The Integrated Control and Management System

By Danny Chan Ber Song

A dissertation submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Science in the University of Wales

Supervisor: Frank Bott

University of Wales, Aberystwyth
02 April 2004

Acknowledgement

I would like to thank my lecturer Mr. Frank Bott his advice and guidance. I also want to acknowledge my classmates for their encouragement. I am grateful to my friend Swee Meng for his valuable comments. Most importantly, I want to thank my wife Soh Lian and my son Song Kai for the understanding and support, without this it would not be possible for this dissertation.

Abstract

A new data monitoring and control system of club facilities has been implemented and utilized in year 2003. The aim of this system is to improve the operating efficiency and save cost. The system consists of mainly two types of subsystem, the Central Management System (CMS) and Site Management Systems (SMS).

The operating functions of the CMS is to collect and display the real time data, historical data, provide trending and data storage for future decision making purpose. The operating functions of SMS is to collect real time data from remote sites and send it to CMS for display or received control instructions from CMS for activating the sensor. The system is developed after detail studies on the requirements and the constraints. Although there are areas of improvement, the new system still meet all the requirements and functions.

CONTENTS PAGE

CHAPTER 5. SOFWARE ARCHITECTURE

CHAPTER 6: NETWORK ARCHITECTURE & SECURITY MANAGEMENT

CHAPTER 7: PROTOCOL AND MEDIA

CHAPTER 8. SYSTEM FAILURE AND RECOVERY

CHAPTER 1: INTRODUCTION AND BACKGROUND

Aberdeen Business Club started operating as a proprietary business club with an appointment of Management Committee to oversee the administration and operation. The club was converted from a proprietary club into a Member's Club and was renamed as Aberdeen Country Club (ACC). With this conversion, the club had greater flexibility and autonomy in developing and managing the facilities. The club continued to improve the quality of services and at the same time reduce operating cost in order to be able to attract more members.

Aberdeen Country Club (ACC) wanted to migrate the present manual building management system to an automated system. ACC's approach was to implement an appropriate Integrated Control and Management System (ICMS) with a high-speed data communication network to interconnect the ACC Singapore to other ACC in the region. This report descripts the functional requirement, system design [2], implementation plan and acceptance test plan for the new system.

I was assigned by my company as the Project Consultant in providing; system analysis, design and Implementation of the ICMS. I worked with the ACC management team in identifier the operational issues and detail requirements for the design of this system. The system has been fully implemented and in operation since Dec 2003.

1.1 The existing manual system

ACC has a workforce of 1380 full time employees and 600 part time workers in ten countries. This large number of workforce has to cater for the current manual system to support the ACC's building management control in the area of operational issue e.g. on/off and off lighting, manual checking of fire alarm system, adjustment of room temperature, on/off air-conditions, on/off of swimming pool water pumps and on/off off of the electrical lighting system etc.

1.2 The need for a Integrated Control and Management System

The current manual operating process requires high manpower to monitor and control the systems, it has taken much of ACC resources. The manually monitoring and control resulted in deficiencies in resources utilization, productivity and staff morale. ACC recognized these problems and decided to use the latest information technologies to automate these manual processes. Hence, the company needs to change its current manual system with the introduction of Integrated Management System (ICMS) to provide monitoring and control of these devices.

The Regional Operational Manager of ACC was tasked by the committee to acquire and implement a cost and effective system, as he was responsible for the day-to-day administration & operation of the club's affairs in accordance with the direction of the Management Committee.

The ICMS provides efficient and reliable control management. This includes air-conditioning system on/off and temperature control, lighting brightness and on/off control, heating on/off and temperature control, water level control, fire alarm monitoring and activation.

The ICMS shall provide the operational status of all the facilities system in ACC. ICMS will capture the events automatically, store it into the database and trigger as an alarm. This accurate and timely information will allow the operational staff to respond quickly to the events occur and also more efficient in deploying their resources.

The key objectives for building the ICMS are,

- An Integrated Control and Management System shall resulted in improvement of the resources utilization, productivity.

- It shall apply DBMS technique into the Integrated Management System (ICMS) for database sharing and updating. The database includes facilities operation data, ACC system failure information, equipment operating hour and monitoring and control of room temperatures etc.

- WEB enable Graphic User Interface (GUI) [6] was to be included in the ICMS software for monitoring and control the facilities from the region.

- Embarking on ICMS program and shall start to implement from year 2001 and operate within two years.

CHAPTER 2: OVERALL SYSTEM FUNCTIONAL REQUIREMENTS

The Control and Data Acquisition [7] functions apply to all facilities and the equipment was to be monitored and controlled. ICMS provides supervision and control of the following sub-systems.

- Electro-mechanical (E&M) systems including:
  - Fire detection and protection system
  - Electrical Lighting System
  - Lifts & Escalators

- Analogue Systems
  - Swimming pool water pumps system
  - Electrical Power System

2.1 Functional Requirement

ICMS functions are provided using the off the shelf data acquisition software package from factorylink [23] based on a real time database representing the status of all the variables of the system. The software provides:

- the management of data exchange (acquisition and sending of data) with the field equipment via Remote Terminal Units (RTUs) and serial links,
- basic processing of acquired data (digital or analogue)
- event detection, triggering alarms or any other type of processing,
- the management of operator actions,
- the management of the automatic issued controls,
- the alarms, lists, and reports display and update

2.1.1 Digital & Electro-Mechanical System Equipment

The following E&M systems or equipment are monitored and controlled by the ICMS:

- Lighting,
- Lifts & Escalator,
- Fire detection and Protection System,

- Status supervision (for instance for an escalator: up / down / stopped / fire / emergency stop),
- Statistical information destined to the GUI (for instance for an escalator: failures, working hours, number of start / stop)
- single control execution (for instance for an escalator : up / down / stop),
- grouped control execution (for instance Setting to work of all the escalators of a station).

The monitoring and control capabilities will strongly depend on the possibilities of the supervised equipment. Operators monitor and control this equipment through the standard ICMS operator position terminal at the Central Management System or at remote Site. All the standard features of the ICMS (Log, alarms, etc.), apply to the E&M equipment.

2.1.2 Analogue System and Equipment

The following analog systems or equipment are monitored and controlled by the ICMS:

- Circuit Breakers, isolators, rectifiers,
- Uninterrupted Power Supply,
- Generators,
- Battery and Charger system,
- Water lever

For analogue systems equipment, ICMS provides the following control and status functions,

- Status supervision,
- Analogue and digital counter monitoring,
- Maximum demand management,
- Peak load shedding and load balancing,

Operators monitor and control the power equipment through the standard ICMS graphic display interface (GUI) at Monitoring Control Center. The control or monitoring access to the power information was granted according to the user rights.

2.1.3 Data Acquisition

Data Acquisition [7] functions are provided using the commercial off the self data acquisition software package the system.

The data acquisition software provides:

- the management of data exchange (acquisition and sending of data) with the field equipment via VME fort end processor.
- processing of acquired data (digital or analogue)
- event detection, triggering alarms or any other type of processing,
- management of operator actions,
- the management of the automatic issued controls,
- the alarms, lists, and reports display and update
- the recording, and archiving of data and events.
- the management of the Human Machine Interface [6]

The Graphic User Interface was provided using the X-window Manager [12] and other application software that was installed in the Operating Terminal including three monitor displays, a keyboard and a mouse, for:

- displaying operator selectable graphical animated images, representing the status of the supervised equipment,
- displaying alarms, either on graphical images or in the form of messages, with operator acknowledgement capabilities,
- displaying lists or reports in windows,
- data input and navigation based on roll-down menus, clicking on graphical objects [6], and dialogue boxes,

X-Windows [12] was a client/server [5] orient software jointly developed by Massachusetts Institute of Technology (M.I.T) and X.org [12]. X-window was a free software, it can be download from M.I.T's home page. X-Org was a international consortium, was an organization to develop, maintain X-Window System technology and standard.

X-Windows software provides the graphical user interface (GUI) windowing environment for Sun Solaris workstations and other types of computers. It was not tied to the operating system and was available on a wide range of platforms.

X-windows provide allows the display into many sections, each of which can be assigned a different task. X windows are used for viewing more than one application at a time.

X-windows provides a public protocol by which client programs can query and update information on X servers. X-windows is a communication protocol can be used within a single computer, or across a network of computers. It utilizes a Client-Server model of network communication. This model allows a user to run a program in one location, but control it from a different location.

The ICMS software package includes a Security Management features, which allows prioritization of access rights of the type of control and the supervised area of each operator. It also includes the monitoring and self-diagnostic of the system itself, with hot stand-by fail-over for redundant servers.

The ICMS is made through a configuration tool, which describes the real-time database (structure of the database, description of the supervised points etc.), and its operating characteristics (including the Graphic User Interface: graphical displays, dialogues, etc.)

2.2 Non-Functional requirement

ACC objectives are to get the system to operate with high availability; high scalability and the system access must be highly secure.

2.2.1 Availability

Any failure of the system will results in lost of revenue and lowering the quality of services to the members. It is therefore very important for the system to be designed to handle all kind of transaction without any failure. The down time of server is very much dependent on how quickly the application can be restarted and how long it takes to fetch the data.

The Integrated Management System (ICMS) shall provide high availability; the system contains redundant components for each subsystem. Each sub system shall provide with dual processor boards with memory and dual I/O, dual network cards, mirrored disk systems with dual power supply and battery back up. Parallel server will be included in the design for high availability,

2.2.2 Scalability

It is possible for the Integrated Control Management System (ICMS) to implement from a small system to a very large-scale system and provide with high availability. The system is scalable to 100 remote sites.

2.2.3 Security

In this system the Security is provided at several levels. Firstly, users need log-in access to the operating system. Secondly, a user needs login access to the system components. Thirdly, all users and terminals have an access level and all data attributes have a security level. If a user does not have access to an attribute, the user cannot change that data point.

CHAPTER 3: OVERALL SYSTEM ARCHITECTURE

The system architecture of the Integrated Control Management System (ICMS) is communicate through a broadband 100mbps Ethernet [10] backbone and by connecting through the Local Area Network (LAN) to the distributed VME industrial computer system.

The Industrial computer system is equipped with a monitoring and control interface is used to monitor and control necessary facilities. The overall architecture of the Integrated Management System's Network is linked around a public Internet broadband communication network. The network has integrating with other ACC clubhouses forming a highly distributed control system.

Each clubhouse is equipped with a Site Management System; it consists of remote terminal unit, Programmable Logic Controller (PLC) and the input/output device and sensors. The Site Management System is to provide monitor and control all facilities equipment, lighting, water pump and Power etc

This distributed System [4] enables physical data acquisition and collection. The distributed system is formed by a two level architecture:

- Programmable Logic Control (PLC) acquires data information on facility equipment of each ACC clubhouse.

- The VME industrial PC acts as front-end computer collects the PLC's information for the real-time data servers.

- Two VME industrial PC will be operating in a hot and stand-by mode in order to achieve maximum availability.

- The two operator terminal station workstations are connected to the real time data server via the 100base/t high speed LAN.

- The PLC is able to operate in autonomous mode and is connected to the central data server through the local area network and router to the Internet broadband service.

- The Central Management System (CMS) consists of two of application servers for data acquisition. The two servers are operating in a hot stand-by mode.

- The Central Management System (CMS) monitors and controls, the information processed at main clubhouse level is acquired at the Site level via the VME front-end processor and the communicate trough the LAN and the Virtual Private Network.

3.1 Site Management System

The Site Management System (SMS) provides physical data acquisition and concentration. This SMS is formed by a two level architecture:

- The PLCs acquire information on each site equipment
- The Remote Terminate Unit (RTU) collects the PLC's information and acts as front-end computer for the real-time data server and the central data servers.

- The Remote Terminal Unit will be duplicated and operating in a hot stand-by mode in order to achieve maximum availability.

The various operator consoles are driven by workstations connected to the server via the Site LAN. They offer a high level window based graphical man machine interface. Each SMS is fully autonomous and connected to the Central Monitoring and Control Room through the WAN.

3.2 Central Management System

At the monitoring control center is the Central Management System (CMS), which supervises all the E&M, Power, supply equipment for the various Sites. This is similar to the Site Management System except that it is display and stores the amount of data collected and provides the control process.

The CMS consists of a pair of application servers, real time application servers, real-time database server, Operator terminal station and network management workstation. Both of the real-time application server are operating in a hot/stand-by mode. The CMS directly monitors and controls, the information processed at central level is acquired at the Site level via the SMS, and transmitted through Internet Virtual Private Network [11].

The LAN network can offer significant bandwidth; the LAN supports various speed configurations in the range from 10 Mbps to 100 Mbps. The Internet broadband network can

be scalable from the range of 2 to 8 Mbps or higher. The Internet broadband network can be configured to satisfy the needs of ACC and can be upgraded in terms of bandwidth if require.

CHAPTER 4: OVERALL HARDWARE ARCHITECTURE

The ICMS consists of two main sub systems, the Central management and Site Management System. The Central Management was designed to collect data from the Site Management System and store it into the data base server for analysis purpose. The Site Management is to take instruction from the Central Management for control and activate the devices or sensors.

4.1 Central Management System

The Central Management system consists of Sun Solaris real time server for ICMS data acquisition, database server for storing the historical data and Network Management workstation for overall network analysis.

4.1.1 Real-Time Servers

The real-time servers are in charge of:

- acquiring data from, and sending controls to the site equipment,
- maintaining the real-time status of all the monitored equipment according to the acquired data
- Performing typical function such as basic remote control, reaction programs, grouped remote controls etc.
- Performing specific functions such as temperatures monitoring, Power monitoring etc.
- Sending information to operator positions data information according to the real-time equipment status and processing the operator actions.

Two of Central Management System real-time application servers are provided, the (ICMS Server) being dedicated to all the other functions. These real-time servers communicate with:

- the RTU of each Site in order to acquire and send site equipment data,
- the Operator terminal positions are the client of these servers, in order to update their display,
- the DBMS server for data archiving
- the Network Management System workstation for network configuration

The real-time servers hardware is based on high performance SUN Microsystems RISC computer, working under the Solaris Operating System. The selected model

come with single processors, it offering high processing and input / output capabilities. These computers will be configured to operate in a hot / stand-by mode.

4.1.2 Database Management Server (DBMS)

The DBMS is in charge of the following functions:

- Archiving all the events of the system for the Central Management System
- Provision for the Decision Support System functions.

The DBMS communicates with all the real-time data servers, including the Central Management System and Site Management System.

The relational database server has disassociate from the real-time data servers for the following reasons:

- Better real-time performance of the real-time database servers which are not influenced by the access to the relational database,
- Symmetrical architecture facilitating functions associated with the database, namely access, update, save, evolution.

The DBMS server can therefore be accessed, through the network, by all the units constituting the overall configuration.

The hardware configuration is SUN Enterprise server. It is non-redundant, as its failure does not immediately affect the operation. However, disk mirroring ensures data security and the disk capacity has been increased to allow the system to support historical data.

4.1.3 Network Management Workstation

The Network Management Workstation is dedicated to the configuration and monitoring of the networked equipment. It communicates with all the networked equipment in the Central Management System, in order to retrieve their status, provided they are SNMP compatible.

SNMP (Simple Network Management Protocol) is a implementation of a SNMP Agent. SNMP [10] is an application-layer protocol designed to facilitate the exchange of management information between network devices. With this protocol the network is able to access management information data, this includes packets per second, network error rates and the network administrators are able to manage network performance and find and solve network problems.

This function is implemented on a dedicated SUN workstation. The Network Management Workstation enables function from the real-time application servers for better real-time performance of the real-time data servers. The selected hardware is a SUN workstation under the Solaris UNIX operating system and Network Node Manager module.

4.1.4 Operating Terminal Position (OTP)

The operating positions MFT are the clients to the real-time data servers using the X windows manager for GUI functions, which are graphic display and dialogue management. They communicate with the real-time data servers, reception of the real-time station site status, and transmission of remote controls issued from the dialogue with DBMS server for access to historical data, the development workstation for data configuration.

The operating positions in Operation Center Control are high performance PCs under the Windows NT operating system equipped with three 21” touch screen VDUs.

4.2 Site Management System

Site Management Systems consists of the fort end processor or Remote Terminal Unit (RTU) and Programmable Logic Controller (PLC). The PLC is to collect the data from the I/O and sensors then send it to the RTU for processing. After data being process, it will then send to the Central Management for display and store into the database for analysis purpose.

4.2.1 Front End Processor/Remote Terminal Unit (RTU)

The Front end Processing Unit is a VME bus based PC system.

The VME standard has been selected following a detailed analysis, which it complies with the following requirements:

- Open standard
- World-wide location of VME cards manufacturers,
- Real time capabilities
- Industrial oriented production.
- support organizations turned towards long term maintenance.
- Wide range of industrial and communication cards.
- Non-proprietary products

The CPU board is based on a modular and multifunction card, allowing it to be used as a CPU card, or as a serial or LAN I/O interface. Combined with a wide range of industrial and generally intelligent I/O boards, it gives the Remote Terminal Unit very high data processing capabilities.

Full compliance with transmission standards like TCP/IP, makes Remote Terminal Unit an open product that can be easily interface with various equipment.

A typical Site configuration is summarized in the following table (per RTU):

	Purpose
	10 slot VME Rack
1.	Main CPU
2.	Standby CPU
3.	4 RS 422 serial ports
4.	Dual 100baseT Ethernet ports

This configuration can vary from one Site to another, depending on the number of acquisition PLCs connected to the RTU.

The site management system comprises a two level architecture:

- the Remote Terminal Unit, which is the fort end processor,
- the direct I/O management system, which as simple Remote I/Os

The main features of the RTU are:

- a VME based architecture, enabling the use of standard boards (CPU, memory, interface and input/output),
- the Vxworks real-time Operating system.

- A 100baseT Ethernet card

From a hardware point of view, the VME bus has the following advantages:

- the VME bus is a widely spread industrial standard, allowing an independence with the boards suppliers hence the RTU is based on off-the-shelf hardware;

- the VME bus enables a high modularity of the RTU product, associated to a high openness to other industrial standards

- the evolution of the VME is under control, completely opposite to the PC world which is in constant evolution.

- the VME components have a long design life cycle

- the high reliability bus system.

From a software point of view, the real time Operating System has the main advantage of providing a high level of functionality (it is Unix-like enhanced with real-time extension), it is compact, enabling diskless configurations.

The C language is used for programming.

The main features of the proposed are:

- a scaleable and modular architecture,
- a rugged design allowing installation in severe environments,
- lEC 1131-3 compliant programming languages. IEC 1131-3 is the international standard for programmable controller programming languages. It specifies the syntax, semantics and display for the PLC programming languages.

4.2.2 Programmable Logic Controller (PLC)

Programmable Logic Controllers (PLCs) are unlike RTU; it includes all the necessary software and hardware interfaces to the process. They are used for automation control

application (e.g. closed loop control) either standalone or connected to distributed inputs/outputs, to other PLCs and/or to front end processor (RTU). The communications are established by means of the field buses.

The MODBUS [14] is being use for connecting all the I/O devices and sensors in the Site Management System. The type of the I/O and sensors use in ICMS is digital input 16x24v, digital output 9x30v relay 1A, analogue input maximum voltages 10V, analogue output 1x 4-20mA and temperature sensor up to 150 degree c.

A typical PLC consists of a CPU, a Input/output modules, a communication modules and a power supply. The PLC have been very popularity for the control application because of the many advantages they offer. It provides cost effective for controlling for complex systems. It can be reapplied to control other systems quickly and easily.

The PLC enable control that is more sophisticated and trouble-shooting aids make programming easier and reduce downtime. There are many manufacturers produce and developed PLCs, this include companies like GE Func, Siemens, Rockwell, Mitsubishi, Honeywell, Yamataka and Philips etc.

PLC usually very reliable, it is likely to operate for years before failure, this equipment provides with the following requirements includes:

- Very high speed scan rates based controllers to increase system output,
- Configurable output fail states for predictable
- Performance in critical applications,
- High isolation levels for noise immunity in high electrically severe environments,

The PLC provides high speed turn On, turn Off circuits, combined with interrupt processing for higher system performance, Hot swap design for simplified maintenance and increased system availability.

The Site Management System’s Programmable Logic Controller (PLC) acts as an Intelligent Remote I/Os.

The software included in the PLC allows:

- Standard I/O exchanges with process environment,
- Communications with the RTU

The software is limited to the I/O configuration and other functionalities such as MODBUS protocol are included in the PLC software module.

The PLC software module is built with three modules:

- a communication module in charge of data exchanges with the MODBUS handler,
- a Digital Outputs (DO) module in charge of the execution of the basic commands Open, Close relay and of the DO cards status management,
- a Digital Inputs (DI) module in charge of the acquisition of DIs through a multiplex. and the multiplex status management.

These modules are executed at each PLC cycle, typically less than 50 ms.

4.3 Hardware design Choice for Site Management System

The design choice for hardware in the Site Management System includes the following,

- VME bus based distribution computer system with Programmable Logic Control (PLC) for facilities equipment interface.
- Real Time Server
- Real time database server
- Router and network equipment for the LAN, WAN and backbone interface with VME distributed PC and facilities hardwired interface

The main design criteria for the hardware are:

- Open architecture in complied to international standard
- High level of performance
- features that most fulfill the operational needs.
- support organizations turned towards long term maintenance

- wide range of industrial and communication cards,
- non-proprietary products
- High availability and Maintainability

The following was the propose hardware solution for the Site Management Systems.

4.3.1 Design Choice of RTU

4.3.1.1 VME

The VME bus (EuropaVersa Module Europa) is a fast, flexible, open-ended bus system that uses the eurocard standard. VME [13] is a 32-bit bus that is widely used in many specialized applications and industries, including industrial controls, military, aerospace, telecommunications, transportation, simulation, medical, scientific, business and military applications. VME bus supports a variety of computing tasks in demanding environmental conditions. VME64 is an expanded version that provides 64-bit data transfer and addressing.

4.3.1.2 VXI

VXI stands for VME extension for Instrumentation. It can accommodate a data transfer speed of up to 80 Mbytes/s. VXI [16] is a multi master bus with 13 slots for different modules.

VXI has more than 100 vendors provide a variety of modules. In control applications, the VME has very low interrupt latencies of up to a few microseconds.

4.3.1.3 Compact PCI

Peripheral Component Interconnect (PCI) bus [17] is a local bus standard developed by Intel Corporation for PC. PCI is a 64-bit bus, it usually implemented as a 32-bit bus. It can run at clock speeds of 33 or 66Mhz. At 32 bits and 33 MHz, it is able to provide a throughput rate of 133 MBytes/s. At 64 bits and 33 Mhz, it is able to provide a throughput of 264 MBytes/s.

The Compact-PCI is a Single board computed developed for industrial application, it is able operate under difference type of real time operating system. The board is able to transfer speed of up to a 264 MBytes/s peak rate for the PCI 64-bit transfers. Interrupt latencies of several milliseconds are standard with Compact-PCI, with some CPU boards based on PowerPC designs, it can go down to 100-µs interrupt latency, but still nowhere close to the performance of VME or VXI.

4.3.1.4 PXI

National Instruments developed PXI or PCI-X [17] standard. The theoretical data transmission rate is 132 MBytes/s for the 32-bit PCI transfer and double that for 64-bit transfers. There is a major drawback. Windows is the mandatory operating system, which prevents any real-time capabilities and PXI currently is not supported by a large number of vendors.

4.3.1.5 Technical Comparison

The following is the technical comparison for the four types of data bus. The comparison is based on the data throughput, real time capability, the analog accuracy, the support of open platform and the numbers of vendors.

	VXI	COMPACT PCI	PXI	VME
Data Throughput	80	132, 264	132	80
Real-Time Capability	Yes	Limited	Limited	Yes
Synchronization	Yes	No	Yes	no
Analog Accuracy	High	Middle	middle	middle

Open Software Platform	Yes	No	No	yes
Size	Middle	Small to middle	Small to middle	Small to middle
Number of Vendors	>100	<30	>8	>100

4.3.1.4 Selection & Choice

We have compared the PC bus systems for their specifications of data acquisition and control. We have chosen VME board, mainly because it provides middle analog performance, real-time capability, low interrupt latency and there are more then 100 vendors supporting this product.

4.2.3 Design Choice of Field Bus

There are many types of field buses and standard in the control industrial. The following are three of the most popular field buses, MODBUS, ProFit Bus and CAN bus. The following descript the operating mode of these there difference field buses.

4.3.2.1 MODBUS

MODBUS [14] is developed by Modicon, Incorporated in USA for industrial automation systems. The Modicon Programmable Logic Controller provides an industry standard method for sending & receiving messages.

MODBUS devices communicate using a master-slave technique, the Master device can initiate transactions. The slaves devices respond by supplying the requested data to the master, or by providing the action requested in the

query. A slave is any peripheral I/O device that processes information and sends its output to the master using MODBUS.

Masters devices can address individual slaves devices, or can initiate a broadcast message to all slaves. Slaves return a response to all queries addressed to them individually, but do not respond to broadcast queries.

Most of the peripheral I/O device and software for the industrial market is available and conform to the MODBUS standard.

4.3.2.2 PROFI Bus

PROFIBUS (PRO cess FIeld BUS) is the leading open field bus system in Europe. This standard provides wide range of applications in manufacturing, process and building automation. Profibus [15] is essentially a master/slave protocol. It uses memory exchanges between master and slaves to transfer input and output values. The drawback is that the master part of the system is more expensive and there's no peer-to-peer communications between slaves. The raw speed 1.5Mbps or 12Mbps but the throughput is usually much slow then the competing field bus. With PROFIBUS, devices of different manufacturers can communicate without any special interface. Siemens of Germany is one of the larger manufacturer companies that produce PROFI Bus PLC for process control and building automation.

4.3.2.3 CAN Bus

Robert Bosch Corporation developed Controller Area Network (CAN). It is originally developed to replace expensive wiring harnesses with a digital network in automobiles and today CAN [27] are also used in industrial automation. CAN primarily used in the interconnection of in-vehicle controllers, such as anti-lock brake systems and engine control units. CAN offers fast response and very good reliability under adverse environmental and electrical conditions. These attributes, along with cost-effective networking technology, also make CAN a good industrial network.

The CAN Protocol is an ISO standard for serial data communication. CAN uses the CAN protocol for peer-to-peer [3] communication . This protocol is not as

established as MODBUS and PROFI Bus protocol but there are a number of devices available in the market.

4.3.2.4 Technical Comparison

The following is the comparison of the MODBUS, PROFI Bus and CAN Bus.

	MODBUS	PROFI BUS	CAN BUS
Maximum number of Nodes without using Repeaters	32 xRS485 [14]	32 x RS485	No limit
Relations between Nodes	Master/ Slave.	Multi- master / slave	Master/Slave, TDMA, Daisy Chain
Speed (Bit rate)	Not higher than 38.4 Kbit/ s and most often 19.2 or 9.6 Kbit/ s	9. 6 / 19. 2 / 93. 75 / 187.5 / 500 Kbit/ s	Low speed 250Kbps, High speed Mbps
Maximum I/ O Per node	250 bytes for inputs and 250 bytes for outputs (analog/ Digital)	244 bytes for inputs and 244 bytes for outputs (analogue/ digital)	8 bytes for input and 8 bytes for output
Network management	Master/ slave.	Via token- ring between masters, otherwise master/ slave	CSMA/CD [5]
Stability of system	High.	High.	High.

4.3.2.5 Selection & choice

We have compared the field bus systems for their technical specifications. We have chosen MODBUS, mainly because of it is commonly adopt by the major PLC manufacturers, it provide very high system stability, it is a single master controller and support many types of sensors and input/output device.

4.3.3 Design Choice for PLC

We have identified three popular PLCs for evaluation. These PLCs include Rockwell, GE Fanuc and SIEMENS to provide real time data collection and data acquisitions.
The comparison is base on the field bus protocol; number of sensors can be configured, speed and scalabilities.

4.3.3.1 Rockwell PLC

The Rockwell controller [24] meets a wide range of data acquisition and control applications. It features ruggedness, low power consumption, broad communications capabilities, historical data archival, scalability, speed, and control.

It interfaces to a wide variety of measurement and control devices using I/O modules. The Modules are designed for accuracy, ruggedness, and survivability. The PLC handles a wide range of applications, including loop control configurable up to 16 control loops.

The rack based PLC enabling all the modules of a station to be fitted with power supply, processor, digital I/O, analogue I/O communication modules and other application specific modules.

4.3.3.2 GE Fanuc PLC

The GE Fanuc [25] provide 32 points digital inputs, 16 points static digital outputs for multiplexed digital inputs acquisition. The PLC come with 16 points relay digital outputs card for sending controls. The PLC support both MODBUS and PROFI Bus field base.

The Fanuc PLC is highly complex to configure and install .It is relative more expensive compare with other PLC in the market**.**

4.3.3.3 SIEMENS PLC

The SIEMENS PLC [26] distributed I/O network designed specifically for data acquisition and control applications. The PLC provides 20-bit measurement resolution and signal conditioning capabilities. Data rates up to 100 megabits/sec provide the speed needed for applications requiring precise real-time readings or control.

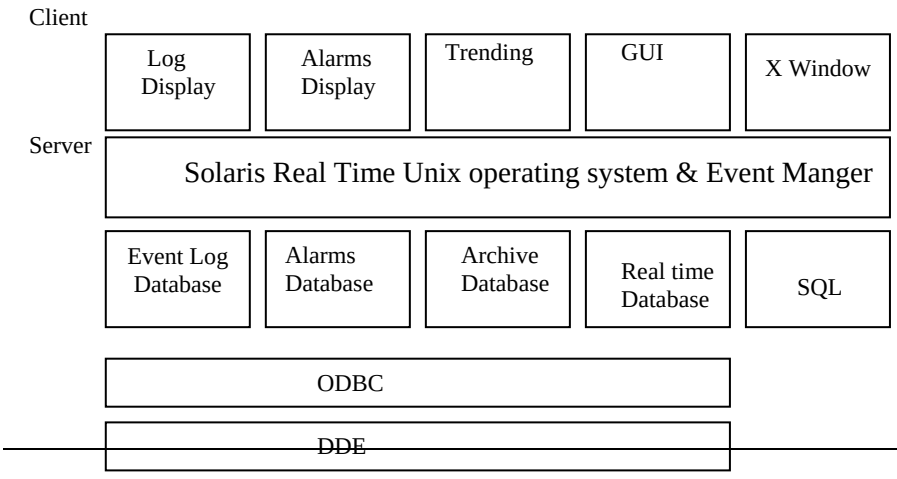
SIEMENS PLC uses a 10/100Base-T Ethernet or MODBUS RTU network and connects sensors, control valves, discrete devices, relays, and other distributed field devices. SIEMENS has been awarded many large-scale control projects in Singapore, it has a very strong local present and after sales support.

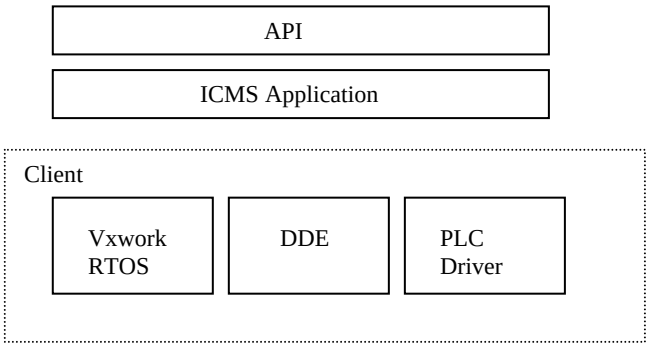
4.3.3.4 Selection & Choice

The SIEMENS PLC is selected based on it is able to operated in distributed I/O data acquisition with the RTU and the field bus is configurable to MODBUS. The most import is SIEMENS have strong present in Singapore and able to provide local technical support 24 hrs per day.

CHAPTER 5: SOFTWARE ARCHITECTURE

The main purpose of the ICMS application software is provide data acquisition and control from the operator console in Singapore to other ACC in the region. There are many commercial software are require for developing the ICMS software. The software includes oracle database software, network software, Embedded real-time operating system Vxworks, Sun Solaris real time UNIX [5] operating system, Factorylink data control and acquisition software, data dynamic exchange driver and X-windows etc.





Software Block diagram for ICMS

5.1 Software Description

The highly scalable software provides the following features and facilities:

- Advanced Graphical User Interface compatible with both X-Window and Windows 2000 multi-user architectures
- Easy to operate windowed interface with Pan and Zoom, de-cluttering, scalable graphics, modal pop-ups, data browse and entry widgets, automatic point details, user definable trends, etc.
- Redundant Server support with automatic fail-over and support for disaster recovery sites
- Redundant network and communications fail-over Support
- Distributed Alarm / Event Manager functions with alarm Distribution to remote servers, time tagging, user notes attachment and alarm/event analysis tools.
- Integrated historical value logging and trending system
- Integrated historical value logging and trending system.
- Structured entity/attribute point database for reduced engineering time.
- Support for manual value substitution, control tagging, bad value detection.
- A fourth generation Script real time applications environment.

- A comprehensive Open Database Connectivity source driver that use RDBMS systems (such as Oracle, Sybase and Microsoft SQL Server) as real time data sources.

Open Database Connectivity (ODBC) is an open specification for providing application developers with a predictable application programmers interface (API) with which to access data sources. ODBC [28] allows us to access several databases with a common code.

Data sources can be by someone has created an ODBC driver for it. The most common data source is an SQL server & Oracle server. The two major advantages of coding an application with the ODBC API are portable data access code.

- An Internet based reporting and display facility that allows corporate and remote data access using Microsoft Internet explorer.

- Front End Processor software that allows Windows 2000 servers to act as intelligent data acquisition gateways for a network of multiple, distributed servers.

- Easy to use, project based systems implementation tools including graphics builder.

- On-line integrated documentation and help system.

5.2 Central Management's Software Function

5.2.1 Devices Interfaces

The software can access field data from many devices. It can retrieve large volumes of data from Programmable Logic Controller, Remote Terminal Units and other field controllers. It can also send data back to these devices; typically this data consists of set point changes, switch settings and forward controls.

The software interfaces to these devices through drivers. Dozens of drivers for communication to site controllers are currently in existence. A driver toolkit that facilitates driver development is also available.

5.2.2 Real Time Data Dictionary and Data Modelling

The real time data that is gathered by the drivers is stored as a real time data dictionary. Each driver updates it's own section in the dictionary. The dictionary is stored in-memory for rapid data access.

The real time data can be retrieved using the entity-attribute model. The entity-attribute model is an object-oriented model where the data is structured to mimic the actual field devices. The structure of the entity-attributes is free format but usually reflects the underlying device or protocol architecture.

5.2.3 Historical Data

The software includes a historian that is used to store and archive historical trend data. The historian takes a list of entities and attributes and stores these at predetermined intervals. The data may be stored as snapshot samples, or as averages, maximum and minimum over a historical period.

The historical data is stored in a compressed format for optimal disk usage. The historical data is accessible through the software Scripts programming/reporting language.

5.2.4 Alarm and Message Manager

The software also includes an alarm manager and a message system. The alarm manager checks the real-time database for pre-determined events. The events may be simple such as the "The room temperature was too high" or complex such as "The backup generator diesel fuel level is running low and the main power is out".

The message manager collects all messages and places them in current and historical tables. Events typically stay in the current table until the alarm condition has been removed and an operator has acknowledged the event. As an option events can be annotated and removed by operators.

As well as the pre-determined events, all processes can generate messages. For example, a driver that communicates to a PLC will generate a message when it detects that the PLC has gone off-line, similarly it will generate another message when it detects that the PLC has come back on-line.

There are also tools to generate messages from GUI displays, reports and user programs.

5.2.5 Web Design Using Script Programming Language

A Web sever is required to be installed for remote control & monitoring from any part of the region. The web page is programmed through the Scripts programming language.

The Scripts language is an easy to use SQL-like language. It provides the user with a simple programming interface. The Scripts language is widely used in displays, reports and high-level control.

The Scripts language provides easy access to real time data, event data and historical data. The Scripts programs are written in simple text files and are interpreted by the Scripts interpreter just before their use.

Scripting languages designed for inclusion within the HyperText Markup Language (HTML) Document. HTML [29] is the basic building block of the design of a web page. The script is an integral part of the HTML Document delivered to the client by the server. It is interpreted and run within the browser application being used by the client. The most commonly used scripting languages today are JavaScript and its variants derived from Java.

- JavaScript
- JScript (Microsoft)

All these scripting languages, along with recent HTML language extensions supported or developed by Netscape and Microsoft for its Internet Explorer browser interact to enable the HTML environment.

5.2.6 Web Server Graphic User Interface (GUI)

All data can be viewed through the easy to use Graphic User Interface GUI. The GUI has a fully featured interface with widgets for panels, windows, simple text updates, color and shape changes, bar graphs, trend charts, browse boxes, various pop-up windows, moving complex lines, sprites and many others.

The graphics are stored in metafiles. The metafiles are an extension of Scripts. The metafile interpreter interprets the metafiles just before they are displayed. The GUI comes supplied with the Navigator. The Navigator is a metafile implementation of a browser. The Navigator contains toolbars on the top and the sides of the displays for ease of navigation through the displays. The Navigator comes with alarm, event, trend and help displays as standard.

The GUI is a thin client application, which means that the clients are easy to set up and administer.

5.2.7 Open Database Connectivity (ODBC) and Dynamic Data Exchange (DDE) interfaces

The software has both an ODBC interface and a DDE [30] interface. The ODBC interface is used to import tables and views from third party RDBMS systems such as Oracle, Sybase and Access. The tables are imported into the system using Scripts and may be manipulated like an internal data table using SELECT, UPDATE, INSERT and DELETE Scripts commands. The Scripts interpreter can also be used to pass on native commands such as SQL stored procedures. Data definition language DDL [2] allows two running application to share the same data. In the ICMS software the Application software and the RTU is able to use DDL to provide the date updating and data manipulation.

5.3 Data Networking Software

In a multi-server environment, the servers are linked together with a TCP/IP network. The source layer processes perform peer-to-peer communication to replicate changes to the data layer between machines. The peer-to-peer communication is normally disabled but can be enabled with some configuration settings.

The system message managers can also perform peer-to-peer communications. In this case each time the message handler is about to process an event that event is passed on to peer message handlers on networked servers. The peer message handler then processes the message on the peer server. The peer to peer [3] architecture makes the network extremely flexible, as there are many configurations possible to network two servers together

5.4 Site Management System Software

The software developed for the RTU processing allows:

- Standard I/O exchanges with process environment,
- Communications with the central computer,
- Diagnostics functions.

This software allows two kinds of access:

- Process data configuration for common users,

- Application program interface for software developers.

5.4.1 RTU Software Modules

The RTU application software is built around three modules:

- a real time kernel ,
- an I/O handlers module, in charge of interfaces with all the VME boards,
- an application module, in charge of the customized software.

The standard RTU software will be customized in order to take into account:

- the absence of direct I/O boards,
- the number of I/O serial lines,
- the Ethernet connection.

5.4.2 Real Time Operating System Module

This system uses a compact, multi-user, modular real-time operating system, well suited to the full spectrum of VME [13] bus-based applications, from mono-processor diskless targets to multi-user disk-based systems.
Ethernet with TCP/IP is fully supported for distributed applications. In addition, most of the VME boards are available with real time OS handlers.

The OS manages multiple I/O requests through time-sharing and multi-tasking. It features an easy-to-use UNIX-like shell and utility command set, a tree structured file system, and a device independent I/O system.
Professional programming environments, high-level language compilers (C, C++, etc.), debuggers, development and communication tools are available.

The generated code is fully re-entrant and is independent of its memory location. The real time OS is embedded into the PLC. It provides kernel and sequential access support.

5.4.3 Real Time Operating System (RTOS) Functions

The major OS functions are:

- Memory management: dynamically assign memory to the tasks, which need it. Real time OS allows a memory partition for specific use (Video RAM, battery save for example) and has a memory protection function.

- Scheduling: At every clock interrupt, real time OS scheduler may suspend the active task and run a higher priority one.
- Communication: Real Time OS provides four inter process communication structures:
  1. Memory modules with R/W accessible by the defined processes,
  2. Pipes (same as UNIX),
  3. Events for shared resources protection,
  4. Signals for synchronization of time-dependent tasks.
- Time handling: Real time OS provides a mechanism using the ALARM function, allowing cyclic or temporized signal emission.
- External events handling: All the external interrupts and exceptions are handled by the real time OS mechanism (IRQ interrupt service routine).

5.4.4 Real Time Operating System I/O Location Module

The real time OS is fully implemented in EPROM. During initialization, the OS code is loaded in RAM for faster execution speed. The real time OS provides an I/O system, which is independent of the hardware and modular. The working rules of the I/O system are the same as the UNIX.

The Real time OS provides five types of I/O managers:

- SOF (Sequential Character File manager) used for serial I/O ports,
- RBF (Random Block File Manager) for hard disks management,
- PIPEMAN (Pipe File Manager) for inter-process communication,
- SBF (Sequential Block File Manager) for sequential files management,
- NFM (Network File Manager) for LAN management

5.4.5 Description of the I/O Handlers module

The I/O Handlers module is dedicated to the monitoring of the RTU direct I/O boards and of the other systems via serial or LAN communication links.
It serves to:

- exchange data with Central Data servers and PLCs or others RTUs,
- Acquire field information,
- Command field information,

- Provide the Application module with the acquired data,
- Execute the commands sent by the Application module.

The I/O Handler module needs as many processes as it has connected servers. This module implements at least the following functions:

- Cyclic digital inputs acquisition with change of state detection,
- Cyclic analogue inputs acquisition,
- Cyclic metering inputs acquisition,
- Digital outputs command (pulse or maintained),
- Analogue outputs command,
- Serial and LAN protocols (TCP/IP, MODBUS)

5.4.6 Description of the application Software module

The main functions realized by the application software are:

- Acquisition of:
  a. digital inputs information
  b. analogue inputs information,
- Acquisition of serial inputs information (from PLCs, others RTUs, etc.),
- Interpretation and commands execution (Digital Outputs, Analogue outputs),
- Emission of serial outputs information (To PLCs, others RTUs, etc.),
- Data exchange with Central Data servers,
- Alarm management of the various RTU components,
- Maintenance with the help of a off-line and on-line test program

To perform these functions, the application module relies on the I/O Handlers module. The application software is based on a limited number of software processes:

- The direct inputs acquisition process: this process is in charge of grouping and packaging the various direct inputs (digital inputs, metering inputs and analogue inputs).

- The serial & LAN inputs acquisition process this process is in charge of grouping and packaging the various serial inputs type MODBUS, TCP/IP, etc.

All the inputs come from the I/O Handlers module. The generation processes which are in charge of updating the various output data (Digital outputs, serial outputs)

- The direct output emission process: This process is in charge of grouping the various outputs depending on their type (digital outputs, analogue outputs), and of the activation of the corresponding I/O handler process.

- The serial output emission process: This process is in charge of grouping the various outputs depending on their type (MODBUS, TCP/IP, etc.), and of the activation of the corresponding I/O handler process.

- The maintenance process which main functions are:

- Real time display of the various kinds of Inputs,

- Commands of the various kinds of I/O Outputs.

Each generation module is able to define a very simple macro language, allowing an easy configuration of the application.
For example, some of these basic operations are:

- Identification and initialization of variables
- Storage and restitution of intermediate results,
- Realization of Boolean operations,
- Loading, unloading of the result of a Boolean operation,
- Messages edition,
- Conditional processing of a list of operations, etc.

5.5 Main Design Choices of Software

The approach in developing of ICMS software was by using commercial off the self, high performance and reliable software. This is to minimize the risk in developments of new ICMS software.

5.5.1 Choice of Data Acquisition Software

Commercial off the Self Control & Data Acquisition Software

Several available Data Acquisition and Control software systems were evaluated, with some emphasis on a commercial off-the-shelf (COTS) solution:

5.5.1.1 iFix

iFix [21] software was developed by Intellusion Inc. It features new capabilities in data accessibility, and security features. The software is able to help reduce development time, improve connectivity, and provide greater overall control over the control processes. It is able to implementing multiple automation solutions in each ACC environment. For example, one of the Data acquisition application controls air-conditions, another controls fire alarms system, a third manages all the events etc.

Users can develop, manage, and alternate between multiple GUI & data acquisition applications from a single development Site. As a result, corporations and system integrators can greatly increase productivity, and effectiveness of their development personnel.

5.5.1.2 FactoryLink

FactoryLink [22] was a "Real-Time Application Development Tool Set" by USDATA Inc. FactoryLink is a process control systems, it provides huge and quite complex software systems with a substantial learning curve and the software come with substantial license costs. FactoryLink software is able to run exclusively under UNIX or other UNIX versions.

5.5.1.3 LabView

LabView is a "graphical programming environment for data acquisition and instrument control applications" by National Instrument. LabView [23] provides many predefined functions for instrument control in the areas of data communication, data processing and data visualization. A large variety of drivers and other software are available for all

kinds of instruments. However, it lacks typical process control functionality, like data logging, trending or alarming.

The LabView functionality is insufficient for the ICMS requirement while iFix is unable to operate in Unix platform and iFix is not scalable for future expansion. FactoryLink are adequate for ICMS requirement.

The following, certainly are the advantages and disadvantages comparison table:

5.5.1.4 Technical Comparison

	SOFTWARE	FUNCTIONALITY	PLATFORM	COST	SOFTWARE ENGINEER REQUIRE
1	Ifix	Insufficient	Windows	Low	Many
3	FactoryLink	Excellence	Windows, SUN, Unix.	Middle	Few
4	LabView	Insufficient	Windows	High	Few

5.5.1.5 Selection & Choice

The choice for the retime data acquisition and control software is Factorylink. The selection is based on platforms and functionality of the software can support and this software has been many proven track records on many large-scale projects.

5.5.2 Main Design Choice of Embedded Real Time Operating System (RTOS)

There are many embedded real time operating system in the market, We have short listed three of the more popular RTOS VxWorks, OS9 and QNx for more details evaluation.

5.5.2.1 VxWorks RTOS

Wind River Systems developed the real-time operating (RTOS) VxWorks [19]. It is a networked real time operating system designed for the distributed environment. VxWorks is the most widely adopted real-time operating system in the embedded industry. VxWorks is flexible, with many application program interfaces (APIs); scalable, from the simplest to the most complex product designs. It is reliable and used in mission-critical applications. It supported host platforms include Sun, and HP. It allows specific embedded platforms that integrate real-time operating systems.

VxWorks run-time system is the highly efficient; it supports a full range of real-time features including fast multitasking, interrupt support, and both preemptive and round-robin scheduling. The design minimizes system overhead and enables fast, response to external events. Vxworks also supports many buses, including PCI, CompactPCI & VME.

5.5.2.2 QNx RTOS

QNX real-time operating system provides a scalable, reliable foundation for embedded systems. QNX RTOS [20] were designed to be source-code identical across CPUs and boards. It enable the same code can run on different boards with the same CPU.

QNX RTOS has developed an efficient suite of embedding tools and runtime software components to provide cross-platform connectivity to a full-featured embeddable windowing system. QNX RTOS can operate with number of leading processors, including many highly integrated chips that save on space and cost. Supported processor families include x86 and PowerPC. QNX also supports many buses, including PCI, CompactPCI, VME

5.5.2.3 OS 9 Real Time Operating System

Microware Systems Corporation developed the Radisys Microware OS-9. It is used in Internet appliances, consumer electronics, wireless communication devices, industrial automation, office automation, automotive control, digital television, telecommunications, and multimedia devices. OS-9 [18] operating system provides a flexible, robust run-time environment. OS-9's middleware includes a multiprotocol

networking stack and advanced multimedia packages. OS-9 is also equipped with a set of APIs for graphics, audio and input.

OS-9 is a system-secure, fault-tolerant RTOS with high availability and reliability. Users can dynamically add and replace modules while the system is up and running. The OS-9 communications middleware and software such as IP internetworking and protocol stacks; platforms based on PCI, Compact PCI.

5.5.2.4 Selection & Choice

Vxworks has been selected as the RTOS for the RTU. It is the most popular RTOS, many API and proven software is available for the data acquisition and control.

5.5.3 Main Design Choice of Data Base Management Server (DBMS)

There are many DBMS in the market; the three most popular databases are Microsoft SQL database server, Oracle [8] database Server and Sybase [8] database server.

5.5.3.1 Microsoft SQL Database Server

Microsoft SQL Server is a relational database management system (RDBMS) [8]. The performance, reliability, scalability and access to information are the important benefits of an RDBMS. The Microsoft SQL sever provides a security storage for important data and built-in language for efficient data access and controls.

Microsoft SQL Server is designed to provide optimum performance even during peak load times. The query processor extracts data quickly and efficiently, returning it to the system with minimal delay.

Structured Query Language (SQL) [8] is the de facto standard language used to manipulate and retrieve data from these relational databases. By using (SQL), it enables a programmer or database administrator to do the following:

- Create table
- Add data
- Delete data
- Modify a database's structure
- Change system security settings

- Add user permissions on databases or tables
- Query a database for information

5.5.3.2 Oracle Database Server

Oracle is one of the world's most popular database management and information retrieval systems. Oracle database software runs on PC's, workstations, Windows Servers, Unix systems and others operating systems. The Oracle9i Database provides the following key features:

- The processing is split between the database server and the client. The data base server handling the database management and client application programs concentrate on the interpretation and display of data.
- Oracle supports very large database sizes and can have a large number of concurrent users while maintaining high throughput transaction processing.
- Oracle uses the SQL language, a standardized language for defining and manipulating data in relational databases.

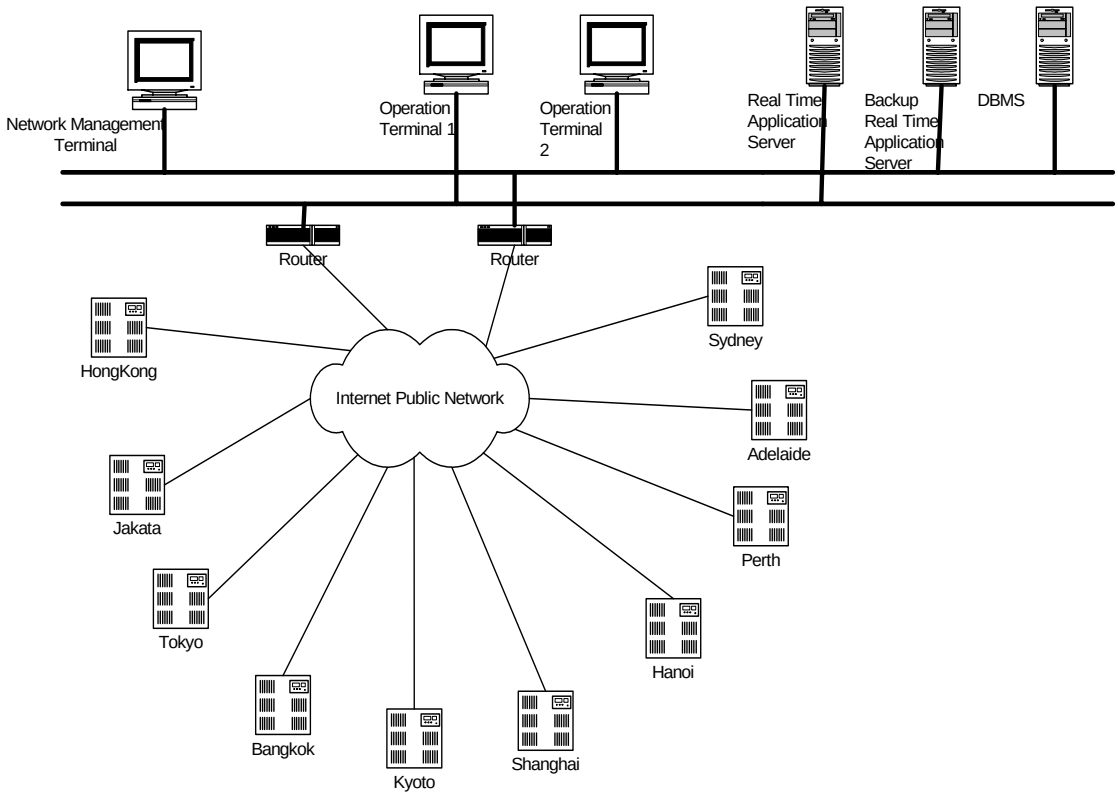
5.5.3.3 Sybase database

Sybase is a commercial SQL server that is highly reliable, very fast, and compatible with MS SQL. Sybase is able operate across both UNIX and Linux platforms.

5.5.3.4 Selection & Choice

We have chosen Oracle as the database management system server based on it can support very large database. It is also popular and proven reliable in the RDBMS market with the ability of interface with ODBC and uses SQL language**.**

CHAPTER 6: NETWORK ARCHITECTURE & SECURITY MANAGEMENT



6.1 Network Architecture

The ICMS Network is made up of individual Local Area Network together through the broadband Internet forming the ICMS Virtual Private Network. Each local LAN interfaces with the Internet broadband network, which is essentially the public network for data transfer between the Control and Monitoring Center and remote sites. The LANs are built on 10/100 Mbps Ethernet switches and routers.

6.2 Interfaces with Internet

The Internet broadband network provides communication links with others ACC, the interfaces equipment are as follows:

- Dual 8 Mbps link Central Management System Center and Site Management System based on 10 remote sites.
- at Monitoring Control Center, a two routers with two broadband interfaces, each with 8 Mbps line speed.
- at remote Sites, two routers; each router supports two broadband interfaces with 512kbps line speed.

The links between the CMS's Monitoring Control Center and each Site will be two number of 2mbps link (1 primary and 1 standby)

At the Monitoring Control Center, the network routing systems includes:

- Dual Internet broadband Router
- Dual 24 ports internet switch
- Dual Power supply

6.3 Local Area Network (LAN)

The local area network architecture is based on dual LAN duplicated Ethernet switches which link Ethernet segments. In principle, each segment is "bridged" toward the other ones. There are equipment; server, workstation, or RTU connected on each segment.

This configuration allows:

- a maximal throughput 100 Mbps with minimum collisions on each segment,
- isolation of faulty segments,
- an easy management of dual connections on separate segments.

6.3.1 Central Management System LAN

The Center Management System is located in the monitoring and control center. The equipment is connected on Ethernet switches, which communicate together. The ICMS real time server and network administration workstation are connected on 10/100 Mbps fast Ethernet [10] dual LAN switches and the Site Management System.

6.3.2 Site Management System LAN

Considering the data flows on the network, 10 Mbps Ethernet redundant switches are used for connecting the equipment. Each server, workstation and Site Management System will have dual connections, each on a switch. Each router is connected on a separate switch, so that in any cases there are two ways for the Site servers to communicate through the Internet broadband network.

6.4 Network Management

A Network Management Workstation using a sun workstation loaded with X-Window and LAN Network Management Software. The workstation is to provide to monitor to all the SNMP enabled network equipment.

6.5 Security Management

6.5.1 Security Measures to the ICMS network

As the networks linked to the Internet may be more easily accessible to cyber attack and hackers. ACC can heighten its level of network security by isolating its ICMS network thereby restricting channels of external access.

Many measures can be taken to secure the network and operating environment from unauthorized access to the ICMS systems. These include:

- Authentication
- Firewalls
- Virtual Private Networks

6.5.1.1 Authentications and Authorization

Authentication [4] is the software process of identifying a user who is authorized to access the ICMS system. Authorization is the process of defining access permissions on the ICMS system and allowing users with permissions to access respective areas of the system. Authentication and authorization are the mechanisms for single point of control for identifying and allowing only authorized users to access the ICMS system, thereby ensuring a high level of control over the system's security.

To provide effective authentication the system must require each user to enter a unique user name and password. Users must be able to be created, edited and deleted within the system while the system is active to ensure that individual passwords can be maintained. It is highly recommended that password aging be implemented. Password aging ensures that operators change their passwords over a controlled time period, such as every week, month or so on.

To provide authorization the system must be able to control access to every component of the control system.

LEVEL OF ACCESS	OPERATORS AND USERS	ACCESS FUNCTIONS
4	All	Monitoring of ICMS screen display
3	Operators	Include all level 4 functions, acknowledge alarms, turn equipment on/off, change & disable controllers and alarms.
2	Instrument Engineers	Include all level 3 functions, view any screen, analyze all alarm reports, & simple configuration
1	Systems Manger	Include all level 2 functions, complex configuration, system modification & assign and authorise level of access.

6.5.1.2 Implement a Secured firewall

The ICMS network has more than one filter firewall, a router separating it from the external network that is not within the network. When examining the firewall solution, we have consider how the firewall can supports security services.

The ICMS has implement two types of firewalls;

- Packet Filtering Firewalls.

- Proxy Servers.

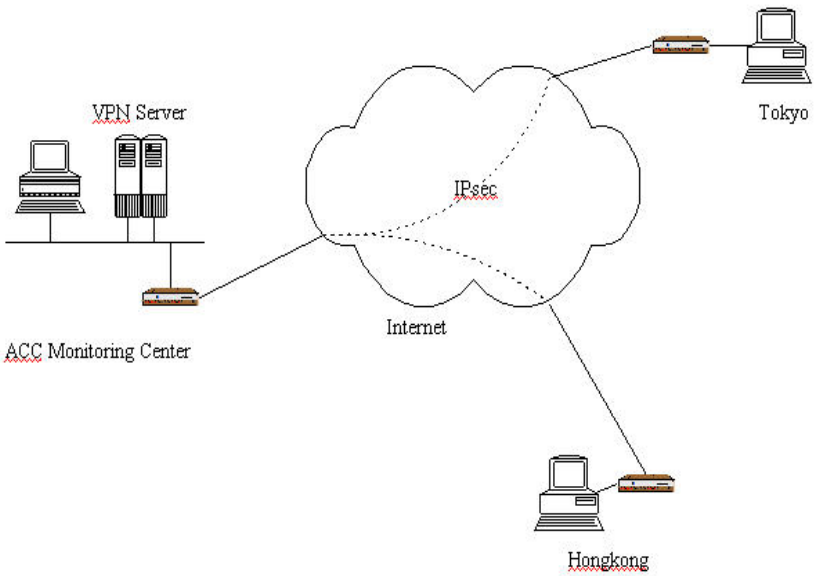
6.5.1.2.1 Packet Filtering Firewalls

A filtering firewall [11] works at the network level; the firewall is built into the network router and switches. The packets received are filtered by their type, destination address, source address, and port information contained in each packet. Data is not allowed to leave the system if the firewall rules do not permit it.

6.5.2.2 Proxy Servers

Proxy Server [11] provides the control and monitor of outbound traffic to the network. It thus also captures the information of what is transferred.

The system has implemented by providing an additional proxy firewall between the Central Management System and the external network. This is to maximize access and minimize the configuration required to maintain this firewall, a proxy server can be used to act as a gateway. Only traffic from the proxy server can pass into the ICMS network and prevent for external applications to be used to attack the control system.



6.5.1.3 Implement Virtual Private Network

One of the main security issues facing more for ICMS networks is remote access through Internet. With a VPN [1] all data are secure and to limited group of persons. In the ICMS network, the VPN main task to identify and to authenticate the remote site. Once this has been done, and each VPN knows who it is talking to, an encrypted tunnel can be set up to protect the passage of data between two VPNs. Each end is responsible for encrypting and decrypting the traffic flowing between them and it is transparently to the users.

VPN is a secured way of connecting to remote ICMS networks. Based on the existing public network infrastructure and incorporating data encryption and tunneling techniques, it provides a high level of data security.

There are several benefits from using VPNs. The first is cost. VPNs allow ICMS to make use of low cost public network and infrastructure. By using the Internet technology it is far cheaper than leased lines or frame relay networks. It is more flexible and it is easier to scale up and down when the demand increases.

6.3.1.3.1 Applied Security Protocol

IPSec (IP Security Protocol) was developed by a IP Security working group of IETF (Internet Engineering Task Force). IPSec [1] is a set of mechanisms designed to protect the traffic at the IP layer, it adds security services to the IP layer. The security services provided by IPsec are data confidentiality, data integrity, data origin authentication and protection against replays.

IPsec can be implemented within a network to provide computer-level authentication, as well as data encryption. IPSec is typically used in one of two modes, gateway-to-gateway or client-to-gateway. IPsec can be used to create a VPN connection between the two remote networks.

In the ICMS network, each site deploys a gateway and then sends data over the public Internet. All traffic between gateways rides in a virtual "tunnel". The tunnel both verifies the authenticity of sender and receiver and encrypts all traffic.

6.3.1.3.2 Communication & Data Storage

Importance data pertaining to a ICMS system must be securely persisted and communicated. It is importance that critical data like a password be stored using an encryption algorithm. Similarly, remote login processes should use VPNs with IPsec encryption to communicate the user name and password over the network. The

importance data like user name and password must be secured and access rights monitored and managed using secured mechanisms like Windows authentication.

6.6 Design Choice for Security Network Equipment

Three gateways Netscreen 1000, Cisco 7100, Bick 80 is able to meet the requirement for the ICMS that provide the best combination of security, scalability, ease of use.

6.6.1 NetScreen 1000 VPN router

NetScreen Technologies Inc developed netScreen-1000 [31]. It is an enterprise class firewall and Internet Protocol Security (IPSec) Virtual Private Network gateway. NetScreen firewalls support the standard security protocol, IPSec.

6.6.2 Cisco 7100 VPN router

The Cisco 7100 [32] VPN Router from Cisco Systems Inc. It offers strong security; VPN Routers integrate key features of VPNs tunneling [11], data encryption, security, firewall, advanced bandwidth management, and service level validation to provide secure, scalable VPN platforms. This router provide good management features and supports more concurrent connections than other gateways.

6.6.3 Lucent Brick 80 VPN router

The VPN Firewall Brick 80 [33] from Lucent Technologies offers excellent management, good performance. The products are firewall-based VPN appliances that are installed between the WAN router and LAN. The VPN Firewall Brick 80 is capable of supporting up to 400 simultaneous tunnels with 8 Mbps encryption throughput. This unit provides the best price performance ratio of any of the high-end devices.

6.6.4 Selection &Choice

Netscreen 1000 was selected for this project based on it meet the security requirements and it was the cheaper available router amount the three choices.

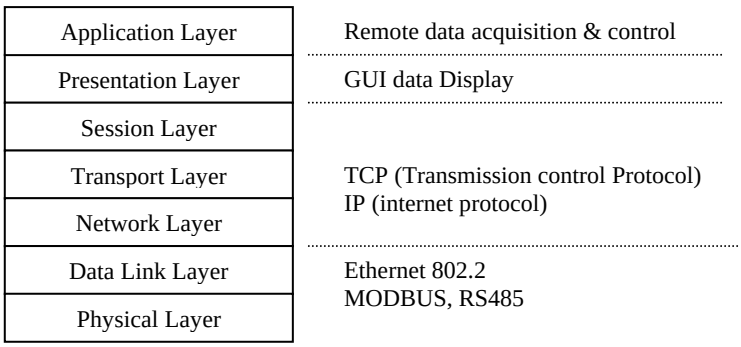
CHAPTER 7: PROTOCOL AND MEDIA

The Local Area Network architecture that we propose uses 100 Mbit/s Ethernet protocol [10] for LAN transmissions. The system in different locations is based on the use of duplicated Ethernet switches, providing independence of the different generated networks, either with 100Mbps bandwidth.

The hardware includes the Router, Switches. The proposed network is based on a dual 100Base-T Ethernet LAN. The hardware used to generate the network consists of two 10Mbps switches. The connection to the Communication Backbone Network is linked by two routers, which are dedicated to the communication with the ICMS. The two routers are connected in a primary and standby link configuration.

The system is complied with Open System Interconnect (OSI) [5] reference model. The protocol architecture defines the guidelines, which regulate data communications over networks. The network is applied to the network layer of the OSI's model; in this environment, it uses the IPX protocol. This encompasses both Local Area Networks (LANs) and Wide Area Networks (WANs). The network was

using the Internet Protocol (TCP/IP) to communicate with others ACC subsidiary in other part of the word.



7.1 Application Layer

The Application layer defines guidelines for application user interfaces and communications between applications. The system uses file transfer protocol (FTP) and simple mail transfer program. File Transfer Protocol (FTP) [10] allows the client to transfer files between local hard drive and a remote server.

One of the ICMS requirement is to monitor and control through the ACC web site, it is done by transferring files to a Web server, it provides monitoring and control the facility of ACC from any location where is internet available.

Hypertext Transfer Protocol (HTTP) [10] is protocol used for browser transfers files in the CMS from web servers to graphically display web content on the operator console.

7.2 Presentation Layer

The ICMS display the real time ACC facilities alarms and control data through GUI graphic display. The Presentation layer provides and defines the guidelines to present data to and data format of the receiver. Presentation layer provide uses services such as Data compression, expansion, encryption [11], and decryption at this layer.

7.3 Transport Layer

Transfer Control Protocol (TCP) is corresponds to the Transport layer, but TCP also contain some session layer function. TCP is responsible for establish a session between the CMS and the RTU user on the ICMS network.

The network has been design to use the TCP/IP protocol [10] to transfer data. The Transport layer defines the guidelines to provide reliable data delivery over networks. TCP/IP protocols conform to a four-layer model based on a three-layer (Link, Transport, and Application). This is accomplished through connection establishment and termination, data acknowledgment receipts, sequencing, and data flow control.

It is primary encapsulating information into a datagram [10] structure, transmitting datagrams and keeping track of their progress. It handles the retransmission and lost datagrams and ensures reliability on the destination receiving of a message, TCP extracts the message from the data structure and forward it in to the destination application program. TCP will add a header containing its control information to any data coming from application program to create diagram. The Internet Protocol IP will add its own header containing its own local network control information n the form of its own header to the datagram.

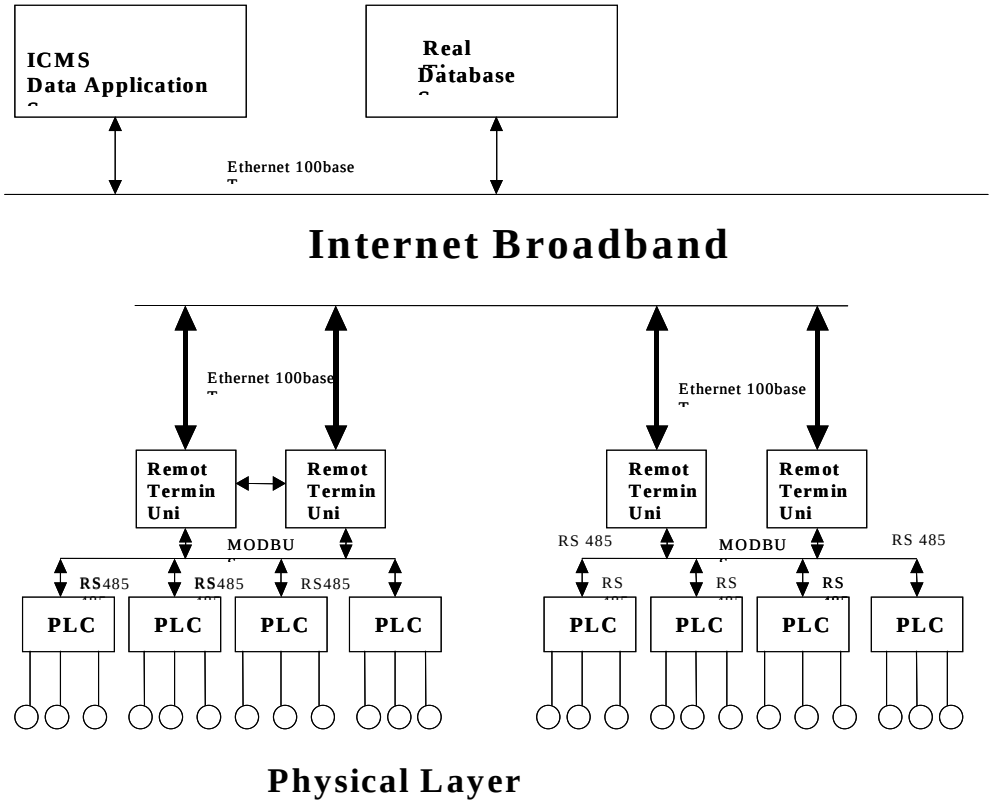
7.4 Network Layer

The packet is forwarded, to the target host. Novell NetWare is the operating system for this network and the protocols comply to an Open Systems Interconnection (OSI) [10] seven-layer model fourth Network layer.

The Network layer defines the logical organizations of data bits into packets and moves information across networks. Examining the network layer address defined in the packet and forwarding the packet to the next point on the network.

7.5 Data-Link Layer

The Data-Link layer defines the logical organization of data bits into frames and provides a transparent, error-free transmission path from the Network layer to the Physical layer. The CMS and RTU use the TCP/IP as the communication protocol for sending and receiving data. TCP/IP protocol stacks [11] are based on different data communication standards. Each layer defines data communications standards that can be implemented through single or multiple protocols. Interfaces between adjoining layers are well defined to allow smooth data flow through the stacks.



7.6 Physical Layer

The Institute of Electrical and Electronics Engineers (IEEE) 802 standards are also partially defined at the Physical layer. In the remote sites the interface physical layer standard is RS-485, the serial port interface use on the remote terminal unit (RTU) to communicate with the Programmable Logic Controllers (PLC). The Physical layer defines the electrical and mechanical characteristics of the network interface hardware and network medium, coaxial, twisted-pair, optical fiber, etc. This also includes methodologies to place and retrieve data from the network

medium. In the design the local area network uses the unshielded twisted pair cable for the switches connection.

7.6.1 Unshielded twisted pair

This type of cable allows the radiation generated within the cable to escape, it preventing interference with the data in the network. The system uses UTP cable to carry the 100Mbps Ethernet transmission in Central Management System (CMS) and RS 485 in Site Management System (SMS).

CHAPTER 8: SYSTEM FAILURE S & RECOVERY

The following paragraphs analyses most of the failure modes and their impact on the availability of the system functions.

8.1 Central Management System Equipment Failures

8.1.1 Operator Position Terminal Failure

The failure of an operator position will have a minimum impact on the operation of the system due to the standardized design of the operator position. Any operator position can backup each other and the assignment of an operating role to an operator position is simply a matter of a user connecting to the system by entering the username and password. So, in case of a failure of an operator workstation, the operator can use any another workstation.

The software installation is identical on the operator positions throughout the system. The only difference resides on the configuration files, which differ slightly from one workstation to another (for instance the IP address of the various workstations are of course different).

8.1.2 Central Management System Data Server Failure

The failure of a ICMS server has a minimum impact on the operation of the ICMS due to the hot / stand-by configuration of the two pairs of servers.

In normal operation, the hot and the stand-by servers both maintain the real-time status of the monitored equipment, but only the hot server communicates with the operator positions, and sends controls to the RTU. The two servers monitor each other continuously through a watchdog facility.

If the stand-by server detects the failure of the hot server, then it automatically recovers all the functions previously assumed by the hot server, and becomes the new hot server. The hand-over only takes a few seconds and has no visible impact on the operator positions. An alarm is raised to inform the operator of the hand-over.

When the failed server is available, it needs to be synchronized with the hot server in order to update its real-time database. When this process is achieved, the failed server becomes the new stand-by server.

8.2 Site Management System Data Server Failure

Site Management System still available, all the data from Site Management System will be sent to the central computer in order to update the status of the Site part of the real time database.

8.2.1 DBMS Server Failure

Since the DBMS server is collect data from the real-time ICMS data servers, the only impact of the failure of this computer is that historical records are only partially available.

8.2.1.1 History Logging

In normal operation, there are two levels of history logging:

- the first level is performed by the real-time ICMS data servers, for short-term,
- the second level is performed by the DBMS server, for long-term.

Cyclically, the historical records of the real-time servers are downloaded to the DBMS server for long-term archiving.

When the DBMS is not available, this download cannot be performed, and only the operators can access the short-term historical data. The historical records of the real--time servers will be dimensioned in such a way that they can support the unavailability of the DBMS (typically one day). If the limit of the historical records on the real-time server is reached, the older events are over-written.

8.3 Central Management System Failure

The Central Management System failure means that equipment is not available within the Monitoring Control Center (Operating Positions, Servers etc.). This case should be very unlikely due to the duplicated architecture, but if such case occurs, two scenarios can be envisaged:

- The Central Management System can recover proper operation within a short time (typically less than one or two hours),
- The Central Management System is unavailable for a long period.

In the first case, the system can be operated from the monitoring center and the operator console, which have most of the control of the Site functionality. In the second case, it should be decided to activate the backup server where all the operation will be available again.

8.4 Site Management System Failure

The Site Management System failure means that no equipment is available within the Site. If the Site Management System is still available, all the data from the remote management

system will be sent to the central computer in order to update the status of the Site part of the real-time database.

8.4.1 RTU Failure

The failure of one RTU has a minimum impact on the global operation of the system, since they are duplicated in a hot / stand-by mode.
In normal operation:

- the hot RTU acquire data from the PLC
- only the hot RTU communicates with the real-time data servers, receiving controls or sending changes of states.
- the stand-by RTU also communicates with the real-time data servers, but only to monitor its proper operation.
- the hot and stand-by RTU communicate with each other to mutually monitor their proper operation using a watchdog facility.

When the stand-by RTU detects the failure of the hot RTU, it automatically becomes the hot RTU and recovers all the functions previously assumed by the hot RTU. The hand-over only takes a few seconds and has no visible impact on the operator positions. An alarm is raised to inform the operator of the hand-over.

8.4.2 PLC Failure

The failure of an acquisition PLC has a minimum impact on the global operation of the system due to the distributed architecture of the Site Management System and only the data acquired from that PLC will be unavailable. The case of a PLC failure is very seldom due to the high availability of the proposed hardware.

8.4.3 Site Management System Total Failure

In case of a Site Management System failure (including both RTUs for instance), all the information coming from this RTU is no longer available. This is very unlikely due to the high availability of the proposed hardware, and to the duplicated hot / stand-by configuration.

8.5 Network Failure

8.5.1 Site Management System LAN Failure

The LAN architecture is based on duplicated Ethernet switches; three scenarios of LAN failure can be envisaged:

- failure of one Ethernet segment : If the connected equipment has a dual connection server, the equipment switches on the other LAN, else the application switches on its stand-by equipment (RTU, server). The hand-over only takes a few seconds and has no visible impact on the operator. An alarm will be raised immediately.

- failure of one router : All the application switches on the other LAN equipment. As in the previous case, the switch only takes a few seconds and has no visible impact on the operator. An alarm is raised immediately.

- Total failure of the Site LAN : The remote Site equipment is no longer available. This case is identical to the PMS total failure. This case is very rare due to the high availability of the proposed hardware, and to the duplicated configuration.

8.5.2 Central Management LAN Failure

The CMS LAN architecture is based on duplicated Ethernet switches and on dual connection to all the equipment. Similar to the SMS LAN, three scenarios of LAN failure can happen:

- failure of one Ethernet segment : If the connected equipment has a dual connection server, the equipment switches on the other LAN, else the application switches on its stand-by equipment (RTU, server). The hand-over only takes a few seconds and has no visible impact on the operator. An alarm is raised immediately.

- failure of one switch : All the application switches on the other LAN equipment. As in the previous case, the switch only takes a few seconds and has no visible impact on the operator. An alarm is raised immediately.

- Total failure of the LAN: ICMS is no longer available and the corresponding enhanced functionalities are not available. This case is identical to the CMS total failure. This case is very seldom due to the high availability of the proposed hardware, and to the duplicated LAN configuration.

CHAPTER 9: ICMS IMPLEMENTATION PLAN

The implementation action plan consists of Project organization, Review of software & hardware requirement, Project management & installation, Overall System acceptance test, Management briefing, User training and Post Implementation review.

ACTIVITIES	RESPONSIBILITIES	COST	SCHEDULE	
		$1,825K	Start	End
1. Project Organization				

• Organize project team. • Objectives & responsibility • Set project milestone • Monitoring and Implementation	Project Manager	-	Jun'00	Jul'00
2. **Review of Software & Hardware Requirement**.				
• Database management • Data acquisition and control • Trending/Historical data • Network Management • Web page & access	• ACC Operation Manager, • Project Manager, Hardware Engineer, • Software Engineer	$300K	Aug'00	Feb'01
3. Project Management/ Installation				
• Hardware installation • Network installation. • Software installation • System performance test	ACC Operation Mgr / ACC Management/ Project Manager	$1500K	June 01	Dec'02
4. Management Briefing				
• Review process flow • System capability overview • Security & Auditing capability • Management Reporting	ACC ops Manager/Project Manager	$5K	Jan '03	Sep'03

5. User Training				
• System Overview • Control & monitoring of site data • Software functionality • User reporting capability • Web access	Training Manager/Admin	$20K	Oct'03	Nov'03
6. Post-Implementation Review				
• Identify slacks and rectifying. • Acceptance of system • Completion of project		-	Nov'03	Dec'03

CHAPTER 10: SYSTEM PERFORMANCE TEST AND RESULTS

There are three types of acceptance test in implementation of ICMS, namely the hardware test in CMS, hardware test in SMS, VPN Network throughput test, Data respond time test, ICMS software application performance test.

The local test is to provide hardware and software system check before it proceeds for the overall acceptance tests. The overall test is to test the overall operational performance of the ICMS.

10.1 Hardware Test in Central Management System

This local test is to check and verify the hardware equipment in CMS is conforming to the specification and requirements by the ICMS. This test is to provide a system check on the equipment to ensure the equipment is able to operate according to specification.

	CENTRAL MANAGEMENT SYSTEM (CMS)	TEST METHODS	RESULTS
1	Operating position terminal Sun Solaris Workstation 1	• Turn on the workstation. • Load in the X- windows • Load in the ICMS software	Satisfactory Satisfactory Satisfactory
		• Run the GUI with test I/0 data to verify the trending, data acquisition & control functions • Ping the Operating terminal two and wait for replay. • Ping the proxy fire wall for and wait reply • Ping the VPN router and wait for reply	Satisfactory Satisfactory Satisfactory
		• Ping the data base server for and wait for reply	Satisfactory Satisfactory
2	Operating position terminal Sun Solaris workstation	• Turn on the workstation. • Load in the X- windows • Load the ICMS software • Run the GUI with test I/0 data to verify the trending, data acquisition & control functions • Ping the Operating Station 2 for and wait replay. • Ping the proxy fire wall for and wait reply • Ping the VPN router for and wait reply	Satisfactory Satisfactory Satisfactory Satisfactory Satisfactory Satisfactory Satisfactory Satisfactory

		• Ping the data base server and wait for reply	
3	Solaris Real Time application & data Server	• Receive monitoring status from sites • Turn on and off air-condition and generator Monitoring of room temperature • Turn on and off lighting • Turn on and of water pump • Monitor the water level	Satisfactory Satisfactory Satisfactory Satisfactory Satisfactory
4	Hot standby Solaris Real Time application & data Server	• Switch of main Solaris application server • Carry out test as item 3	Satisfactory Satisfactory
5	Oracle Database Server	Create, edit, delete and display of 50 records	Satisfactory
6	Netscreen 1000 Firewalls and Proxy Server & router	• enter wrong password to denies access of unauthorized user • denies access from unauthorized IP address • denies access to unauthorized IP address	Satisfactory Satisfactory Satisfactory

10.2 Hardware Test in Site Management System

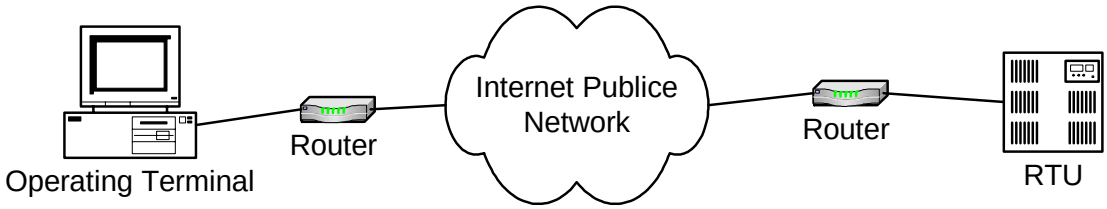
There are totally ten remote sites to be control by the CMS. This test is to cover all the remote sites require monitoring and control by ICMS form Singapore. The purpose of this local test is to check and verify the hardware equipment in SMS is conforming to the specification and requirements by the ICMS. This test is to be conducted before the ICMS Application Software performance Test.

	SITE MANAGEMENT SYSTEM (SMS)	**TEST METHODS**	**RESULTS**
1	Remote Terminal Unit (RTU)	• Set up the RTU with the PLC • Connect the PC with the ICMS software to RTU to receive and send logical test data from/to PLC	Satisfactory
2	Programmable Logic Controller (PLC) Digital Inputs	• Provide a logical “0” and “1” to the digital I/O input until RTU received this data	Satisfactory
3	Programmable Logic Controller (PLC)	• Send logical “0” and “1” from RTU to the digital outputs. • Monitor the outputs from the ICMS	Satisfactory

	Digital I/O Outputs	software in correspond to the logical input data.	
4	Programmable Logic Controller (PLC) Analogue I/O inputs	• Connect the dc power supply to the analogue input. • Adjust at the input of PLC from 1v to 12vdc in the steps of 0.5Vdc. • Monitor the analog input level from the ICMS software in correspond to the PLC input	Satisfactory
5	Programmable Logic Controller (PLC) Analogue I/O outputs	• Set the analog output level for 1Vdc to 12Vdc in the steps of 0.5Vdc from the ICMS software • Monitor the analogue output voltage of PLC from 1v to 12vdc in the steps of 0.5Vdc according to the ICMS setting.	Satisfactory
6	Router and 100base T switches	• Connect a PC Ethernet port to the router with the100 base T switch. • Use IPCONFIG/All command at dos prompt to find out the IP address of the router. • Use the ping command to ping the router's IP address. • Monitor the packet reply from the router.	Satisfactory

10.3 VPN Network Throughput Test

This test is a measurement of how fast data flows through the router. The test is to send a one Megabyte file from operating terminal to the remote RTU. It then measures how much time it takes from the transmit terminal to the receive terminal. From the file size and the time takes, it can then compute the data transfer rate, the result is in Megabits per second. The data transfer rate usually run between 0.5 to 1 Mbps with the 2 Mbps Internet communication backbones.

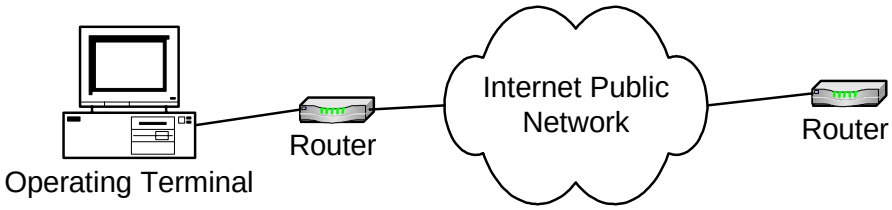


	CENTRAL	OVERSEAS SITES	DATA TRANSFER RATE
1.	Singapore ACC control center	Hong Kong ACC	1.5 Mbps
2.	Singapore ACC control center	Bangkok ACC	1.2 Mbps
3.	Singapore ACC control center	Tokyo ACC	1.8 Mbps
4.	Singapore ACC control center	Kyoto ACC	1.8 Mbps
5.	Singapore ACC control	Shanghai ACC	1.6 Mbps

	center		
6.	Singapore ACC control center	Jakarta ACC	0.5 Mbps
7.	Singapore ACC control center	Hanoi ACC	0.8 Mbps
8.	Singapore ACC control center	Perth ACC	1.6 Mbps
9.	Singapore ACC control center	Adelaide ACC	1.6 Mbps
10.	Singapore ACC control center	Sydney ACC	1.6 Mbps

10.4 Date Response Time Test

This test is to measure the latency of the router and proxy server introduces into a data stream. It is measure by using the ping command from the one of CMS's operating terminal to remote router. This test sends a small packet of data from one computer to RTU and measures the time it takes to receive a reply. Repeat this test ten times to compute the average and maximum times for the packet transfer. The typical time requires shall not greater than 10 milliseconds. The delay is probably greater if the connection is connected through Internet.



	CENTRAL	OVERSEAS SITES	LATENCY (MS)
1.	Singapore ACC control center	Hong Kong ACC	6 ms
2.	Singapore ACC control center	Bangkok ACC	5 ms
3.	Singapore ACC control center	Tokyo ACC	7 ms
4.	Singapore ACC control center	Kyoto ACC	7 ms
5.	Singapore ACC control center	Shanghai ACC	9 ms
6.	Singapore ACC control center	Jakarta ACC	8 ms
7.	Singapore ACC control center	Hanoi ACC	10 ms
8.	Singapore ACC center control center	Perth ACC	3 ms
9.	Singapore ACC control center	Adelaide ACC	3 ms
10.	Singapore ACC control center	Sydney ACC	3 ms

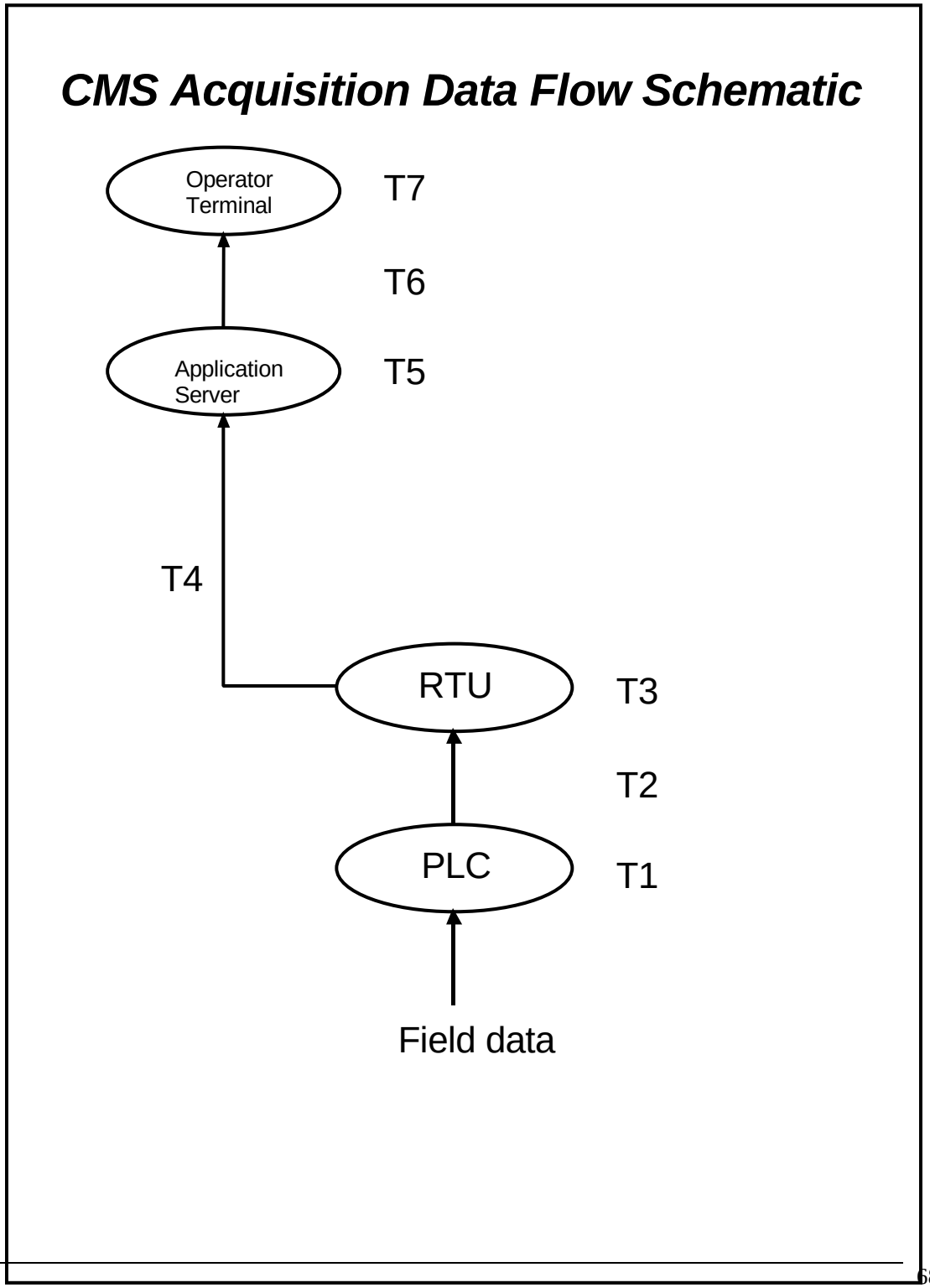
10.5 ICMS Application Software Performance Test

The following is the test procedures for the ICMS software, the various tests;

- The log in test is to authentic the user id and password for the authorized user access.
- The data acquisition test is to activate on/off switch, open/close contacts and level adjustment for the selected equipment. The system will automatically capture the time takes for every event activated.
- The Analog value test is to measure and adjust the analog value with the in compare with the actual value. Room Temperatures, water level, fuel tank level is some of the events to be tested.
- The Analog value test is to measure and adjust the analog value with the in compare with the actual value. Room temperatures, water level, fuel tank level is some of the test points to be tested.
- The historical database test was to retrieve the event-triggered value from the Oracle database. Every event will record with the time stamp and value for analysis.
- The trending test was to retrieve the analog event values from Oracle database and plot a chart over a period of time. e.g. to retrieve a room temperature over one week.
- The Availability test was to the switch over to the hot standby servers. The test will conduct on the ICMS serve and Oracle database server in CMS. The test will also will be conduct for the hot standby RTU in various sites.
- The system reliability test was to continue to conduct the data acquisition test, analog value test and historical database test for 48 hours without any failure.

	ICMS Application Software Performance Test	**Types of Test**	**Location**	**Results**
1	The ICMS software was able to log in to the Solaris server	Log in Test	Central / Remote Site	Satisfactory
2	i. The ICMS software was able to read the acquired and control data with proper tag name from the ICMS Site. ii. Repeat the test for another site.	Data acquisition test i. on/off, ii. open/close iii. Level adjustment	Central/ Remote Site	Satisfactory
3	The ICMS software get the correct temperature and water level value	Analog value test	Central/ Remote Site	Satisfactory
4	The ICMS software is able to store and retrieve data value from the database.	Historical Database Retrieve Test	Central/ Remote Site	Satisfactory
5	The ICMS software is able to plot the trend with the historical data	Trending with historical data	Central/ Remote Site	Satisfactory
6	Switch off one server and activate the failure take over function	Availability Test	Central/ Remote Site	Satisfactory
7	Repeat data acquisition test, Analogue Value Test, Historical database test for 48 hrs	Reliability Test	Central/ Remote Site	Satisfactory

10.6 Evaluation of data acquisition and update time
(From CMS Operator Terminal)



10.6.1 Data Acquisition Time from CMS operator terminal

TIME REQUIRED (MS)		MIN (MS)	MAX (MS)	MED (MS)	REMARKS
PLC Acquisition	T1	1	200	100	
RTU Acquisition	T2	300	600	450	RTU polling frequency: 2 Hz Transmission Time: 100 ms
RTU Processing	T3	100	100	100	
Application Acquisition	T4	1	1	1	TCP/IP Transmission
CMS Processing	T5	100	150	125	Min : 1 change of state Max : 100 changes of state
Operator Acquisition	T6	1	500	250	500 ms cyclic scanning
Data Display	T7	100	300	200	Min : 1 change of state Max : 100 changes of state
Total		603	1851	1226	

CHAPTER 11: CRITICAL EVALUATION AND CONCLUSIONS

The ICMS system helps to automate the building control process for ACC. ICMS collects the real time data from sites and store it in the database, it helps user to monitor the trend of the temperature, equipment failure rate, water lever, energy usage rate and generate reports to the Operation Management for making decision.

This project actually provided an opportunity for user to monitor and control the facility and equipment remotely by the software control. And at the end of project, some of items has been changed and replace by more cost effective equipment.

11.1 Critical Evaluation

Despite the advantages of having the system, there are rooms of improvement that can be done if more time and resources is given.

The data updating and retrieve will be performed better in the following areas:

- Improve the network by using private network
- New software to improve the data update rate
- Include additional backup database server
- Include decision support software (DSS)

During the initial project designed phase, we proposed to install a private communication backbone. However, because of budget constrain, the original designed of private network have been replaced with Internet broadband public network. An additional change was needed to prevent unauthorized access to the ICMS system. We have include a proxy firewall server and connected as a Virtual private network (VPN). The data is encrypted during transmission and additional overhead bits is require for the coding purpose. Some feedback from the users indicated that the data update rate could be slow when the Internet traffic is heavy.

Additional software code needs to be written to overcome the slow update by changing the data-updating mode from polling mode to report with exception mode. Polling mode is the data update mode whereby the Central Management System constantly requests remote sites to update status. The

exception mode is the data update mode whereby the remote sites only update to Central Management System when there is a change in status.

The system was developed with only a database server and no additional backup database server was included. If this database server fails, it will not be able to provide historical data retriever and trending. It will be good if additional backup database sever can be included during the next system upgrade.

Decision support system (DSS) [2] can be installed to further improve the system capabilities. The software is able to provide prediction on the possible failure & action to be taken by analyzing the historical data and events stored in the database.

11.2 Overall Conclusion

Although there are rooms for improvement in the system, the Integrated Control Management System is able to perform according to ACC's requirements. ACC has managed to achieve their goal in automated the club facilities within the two year time frame. It also provided significantly saving on the operating cost.

BIBLIOGRAPHY

[1] Elizabeth Kaufman and Andrew Newman (1999) *Implementing IPsec*. Wiley Computing Publishing, John Wiley & Son, Inc.

[2] Jeffrey L. Whitten and Lonnie D. Bentley (1994) *System Analysis and Design Methods.* McGraw-Hill, Boston.

[3] Andy Oram (2001) *peer to peer*. Wiley Computing Publishing, John Wiley & Son, Inc.

[4] Sape Mullender(1993) *Distributed System.* Addison-Wesley, New York.

[5] Bruce Elbert and Bobby Martyna (1994) *Client/Server Computing*. Artech House, Inc. Norwood.

[6] Alan Dix,Janet Finlay, Gregory and Russell Beale (1993) *Human Computer Interaction.* Prentice Hall International, UK.

[7] IEEE (1987) *IEEE Standard Definition, Specification, and Analysis of System Used for Supervisory Control, Data Acquisition, and Automatic Control*. New York.

[8] Date C.J (1995) *An Introduction to Database Syste*m. Addison Wesley, New York.

[9] Barret, M.L. Wagner C.H., (1996) *C and Unix: Tools for Software Desig*n. John Wiley & Sons, New York.

[10] Alexis Ferrero(1996) *The evolving ethernet* . Addison-Wesley, New York.

[11] Kaufman, Perlman and Speciner(2002) *Network Security, private network in a public world* . Prentice Hall., New Jersey.

[12] http://www.x.org/XOrg_Foundation.html

[13] http://standards.ieee.org/reading/ieee/std_public/description/busarch/1014-1987_desc.html

[14] http://www.modbus.org/

[15] http://www.profibus.com/

[16] http://www.vita.com/vmefaq/index.html

[17] http://www.quatech.com/support/comm-over-pci.php

[18] http://www.radisys.com/microware.cfm

[19] http://www.windriver.com/products/device_technologies/os/vxworks5/

[20] http://www.qnx.com/

[21] http://www.gefanucautomation.com/products/intellution_dynamics/ifix/default.asp

[22] http://www.tecnomatix.com/usdata.asp

[23] http://www.ni.com/labview/

[24] http://domino.automation.rockwell.com/applications/gs/region/gtswebst.nsf/pages/ProcessLogix

[25] http://www.geindustrial.com/cwc/gefanuc/index.jsp

[26] http://www.sea.siemens.com/automat/product/plc/auov.html

[27] http://www.can.bosch.com/content/What_is_CAN.html

[28] http://www.orafaq.com/faqodbc.htm

[29] http://www.w3.org/TR/REC-html40/

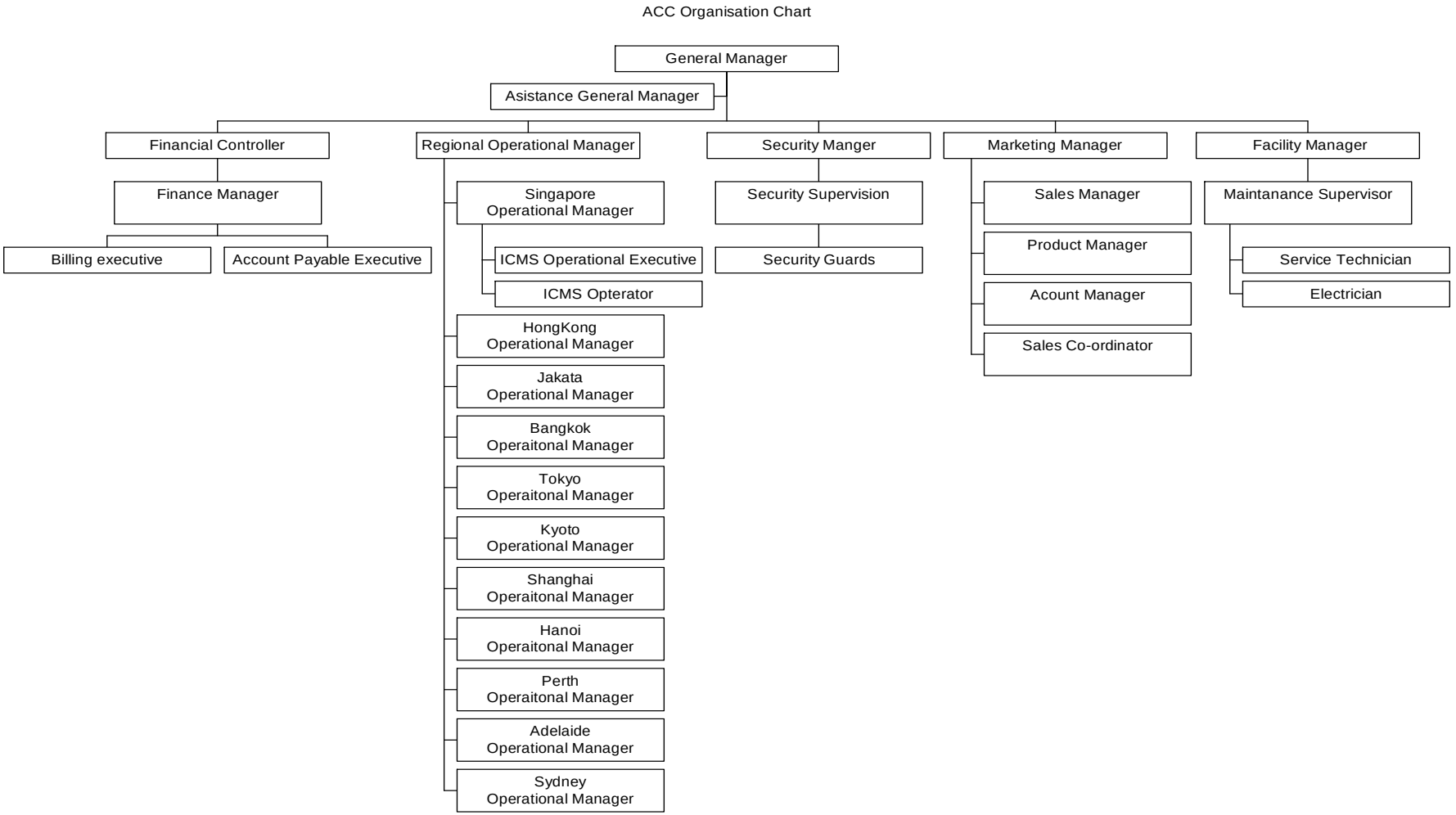
[30] http://www.angelfire.com/biz/rhaminisys/ddeinfo.html#DDEtop

[31] http://www.onshore.com/downloads/partners/netscreen/Systems_datasheet.pdf

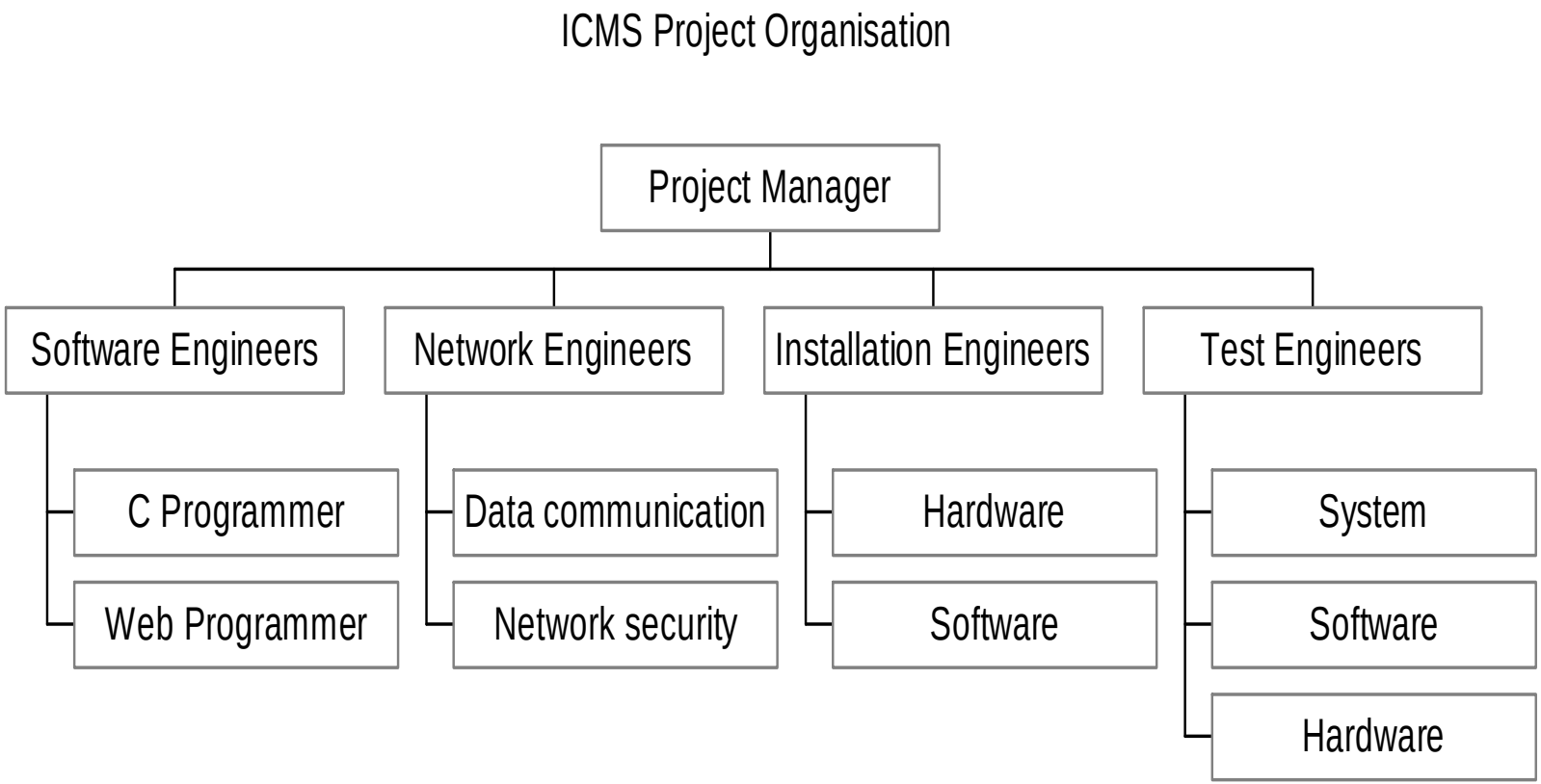
[32] http://www.**cisco**.com/warp/public/cc/pd/rt/**7100**/index.shtml

[33] http://www.lucent.com/products/solution/0,,CTID+2017-STID+10080-SOID+1223-LOCL+1,00.html

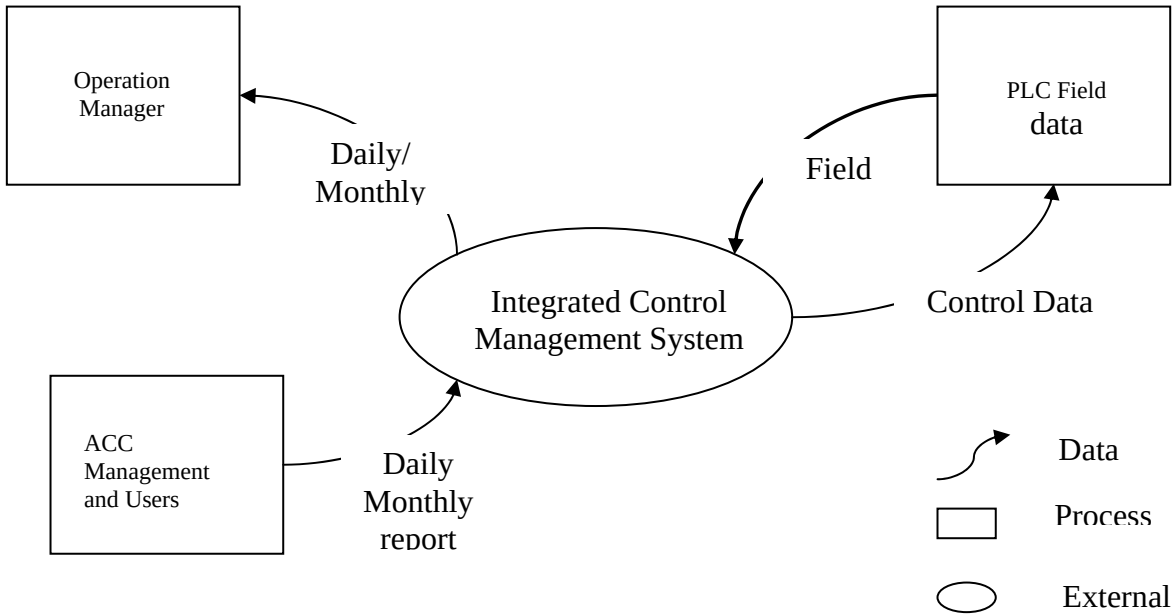
Appendix A-ACC Organization Structure



Appendix B - Project Organization

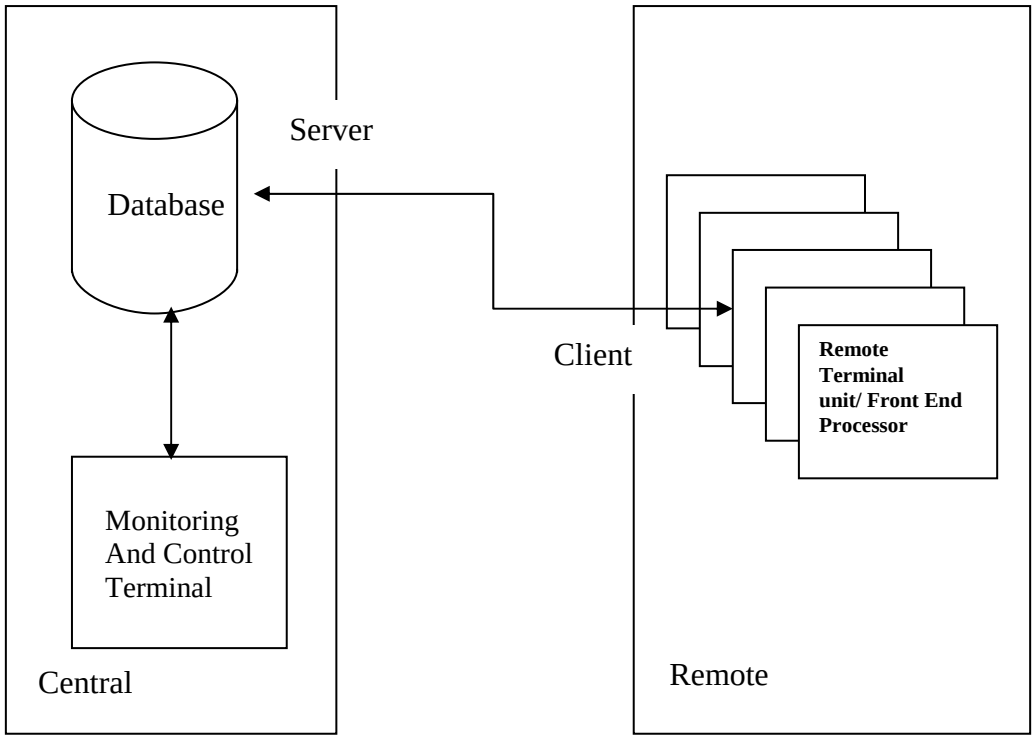


Appendix C - DFD-0 Context Diagram

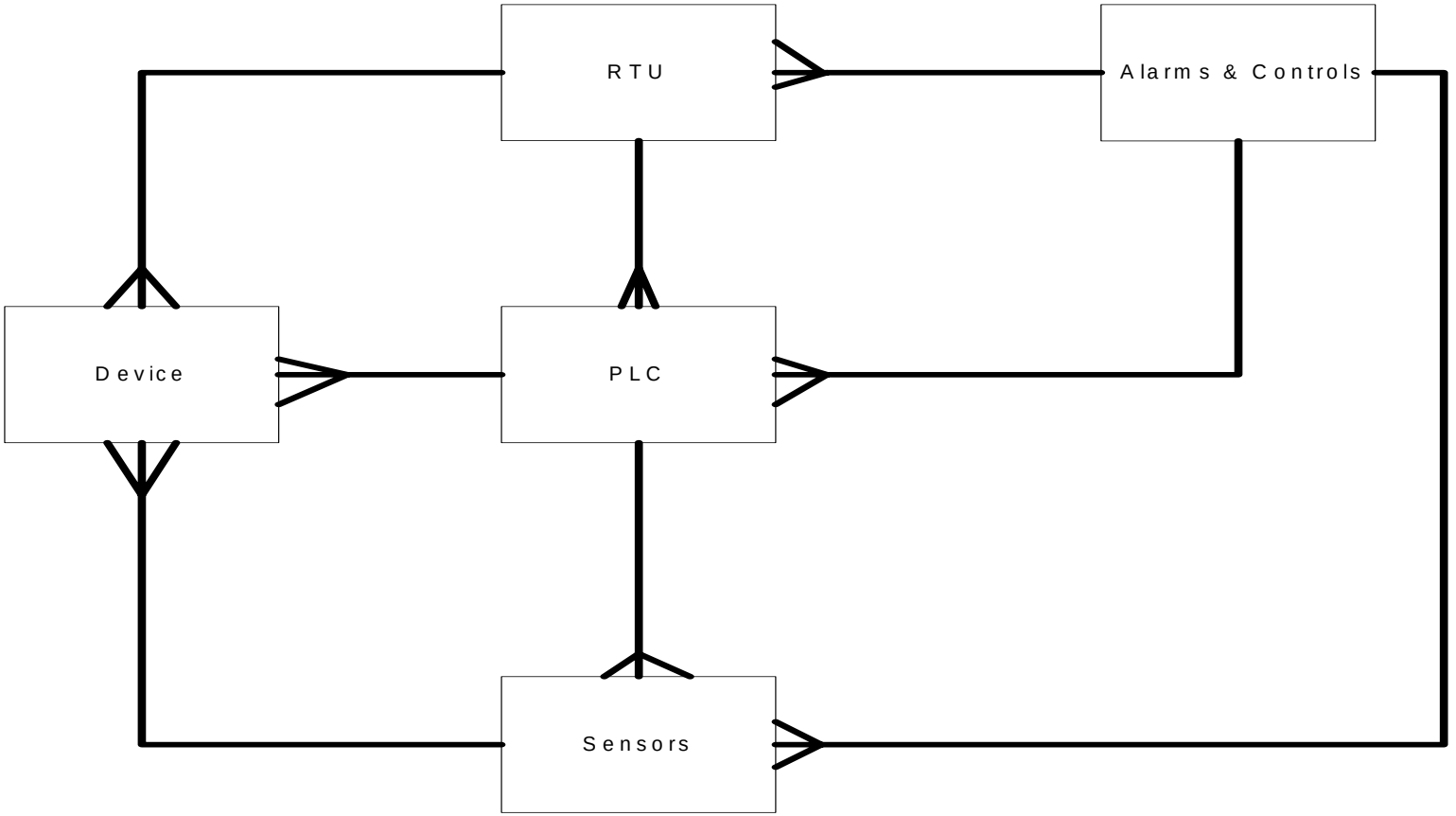


Context Diagram

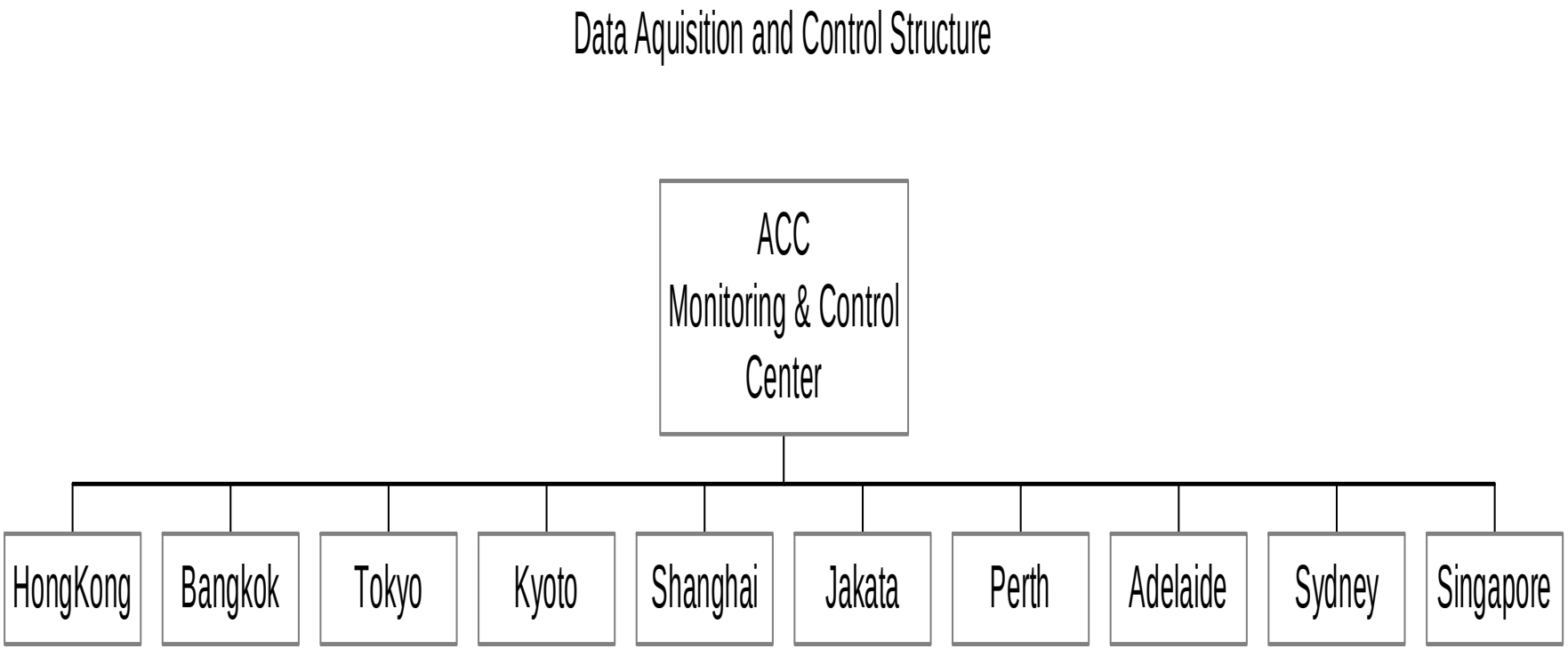
Appendix D - Database Storage Diagram


Server
Database
Client
Remote
Terminal
unit/ Front End
Processor
Monitoring
And Control
Terminal
Central
Remote

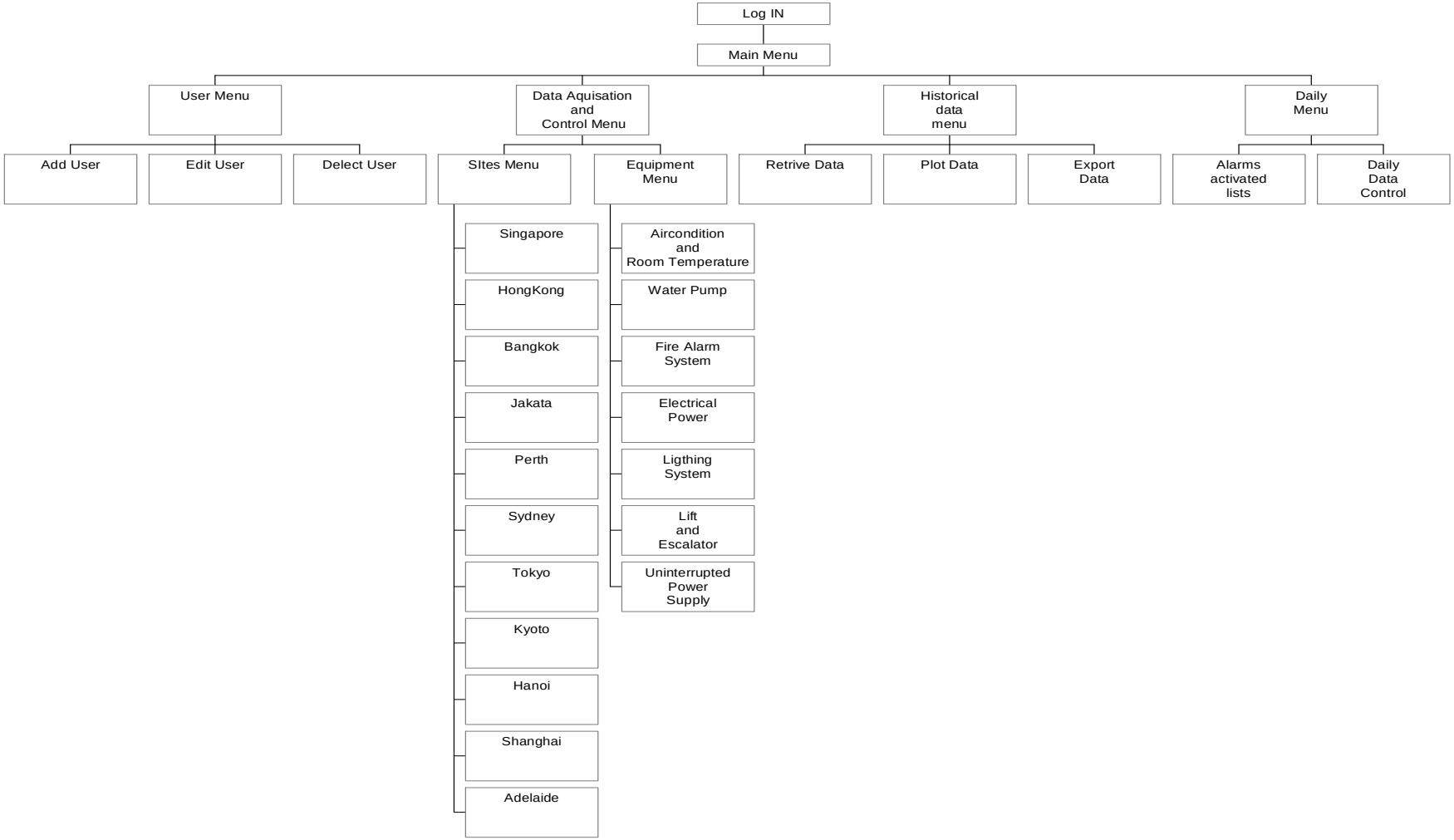
Appendix E - Entity Relationship Diagram



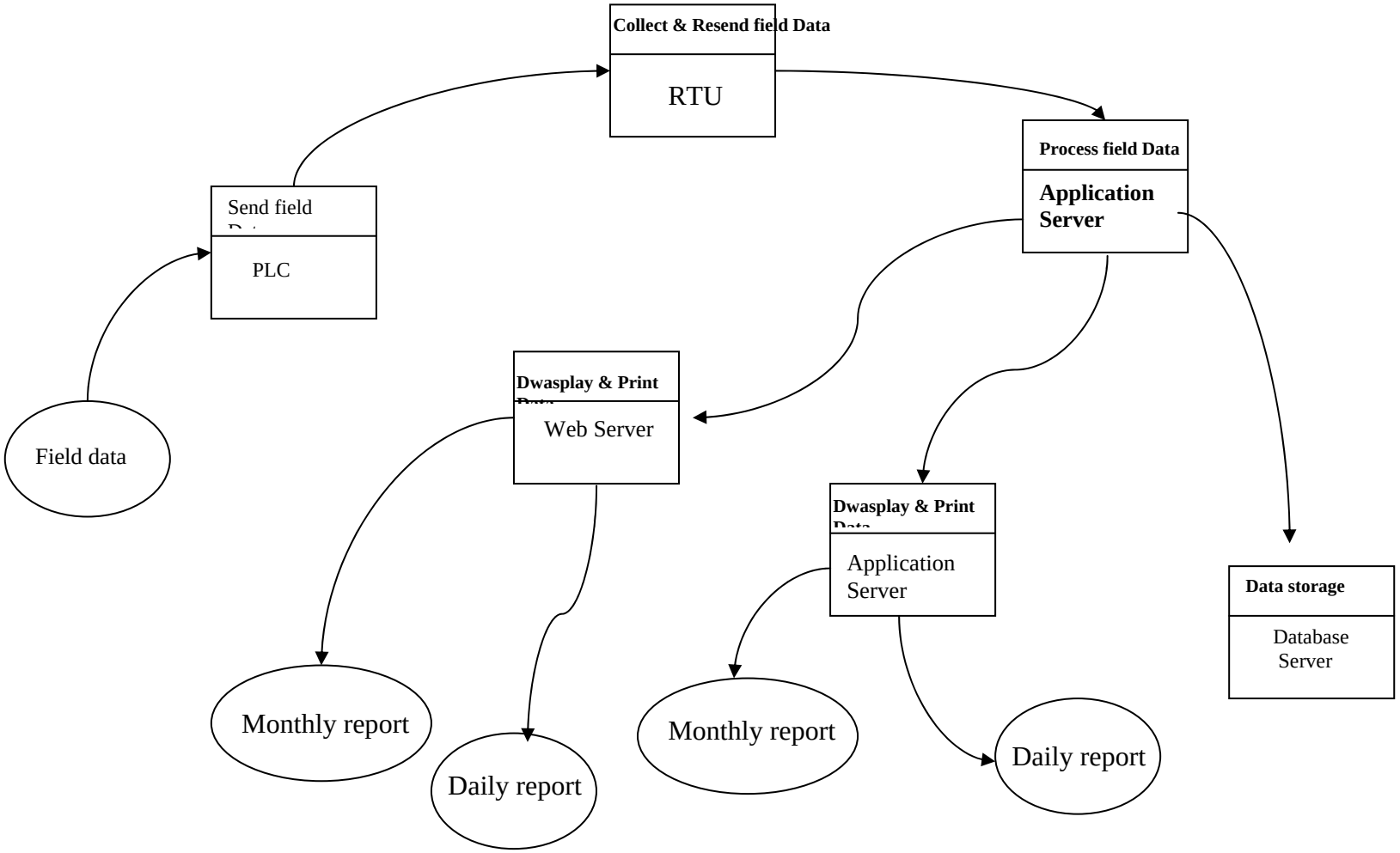
Appendix F - Data Acquisition and Control Structure



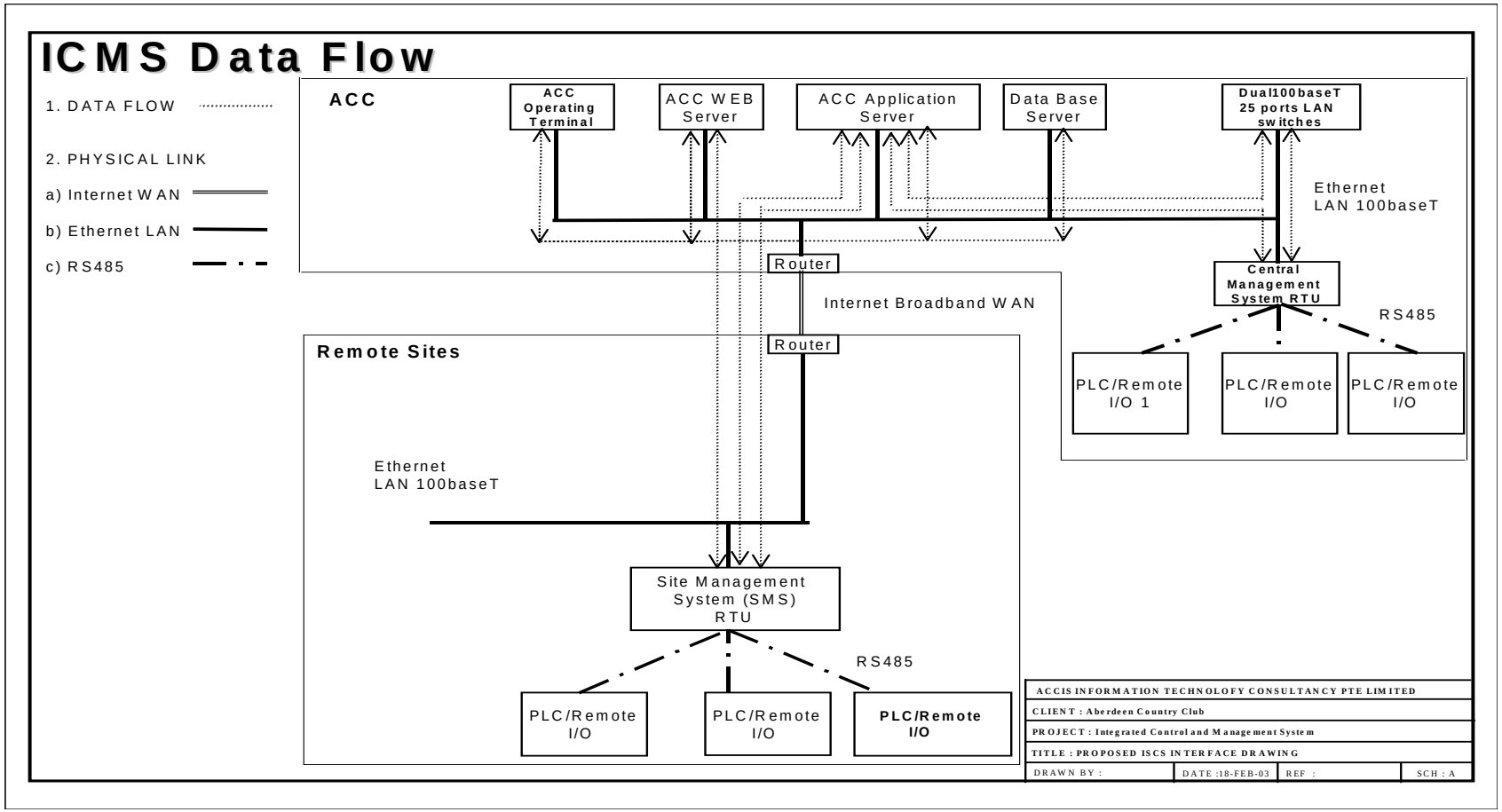
Appendix G - ICMS Log In Manu



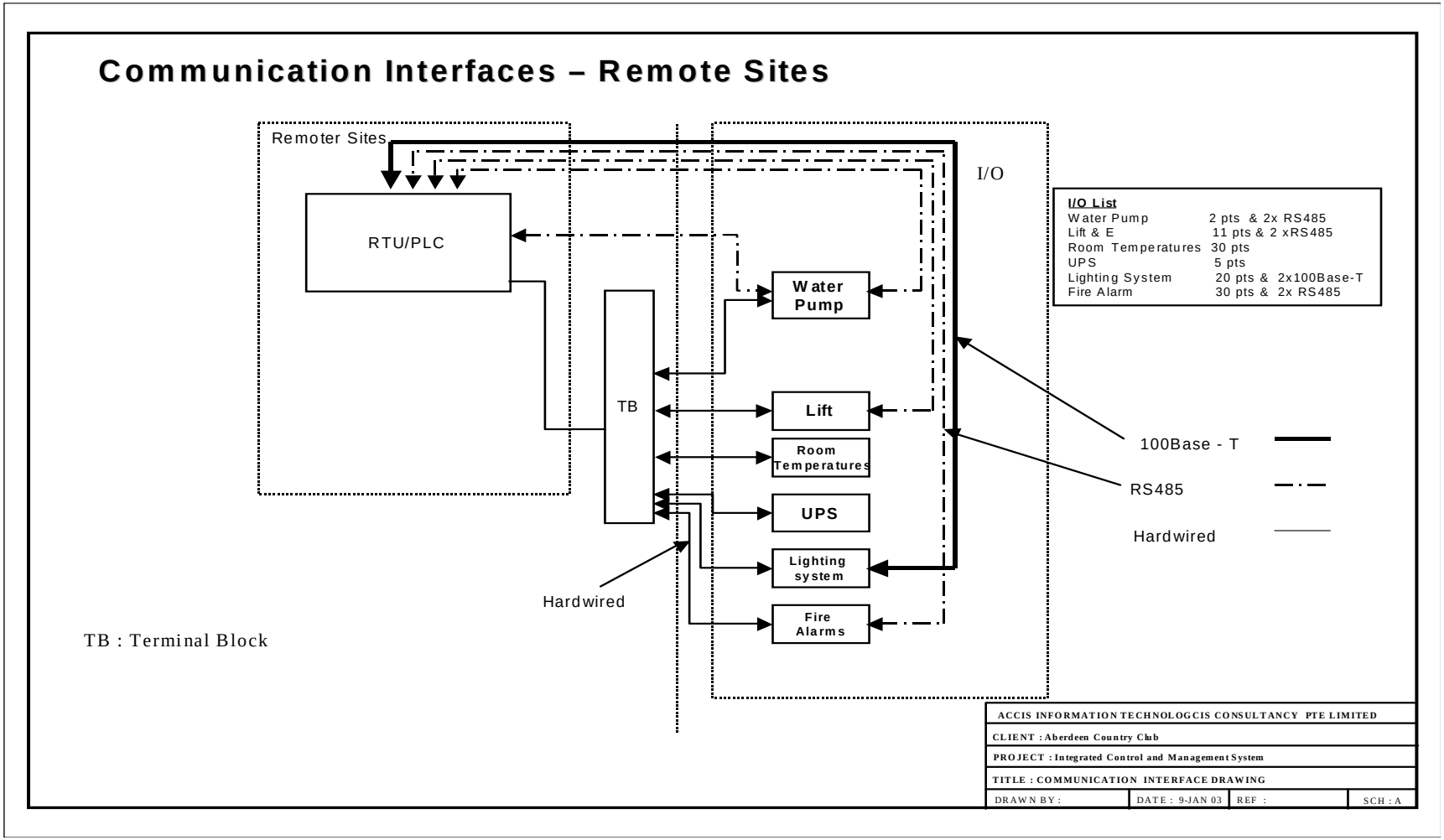
Appendix H - ICMS Data Flow Diagram a



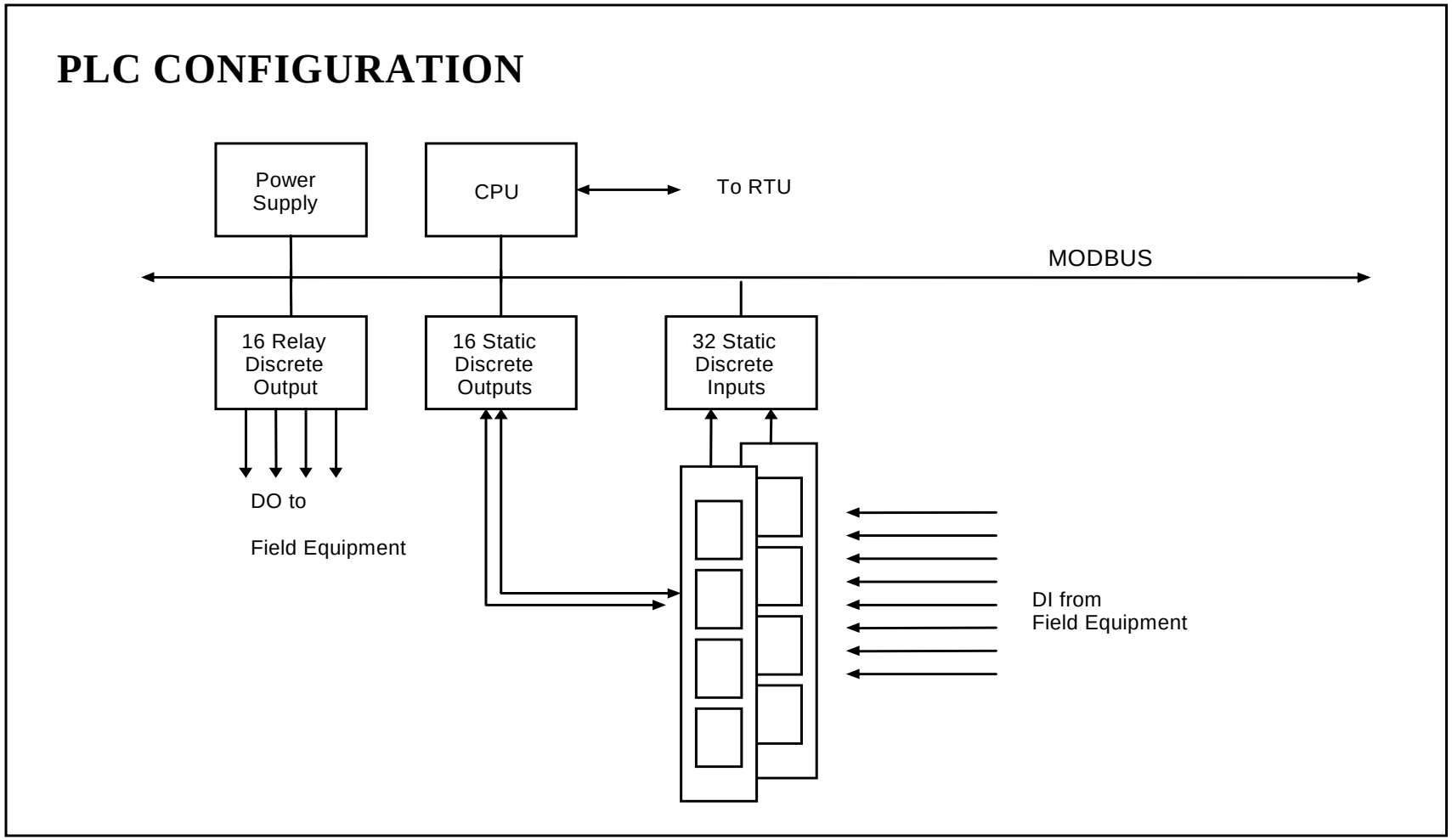
Appendix I - ICMS Data Flow Diagram b



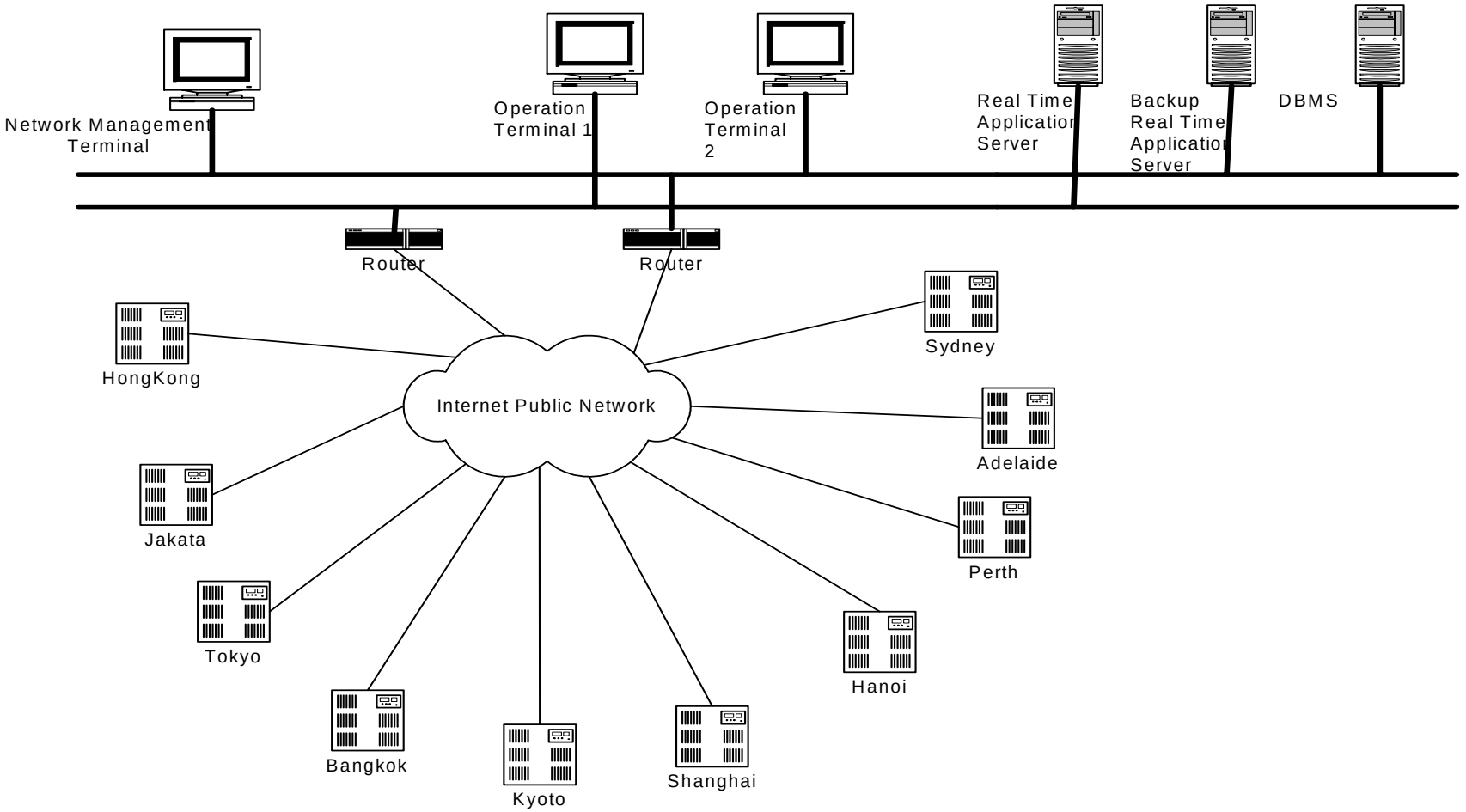
Appendix J - Communication Interfaces



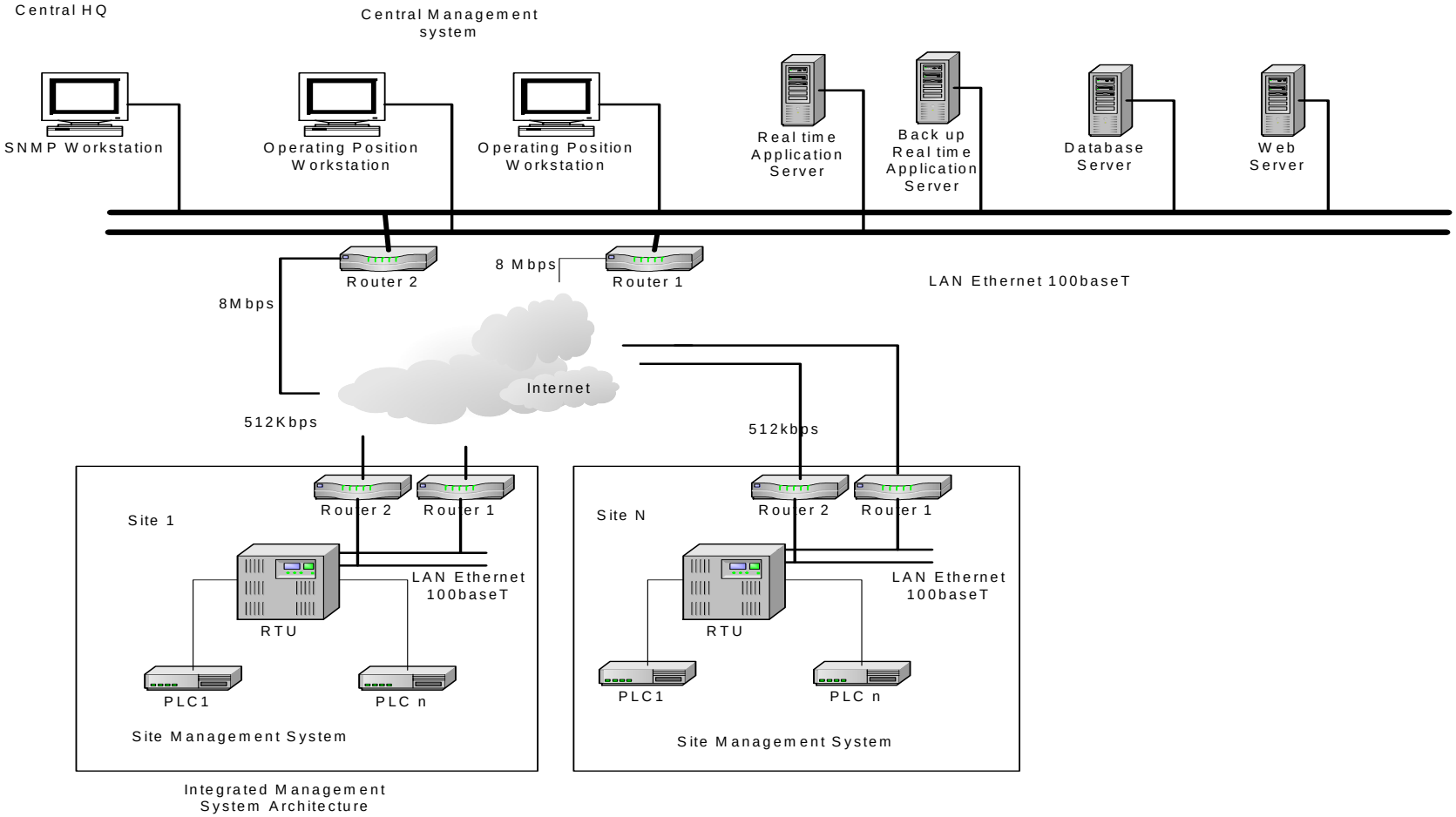
Appendix K - PLC Configuration Diagram



Appendix L - Internet Remote Site Configuration Diagram



Appendix M - Overall System Configuration Diagram



Integrated Management System Architecture