้ในวงการอุตสาหกรรมอย่างแพร่หลาย

- Computer Control Center ทำหน้าที่ในการรวบรวม แสดงผลข้อมูลและรายงานผลข้อมูลนอกจากนั้นยังทำการประมวลผลข้อมูลที่ได้รับจาก RTU แต่ละตัวให้เป็นไปตามความต้องการของระบบควบคุมและแสดงผลทั้งระบบซึ่งในปัจจุบันระบบ Computer ที่นำมาต่อกับระบบ SCADA เป็นได้ทั้ง Stand Alone Computer หรือ Network Computer

1) **Field Interface Unit**

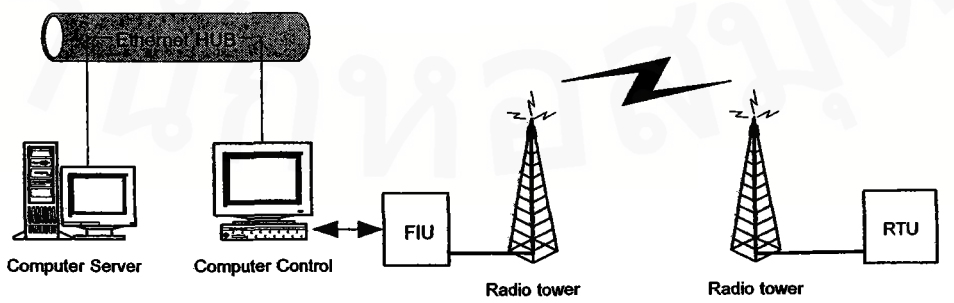
Field Interface Unit ทำหน้าที่เสมือนเป็น Gateway ซึ่งทำหน้าที่ในการแปลงโปรโตคอลที่สามารถที่จะติดต่อกับ Computer เนื่องจากบริษัทที่ผลิตระบบ SCADA อาจจะใช้โปรโตคอลในการสื่อสารของบริษัทเองซึ่งอาจจะทำให้ไม่สามารถติดต่อกับระบบ Computer ได้ และบริษัทที่ผลิต Computer ก็ไม่ได้ผลิตระบบ SCADA ดังนั้นในการที่จะนำระบบทั้ง 2 ระบบมาต่อเชื่อมกันจึงต้องใช้ Gateway เป็นตัวต่อเชื่อมซึ่งกันและกัน ในที่นี้ใช้ MODBUS โปรโตคอลในการติดต่อสื่อสารกับ Computer ซึ่ง MODBUS โปรโตคอลเป็นโปรโตคอลมาตรฐานที่มีใช้อย่างแพร่หลายในวงการอุตสาหกรรม

2) Computer Control Center

Computer Control Center ในระบบ SCADA ทำหน้าที่ในการรวบรวมและจัดการระบบ SCADA ทั้งหมด โดยทำการรวบรวมข้อมูลที่ได้รับจาก RTU ทุกตัวในระบบโดยผ่าน Field Interface Unit (FIU) ซึ่งจะทำการแปลงโปรโตคอล และทำการจัดการระบบสื่อสารทั้งหมดของระบบ SCADA ทั้ง Time Mode Transmission และ Event Mode Transmission นอกจากนั้นยังทำหน้าที่ในการแสดงผลข้อมูลของ RTU ทุกตัวในระบบ SCADA และทำการเก็บข้อมูลที่ได้จากการประมวลผลข้อมูลทั้งระบบลงไว้ในฐานข้อมูลเพื่อเก็บเอาไว้ใช้ในการวิเคราะห์ข้อมูลต่อไป ซึ่ง Computer Control Center สามารถเป็นได้ทั้ง Computer Network ดังแสดงในภาพที่ 2.4 หรือ Stand Alone ดังแสดงในภาพที่ 2.5 ตามลำดับ

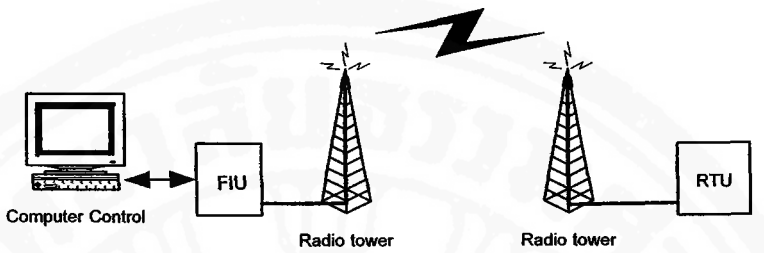
ภาพที่ 2.4

Network Computer ของระบบ SCADA ที่ห้องควบคุม



ภาพที่ 2.5

Stand Alone Computer ของระบบ SCADA ที่ห้องควบคุม



จากภาพที่ 2.4 และ ภาพที่ 2.5 เป็นรูปแสดงระบบ SCADA ที่ใช้ Computer ที่ Master Station เป็น Network Computer และ Stand Alone Computer ตามลำดับ ซึ่ง Computer จะทำหน้าที่ในการจัดการระบบเช่น รวบรวมข้อมูลต่างๆที่รับมาจาก RTU และทำการประมวลผลข้อมูลของระบบทั้งหมดและทำหน้าที่ในการจัดการกับระบบสื่อสารทั้งหมดของระบบ SCADA โดยข้อมูลทั้งหมดที่ส่งมาที่ Computer จะส่งผ่าน Field Interface Unit ซึ่งทำหน้าที่ในการแปลงโปรโตคอลในการสื่อสารข้อมูล นอกจากนั้น Computer ยังทำหน้าที่ในการจัดเก็บข้อมูลต่างๆ ลงฐานข้อมูลเพื่อเก็บข้อมูลเพื่อใช้เป็นฐานข้อมูลในการวิเคราะห์และใช้ในเชิงสถิติ

สรุปลักษณะการทำงานของระบบโทรมาตร หรือระบบ SCADA

1) เป็นระบบที่ใช้ตรวจวัดข้อมูลและใช้ควบคุมการทำงานของอุปกรณ์เครื่อง พร้อมทั้งรายงานข้อมูลทางไกลแบบอัตโนมัติ

2) การตรวจวัดข้อมูลแบบ Analog และแบบ Digital

3) ระบบควบคุมการส่งข้อมูลแบบ Self Reporting Mode และ Interrogation Mode

4) ระบบการส่งข้อมูลเป็นแบบ Event หรือ Time Mode

5) ระบบสามารถตรวจสอบการทำงานด้วยตนเอง (Self Diagnosis)

6) การทำงานเป็นแบบ Automatic Real Time System

7) สามารถขยายการตรวจวัดข้อมูล (Sensor) ที่สถานีสนามและโครงข่ายสถานีตรวจวัด (Station Network) ได้โดยไม่มีผลกระทบต่อการทำงานประจำ (Routine Performance)

ความเข้าใจในอุปกรณ์ตรวจวัดข้อมูล

ในการนำระบบ SCADA มาใช้ในการตรวจวัดข้อมูลอุตุ-อุทกวิทยานั้นได้มีการนำเอาเครื่องมือตรวจวัด (Sensors) มาต่อกับ Input / Output Module ของ RTU ซึ่งเครื่องมือวัดที่นำมาใช้ได้แก่

เครื่องมือวัดปริมาณน้ำฝน

การวัดปริมาณน้ำฝน จะใช้เครื่องมือแบบถาดกระดก (Tipping Bucket) โดย Bucket จะถูกต่อเข้ากับ Switch และนำเอาสัญญาณจาก Switch มาต่อเข้ากับ Digital Input ของ RTU ซึ่งลักษณะของสัญญาณเป็นสัญญาณ Pulse โดยปริมาณน้ำฝนที่ทำให้เกิดสัญญาณ Pulse 1 สัญญาณหรือ 1 ครั้ง จะมีค่า 0.2, 0.5, 1.0 หรือ 2 มิลลิเมตร ตามข้อกำหนดของเครื่องวัดปริมาณน้ำฝน ซึ่งในข้อกำหนดของโครงการนี้ให้ทำการตรวจวัดทุก 1 มิลลิเมตร

เครื่องวัดปริมาณน้ำฝน แบบ Tipping Bucket เป็นเครื่องมือที่เหมาะสมกับการใช้งานของระบบโทรมาตร

เครื่องมือวัดระดับน้ำ

เครื่องมือวัดระดับน้ำโดยปกติจะวัดระดับความลึกของระดับน้ำในแม่น้ำ โดยค่าที่วัดได้จะถูกแปลงเป็นค่าสัญญาณมาตรฐานซึ่งอาจจะเป็น 0 - 5 Volts หรือ 4 - 20 mA เช่น เครื่องมือวัดระดับน้ำ 0 - 10 เมตร 4 - 20 mA หมายความว่าเครื่องมือวัดระดับน้ำจะส่งสัญญาณ ระดับน้ำ 0 เมตร ด้วยกระแสไฟฟ้า 4 mA และที่ 10 เมตร ด้วยกระแสไฟ 20 mA เป็นต้น

ในการนำเครื่องมือวัดระดับน้ำมาต่อกับ RTU ทำได้โดยต่อสัญญาณ 4 – 20 mA เข้ากับ Analog Input Module ของ RTU ซึ่ง Analog Input Module ก็จะทำการแปลงค่า Analog เป็น Digital โดยใช้ Analog To Digital Converter เพื่อให้ CPU ของ RTU สามารถนำเอาค่า Digital ดังกล่าวเพื่อนำเอาไปประมวลผลต่อไป สำหรับข้อกำหนดของเครื่องวัดระดับน้ำของโครงการนี้มีอยู่ 2 แบบ ได้แก่ แบบลูกลอย (Float Gauge) จำนวน 9 สถานี และแบบแรงดันก๊าซ (Bubble Gauge) จำนวน 1 สถานี และมีพิสัยการวัด (Range) ที่แตกต่างตามความลึกของแต่ละสถานีซึ่งมีค่าไม่เท่ากัน ซึ่งเครื่องวัดระดับน้ำทั้งสองแบบเป็นเครื่องมือที่เหมาะสมกับการใช้งานของระบบโทรมาตร

2.3 ทฤษฎีเกี่ยวข้องกับระบบเน็ตเวิร์ค (NETWORK)

2.3.1 ความหมายของเครือข่าย (Network)

ในปัจจุบันมีการนำคอมพิวเตอร์เข้ามาใช้งานในหน่วยงานประเภทต่างๆ มากมาย ซึ่งมีผลทำให้การทำงานในองค์กรหรือหน่วยงาน สามารถทำงานได้อย่างเป็นระบบ และสามารถพัฒนาการทำงานได้อย่างต่อเนื่อง ซึ่งการนำคอมพิวเตอร์เข้ามาใช้ในองค์กรหรือหน่วยงานก็เริ่มมีการพัฒนาขึ้นแทนที่จะใช้ในลักษณะหนึ่งเครื่องต่อหนึ่งคน ก็ให้มีการใช้เครื่องคอมพิวเตอร์ อุปกรณ์ และข้อมูลต่างๆร่วมกัน โดยนำคอมพิวเตอร์มาต่อเชื่อมกัน ซึ่งเรียกสิ่งนี้ว่า "ระบบแลน" ความจริงแล้วระบบแลนถูกนำมาใช้เป็นเวลานานแล้ว แต่จะจำกัดการใช้งานอยู่ในเฉพาะกลุ่มคนบางกลุ่มเท่านั้น แต่ในปัจจุบันระบบแลนถูกนำมาใช้อย่างแพร่หลายมากขึ้น จึงจำเป็นต้องมีการจัดระบบการใช้งาน นิยามความหมายของเน็ตเวิร์กสามารถจำกัดได้มากมายหลายวิธี ดังนั้นระบบเครือข่าย หรือเน็ตเวิร์ก (Network) คือ ระบบที่มีคอมพิวเตอร์ ตั้งแต่ 2 เครื่องขึ้นไป เชื่อมต่อกันอยู่

2.3.2 ความสำคัญและประโยชน์ของระบบเครือข่าย ในด้านต่าง ๆ ดังนี้

1. สามารถใช้อุปกรณ์ร่วมกัน (Peripheral sharing)
2. การใช้ซอฟต์แวร์ร่วมกัน (Software sharing)
3. การใช้ข้อมูลร่วมกัน (File sharing)
4. การสื่อสารระหว่างบุคคล (Electronic communication)
5. ค่าใช้จ่าย (Cost)
6. การบริหารเครือข่าย (Network Management)
7. ระบบรักษาความปลอดภัย (Security system)
8. เสถียรภาพของระบบ (Stability)
9. การสำรองข้อมูล (Back up

2.3.3 ประเภทของเครือข่าย

ในปัจจุบัน เรานิยมจัดประเภทของเครือข่ายตามขนาดทางภูมิศาสตร์ที่ระบบเครือข่ายนั้นครอบคลุมอยู่ ซึ่งสามารถแบ่งได้เป็น 3 ระบบ ดังนี้

1. **ระบบเครือข่ายคอมพิวเตอร์ระยะใกล้** (Local Area Network **หรือ** LAN) เป็นระบบเครือข่ายระดับท้องถิ่น มีขนาดเล็ก ครอบคลุมพื้นที่จำกัด เชื่อมโยงกันในรัศมีใกล้ ๆ ในเขตพื้นที่เดียวกัน เช่น ในอาคารเดียวกัน ห้องเดียวกัน ภายในตึกเดียวกันหรือหลาย ๆ ตึกใกล้กัน เป็นต้น โดยไม่ต้องเชื่อมการติดต่อกับองค์การโทรศัพท์หรือการสื่อสารแห่งประเทศไทย ระบบแลนมีประโยชน์คือ สามารถทำให้เครื่องคอมพิวเตอร์หลาย ๆ เครื่องที่เชื่อมต่อกัน สามารถส่งข้อมูลแลกเปลี่ยนกันได้อย่างสะดวก รวดเร็ว และยังสามารถใช้ทรัพยากรร่วมกันได้อีกด้วย ระบบเครือข่าย LAN จะเป็นระบบเครือข่ายที่มีการใช้งานในองค์กรต่าง ๆ มากที่สุด

2. **ระบบเครือข่ายคอมพิวเตอร์ระดับเมือง** (Metropolitan Area Network **หรือ** MAN) เป็นระบบเครือข่ายระดับเมือง คือมีการเชื่อมโยงกันในพื้นที่ ที่กว้างไกลกว่าในระบบ LAN อาจจะเชื่อมโยงกันภายในจังหวัด โดยมีลักษณะการเชื่อมโยงคอมพิวเตอร์ที่มีระยะห่างไกลกันในช่วง 5-40 กิโลเมตร ผ่านสายสื่อสารประเภทต่าง ๆ เช่น เส้นใยแก้วนำแสง สายเคเบิลหรือสายโคแอกเชียล

3. **ระบบเครือข่ายระยะไกล** (Wide Area Network **หรือ** WAN) เป็นระบบเครือข่ายระดับไกล คือ จะเป็นเครือข่ายที่เชื่อมคอมพิวเตอร์หรืออุปกรณ์ที่อยู่ห่างไกลกันเข้าด้วยกัน อาจจะต้องเป็นการติดต่อสื่อสารกันในระดับประเทศ ข้ามทวีปหรือทั่วโลกก็ได้ ตัวอย่างเช่น อินเทอร์เน็ตถือว่าเป็นเครือข่าย WAN ประเภทหนึ่ง แต่เป็นเครือข่ายสาธารณะ ที่ไม่มีใครเป็นเจ้าของทั้งหมด

2.3.4 <u>สถาปัตยกรรมของระบบเครือข่าย</u>

สถาปัตยกรรมของระบบเครือข่าย (Network Architecture) หรือโทโปโลยี (Topology) คือลักษณะทาง กายภาพ (ภายนอก) ของเครือข่ายซึ่งหมายถึง ลักษณะของการเชื่อมโยงสายสื่อสารเข้ากับอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ภายในเครือข่ายด้วยกัน

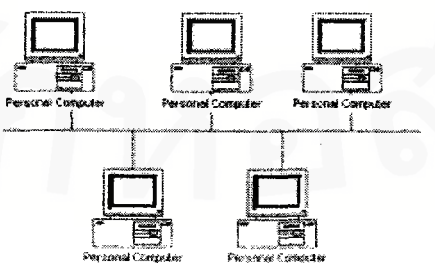
รูปแบบของโทโปโลยีของเครือข่ายหลักๆ มีดังต่อไปนี้

1. โทโปโลยีแบบบัส (Bus Topology)

เป็นโทโปโลยีที่ได้รับความนิยมใช้กันมากที่สุดมาตั้งแต่อดีตจนถึงปัจจุบัน ลักษณะการทำงานของเครือข่ายโทโปโลยีแบบบัส คืออุปกรณ์ทุกชิ้นหรือโหนดทุกโหนด ในเครือข่ายจะต้องเชื่อมโยงเข้ากับสายสื่อสารหลักที่เรียกว่า"บัส" (BUS) เมื่อโหนดหนึ่งต้องการจะส่งข้อมูลไปให้ยังอีกโหนด หนึ่งภายในเครือข่าย จะต้องตรวจสอบให้แน่ใจก่อนว่าบัสว่างหรือไม่ ถ้าหากไม่ว่างก็ไม่สามารถจะส่งข้อมูลออกไปได้ ทั้งนี้เพราะสายสื่อสารหลักมีเพียงสายเดียว ในกรณีที่มีข้อมูลวิ่งมาในบัส ข้อมูลนี้จะวิ่งผ่านโหนดต่างๆ ไปเรื่อยๆ ในขณะที่แต่ละโหนดจะคอยตรวจสอบข้อมูลที่ผ่านมาว่าเป็นของตนเองหรือไม่ หากไม่ใช่ ก็จะปล่อยให้ข้อมูลวิ่งผ่านไป แต่หากเลขที่อยู่ปลายทาง ซึ่งกำกับมากับข้อมูลตรงกับเลขที่อยู่ของตน โหนดนั้นก็จะรับข้อมูลเข้าไป

ภาพที่ 2.6

โทโปโลยีแบบบัส



ข้อดีข้อเสียของโทโปโลยีแบบบัส

ข้อดี

1. ใช้สายส่งข้อมูลน้อยและมีรูปแบบที่ง่ายในการติดตั้ง ทำให้ลดค่าใช้จ่ายในการติดตั้งและบำรุงรักษา
2. สามารถเพิ่มอุปกรณ์ชิ้นใหม่เข้าไปในเครือข่ายได้ง่าย

ข้อเสีย

1. ในกรณีที่เกิดการเสียหายของสายส่งข้อมูลหลัก จะทำให้ทั้งระบบทำงานไม่ได้
2. การตรวจสอบข้อผิดพลาดทำได้ยาก ต้องทำจากหลาย ๆจุด

2. โทโปโลยีแบบวงแหวน (Ring Topology)

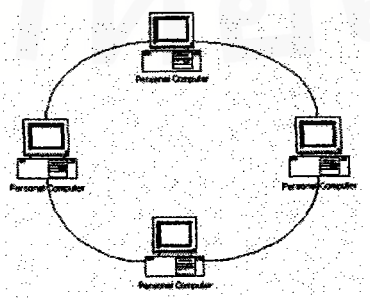
เป็นการเชื่อมต่ออุปกรณ์ต่างๆ เข้ากันเป็นวงกลม ข้อมูลข่าวสารจะถูกส่งจากโหนดหนึ่งไปยังอีกโหนดหนึ่ง วนอยู่ในเครือข่ายไปใน ทิศทางเดียวเหมือนวงแหวน (ในระบบเครือข่ายรูปวงแหวนบางระบบสามารถส่งข้อมูลได้สองทิศทาง)

ในแต่ละโหนดหรือสถานี จะมีรีพีตเตอร์ประจำโหนด 1 ตัว ซึ่งจะทำหน้าที่เพิ่มเติมข่าวสารที่จำเป็นต่อการ สื่อสาร ในส่วนหัวของแพ็กเกจข้อมูล

สำหรับการส่งข้อมูลออกจากโหนด และมีหน้าที่รับแพ็กเกจข้อมูลที่ไหลผ่านมาจากสายสื่อสาร เพื่อตรวจสอบว่าเป็นข้อมูลที่ส่งมาให้โหนดตนหรือไม่ ถ้าใช่ก็จะคัดลอกข้อมูลทั้งหมดนั้นส่งต่อไปให้กับโหนดของตน แต่ถ้าไม่ใช่ก็จะปล่อยข้อมูลนั้นไปยังรีพีตเตอร์ของโหนดถัดไป

ภาพที่ 2.7

โทโปโลยีรูปวงแหวน



ข้อดีข้อเสียของโทโปโลยีรูปวงแหวน

ข้อดี

1. การส่งข้อมูลสามารถส่งไปยังผู้รับหลาย ๆ โหนดพร้อมกันได้ โดยกำหนดตำแหน่งปลายทางเหล่านั้นลง ในส่วนหัวของแพ็กเกจข้อมูล รีพีตเตอร์ของแต่ละโหนดจะตรวจสอบเองว่ามีข้อมูลส่งมาให้ที่โหนดตนเองหรือไม่
2. การส่งข้อมูลเป็นไปในทิศทางเดียวกัน จึงไม่มีการชนกันของสัญญาณข้อมูล

ข้อเสีย

1. ถ้ามีโหนดใดโหนดหนึ่งเกิดเสียหาย ข้อมูลจะไม่สามารถส่งผ่านไปยังโหนดต่อไปได้ และจะทำให้เครือข่ายทั้ง เครือข่ายขาดการติดต่อสื่อสาร
2. เมื่อโหนดหนึ่งต้องการส่งข้อมูล โหนดอื่น ๆ ต้องมีส่วนร่วมด้วย ซึ่งจะทำให้เสียเวลา

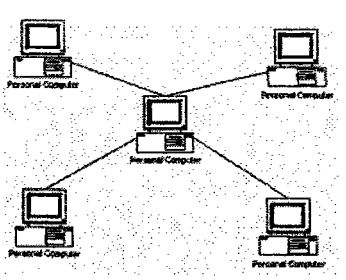
3. โทโปโลยีรูปดาว (Star Topology)

เป็นการเชื่อมโยงการติดต่อสื่อสารที่มีลักษณะคล้ายรูปดาว หลายแฉก โดยมีสถานีกลาง หรือฮับ (Hub) เป็นจุดผ่านการติดต่อกันระหว่างทุกโหนดในเครือข่าย สถานีกลางจึงมีหน้าที่เป็นศูนย์ควบคุมเส้นทางการสื่อสาร ทั้งหมด นอกจากนี้สถานีกลางยังทำหน้าที่เป็นศูนย์กลางคอยจัดส่งข้อมูลให้กับโหนดปลายทางอีกด้วย

การสื่อสารภายใน เครือข่ายแบบดาว จะเป็นแบบ 2 ทิศทางโดยจะอนุญาตให้มีเพียงโหนดเดียวเท่านั้นที่สามารถส่งข้อมูลเข้าสู่เครือข่ายได้ จึงไม่มีโอกาสที่หลายๆ โหนดจะส่งข้อมูลเข้าสู่เครือข่ายในเวลาเดียวกัน เพื่อป้องกันการชนกันของสัญญาณข้อมูล เครือข่ายแบบดาว เป็นโทโปโลยีอีกแบบหนึ่งที่เป็นที่นิยมใช้กันในปัจจุบัน

ภาพที่ 2.8

โทโปโลยีแบบดาว



ข้อดีและข้อเสียของโทโปโลยีแบบดาว

ข้อดี

1. การติดตั้งเครือข่ายและการดูแลรักษาทำได้ง่าย
2. หากมีโหนดใดเกิดความเสียหายก็สามารถตรวจสอบได้ง่าย และเนื่องจากใช้อุปกรณ์ 1 ตัวต่อสายส่งข้อมูล 1 เส้น ทำให้การเสียหายของอุปกรณ์ใดในระบบไม่กระทบต่อการทำงานของจุดอื่นๆ ในระบบ
3. ง่ายในการให้บริการเพราะโทโปโลยีแบบดาวมีศูนย์กลางทำหน้าที่ควบคุม

ข้อเสีย

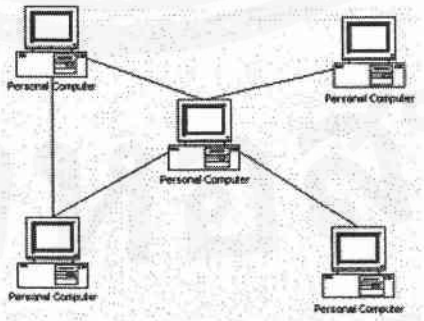
1. ถ้าสถานีกลางเกิดเสียขึ้นมาจะทำให้ทั้งระบบทำงานไม่ได้
2. ต้องใช้สายส่งข้อมูลจำนวนมากกว่าโทโปโลยีแบบบัส และ แบบวงแหวน

4. โทโปโลยีแบบผสม (Hybridge Topology)

เป็นเครือข่ายการสื่อสารข้อมูลแบบผสมระหว่างเครือข่ายแบบใดแบบหนึ่ง หรือมากกว่า เพื่อความถูกต้องแน่นอน ทั้งนี้ขึ้นอยู่กับความต้องการและภาพรวมขององค์กร

ภาพที่ 2.9

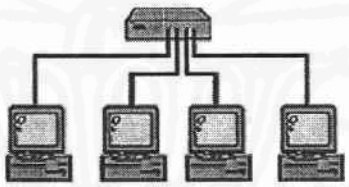
โทโปโลยีแบบผสม



2.3.5 ลักษณะการทำงานของ LAN

LAN แบ่งลักษณะการทำงานได้เป็น 2 ประเภทคือ peer to peer และ client-server

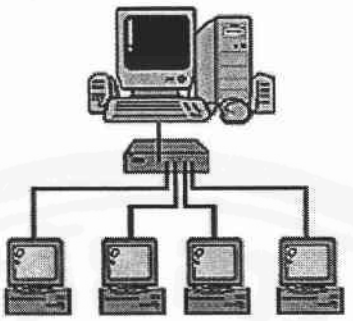
1. **แบบ** peer to peer เครื่องคอมพิวเตอร์แต่ละเครื่องจะสามารถแบ่งทรัพยากรต่างๆ ไม่ว่าจะเป็นไฟล์หรือเครื่องพิมพ์ซึ่งกันและกันภายในเน็ตเวิร์ก เครื่องแต่ละเครื่องจะทำงานในลักษณะทีทัดเทียมกัน การเชื่อต่อแบบนี้มักทำในระบบที่มีขนาดเล็กๆ เช่น หน่วยงานขนาดเล็กที่มีเครื่องทีทำการเชื่อมต่อกันประมาณไม่เกิน 10 เครื่อง เน็ตเวิร์กประเภทนี้สามารถจัดตั้งได้ง่ายๆ ด้วยซอฟแวร์ธรรมดาๆ เช่น Windows 95 และ 98 โดยเครื่องคอมพิวเตอร์ในระบบจะสามารถเป็นได้ทั้งเครื่องลูกข่าย (client) และเครื่องผู้ให้บริการ (server) โดยขึ้นอยู่กับว่าขณะใดขณะหนึ่งเครื่องไหนเป็นผู้ร้องขอทรัพยากรหรือว่าเป็นผู้แบ่งปันทรัพยากร



ข้อดีของการต่อแบบ Peer to Peer

- ประหยัดค่าใช้จ่ายเมื่อเทียบกับการต่อ Network แบบอื่น ๆ
- สามารถแชร์ข้อมูล เครื่องพิมพ์ ของแต่ละเครื่องได้
- ง่ายในการติดตั้ง และสามารถขยายต่อไปในอนาคตได้ดี

2. **แบบ** client-server เป็นระบบที่เครื่องคอมพิวเตอร์เครื่องหนึ่ง ต่อเข้ากับคอมพิวเตอร์อีกเครื่องหนึ่งเป็นอย่างน้อย ซึ่งเครื่องที่เชื่อมต่อด้วยนี้จะมีขนาดใหญ่ มีโปรเซสเซอร์ตั้งแต่หนึ่งตัวขึ้นไป ซึ่งอาจเป็นไปได้ทั้งเครื่องในระดับ Pentium หรือ RISC(Reduced Instruction Set Computing เช่น DEC Alpha AXP) แล้วก็ใช้ระบบปฏิบัติการที่เป็นเน็ตเวิร์ก (NOS หรือ Network Operating System)



Client / Server

ข้อดีของการต่อแบบ Client / Server

- สามารถแชร์ข้อมูล เครื่องพิมพ์ ของแต่ละเครื่องได้
- มีระบบ Security ที่ดีมาก
- รับส่งข่าวสารในลักษณะของ Email ได้ดี
- สามารถจัดสรร แบ่งปันการใช้ทรัพยากรได้จากจุดศูนย์กลาง

ประเภทของเครือข่ายคอมพิวเตอร์แบ่งตาม Bangwidth : แบบเบสแบนด์ และบรอดแบนด์

1. ระบบเครือข่ายแบบเบสแบนด์ (Baseband)

เป็นการสื่อสารข้อมูลที่สายสัญญาณหรือตัวกลางในการส่งผ่านสัญญาณสามารถส่งได้เพียงหนึ่งสัญญาณ ในเวลาขณะใดขณะหนึ่งเท่านั้น

นั่นคืออุปกรณ์ที่ใช้งานสายสัญญาณขณะนั้นจะครอบครองช่องสัญญาณทั้งหมด โดยอุปกรณ์อื่นจะไม่สามารถร่วมใช้งานได้เลย เช่น ระบบโทรศัพท์ เป็นต้น

การสื่อสารระหว่างคอมพิวเตอร์ส่วนมากจะเป็นการสื่อสารแบบนี้ รวมทั้งการสื่อสารระหว่างคอมพิวเตอร์ และอุปกรณ์อื่นๆ

2. ระบบเครือข่ายแบบบรอดแบนด์ (Broadband)

เป็นการสื่อสารข้อมูลที่ตัวกลางในการส่งผ่านสัญญาณ สามารถส่งสัญญาณผ่านได้หลายๆ ช่องทางพร้อมๆ กัน โดยใช้วิธีแบ่งช่องความถี่ออกจากกัน ทำให้อุปกรณ์ต่างๆ สามารถสื่อสารกันโดยใช้ช่องความถี่ของตนเองผ่านตัวกลางเดียว ตัวอย่างเช่น ระบบเครือข่ายเคเบิลทีวี เป็นต้น

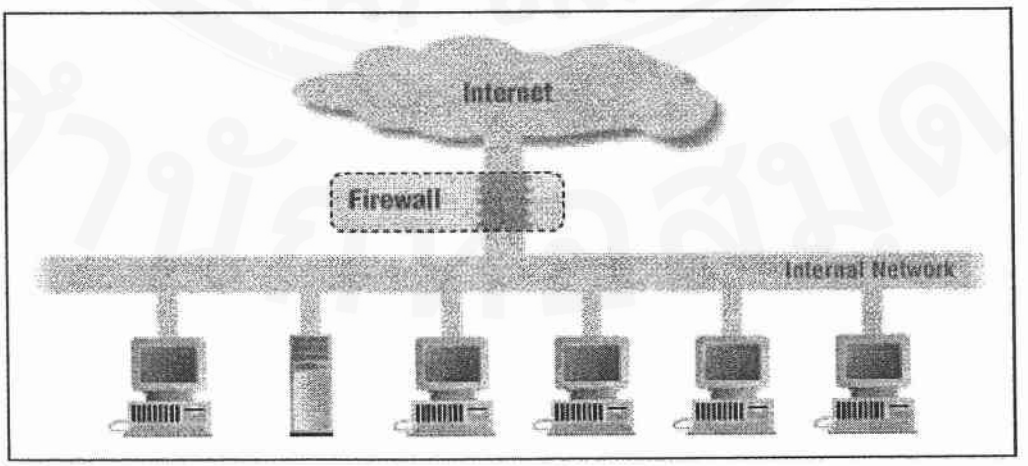
2.3.6 ความหมายของไฟร์วอลล์ (Firewall)

ในความหมายทางด้านการก่อสร้างแล้ว ไฟร์วอลล์ จะหมายถึง กำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ส่วนทางด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆ กันก็คือ เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเน็ตเวิร์กภายนอกนั่นเอง

ไฟร์วอลล์ เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกหรือเน็ตเวิร์กที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์กภายในหรือเน็ตเวิร์กที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราเตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์กประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้

ภาพที่ 2.10

ไฟร์วอลล์กั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายใน



การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้เซอร์วิสอะไรได้บ้าง จากที่ไหน เป็นต้น

สิ่งที่ไฟร์วอลล์ช่วยได้

ไฟร์วอลล์สามารถช่วยเพิ่มความปลอดภัยให้กับระบบได้โดย

1. บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้เซอร์วิสชนิดใด
2. ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเน็ตเวิร์กภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของเน็ตเวิร์ก (Network-based Security)
3. บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์กได้อย่างมีประสิทธิภาพ
4. ป้องกันเน็ตเวิร์กบางส่วนจากการเข้าถึงของเน็ตเวิร์กภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้เซอร์วิส (เช่นถ้ามีเว็บเซิร์ฟเวอร์) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามากรณีเช่นนี้เราสามารถใช้ไฟร์วอลล์ช่วยได้
5. ไฟร์วอลล์บางชนิด [1] สามารถป้องกันไวรัสได้ โดยจะทำการตรวจไฟล์ที่โอนย้ายผ่านทางโปรโตคอล HTTP, FTP และ SMTP

อะไรที่ไฟร์วอลล์ช่วยไม่ได้

ถึงแม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความปลอดภัยให้กับเน็ตเวิร์กได้มากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่อย่าลืมว่าสิ่งเหล่านี้ไม่สามารถป้องกันได้จากการใช้ไฟร์วอลล์

1. อันตรายที่เกิดจากเน็ตเวิร์กภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเน็ตเวิร์กเองไม่ได้ผ่านไฟร์วอลล์เข้ามา

2. อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์ เช่นการ Dial-up เข้ามายังเน็ตเวิร์กภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์

3. อันตรายจากวิธีใหม่ๆ ที่เกิดขึ้น ทุกวันนี้มีการพบช่องโหว่ใหม่ๆ เกิดขึ้นทุกวัน เราไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วก็หวังให้มันปลอดภัยตลอดไป เราต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ

4. ไวรัส ถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆ โปรโตคอล

2.3.7 <u>ชนิดของไฟร์วอลล์</u>

ชนิดของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

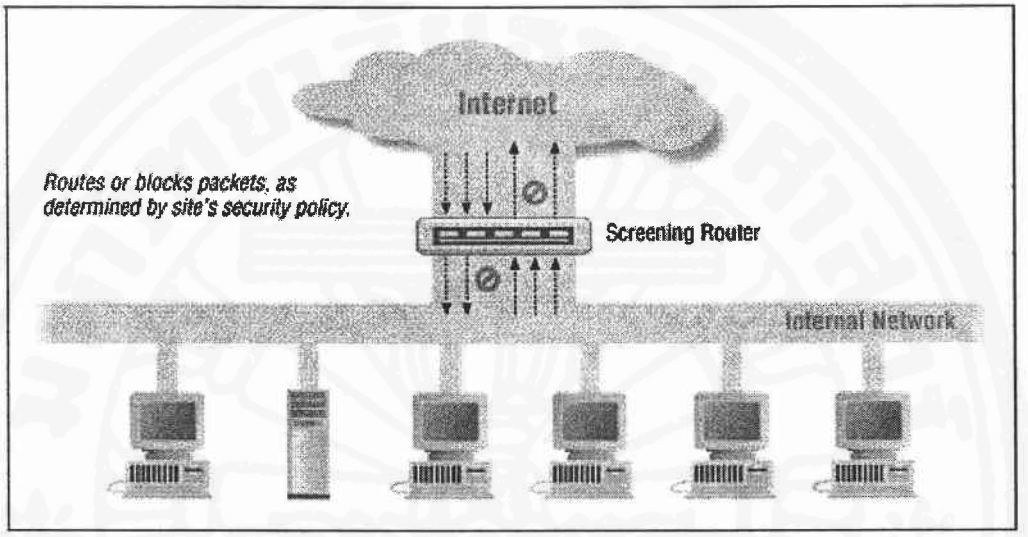
1. Packet Filtering
2. Proxy Service
3. Stateful Inspection

Packet Filtering

Packet Filter คือเราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้

ภาพที่ 2.11

ใช้ Screening Router ทำหน้าที่ Packet Filtering



ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเตอร์เน็ตโมเดล ซึ่งในอินเตอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้

- ไอพีต้นทาง
- ไอพีปลายทาง
- ชนิดของโปรโตคอล (TCP UDP และ ICMP)

และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ

- พอร์ตต้นทาง
- พอร์ตปลายทาง
- แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)
- ชนิดของ ICMP message (ในแพ็กเก็ต ICMP)

ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่

ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต หรือ ชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเน็ตเวิร์ก 203.154.207.0/24 , ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเน็ตเวิร์ก 203.154.207.0/24 ผ่านเราเตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น

Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ

- เราเตอร์ที่มีความสามารถในการทำ Packet Filtering (ซึ่งมีในเราเตอร์ส่วนใหญ่อยู่แล้ว)
- คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์

ซึ่งจะมีข้อได้เปรียบเสียเปรียบกันดังนี้

ตารางที่ 2.2

เปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ Packet Filtering

	ข้อดี	ข้อเสีย
เราเตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก, อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลาง,จำนวนอินเตอร์เฟสน้อย,อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ข้อดี-ข้อเสียของ Packet Filtering

ข้อดี

- ไม่ขึ้นกับแอพพลิเคชัน
- มีความเร็วสูง

- รองรับการขยายตัวได้ดี

ข้อเสีย

- บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ

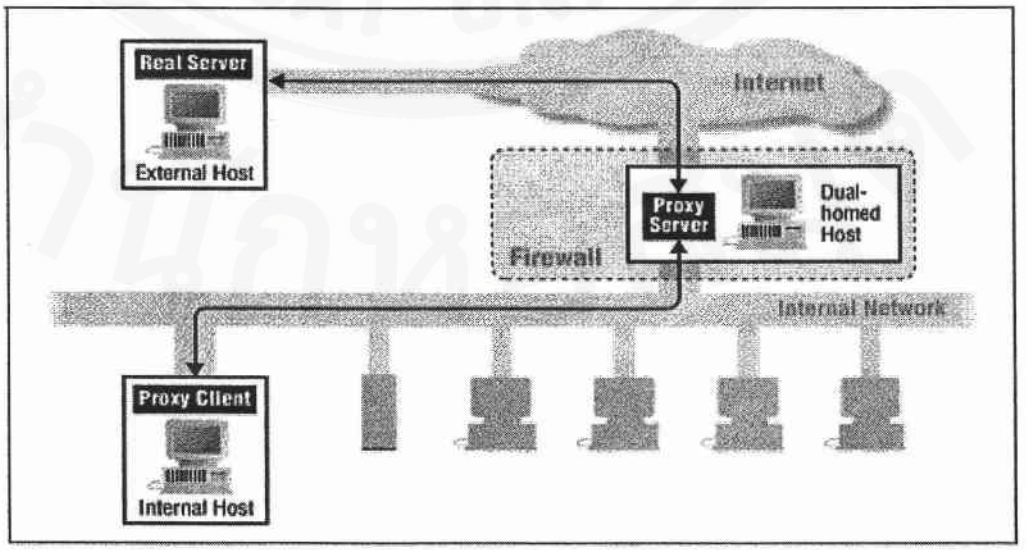
Proxy

Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)

เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา (negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่

ภาพที่ 2.12

ใช้ Dual-homed Host เป็น Proxy Server



ข้อดี-ข้อเสียของ Proxy

ข้อดี

- มีความปลอดภัยสูง
- รู้จักข้อมูลในระดับแอพพลิเคชัน

ข้อเสีย

- ประสิทธิภาพต่ำ
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

Stateful Inspection Technology

โดยปกติแล้ว Packet Filtering แบบธรรมดา (ที่เป็น Stateless แบบที่มีอยู่ในเราเตอร์ทั่วไป) จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละแพ็กเก็ตนำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

ตัวอย่างผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology ได้แก่

- Check Point Firewall-1
- Cisco Secure Pix Firewall
- SunScreen Secure Net

และส่วนที่เป็น open source แจกฟรี ได้แก่

- NetFilter ใน Linux (iptables ในลีนุกซ์เคอร์เนล 2.3 เป็นต้นไป)

2.3.8 Firewall Architecture

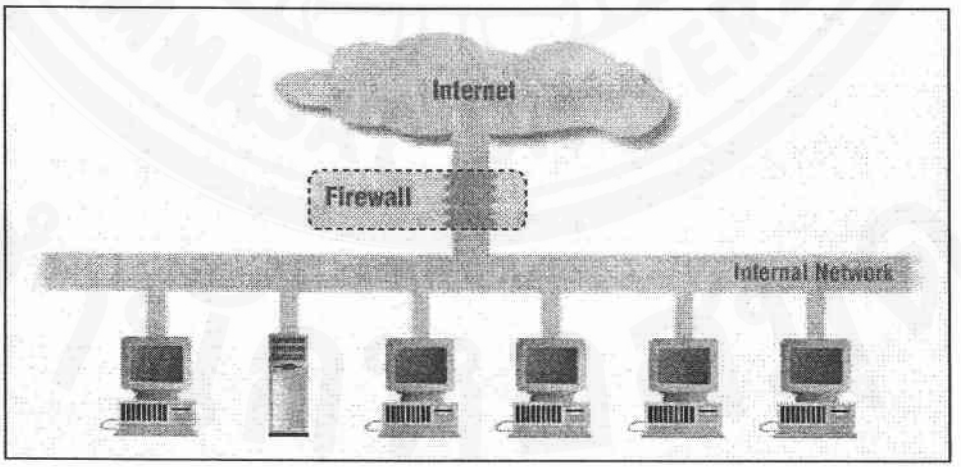
ในส่วนของ Firewall Architecture นั้น จะพูดถึงการจัดวางไฟร์วอลล์คอมโพเน็นต์ในแบบต่างๆ เพื่อทำให้เกิดเป็นระบบไฟร์วอลล์ขึ้น

Single Box Architecture

Single Box Architecture เป็น Architecture แบบง่ายๆ ที่มีคอมโพเน็นต์ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเน็ตเวิร์กภายในกับเน็ตเวิร์กภายนอก ข้อดีของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความปลอดภัยเน็ตเวิร์ก ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ ทำให้มีความเสี่ยงสูง หากมีการคอนฟิกูเรชันผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้

ภาพที่ 2.13

Firewall Architecture แบบชั้นเดียว



คอมโพเน็นต์ที่ใช้ใน Architecture นี้อาจเป็น Screening Router , Dual-Homed Host หรือ Multi-purposed Firewall Box ก็ได้

1) Screening Router

เราสามารถใช้เราเตอร์ทำ Packet Filtering ได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่าย เนื่องจากส่วนใหญ่จะใช้เราเตอร์ต่อกับเน็ตเวิร์กภายนอกอยู่แล้ว แต่วิธีนี้อาจไม่ยืดหยุ่นมากนักในการคอนฟิกกูเรชัน

Architecture แบบนี้เหมาะสำหรับ

- เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์ (Host security) เป็นอย่างดีแล้ว
- มีการใช้โปรโตคอลไม่มาก และโปรโตคอลที่ใช้ก็เป็นโปรโตคอลที่ไม่ซับซ้อน
- ต้องการไฟร์วอลล์ที่มีความเร็วสูง

2) Dual-Homed Host

เราสามารถใช้ Dual-Homed Host (คอมพิวเตอร์ที่มีเน็ตเวิร์กอินเตอร์เฟสอย่างน้อย 2 อัน) ใช้การบริการเป็น Proxy ให้กับเครื่องภายในเน็ตเวิร์ก

Architecture แบบนี้เหมาะสำหรับ

- เน็ตเวิร์กที่มีการใช้งานอินเตอร์เน็ตค่อนค่างน้อย
- เน็ตเวิร์กที่ไม่ได้มีข้อมูลสำคัญๆ

3) Multi-purposed Firewall Box

มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆ เดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้ง Packet Filtering, Proxy แต่ก็อย่าลืมว่านี่คือ Architecture แบบชั้นเดียว ซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งเน็ตเวิร์กได้

Screened Host Architecture

Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการ Proxy เหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ภายในเน็ตเวิร์กไม่ต่ออยู่กับเน็ตเวิร์กภายนอกอื่นๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้ Dual Homed Host) และจะมีเราเตอร์ที่ทำหน้าที่ Packet Filtering ช่วยบังคับให้เครื่องภายในเน็ตเวิร์กต้องติดต่อเซอร์วิสผ่าน

Proxy โดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะ Bastion host (คือโฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเตอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ) เท่านั้น

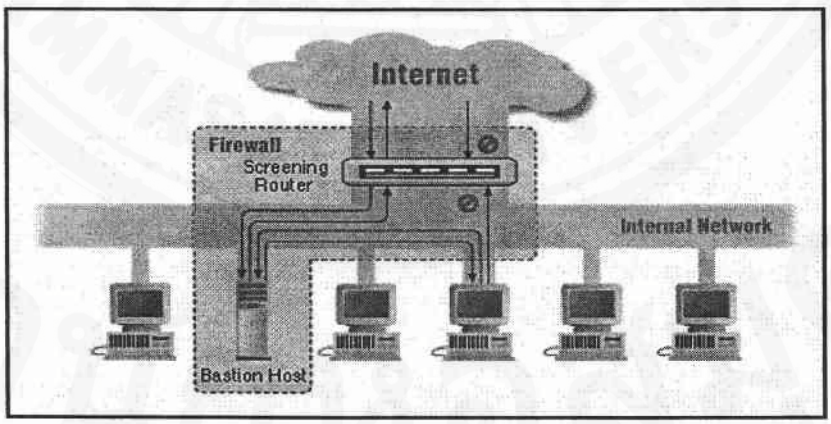
จากภาพที่ 2.14 ใน Architecture แบบนี้จะประกอบไปด้วยเราเตอร์ทำหน้าที่ Packet Filtering และภายในเน็ตเวิร์กจะมี Bastion Host ให้บริการ Proxy อยู่ โดยที่เราเตอร์นั้นอาจจะถูกเซ็ตดังนี้

- อาจจะอนุญาตให้เครื่องภายในใช้เซอร์วิสบางอย่างได้โดยตรง
- ส่วนเซอร์วิสอื่นๆ จะไม่ยอมให้เครื่องภายในติดต่อผ่านออกไปโดยตรง ยกเว้น Bastion Host เท่านั้นที่สามารถติดต่อกับเน็ตเวิร์กภายนอกได้ทั้งนี้เพื่อเป็นการบังคับให้ใช้บริการ Proxy ผ่านทาง Bastion Host เท่านั้น

หรืออาจจะเซ็ตให้เซอร์วิสส่วนใหญ่ผ่านเราเตอร์ออกไปได้โดยตรงแล้ว ให้บางส่วนต้องใช้เซอร์วิสผ่าน Proxy ก็แล้วแต่นโยบายและความเหมาะสมขององค์กร

ภาพที่ 2.14

Screened Host Architecture



วิธีนี้ถึงแม้ว่าจะมีทั้ง Proxy และเราเตอร์ทำหน้าที่ Packet Filtering แต่ก็ยังคงอันตรายอยู่ เพราะว่าเราเตอร์ต้องยอมให้ภายนอกสามารถติดต่อกับ Bastion Host ได้อยู่แล้ว หากแฮกเกอร์สามารถเจาะเข้ามายัง Bastion Host ได้ก็เสร็จ

Architecture นี้เหมาะสำหรับ

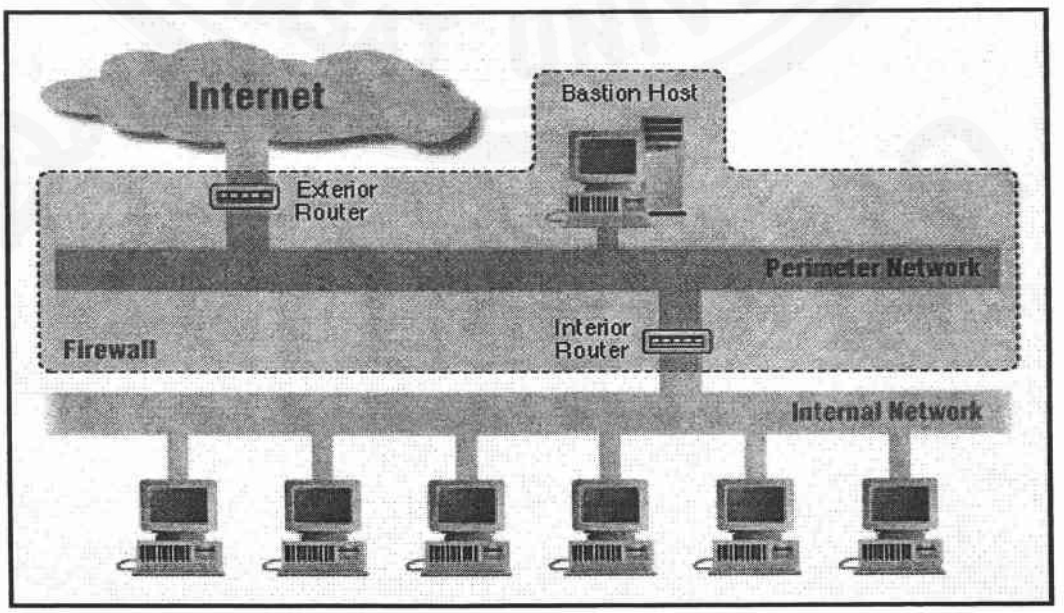
- เน็ตเวิร์กที่มีการติดต่อกับเน็ตเวิร์กภายนอกน้อย
- เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดีแล้ว

Multi Layer Architecture

ในสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากคอมโพเน็นต์หลายๆส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีเกิดความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้น หากในชั้นแรกถูกเจาะ ก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่นๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรมแบบหลายชั้นจะเป็นการต่อกันเป็นซีรี่โดยมี Perimeter Network (หรือบางทีเรียกว่า DMZ Network) อยู่ตรงกลาง เรียกว่า Screened Subnet Architecture

ภาพที่ 2.15

Screened Subnet Architecture



Screened Subnet Architecture

Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม Perimeter Network เข้าไปกั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์กภายในมีความปลอดภัยมากขึ้น

ในภาพที่ 2.15 แสดง Screened Subnet Architecture อย่างง่าย ประกอบไปด้วยเราเตอร์ 2 ตัว ตัวนึงอยู่ระหว่างอินเตอร์เน็ตกับ Perimeter Network ส่วนอีกตัวหนึ่งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ถ้าหากแฮกเกอร์จะเจาะเน็ตเวิร์กภายในต้องผ่านเราเตอร์เข้ามาถึง 2 ตัวด้วยกัน ถึงแม้ว่าจะเจาะชั้นแรกเข้ามายัง Bastion host ได้ แต่ก็ยังต้องผ่านเราเตอร์ตัวในอีก ถึงจะเข้ามายังเน็ตเวิร์กภายในได้

คอมโพเน็นต์ของ Screened Subnet Architecture ในภาพที่ 2.15

- Perimeter Network เป็นเน็ตเวิร์กที่เพิ่มเข้ามาเพื่อความปลอดภัย อยู่ระหว่างเน็ตเวิร์กภายนอกกับเน็ตเวิร์กภายใน ประโยชน์ของ Perimeter Network ที่เห็นได้ชัดก็คือ การแบ่งเน็ตเวิร์กออกเป็นส่วนๆ ทำให้การไหลของข้อมูลถูกแบ่งออกเป็นส่วนๆตามเน็ตเวิร์กด้วย เนื่องจากโดยทั่วไปแล้ว เน็ตเวิร์กที่เป็นแลนนั้น จะเป็นแบบ Ethernet ซึ่งจะมีการส่งข้อมูลแบบ Broadcast ดังนั้นถ้ามีใครคอบดักจับข้อมูลอยู่ในเน็ตเวิร์กนั้น ก็จะได้พาสเวิร์ด ข้อมูลต่างๆ ไปหมด ดังนั้นหากไฟร์วอลล์เรามีชั้นเดียวและแฮกเกอร์สามารถเข้ามาได้ โดนดักจับข้อมูลก็เสร็จหมด แต่ถ้าเรามี Perimeter Network ถึงจะดักจับข้อมูลได้แต่ก็จะได้เพียงที่อยู่บน Perimeter Network เท่านั้น

- Bastion Host ตั้งอยู่บน Perimeter Network ทำหน้าที่ให้บริการ Proxy กับเน็ตเวิร์กภายใน และให้บริการต่างๆ กับผู้ใช้บนอินเตอร์เน็ต Bastion Host นั้นจะมีความเสี่ยงต่อการโจมตีสูง จึงต้องมีการดูแลความปลอดภัยเป็นพิเศษ

- Interior Router ตั้งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ทำหน้าที่ Packet Filtering ป้องกันเน็ตเวิร์กภายในจาก Perimeter Network ในการเซ็ต configuration ระหว่าง เน็ตเวิร์กภายในกับ Perimeter Network ควรกำหนดอย่างรอบคอบ อนุญาตเฉพาะเซอร์วิสที่จำเป็นเท่านั้นอย่างเช่น DNS, SMTP

- Exterior Router ตั้งอยู่ระหว่างเน็ตเวิร์กภายนอกกับ Perimeter Network เนื่องจาก Exterior Router นี้เป็นจุดที่ต่ออยู่กับเน็ตเวิร์กภายนอก จึงมีหน้าที่ที่สำคัญอย่างหนึ่งคือ

การป้องกันแพ็กเก็ตที่มีการ Forged IP Address เข้ามา โดยอ้างว่ามาจากเน็ตเวิร์กภายในทั้งๆ ที่จริงๆ แล้วมาจากเน็ตเวิร์กภายนอก

2.4 ทฤษฎีที่เกี่ยวกับความคุ้มค่าในด้านการลงทุน

2.4.1 การประเมินความคุ้มค่าในการลงทุน

การที่จะทำโครงการขึ้นมาไม่ว่าโครงการนั้นจะมีขนาดเล็ก หรือใหญ่ขนาดไหน สิ่งสำคัญที่ควรคำนึงถึงเป็นอย่างยิ่งก็คือ ความคุ้มค่าในการลงทุน ซึ่งก่อนที่จะตัดสินใจลงทุนทำอะไรขึ้นมา ก็ต้องมีการคิดดูแล้วว่าสิ่งเหล่านั้นมีความคุ้มค่าเพียงพอที่ควรจะลงทุนหรือไม่ ซึ่งวิธีที่จะนำมาใช้ในการประเมินความคุ้มค่าในการลงทุนของงานวิจัยนี้ มี 3 วิธี คือ ระยะเวลาในการคืนทุน (Payback Period : PB) , มูลค่าปัจจุบันสุทธิ (Net Present Value : NPV) และอัตราผลตอบแทนการลงทุน (Internal Rate Of Return : IRR) ซึ่งจะมีวิธีคิด ดังต่อไปนี้

1. ระยะเวลาในการคืนทุน (Payback Period: PB) หมายถึง ระยะเวลาที่การลงทุนนั้นใช้ไปในการลงทุน เพื่อให้กระแสเงินสดรับสุทธิที่ได้จากการลงทุนคุ้มค่ากับต้นทุนที่ต้องลงทุนไป ระยะเวลาคืนทุน เป็นการคำนวณหาจุดคุ้มทุนของโครงการที่ทำ โดยมีหน่วยวัดเป็นเวลา ว่าเมื่อมีการลงทุนในโครงการนั้นแล้วจะใช้ระยะเวลากี่งวดในการคืนทุน ซึ่งโดยปกติแล้ว ในการลงทุนมักจะประมาณการกระแสเงินสดในแต่ละงวดมีหน่วยเป็นปี

$$\text{ระยะเวลาในการคืนทุน (PB)} = \frac{\text{จำนวนเงินลงทุนสุทธิเมื่อเริ่มโครงการ}}{\text{กระแสเงินสดสุทธิที่คาดว่าจะได้รับต่อปี}}$$

เกณฑ์ในการประเมินความคุ้มค่า

- ระยะเวลาในการคืนทุนที่คำนวณได้น้อยกว่าระยะเวลาในการคืนทุนที่ต้องการ ถือว่าคุ้มค่า
- ระยะเวลาในการคืนทุนที่คำนวณได้มากกว่าระยะเวลาในการคืนทุนที่ต้องการ ถือว่าไม่คุ้มค่า

2. มูลค่าปัจจุบันสุทธิ (Net Present Value: NPV)

เป็นการคำนวณหาผลต่างระหว่างมูลค่าปัจจุบันของกระแสเงินสดรับ กับมูลค่าปัจจุบันของกระแสเงินสดจ่าย ที่ใช้ในโครงการลงทุน

มูลค่าปัจจุบันสุทธิ (Net Present Value or NPV) = มูลค่าปัจจุบันของเงินสดรับ - มูลค่าปัจจุบันของเงินสดจ่าย

$$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t} \quad \text{..... (2.1)}$$

โดยที่

NPV	=	มูลค่าปัจจุบันสุทธิ
CFt	=	กระแสเงินสดที่คาดหวัง ณ ช่วงเวลา t
n	=	ช่วงอายุของโครงการลงทุน
r	=	อัตราคิดลด หรือ ต้นทุนถัวเฉลี่ย

<u>เกณฑ์ในการประเมินความคุ้มค่า</u>

- กรณีมูลค่าปัจจุบันสุทธิ (NPV) มีค่าเป็นบวก จะยอมรับความคุ้มค่า
- กรณีมูลค่าปัจจุบันสุทธิ (NPV) มีค่าเป็นลบ จะไม่ยอมรับความคุ้มค่า

3. อัตราผลตอบแทนการลงทุน (Internal Rate of Return: IRR)

อัตราผลตอบแทนที่ทำให้ค่า NPV ของโครงการลงทุนนั้นมีค่าเท่ากับศูนย์

<u>เกณฑ์ในการประเมินความคุ้มค่า</u>

- กรณีอัตราผลตอบแทนการลงทุนที่คำนวณได้ เท่ากับ หรือมากกว่า ต้นทุนของเงิน หรืออัตราผลตอบแทนที่ต้องการ จะยอมรับความคุ้มค่า
- กรณีอัตราผลตอบแทนการลงทุนที่คำนวณได้ น้อยกว่าต้นทุนของเงินหรืออัตราผลตอบแทนที่ต้องการ จะไม่ยอมรับความคุ้มค่า

2.5 SWOT Analysis

2.5.1 ความหมายของ SWOT Analysis

SWOT Analysis เป็นการวิเคราะห์สภาพองค์กร หรือหน่วยงานในปัจจุบัน เพื่อค้นหาจุดแข็ง จุดเด่น จุดด้อย หรือสิ่งที่อาจเป็นปัญหาสำคัญในการดำเนินงานสู่สภาพที่ต้องการในอนาคต

SWOT เป็นตัวย่อที่มีความหมายดังนี้

1. Strengths - จุดแข็งหรือข้อได้เปรียบ
2. Weaknesses - จุดอ่อนหรือข้อเสียเปรียบ
3. Opportunities - โอกาสที่จะดำเนินการได้
4. Threats - อุปสรรค ข้อจำกัด หรือปัจจัยที่คุกคามการดำเนินงานขององค์การ

หลักการสำคัญของ SWOT ก็คือการวิเคราะห์โดยการสำรวจจากสภาพการณ์ 2 ด้าน คือ สภาพการณ์ภายในและสภาพการณ์ภายนอก ดังนั้นการวิเคราะห์ SWOT จึงเรียกได้ว่าเป็นการวิเคราะห์สภาพการณ์ (Situation Analysis) ซึ่งเป็นการวิเคราะห์จุดแข็ง จุดอ่อน เพื่อให้รู้ตนเอง รู้จักสภาพแวดล้อมชัดเจน และวิเคราะห์โอกาส-อุปสรรค การวิเคราะห์ปัจจัยต่าง ๆ ทั้งภายนอกและภายในองค์กร ซึ่งจะช่วยให้ผู้บริหารขององค์กรทราบถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นภายนอกองค์กรทั้งสิ่งที่ได้เกิดขึ้นแล้วและแนวโน้มการเปลี่ยนแปลงในอนาคต รวมทั้งผลกระทบของการเปลี่ยนแปลงเหล่านี้ที่มีต่อองค์กรธุรกิจ และจุดแข็ง จุดอ่อน และความสามารถด้านต่าง ๆ ที่องค์กรมีอยู่ ซึ่งข้อมูลเหล่านี้จะเป็นประโยชน์อย่างมากต่อการกำหนดวิสัยทัศน์ การกำหนดกลยุทธ์และการดำเนินตามกลยุทธ์ขององค์กรระดับองค์กรที่เหมาะสมต่อไป

2.5.2 ประโยชน์ของการวิเคราะห์ SWOT

วิเคราะห์ SWOT เป็นการวิเคราะห์สภาพแวดล้อมต่าง ๆ ทั้งภายนอกและภายในองค์กร ซึ่งปัจจัยเหล่านี้แต่ละอย่างจะช่วยให้เข้าใจได้ว่ามีอิทธิพลต่อผลการดำเนินงานขององค์กรอย่างไร จุดแข็งขององค์กรจะเป็นความสามารถภายในที่ถูกใช้ประโยชน์เพื่อการบรรลุเป้าหมาย

ในขณะที่จุดอ่อนขององค์กรจะเป็นคุณลักษณะภายใน ที่อาจจะทำลายผลการดำเนินงาน โอกาสทางสภาพแวดล้อมจะเป็นสถานการณ์ที่ให้โอกาสเพื่อการบรรลุเป้าหมายองค์กรในทางกลับกัน อุปสรรคทางสภาพแวดล้อมจะเป็นสถานการณ์ที่ขัดขวางการบรรลุเป้าหมายขององค์กร ผลจากการวิเคราะห์ SWOT นี้จะใช้เป็นแนวทางในการกำหนดวิสัยทัศน์ การกำหนดกลยุทธ์ เพื่อให้องค์กรเกิดการพัฒนาไปในทางที่เหมาะสม

2.5.3 ขั้นตอน / วิธีการดำเนินการทำ SWOT Analysis

การวิเคราะห์ SWOT จะครอบคลุมขอบเขตของปัจจัยที่กว้าง ด้วยการระบุจุดแข็ง จุดอ่อน โอกาสและอุปสรรคขององค์กร ทำให้มีข้อมูล ในการกำหนดทิศทางหรือเป้าหมายที่จะถูกสร้างขึ้นมาบนจุดแข็งขององค์กร และแสวงหาประโยชน์จากโอกาสทางสภาพแวดล้อม และสามารถ กำหนดกลยุทธ์ที่มุ่งเอาชนะอุปสรรคทางสภาพแวดล้อมหรือลดจุดอ่อนขององค์กรให้มีน้อยที่สุดได้ ภายใต้การวิเคราะห์ SWOT นั้น จะต้องวิเคราะห์ทั้งสภาพแวดล้อมภายในและภายนอก องค์กร โดยมีขั้นตอนดังนี้

2.5.3.1 การประเมินสภาพแวดล้อมภายในองค์กร

การประเมินสภาพแวดล้อมภายในองค์กร จะเกี่ยวกับการวิเคราะห์และพิจารณาทรัพยากรและความสามารถภายในองค์กร ทุกๆ ด้าน เพื่อที่จะระบุจุดแข็งและจุดอ่อนขององค์กร แหล่งที่มาเบื้องต้นของข้อมูลเพื่อการประเมินสภาพแวดล้อมภายใน คือระบบข้อมูลเพื่อ การบริหารที่ครอบคลุมทุกด้าน ทั้งในด้านโครงสร้าง ระบบ ระเบียบ วิธีปฏิบัติงาน บรรยากาศในการทำงานและทรัพยากรในการบริหาร(คน เงิน วัสดุ การจัดการ รวมถึงการพิจารณาผลการดำเนินงานที่ผ่านมาขององค์กรเพื่อที่จะเข้าใจสถานการณ์และผลกลยุทธ์ก่อนหน้านี้ด้วย

- จุดแข็งขององค์กร (S-Strengths) เป็นการวิเคราะห์ปัจจัยภายในจากมุมมองของผู้ที่อยู่ภายในองค์กรนั้นเองว่าปัจจัยใดภายในองค์กรที่เป็นข้อได้เปรียบหรือจุดเด่นขององค์กรที่องค์กรควรนำมาใช้ในการพัฒนาองค์กรได้ และควรดำรงไว้เพื่อการ เสริมสร้างความเข็มแข็งขององค์กร

- จุดอ่อนขององค์กร (W-Weanesses) เป็นการวิเคราะห์ ปัจจัยภายในจากมุมมองของผู้ที่อยู่ภายในจากมุมมอง ของผู้ที่อยู่ภายในองค์กรนั้น ๆ เองว่าปัจจัยภายในองค์กรที่เป็นจุด

ด้อย ข้อเสียเปรียบขององค์กรที่ควรปรับปรุงให้ดีขึ้นหรือขจัดให้หมดไป อันจะเป็นประโยชน์ต่อองค์กร

2.5.3.2 <u>การประเมินสภาพแวดล้อมภายนอก</u>

ภายใต้การประเมินสภาพแวดล้อมภายนอกองค์กรนั้น สามารถค้นหาโอกาสและอุปสรรคทางการดำเนินงานขององค์กรที่ได้รับผลกระทบจากสภาพแวดล้อมทางเศรษฐกิจทั้งในและระหว่างประเทศที่เกี่ยวกับการดำเนินงานขององค์กร เช่น อัตราการขยายตัวทางเศรษฐกิจ นโยบาย การเงิน การงบประมาณ สภาพแวดล้อมทางสังคม เช่น ระดับการศึกษาและอัตรารู้หนังสือของประชาชน การตั้งถิ่นฐานและการอพยพของ ประชาชน ลักษณะชุมชน ขนบธรรมเนียมประเพณี ค่านิยม ความเชื่อและวัฒนธรรม สภาพแวดล้อมทางการเมือง เช่น พระราชบัญญัติ พระราชกฤษฎีกา มติคณะรัฐมนตรี และสภาพแวดล้อมทางเทคโนโลยี หมายถึง กรรมวิธีใหม่ๆและพัฒนาการทางด้านเครื่องมือ อุปกรณ์ที่จะช่วยเพิ่มประสิทธิภาพในการผลิตและให้บริการ

- โอกาสทางสภาพแวดล้อม (O-Opportunities) เป็นการวิเคราะห์ว่าปัจจัยภายนอกองค์กร ปัจจัยใดที่สามารถส่งผล กระทบประโยชน์ ทั้งทางตรงและทางอ้อมต่อการดำเนินการขององค์กรในระดับมหาภาค และองค์กรสามารถฉกฉวยข้อดีเหล่านี้มาเสริมสร้างให้ หน่วยงานเข็มแข็งขึ้นได้

- อุปสรรคทางสภาพแวดล้อม (T-Threats) เป็นการวิเคราะห์ว่าปัจจัยภายนอกองค์กรปัจจัยใดที่สามารถส่งผล กระทบในระดับมหภาคในทางที่จะก่อให้เกิดความเสียหายทั้งทางตรงและทางอ้อม ซึ่งองค์กรจำต้องหลีกเลี่ยง หรือปรับสภาพองค์กรให้มี ความแข็งแกร่งพร้อมที่จะเผชิญแรงกระทบดังกล่าวได้