UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATION ENGINEERING

YANG LIU

A SECURED WIRELESS REMOTE CONTROL AND MONITORING SYSTEM WITH REDUNDANCY

Master's thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 11 November 2005.

Supervisor	Riku Jäntti
Instructor	Riku Jäntti

FOREWORD

This thesis work has been carried out at Technobothnia and Department of Information Technology, Faculty of Technology, University of Vaasa, as a pilot of the TEKES project ICT of Electric distribution network.

I would like to express my deep gratitude to my supervisor, Prof. Riku Jäntti for his constant guidance, encouragement, support and intensive examination of this thesis. I would like to thank Prof. Kimmo Salmenjoki and Prof. Matti Linna who have carefully reviewed the thesis to give valuable suggestions, Dr. Mohammed Elmusrati for his nice idea and support in wireless network QoS analysis, Dr. Minmin Zhang for her support in mathematical modelling, Tobias Glocker for his support in Linux shell programming, Johan Dams for his support in MCU programming and Linux system setup, Jani Ahvonen for his support in embedded system PCB design, Juha Miettinen and Veli-Matti Eskonen for supplying equipments, and all other people who have supported this thesis work.

Finally but most importantly, my thanks go to my parents Jiongdan Liu, Ying He and my love Ting Sun. This thesis work can never be achieved without their encouragement and support.

Vaasa, 11 November 2005

Yang Liu

UNIVERSITY OF VAASA	
Faculty of Technology	
Author:	Yang Liu
Topic of the Thesis:	A Secured Wireless Remote Control and Monitoring System with Redundancy
Supervisor:	Riku Jäntti
Instructor:	Riku Jäntti
Degree:	Master of Science in Technology
Major of Subject:	Telecommunication Engineering
Year of Entering the University:	2002
Year of Completing the Thesis:	2005 **Pages:** 136

ABSTRACT

Automated substation monitoring, diagnostics, and remote control systems provide many useful operating and reliability advantages. Their widespread use is, however, limited because of high costs making them economically infeasible. The needs have been concluded as a joint project to develop new low cost communication and control concepts for medium voltage devices such as switches and disconnectors that would enable the electrical grid operators to benefit from the advantages of the remote monitoring, diagnostics, and control by making such solutions economically feasible.

This thesis work looks into different solutions to the distance control and monitoring of medium voltage devices in the power grid and targets to implement a pilot system as an approach to validate the ideas and find possible improvements for the future deployment of such system in real industrial use. The objective is to design and implement a reliable and secured wireless remote control and monitoring system based on current available 2.5G/2.75G/3G commercial wireless communication networks e.g. GPRS/EDGE/UMTS. Such remote access solution is completely based on wireless communication network due to the fact that the control devices in the power grid are distributed over a geographically wide area and normally situated in remote locations. Besides the development of a traditional remote control and monitoring system, various solutions involving system modular structures, communication means, reliability and security enhancement etc have been proposed and analysed according to the strict requirements of the project with reference to military communication system standard, out of which comes the design and implementation of the pilot system.

In this work, the enhancement of reliability and security over wireless link is greatly emphasised. The redundancy design which ensures the system is highly reliable and fail-safe under abnormal operating circumstances has been theoretically analysed to evaluate the system reliability performance. The security design involving various countermeasures and cryptographies has been implemented on hardware and software levels of the system, to ensure system security and data security. The reliability performance in wireless communication network has been analytically evaluated.

Keywords: remote access, reliability, security, wireless network performance

ABBREVIATIONS

AES	Advanced Encryption Standard
ARPANet	Advanced Research Projects Agency Network
BCCH	Broadcasting Control Channel
BER	Bit Error Rate
COTS	Commercial-Off-The-Shelf
CRC	Cyclic Redundancy Check
CS	Coding Scheme
CSD	Circuit Switched Data
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMAC	Direct Memory Access Controller
DNS	Domain Name System
ECSD	Enhanced Circuit Switched Data
EDGE	Enhanced Data rates for Global Evolution
EGPRS	Enhanced General Packet Radio Service
EIR	Equipment Identity Register
ESP	Encapsulating Security Payload
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communication
HCI	Human-Computer Interaction
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
ICT	Information and Communication Technology
IIS	Internet Information Services
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPSec	Internet Protocol Security

I/O	Input/Output
ISDN	Integrated Service Digital Network
ITU	International Telecommunication Union
L2TP	Layer Two Tunnelling Protocol
MBWA	Mobile Broadband Wireless Access
MCU	Micro-Controller Unit
MIMO	Multiple-Input Multiple-Output
MMS	Multimedia Message Service
PCB	Printed Circuit Board
PCMCIA	Personal Computer Memory Card International Association
PDCH	Packet Data Channel
PIN	Personal Identification Number
PLL	Phase-Locked Loop
PPP	Point-to-Point Protocol
QoS	Quality of Service
SFR	Special Functions Register
SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signalling System 7
SSH	Secure Shell
TCP/IP	Transport Control Protocol and Internet Protocol
UART	Universal Asynchronous Receiver/Transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWW	World Wide Web

CONTENTS

1. INTRODUCTION

1.1. Background

According to (Jäntti & Luoma 2005), the future of power industry will require the development of two infrastructures: the existing power delivery infrastructure and the digital infrastructure consisting of data networks and information systems.

In the current electrical grid, the high cost of telecontrol equipment has had major impact in shaping the network topology. Telecontrol equipment has been economically viable only in network nodes connecting many distribution lines and having low operation voltage, i.e. transformer, available. The energy production paradigm is currently shifting from large scale centralized systems towards smaller scale distributed energy systems. This change of paradigm will have great impact on topology of the power-distribution network which in turn will require new control solutions. Present remote control devices need to be updated due to new requirements. Also the usability of present network can be improved by using new Information and Communication Technology (ICT) solutions.

Automated substation monitoring, diagnostics, and remote control systems provide many useful operating and reliability advantages. Their widespread use is, however, limited because of high costs of communication, making them economically infeasible. The costs are mostly due to the present way of developing special devices for remote control and monitoring of the electrical network applications; the high production volumes of standard devices and communication networks have not been utilized. The application environment is harsh to wireless technology, because of the electromagnetic environment interfering with the radio communications. Another issue is the power source for the transmitters as they are typically located next to medium voltage components. Study is needed in appropriate wireless technology.

This thesis work supports the “ICT of Electric distribution network (ICT-E)” project, which seeks to develop cost efficient methods for wireless telecontrol of medium voltage devices in the power grid. The project bears close resemblance with TESLA projects (TEKES 2002) on distribution network automation and the ongoing DENSY project (TEKES 2003) “TCP/IP-architecture in distributed generation monitoring and control”. In fact, the starting point of the project is the results obtained by VTT Energy in the TESLA project. The rapid advancement of the ICT has created new opportunities for telecontrol applications even in this short time period since the last TESLA project. For instance, multimedia messaging has gained momentum only recently, session initiation protocol (SIP) based signalling has started replacing SS7 based signalling from the ISDN era in the radio access networks allowing more flexible control and richer content and more importantly faster response times for multimedia calls, commercial use of third generation networks has only recently started in Finland.

The purpose of the ICT-E project is to tract the state of art in ICT in order to find the best solutions for the remote control and monitoring applications of power distribution networks, and also to find out the barriers preventing the use of these new technologies. It differs from the TCP/IP project by focusing on wireless communication solutions considering also non-IP-based signalling solutions.

1.2. Objectives

This thesis work looks into different solutions to the remote control and monitoring of medium voltage devices in the power grid and targets to implement a pilot system as an approach to validate the ideas and find possible improvements for the future deployment of such system in real industrial use. Typically the amount of data needed in remote control of such devices has been very small, i.e. in case of disconnectors, only the contact information, open/closed, is transmitted. Remote monitoring is also possible by transmitting live updated pictures of the disconnector’s state to eliminate the need of the maintenance crew to visit the site to visually verify that the disconnector is really in open position before grounding the line. The time constant of the disconnector is in the order of magnitude of seconds, thereby tolerating up to one second of propagation delay. This suggests that even GSM/GPRS networks could in some cases be utilized in such applications.

The objective of this thesis work is to design and implement a reliable and secured wireless remote control and monitoring system as a pilot of the ICT-E project, based on current available 2.5G/2.75G/3G commercial wireless communication networks e.g. GPRS/EDGE/UMTS. Such remote access solution is completely based on wireless communication network due to the facts that the control devices in the power grid are distributed over a geographically wide area and normally situated in remote locations. The enhancement of reliability and security over wireless link is greatly emphasised in this work. The system should be highly reliable and fail-safe under abnormal operating circumstances. The system should be highly secure against security attacks and unauthorised access. The performance in wireless communication network should be highly reliable.

1.3. Scope, contribution and limitation

The scope of this thesis work tries to find a feasible solution for the telecontrol problem described in the ICT-E project. The study, design and implementation of a secured wireless remote control and monitoring system with redundancy are carried out in the work based on current available wireless communication networks. The reliability and security measures designed for wireless communication as well as the system itself are developed and implemented.

The major contribution of this work provides a secure, reliable and economical solution for the desired remote control and monitoring application using current available wireless communication networks which are considered to be insecure and unreliable. Redundancy design ensures the system is fail-safe and self-recoverable under abnormal operating circumstance. Security designs including cryptographies and countermeasures are implemented to ensure data security and system security. Various cryptographies secure data transmission while data travels through insecure network. Various countermeasures secure the system in order to identify and resist known attacks. The pilot system developed from this work has been found to be effective in reliability and security according to the trails. Analytical evaluations of the system reliability and performance in wireless communication network have also proven that the demanded requirements are met.

However, the work has limitations. This work is just an initial attempt to find an approach to the solutions for such telecontrol problem. Only a primitive prototype is developed to validate the ideas and possible improvements. There are still technical problems and limitations which affect the system performance and this requires much more future work to improve such solution into a mature status in order to be able to deploy into real industry use. There is still distance from the real application which requires more research and development work. More and more advanced features can be developed based on the concept of the ideas contributed in this work.

1.4. Structure of the thesis

Chapter 1 gives brief introduction to the thesis topic. Chapter 2 describes the specific part of the ICT-E project as focus of the thesis involving proposals of feasible solutions, comparisons, analysis and decision making. Chapter 3 covers a complete approach of implementation of the proposed pilot system. Chapter 4 focuses on especially security enhancement to the system. Chapter 5 focuses on the analytical evaluation of the system reliability performance in wireless communication network. Chapter 6 concludes the thesis.

2. GENERAL SYSTEM OVERVIEW

2.1. Introduction to the case study

In this thesis work, the main objective is to develop and implement a feasible solution for the remote control and monitoring of a disconnector as proposed major part in the ICT-E project. The work mainly involves proposals of solutions, study and comparison of different solutions, development and implementation of a pilot system based on the selected solution, design and implementation of reliability and security features for the system, testing and validating the system in real life, and possible improvement for future development.

The pilot system is a solution designed for remote control and monitoring of the disconnector application. It has following features: remote control of the disconnector to switch between open/closed statuses, remote monitoring of the disconnector to verify the status visually. The application is highly reliable and secure while working with wireless communication network. Therefore, besides the development of a normal remote control and monitoring system, reliability and security features are greatly emphasised in such system due to the nature requirements of the application field. Such remote control and monitoring system has to be operationally reliable and highly secured. With redundancy design, the remote control and monitoring functions should be as little as possible affected by any communication troubles, and the system itself should be operational trouble free and self recoverable under majority of circumstances. The system should be highly secured, highly alert for any possible attacks and always able to override unauthorised access, so that it cannot be easily cracked or hacked. Design and implementation of system redundancy and data security are described in details in the following chapters of this thesis, and testing will put system into various trials to verify its reliability and security features.

From the discussions the requirements of ICT-E project have been summarised. The main considerations for development of the remote features of such control and monitoring system are:

- What kind of communication means to be used?
- How to make the system and communication reliable and secure?

The first question is quite straight forward, as the available communication means will be studied and analysed for their advantages and disadvantages to make up a proper choice. The second question is relatively much more complex since it will be directly affected by the system structural design. Several system modular structures will be proposed, analysed, compared for their advantages and disadvantages, especially the system reliability will be studied and analysed for each proposed individual modular structure to make up a proper choice. The following sections will cover studies and analysis towards these questions.

2.2. Communication technology review

Although the telecontrol application considered in this thesis is designated for civilian use, the normal commercial solutions however can hardly fulfill the application requirements due to their limitations. To find a better approach we would rather extend the scope to look into solutions for military use. Despite their much higher standards compared to the civilian ones, military solutions would be valuable proposals under circumstances where the civilian solutions are defective that cannot fulfill the technical requirements. On the other hand, it’s also natural to study the possible semi-military solutions which could even be totally based on civilian infrastructure. Such solutions are also very much interested in safety-critical industrial applications, i.e. the ICT-E project.

2.2.1. Studies of military communications

MOD (2005) has shown that in order to maintain information dominance, military communications must be maintained when and where needed. What make military communication systems different from civilian systems is that they have traditionally been designed to resist geo-location, jamming and other electronic warfare threats.

A well-designed military communications system aims to be resilient to disruption by the enemy. Physical attack is an obvious strategy but more sophisticated approaches collectively known as electronic warfare are possible which includes jamming by enemy signals and also includes interception of the signal to ascertain that messages are being sent, to analyse the characteristics of the messages or perhaps to even decode the messages. In addition it also includes direction finding of signals to determine the location of the transmitter.

As a separate issue they must provide end-to-end message security in order to maintain confidentiality. The network must also be robust to physical disruption; architectures employing a single critical communications node, such as a computer or radio station, have to be avoided if possible. Also many military communications have to be maintained on the move, perhaps between fast moving vehicles such as aircraft or perhaps between command posts and moving troops. Meeting these latter requirements significantly complicates radio system architectures and information flow rates compared to those that are achieved in civilian systems. Against this background of military requirements there come products offered by civilian telecommunications companies and their research and development (R&D).

From above studies to the military communication systems, the requirements of communication system for the power grid application can be easily adopted as part of the requirements of military communication systems. In the telecontrol application, normally the fictitious enemies are hackers who try to gain unauthorized access to the system. It does need to be designed to resist geo-location, jamming and other electronic warfare threats. Probably jamming threat is major one and geo-location is minor one. Data security is also put important considerations. Robust network and system structure with redundancy are required. Compared to the military systems the only thing left which does not need to be considered is the requirement of mobility, since the system is not designed for mobile use. It’s obvious that the required communication system for the ICT-E project is close to the standards of military communication systems. Therefore it’s interesting to discuss questions e.g. can civilian communication systems meet the military requirements, or should new military communications systems try to harness the underlying civilian technology rather than the systems.

2.2.2. The civilian world of communications

The recent rapid advances in communications are due to the fabrication of cheap, integrated circuits of huge capacity and complexity. These led the way to a branch of communications system design which relies solely on the transmission of digital information, rather than analogue information, and the application of advanced signal processing within communication systems.

- Cellular radio systems (1G, 2G and 3G)

The first operational cellular communication system was deployed in Norway in 1981 and was followed by similar systems in the US and Europe. These first generation (1G) systems provided voice transmissions only using frequencies around 900 MHz, which used analogue modulation and provide only for voice transmission. Second generation (2G) Global System for Mobile communications (GSM) was first used in Europe in the early 1990s. GSM provides voice and limited data services and uses digital modulation with improved audio quality. So-called 2.5G systems i.e. General Packet Radio Service (GPRS) and 2.75G systems i.e. Enhanced Data rates for Global Evolution (EDGE) recently introduced enhance the data capacity of GSM and mitigate some of its limitations. The third generation (3G) cellular services known as Universal Mobile Telecommunications System (UMTS) or IMT-2000 will sustain higher data rates still and opens the door to many internet style applications (Eberspächer, Vögel, Bettstetter 2001). The longer-term commercial vision is high data rate wireless communications between portable terminals that may be located anywhere in the world and may be located either indoors or outdoors. High Speed Downlink Packet Access (HSDPA) is a new mobile telephony protocol also called 3.5G. HSDPA is a packet based data service with data transmission up to 8~10 Mbit/s and 20 Mbit/s for Multiple-Input Multiple-Output (MIMO) systems over a 5 MHz bandwidth in WCDMA downlink. High Speed Uplink Packet Access (HSUPA) is a data access protocol for mobile phone networks with extremely high upload speeds up to 5.8 Mbit/s (Sharma & Kumar 2005). The fourth generation (4G) is targeting for communication at 1 Gbit/s while still, and 100 Mbit/s while moving (Safwat & Mouftah 2005).

- Wireless broadband access and satellite networks

Fixed wireless access technologies i.e. IEEE 802.11 Wireless LAN, IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMax) and IEEE 802.20 Mobile Broadband Wireless Access (MBWA) are also being developed to bring high speed Internet access, multimedia and other broadband services to the home (IEEE 2005). Satellite systems and wireless access to the terrestrial broadband (cable and fibre) networks are possibilities. The combination of new mobile cell phones with global positioning system (GPS) technology also allow the concepts of ‘messages in space’, which will only be received or picked-up when the user gets near to or in a certain area. Such concepts will be useful for personalised local advertising and information services.

2.2.3. Military communication systems based on civilian systems

MOD (2005) has shown that military communications are needed for a wide variety of circumstances from peace keeping to war. Many of these circumstances mirror the requirements in the home so there is a strong temptation to believe that consumer driven systems can be used by the military for all operations. This is known as the commercial-off-the-shelf (COTS) approach. So, can a COTS policy for procuring military communication systems really work?

Potential problems with COTS:

- Civilian communication systems have been designed with interoperability between systems in other countries as a prerequisite and this would provide a simple route to coalition compatibility but it would also allow for very easy intercept and potential eavesdropping.
- Civilian cellular networks are very fragile to physical attack of the base stations and the support infrastructure; conventional military communications systems avoid the use of base stations to minimize physical attack.
- Electronic warfare (jamming and intercept) makes it relatively easy to render most, if not all commercial radio systems inoperative.

Bespoke enhancements to civilian systems are another possibility. However the increasing level of system integration makes this approach more difficult as time progresses. The economics of the use of COTS systems or COTS technologies need to be constantly reviewed.

2.2.4. Physics laws and new enabling technologies

The direct application of commercial wireless communications systems for operational use by the military is problematical. Perhaps more important for the design of new military communication systems is the transfer of technology, algorithms and know how from the commercial sector and vice-versa, for example the Internet, ARPANet and the underlying technology and concepts for 3G.

A defining feature of both the commercial and military information technology industries is an unrelenting increase in requirement for data throughput. In a fixed wired system the capacity can be increased by virtue of adding new physical resources e.g. new optical fibre etc. In contrast wireless communications require sharing of a finite natural resource: the radio frequency spectrum. The wireless channel, defining the characteristics of the medium over which the information is passed, presents a fundamental technical challenge to reliable communications, constrained by propagation conditions and the Shannon's equation.

- Propagation

The propagation of radio signals constrains the range and performance of any radio system. Radio propagation and its interaction with the environment is more problematical for military systems than civilian systems and consequently, although much can be learnt from civilian studies this is a critical niche research and development area.

Absorption (signal loss), refraction and diffraction (signal bending) are just some of the important propagation effects that can occur for a variety of reasons. At different frequencies radio signals may be affected by passing round or through obstacles. The terrain contours are particularly problematical for both military and civilian Personal Communication Systems (MOD 2005). Radio signals may also be absorbed as they pass through clouds or rain or, they may be bent by the earth's atmosphere (also known as ducting) consequently covering unexpected distances or creating holes in coverage. For these signals we are interested in how the radio waves interact with weather phenomena. Other radio signals may be slowed down and bent by electrons in the ionosphere at altitudes above 100 km and for these we need to study Space Weather, which describes variations of electrons and other charged particles in the earth's near space environment. Space weather is especially problematic in power grid application, e.g. solar winds tend to harm the operation of grid and the wireless control networks simultaneously.

Radio propagation studies (MOD 2005) for commercial Personal Communication Systems have, in recent years, concentrated on supporting cellular systems but exciting new work is now being undertaken to support in-building deployment. Such work is important for covert and other military operations. New and challenging research is also likely to be needed on assimilation of real-time environmental data into the military propagation models. Such work draws on weather forecasting research using 3-D variational techniques. Work in the USA is providing new capabilities for ensuring receipt of communications traffic and equally for ensuring signal denial.

Industrial environment can yield harsh propagation environment, where there are a lot of metal objects that affect the signal propagation. In addition, operation of electrical devices can interfere with the wireless communications. All these problems should be taken into account when designing communication systems for substation automation.

- Channel capacity

Probably the most famous and important equation in communications system design and research is that due to Claude Shannon and which was published in 1948. This important Shannon capacity equation describes fundamental limits on any wireless communications system. (Shannon 1949)

$$C = B \times \log_2(1 + \frac{S}{N}),$$

where *C* is the Capacity, *B* is the Bandwidth, and *S/N* is the Signal-to-Noise ratio of the link. If the rate of data transmission *R*, is less than *C*, then we can transmit over the channel with an arbitrarily small BER using complex modulation and coding schemes.

The so-called Shannon-Hartley equation states that the capacity for error-free communications is limited and is both proportional to the bandwidth that the signal occupies and to the ratio of the received signal power to the received noise power. The signal-to-noise ratio term simply expresses the need to reduce natural and random noise relative to the man made communications signal. This can be done by increasing the transmitter power or by improving the antenna system.

The bandwidth used for signal transmission varies from system to system. For example in 2G cellular system the bandwidth is 200 kHz and in 3G the bandwidth is 5 MHz, while it is typically 60 MHz in the military Skynet channels (MOD 2005).

If the required information transfer is less than the capacity as defined by the Shannon-Hartley equation, then error free communication is possible. If information transfer at a rate greater than this limit is attempted, errors in transmission will always occur no matter how well the equipment is designed. The Shannon-Hartley equation is a very good first step in evaluating the feasibility of any digital communications system design. It provides an upper bound, only achievable with infinite signal processing resources.

- Information theory and error coding

All radio communications systems users want the impossible: worldwide, error free communications. The military user also needs to be able to achieve this without suffering any degradation in performance from electronic warfare attacks (jamming and intercept). Shannon's Theorem gives us some insights into why this is difficult or impossible to achieve but propagation and information theory specialists are striving to push the physical laws to the limit.

During the last ten years has witnessed a revolution in error control coding led by the invention of Turbo coding in 1993 (Berrou, Glavieux, Thitimajshima, 1993). Turbo codes achieve a performance very close to the Shannon limit but at the expense of considerable processing complexity and decoding delays. With modern very large scale integration (VLSI) techniques this complexity is tractable. Recently there has also been considerable interest in adaptive coding strategies that vary the coding complexity as a function of the signal strength and also in special aperiodic codes (chaotic in nature) for highly secured links.

There is a fundamental trade-off between the bandwidth needed for transmitting signals and information and the amount of information and signal processing required (which also needs battery power) for coding and compression. Most military communication systems need to use both efficiently.

- COTS as an enabling technology

ASICs: Application Specific Integrated Circuits and FPGAs: Field Programmable Gate Arrays. The semiconductor industry has evolved from integrated circuits (ICs) developed in the late 1960s which had 10s of logic gates amounting to a few hundred transistors through medium scale integration (MSI) to very large scale integration (VLSI) with millions of transistors.

ASICs are dedicated micro-circuits tailored for a unique application or function. Eventually one chip or microcircuit might be a complete 2-way radio and would provide greatly improved reliability, reduced size and lower battery consumption. FPGAs are micro-circuits or chips with large numbers of undefined switches, (logic elements) that can be programmed when desired. The functionality is less than an ASIC but the circuit can be programmed during its life or operation to cope with changing standards or functions and upgrades. Both technologies are important for the military radio designer since they provide the technology to quickly develop and bring to service new radios such as ‘Software Radios’. Commercial designs and experience should provide an important technology insertion route into military communications systems.

- Software radios

According to (Razavilar, Rashid-Farrokhi, Liu 1999), software radios describe an exciting approach using both ASICs and FPGAs and other new technology to allow a re-configurable radio, which can be adapted at the point of use and for different applications.

Conventional radio technology uses a number of analogue hardware components to process the signal. The design is specific to the application as well as having a number of technical disadvantages. Software radio technology is a way of realising a multi-band, multipurpose radio. In the ideal software radio the radio frequency (RF) signals are digitised directly at the antenna and all other radio functions are performed in the digital domain by software on the host platform which might be a flexible digital signal processing (DSP) chip, a computer or even a mobile telephone. In reality, rather than solely processing the signals in software, a combination of hardware logic circuits, for example ASICs and FPGAs, may be used in combination with the DSP. This approach reduces power, size and cost but at the expense of flexibility. This is sometimes referred to as a digital programmable radio.

Future military radios are likely to be based on the software radio principle since the approach offers flexibility for implementing multi-mode and multi-band radios. In principle the specification could be changed on the fly or implemented quickly and cheaply by utilizing a library of standard operating routines. The commercial technology push is currently in respect to 3G systems but huge investments are still required to implement this vision. The DSP requirements for 3G commercial systems will require 1~2 thousand million-instructions-per-second (MIPS) and this is stretching the industry thus providing new opportunities for technology pull-through by the military. Chip technology is improving through improvements in the chip architecture and in the semiconductor process technology. Clock rates and transistor numbers are being increased, whilst power consumption is being decreased. Such radio systems have great implications for military users, who are required to adapt to legacy systems and standards and to insert new technology as it emerges from the civilian sector.

- Smart antennas

Smart antennas involve electronic control of the critical elements and provide intelligent functions such as suppression of interference signals auto-tracking of desired signals, and can increase network capacity. They have enormous potential for military operations. Conventional antenna arrays use mechanically steered beams to direct energy to the desired recipient and reduce interference effects. For the future exciting possibilities relate to the use of "Space-Time Adaptive" processing where multi-path is used to advantage to establish a number of parallel and simultaneous channels in the same frequency band. The 3G standard supports the use of smart antennas by having separate pilot sequences for each dedicated channel. (Bhobe & Perini 2001)

Smart Antennas are the subject of research at the moment; work is required to ascertain the vulnerability and applicability of these techniques to military systems. However, Smart Antennas have to be achieved at low cost; adaptive antenna arrays are notoriously expensive and any such array has to be immune to jamming. The latter issue distinguishes the military research from related civilian research into Smart Antennas.

- Infrastructure free networking

The last 25 years have seen an explosive growth in fixed wired networking via cables and optical fibres where connectivity is assured and where the link quality is good and reliable. Wireless networks, particularly mobile wireless networks, do not benefit from these attributes and so cause problems for the Internet transport control protocol (TCP).

Research is currently investigating better strategies to maintain the network quality of service in a mobile environment. In particular the use of ad-hoc or infrastructure free networks is currently receiving attention (Goldsmith & Wicker 2002). For example current civilian cellular systems consist of a radio link between the mobile handset and a base station but which also need a network infrastructure and control signals. The network connects one subscriber to another, the latter being perhaps part of another mobile or conventional telephone network. In contrast in the ad-hoc network concept, the message from one mobile handset will be passed on by another, to another and onward to the recipient without entering the telephone company's network infrastructure. There are of course significant problems, not least overload of the frequency spectrum and available bandwidth (Shannon's Theorem again), but the lack of infrastructure does make it particularly attractive for resilient military applications.

2.3. Communication means

2.3.1. Background

As stated in the ICT-E project description, a highly reliable and secured wireless data link is required for the remote control and monitoring where there is no wired network available. Of course in case there is wired network available, communication through wired network is absolutely the first choice while the wireless solutions can be backup option. However in this thesis work we will focus on only the wireless solutions developed for the areas without any wired network.

To achieve reliable and secured wireless link, normally the solutions are dedicated radio link or satellite link which are typically used in e.g. military communication. However these communication means are not economically feasible for the ICT-E project. The economical communication means are using the commercial wireless communication networks e.g. 2G/2.5G/2.75G GSM/GPRS/EDGE or 3G UMTS, but the question is, are they eligible for the strict requirements set for the power grid application?

Although the ICT-E project demands a highly reliable and secured wireless link which is unlikely to be achieved based on civilian wireless communication network rather than military wireless communication network, this does not necessarily mean civilian wireless communication network is not capable. On the other hand, the ICT-E project tries to look for solutions which are economically feasible, which implies that the solutions should be based on civilian wireless communication network. Of course to fulfill the project requirements, there must be modifications and enhancements in system design and implementation level, using existing technologies based on civilian wireless communication network.

Let’s analyse the existing technologies based on civilian wireless communication network one by one to conclude whether they are eligible to fulfill the strict requirements for the power grid telecontrol applications.

2.3.2. CSD/HSCSD/ECSD

Circuit Switched Data (CSD) is the original form of data transmission developed for the GSM mobile phone system. CSD uses a single radio time slot to deliver 9.6 Kbit/s data transmission to the GSM network and switching subsystem where it could be connected through the equivalent of a normal modem to the Public Switched Telephone Network (PSTN) allowing direct calls to any dial-up service.

High Speed Circuit Switched Data (HSCSD) is a specification for data transfer over GSM networks. HSCSD utilizes up to four 9.6 Kbit or 14.4 Kbit time slots, for a total bandwidth of 38.4 Kbit or 57.6 Kbit. 14.4 Kbit time slots are only available on GSM networks that operate at 1800 MHz. 900 MHz GSM networks are limited to 9.6 Kbit time slots. Therefore, HSCSD is limited to 38.4 Kbit/s on 900 MHz GSM networks and 57.6 Kbit/s on 1800 MHz GSM networks. (Eberspächer, Vögel, Bettstetter 2001)

HSCSD is an enhancement to earlier CSD standard. Enhanced Data rates for Global Evolution (EDGE) enabled GSM networks are able to implement Enhanced Circuit Switched Data (ECSD), an enhanced version of HSCSD. ECSD increases the bandwidth of each timeslot to 48 Kbit and allows the use of eight timeslots, which gives a total transmission speed of 384 Kbit/s. (Eberspächer, Vögel, Bettstetter 2001)

CSD is relatively reliable for data transmission at low data rate as long as the data call can be favourably established. Consider that the remote control application in a power grid application is normally just to manipulate e.g. disconnectors, communication data rate is as low as only the contact information, open/closed, is transmitted. Therefore the CSD is already eligible for the remote control application, however to gain a more smooth operation and lower propagation delay HSCSD is a great advantage. But for the remote monitoring application which requires transmitting video of the operating controlled unit, CSD is definitely ineligible, whereas HSCSD/ECSD can still be considered as candidate because of its own advantage, for circuit switched data is much better than packet switched data in such delay-sensitive application. For the response time, in HSDPA is around 50 ms which should be small enough for many industrial applications, but for Release 99 UMTS and GSM it is typically several hundred milliseconds. For the remote control application of power grid, since the time constant of the disconnector is in the order of magnitude of seconds, thereby tolerating up to one second of propagation delay, even the time response in GSM is not a problem.

The main problem in consideration for CSD/HSCSD will be the blocking probability of the network from initialising a data call. The control of the remote system will be completely lost in case of call blocking. This is most unwanted situation and should be avoided at all expenses. However the nature of commercial wireless communication network implies that blocked call is ineluctable, since it's not a dedicated wireless link and thereby shared by many users. No matter what level of Quality of Service (QoS) the service provider may be able to guarantee, blocking can never be eliminated, neither can any wireless communication network guarantee an access without blocking. The point is how to minimize the blocking probability of data calls to a tolerable level so that it's most unlikely to occur. The solution is to use multiple data terminals for the remote control and monitoring system with different support of wireless network service providers. Of course these different network operators should be physically independent, which means they have separated network infrastructures and are not virtual operators who just rent other operators' networks. In Finland there are three independent networks operators who own their networks, and they are Sonera, Elisa and DNA, in which Sonera and Elisa have better network infrastructures than DNA in sense of coverage and capacity etc from measurements.

Look into the case that there are two data terminals which are supported by two different operators. In case the data call with primary operator is blocked, it goes automatically to secondary operator, and therefore to ensure the entire remote control and monitoring system is still operable under user control despite of the blocked data call. The total blocking probability is dramatically reduced by utilizing two operators, and if necessary there can be a third backup operator to reduce the blocking probability even more. This application could use e.g. Sonera as primary operator and Elisa as secondary. How such solution is able to dramatically reduce the network blocking probability will be later studied and analysed in Section 5.1.

2.3.3. GPRS/EGPRS

General Packet Radio Service (GPRS) is a mobile data service available to users of GSM mobile phones. It is often described as 2.5G, that is, a technology between the 2G and 3G of mobile telephony. It provides moderate speed data transfer, by using unused Time Division Multiple Access (TDMA) channels in the GSM network. GPRS is integrated into GSM standards releases starting with Release 97 and onwards. Enhanced GPRS (EGPRS) in EDGE enabled GSM networks can be used for any packet switched applications such as an Internet connection. High-speed data applications such as video services and other multimedia benefit from its increased data capacity.

Packet switched data under GPRS is achieved by allocating unused cell bandwidth to transmit data. As dedicated voice (or data) channels are setup by phones, the bandwidth available for packet switched data shrinks. A consequence of this is that packet switched data has a poor bit rate in busy cells. The theoretical limit for packet switched data is approximately 170 Kbit/s. A realistic bit rate is 30~70 Kbit/s. A change to the radio part of GPRS called EDGE allows higher bit rates of between 20 and 200 Kbit/s using adaptive coding and modulation (Eberspächer, Vögel, Bettstetter 2001). The maximum data rates are achieved only by allocation of more than one time slot in the TDMA frame. Also, the higher the data rate, the lower the error correction capability. Generally, the connection speed drops logarithmically with distance from the base station. This is not an issue in heavily populated areas with high cell density, but may become an issue in sparsely populated or rural areas, where many of the remote systems of the power grid are likely to be situated in. Therefore the data rate and propagation delay will be the main problem and consideration for using GPRS.

For the remote control application, the propagation delay is more critical than the data rate. But for the remote monitoring application which requires transmitting video of the operating controlled unit, both the propagation delay and the data rate are critical. Now let's see the capable data rate of GPRS.

GPRS is classified to various multi slot classes (Andersson 2001). Multi slot classes are product dependant, and determine the maximum achievable data rates in both the uplink and downlink directions. Written as (for example) 3+1 or 2+2, the first number indicates the amount of downlink timeslots. The second number indicates the amount of uplink timeslots. The active slots determine the total number of slots the GPRS device can use simultaneously for both uplink and downlink communications. Table 2.1 shows the configurations of GPRS multi slot classes.

Multi Slot Class	Downlink Slots	Uplink Slots	Active Slots
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5

Table 2.1 GPRS multi slot classes

Mobile station class indicates the mobile phone capabilities. Class A mobile phones can be connected to both GPRS and GSM services simultaneously. Class B mobile phones can be attached to both GPRS and GSM services, using one service at a time. Class B enables making or receiving a voice call, or sending/receiving an SMS during a GPRS connection. During voice calls or SMS, GPRS services are suspended and then resumed automatically after the call or SMS session has ended. Class C mobile phones are attached to either GPRS or GSM voice service, and needed to switch manually between services.

Analysing the multi slot classes, for example, GPRS class 8 is also known as 4+1. This means that four slots are allocated to downloading and one slot to uploading. This profile is appropriate for applications where data is mostly downloaded, such as web browsing. If the user reads more email than he or she sends, this is also an appropriate profile. Class 8 is usually selected by default on mobile devices that support GPRS. GPRS class 10 is also known as 4+2. This means that four slots are allocated to downloading and two slots to uploading, but no more than five slots may be used at the same time. This profile is appropriate for applications where data is sent back-and-forth in roughly equal amount, such as instant messaging. Other classes exists, including GPRS class 6 (3+2) and GPRS class 4 (3+1) used in older devices. Some rare devices can do as much as 4+4 (up to four slots in both upload and upload, but maximum five in total). Those are for industrial use only, though. Consider the remote monitoring application of power grid which demands highest possible bandwidth for uploading live video or updating motion pictures, the only choice which may be capable is GPRS class 12 (4+4) working in (1+4) mode. But the maximum supported uploading data rate is still doubtable.

The transfer speed depends also on the channel encoding used. Table 2.2 shows the coding schemes used in GPRS. The least robust (but fastest) encoding scheme (CS-4) is available near the Base Transceiver Station (BTS) while the most robust encoding scheme (CS-1) is used when the Mobile Station (MS) is further away from the BTS. Using the CS-4 it is possible to achieve a speed of 21.4 Kbit/s per time slot. However by using this scheme the cell coverage is 25% from the normal. CS-1 can achieve a speed of 9.05 Kbit/s per time slot and has 98% of the normal coverage. Newer network equipments can adapt the transfer speed automatically depending on the mobile location. In power grid application, the locations of the wireless terminals are unlikely to have excellent network coverage, therefore it is unlikely to achieve CS-4 and hence the worst case i.e. CS-1 is assumed.

Coding Scheme	Speed (Kbit/s)
CS-1	9.05
CS-2	13.4
CS-3	15.6
CS-4	21.4

Table 2.2 GPRS coding schemes

The mentioned speed includes overhead of various protocols used. Net data speed is somewhat lower. Table 2.3 compares the speed of different mobile data technologies, assuming that CS-3 is used with actual speed about 14.4 Kbit/s for GPRS.

Mobile data technologies	Download	Upload
GPRS 1+4 (class 12)	14.4 Kbit/s	57.6 Kbit/s
GPRS 4+1 (class 8 & 10 & 12)	57.6 Kbit/s	14.4 Kbit/s
GPRS 3+2 (class 10)	43.2 Kbit/s	28.8 Kbit/s
CSD	9.6 Kbit/s	9.6 Kbit/s
HSCSD (2+1)	28.8 Kbit/s	14.4 Kbit/s
HSCSD (3+1)	43.2 Kbit/s	14.4 Kbit/s

Table 2.3 Comparisons of different mobile data transmission rates

The best possible uploading rate for GPRS 1+4 is 57.6 Kbit/s. Consider that the GPRS terminal still needs to handle other communications besides uploading video, the real bandwidth which can be guaranteed for uploading video will be much less, so it will not be sufficiently capable for use with the remote monitoring application. Backup options which give higher bandwidth e.g. EDGE or UMTS must be available.

As a summary, GPRS can be used for event based signalling or periodic updates with long sampling interval for i.e. the remote control application, while EGPRS is useful for streaming applications for i.e. the remote monitoring. Packet switched data is cost and bandwidth efficient but less reliable. The traffic may be congested and the propagation delay cannot be guaranteed. GPRS can be used as primary communication means for the remote control application, however it cannot be relied on as standalone communication means, so there must be a reliable backup solution, which CSD is proved to be most suitable, as secondary communication means. It is very important that the remote control application is able to switch from GPRS to CSD in case of traffic congestion to keep the remote controlled devices controllable. EGPRS would be primary communication means for the remote monitoring application and secondary communication means would be ECSD to keep a minimal bandwidth at a higher cost.

How such solutions are able to improve the system reliability will be later studied and analysed in Section 5.1.

2.3.4. UMTS

Universal Mobile Telecommunications System (UMTS) is one of the 3G mobile phone technologies. It uses WCDMA as the underlying standard, is standardized by the 3GPP, and represents the European/Japanese solution to the ITU IMT-2000 requirements for 3G Cellular radio systems.

UMTS supports up to 1920 Kbit/s data transfer rates, although at the moment users in the real networks can expect performance up to 384 Kbit/s - in Japan upgrades to 3 Mbit/s are in preparation. However, this is still much greater than the 14.4 Kbit/s of a single GSM error-corrected CSD channel or multiple 14.4 Kbit/s channels in HSCSD, and in competition to other network technologies such as CDMA-2000, PHS or WLAN, it offers access to the World Wide Web (WWW) and other data services on mobile devices. (Holma & Toskala 2001)

From data rate point of view, UMTS can definitely fulfill the requirements. However UMTS will be considered only for future development in this application, due to several technical and practical reasons at the moment, e.g. the UMTS network coverage is not wide enough, the cost performance is not economical, the technology is still relatively not mature enough and lack of sufficient trials, etc.

2.3.5. Comparison and conclusion

GSM data transmission has advanced since the introduction of CSD. GPRS is different from the older CSD connection included in GSM standards releases before Release 97. In CSD, a data connection establishes a circuit, and reserves the full bandwidth of that circuit during the lifetime of the connection. GPRS is packet switched which means that multiple users share the same transmission channel, only transmitting when they have data to send. This means that the total available bandwidth can be immediately dedicated to those users who are actually sending at any given moment, providing higher utilization where users only intermittently send or receive data. Web browsing, receiving emails as they arrive and instant messaging are examples of uses that require intermittent data transfers, which benefit from sharing the available bandwidth.

HSCSD has an advantage over GPRS in that HSCSD supports guaranteed quality of service because of the dedicated circuit switched communications channel. This makes HSCSD a better protocol for timing-sensitive applications such as image or video transfer. GPRS has the advantage over HSCSD for most data transfer because HSCSD, which is circuit switched, is less bandwidth efficient with expensive wireless links than GPRS, which is packet switched. Usually, GPRS data is billed per kilobytes of information transceived while circuit switched data connections are billed per second. The latter is to reflect the fact that even during times when no data is being transferred, the bandwidth is unavailable to other potential users.

HSCSD is a system which was based on and quite similar to CSD but designed to provide higher data rates. GPRS on the other hand provides a packet based data transmission directly from the mobile phone. Finally EDGE and UMTS provide improved radio interfaces with higher data rates, but still, in large part, compatible with the same GSM core network. Both HSCSD/ECSD and GPRS are likely to eventually be phased out in favour of UMTS, which is a packet switched technology with speeds up to 2 Mbps.

As conclusion of which communication means should be used in the remote control and monitoring system, we leave UMTS as an option only for future development due to various technical and practical reasons. For the remote control application, the primary communication means will use GPRS and CSD as backup. For the remote monitoring application, the primary communication means will use EGPRS and ECSD as backup. Both the primary and backup terminals support such hybrid communication means. Both the remote control application and remote monitoring application can share the same primary terminal and backup terminal(s).

2.4. System modular structure

2.4.1. Redundancy design

From above argumentations, to use completely commercial wireless communication network based solution have been agreed. As the power grid application demands highly reliable and secured wireless data link, this can only be resolved from improving system redundancy design point of view rather than improving network technology point of view, because of the nature of commercial wireless communication network.

Redundancy, in general terms, refers to the quality or state of being redundant, that is: exceeding what is necessary or normal, containing an excess. Redundancy is serving as a duplicate for preventing failure of an entire system. In engineering, the duplication of critical components of a system with the intention of increasing reliability of the system is called redundancy. In safety-critical systems, some parts of the control system may be triplicated. An error in one component then may be out-voted by the other two. In a triply redundant system, the system has three sub components, all three of which must fail before the system fails. Since each one rarely fails, and the sub components are expected to fail independently, the probability of all three failures is calculated to be extremely small.

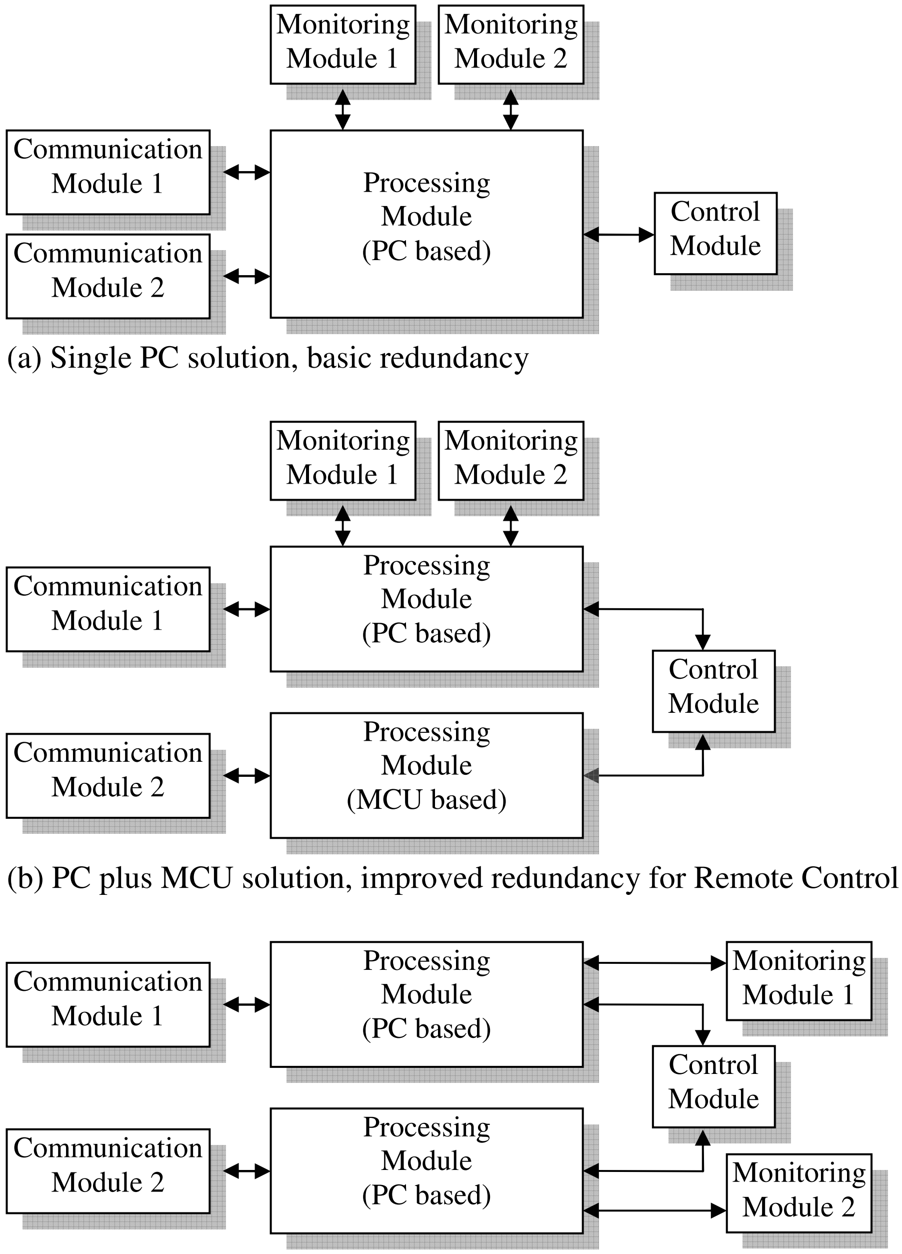
In our case, the idea is that the system with redundancy design will always have multiple possibilities to maintain an operational status in case of failure of part of its components. Of course a 100% reliable system could never possibly exist, however the idea is to employ redundancy design to dramatically improve the system reliability to be very close to 100%.

The desired wireless remote control and monitoring system normally consists of the following modules: communication module, processing module, control module, monitoring module. According to the reliability theory (El Mahdy 2001), the most critical part of the system should have redundancy design to be duplicated or even triplicated, which is particularly the communication module in our case. The communication module has relatively higher probability to fail, not because of the failure of data terminal but because of the network traffic congestion. Since the entire remote control and monitoring system totally relies on wireless communication which failure probability is based on majority of the sophisticated network traffic rather than the reliability of the components, it is the most critical part in the system. Of course each component of the modules has a probability to fail, but the idea is to utilize redundancy design for the modules which are more likely to fail. In this case, the focuses are the communication module and also the processing model. The other modules i.e. control module is relatively much more reliable.

2.4.2. Proposed structures

Several different system modular structures are considered to be eligible. Redundancy design is used as main technique to improve the reliability in order to fulfill the project requirement. Based on different considerations, 3 different system modular structures are proposed, as illustrated in Figure 2.1.

From typical experiences in such system, the Communication Module is the most critical part, the Monitoring Module is the second, and the Processing Module is the third. For all the proposed models, absolutely the Communication Module needs redundancy design, and therefore duplicated Communication Modules appear in every design. On the other hand, considering the Monitoring Module has higher failure probability than the Processing Module, therefore duplicated Monitoring Modules also appear in every design. Such design dramatically improves the system reliability without increasing much of the expenses. Whether to use redundancy design for the Processing Module depends on more specified requirement, since the expense is considerable and may contribute very little to improve the system overall reliability.



(a) Single PC solution, basic redundancy

(b) PC plus MCU solution, improved redundancy for Remote Control

(c) Duplicated PC solution, complete parallel redundant system

Figure 2.1 Proposed system modular structures

Model (a) is based on single personal computer (PC) solution. The main focuses of redundancy design are towards Communication Module and Monitoring Module, and there is no redundancy for Processing Module. Depending on the requirements, this design provides basic redundancy and may already be sufficient for most situations.

Model (b) is originated from model (a) while adding redundancy for Processing Module by employing highly reliable Processing Module based on microcontroller (MCU). The main purpose is to dramatically improve the reliability of Remote Control Function based on model (a). However, the limitations of Processing Module based on MCU cause the degrading of the reliability of Remote Monitoring Function, since the duplicated Monitoring Modules have to be served by only one Communication Module. This design may suitable for certain requirements which need extremely reliable Remote Control Function rather the Remote Monitoring Function.

Model (c) is based on a complete parallel redundancy design, to have everything duplicated, only except the Control Module as it cannot have duplicated design. This design improves the reliability of both Remote Control Function and Remote Monitoring Function to a higher level, with the cost of higher expenses by employing duplicated Processing Module based on PC. Such design is able to fulfill the strictest requirements.

Certainly there can be many more models or variations other than these described 3 models, but these 3 are most typical and representative ones. In next section, reliability analysis will be performed and numerical evaluations will be done, so that the differences between these 3 designs can be easily seen.

2.5. System reliability study and analysis

2.5.1. Reliability theory

Reliability theory is the foundation of reliability engineering. For engineering purposes, reliability is defined as: the probability that a system will perform its intended function during a specified period of time under stated conditions.

Mathematically, this may be expressed as,

$$F(t) = \int_{t}^{\infty} f(x)dx\,, \tag{2.1}$$

where $F(t)$ is the failure probability from time *t*, and $f(x)$ is the failure probability density function.

From (El Mahdy 2001), there are four key elements in the definition of reliability. Reliability engineering is concerned with each of these elements of reliability.

First, reliability is a probability. This means that there is always some chance for failure. Reliability engineering is concerned with meeting the specified probability of success, at a specified statistical confidence level.

Second, reliability is predicated on performing its "intended function". Generally, this is taken to mean operation without failure. However, even if no individual part of the system fails, yet the system does not do what it was supposed to do, then it is still charged against the system reliability. The system requirements specification is the criterion against which reliability is measured. Reliability engineering ensures adequate system testing and other assessments to ensure compliance to the requirements.

Third, reliability applies to a specified period of time. In practical terms, this means that a system has a specified chance that it will operate without failure before time *t*. Reliability engineering ensures that components and materials will meet the reliability requirements during the specified time.

Fourth, reliability is restricted to operation under stated conditions. This constraint is necessary because it is impossible to design a system for unlimited conditions. Reliability engineering ensures that the operating environment is adequately addressed during system design and test.

2.5.2. Reliability design

According to (El Mahdy 2001), it is axiomatic that reliability must be designed in to the system. During system design, the top-level reliability requirements are flowed down, or allocated, to subsystems and lower levels.

Reliability design often begins with a system reliability model. Reliability models are usually expressed using reliability block diagrams and fault trees. They provide a graphical means of evaluating the relationships between different parts of the system for reliability purposes. Reliability models often incorporate reliability predictions based on parts count failure rates. These predicted failure rates come from databases of historical failure data. While these predictions are often not accurate in an absolute sense, they are very valuable to assess relative differences in design alternatives. Reliability models and predictions are performed using commercially available software tools and databases.

Several reliability design techniques are employed to meet the specified reliability. One of the most important techniques is redundancy. This means that, if one part of the system fails, there is an alternate success path, such as a backup system. Redundancy significantly increases system reliability, and is often the only viable means of doing so. However, redundancy is usually difficult and expensive, and therefore limited to critical parts of the system. Another design technique is physics of failure. Physics of failure relies on understanding the physical processes of stress, strength and failure at a very detailed level. Then, the material or component can be re-designed to reduce the probability of failure. Another common design technique is component de-rating. This means selecting components whose tolerances significantly exceed the expected stress. It’s obvious that in our case the most suitable technique to improve reliability is to apply redundancy design.

2.5.3. Computation theory

From (Trivedi 2002, pp. 29-31), a series system is one in which all components are so interrelated that the entire system will fail if any one of its components fails. On the other hand, a parallel system is one that will fail only if all if its components fail. We will assume that failure events of complements in a system are mutually independent.

Consider a system of n independent components. For $i = 1,2,...,n$, define event $A_i =$"components i is functioning properly". Let the reliability, R_i, of component i be defined as the probability that the component is functioning properly; then $R_i = P(A_i)$. Let $F_i = 1 - R_i$ be the unreliability of component *i*. Then since A_i and $\overline{A_i}$ are mutually exclusive and collectively exhaustive events, we have

$$1 = P(A_i) + P(\overline{A_i}) \text{ and } F_i = P(\overline{A_i}) = 1 - P(A_i)$$

For series connection:

$$R_s = P(A_1 \cap A_2 \cap \cdots \cap A_n) = P(A_1)P(A_2)\cdots P(A_n) = \prod_{i=1}^{n} R_i \tag{2.2}$$

$$F_s = 1 - R_s = 1 - \prod_{i=1}^{n}(1 - F_i) \tag{2.3}$$

For parallel connection:

$$F_p = P(\overline{A_p}) = \prod_{i=1}^{n} F_i \tag{2.4}$$

$$R_p = 1 - F_p = 1 - \prod_{i=1}^{n}(1 - R_i) \tag{2.5}$$

Therefore, product law of reliabilities (Eq. 2.2) is applicable to series systems of independent components, and product law of unreliabilities (Eq. 2.4) is applicable to parallel systems of independent components. The basic formulas for the reliability computation of series and parallel systems can be used in combination to compute the reliability of a system having both series and parallel parts (series-parallel systems).

2.5.4. A case study

The objective of this case study is intended to analyse and evaluate the 3 proposed models of system modular structures, to have a straightforward idea about the differences between the models and therefore to be able to make a proper choice.

Assume the failure probabilities of individual modules are known parameters, from these parameters we derive respectively the failure probability of Remote Control Function and Remote Monitoring Function for each proposed model. The problem is described as following.

Definition of known parameters:

Failure Probability of Communication Module 1: P_{CM1}

Failure Probability of Communication Module 2: P_{CM2}

Failure Probability of Processing Module (PC based): P_{PMpc}

Failure Probability of Processing Module (MCU based): P_{PMmcu}

Failure Probability of Control Module: P_{CtM}

Failure Probability of Monitoring Module 1: P_{MM1}

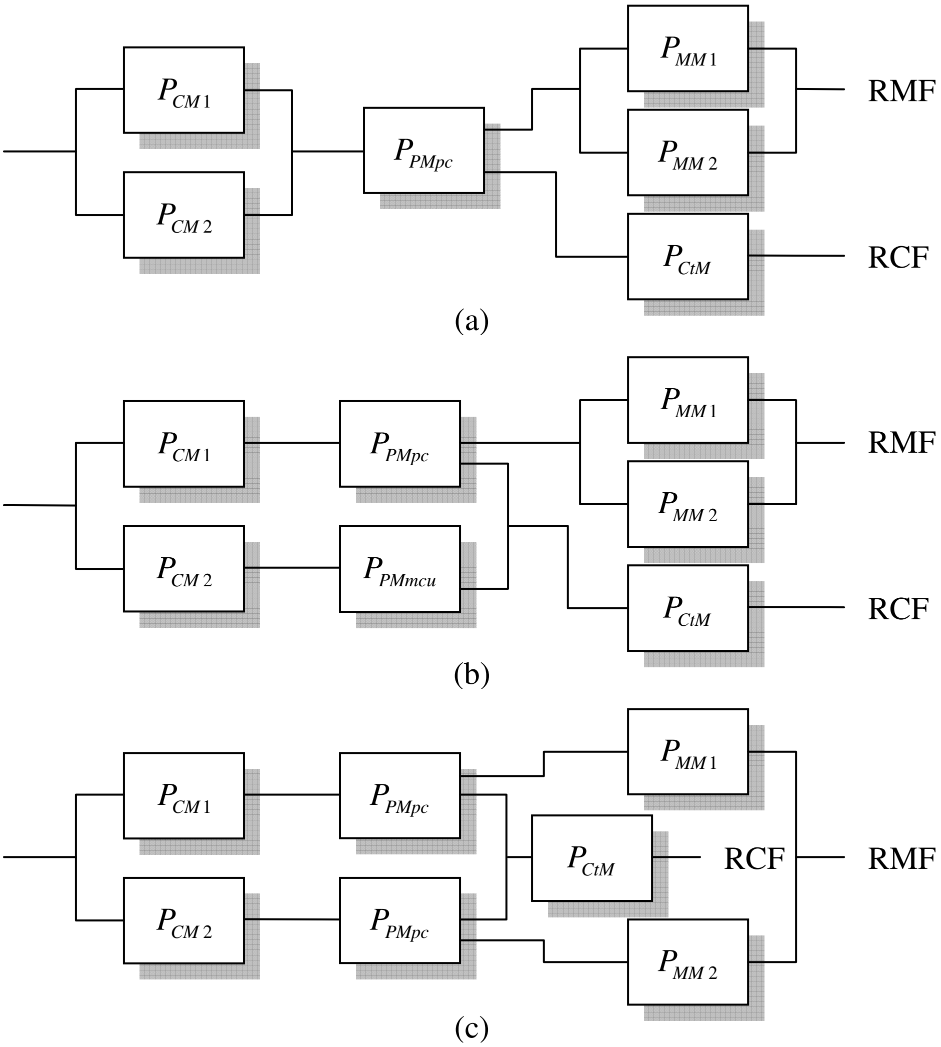
Failure Probability of Monitoring Module 2: P_{MM2}

Solve:

Failure Probability of Remote Control Function (RCF): P_{RCF}

Failure Probability of Remote Monitoring Function (RMF): P_{RMF}

Block diagrams for reliability analysis of each model are illustrated in Figure 2.2. As can be seen that they are various series-parallel systems, the failure probability of Remote Control Function and Remote Monitoring Function for each model can be derived using the above described formulas.



(a)

(b)

(c)

Figure 2.2 Block diagrams for reliability analysis

In this case study, the analysis for the failure probability of Communication Module is a bit different than other models. Here is a brief explanation. For a given instant of time the Communication Module is rendered failed if either one of its components fails or its supporting network is congested. These two events can be assumed to be independent of each other. Therefore the failure probability given here refers to joint probability of component failure and network blocked of the Communication Module. Their relations are:

P{Communication Module inaccessible | at least one component fails}=1

P{Communication Module inaccessible | all component OK}
= P{Network blocked}=*Blocking Probability*

P{Communication Module inaccessible}
= P{at least one component fails}+(1- P{at least one component fails}) P{Network blocked}

For the Communication Module, define:

Hardware Component Failure Probability of Communication Module 1: P_{CMhw1}
Blocking Probability of Network used by Communication Module 1: P_{B1}
Hardware Component Failure Probability of Communication Module 2: P_{CMhw2}
Blocking Probability of Network used by Communication Module 2: P_{B2}

Therefore,

$$P_{CM1} = P_{CMhw1} + (1 - P_{CMhw1}) \cdot P_{B1}$$
$$P_{CM2} = P_{CMhw2} + (1 - P_{CMhw2}) \cdot P_{B2}$$

Derived results for model (a), (b), (c) respectively:

$$P_{RCFa} = 1 - (1 - P_{CM1} P_{CM2})(1 - P_{PMpc})(1 - P_{CtM})$$
$$P_{RMFa} = 1 - (1 - P_{CM1} P_{CM2})(1 - P_{PMpc})(1 - P_{MM1} P_{MM2})$$

$$P_{RCFb} = 1 - \{1 - [1 - (1 - P_{CM1})(1 - P_{PMpc})][1 - (1 - P_{CM2})(1 - P_{PMmcu})]\}(1 - P_{CtM})$$
$$P_{RMFb} = 1 - (1 - P_{CM1})(1 - P_{PMpc})(1 - P_{MM1} P_{MM2})$$

$$P_{RCFc} = 1 - \{1 - [1 - (1 - P_{CM1})(1 - P_{PMpc})][1 - (1 - P_{CM2})(1 - P_{PMpc})]\}(1 - P_{CtM})$$
$$P_{RMFc} = [1 - (1 - P_{CM1})(1 - P_{PMpc})(1 - P_{MM1})][1 - (1 - P_{CM2})(1 - P_{PMpc})(1 - P_{MM2})]$$

where $P_{CM1} = P_{CMhw1} + (1 - P_{CMhw1}) \cdot P_{B1}$, $P_{CM2} = P_{CMhw2} + (1 - P_{CMhw2}) \cdot P_{B2}$

Consider the results of failure probability. Generally, P_{RCFa} and P_{RMFa} will be already quite low, thanks to the redundant design of Communication Module. P_{RCFb} will be even much lower than P_{RCFa} due to the additional redundant design of Processing Module, while P_{RMFb} will be much higher than P_{RMFa} since there is only single dedicated Communication Module. Both P_{RCFc} and P_{RMFc} will be extremely low, thanks to the redundant design of both Communication Module and Processing Module.

Numerical evaluation is shown in Table 2.4:

Assumption values of known parameters	Calculation results:
$P_{CM1} = 0.015$ $P_{CM2} = 0.017$ $P_{PMpc} = 0.005$ $P_{PMmcu} = 0.002$ $P_{CtM} = 0.001$ $P_{MM1} = 0.011$ $P_{MM2} = 0.019$	$P_{RCFa} = 0.0062$ $P_{RMFa} = 0.0055$ $P_{RCFb} = 0.0014$ $P_{RMFb} = 0.0201$ $P_{RCFc} = 0.0014$ $P_{RMFc} = 0.0012$

Table 2.4 Numerical evaluation

From the numerical evaluation results, it’s straightforward to see that the redundancy design has been proved to be effective which dramatically improves the system reliability. It can be easily seen that model (c) can provide best reliability for both Remote Control Function and Remote Monitoring Function, and therefore is recommended for most critical requirements. While model (a) and model (b) have also very good reliabilities, they can be adopted to corresponding cases where the requirements are not most critical but with different emphasises of reliability needs. The system implementation is carried out in modular structures, so that the implemented modules can be easily assembled together to form a complete system based on any one of the designed models or even new models.

3. APPROACH TO SYSTEM IMPLEMENTATION

As stated in the initial design, from consideration of many aspects the remote control and monitoring tasks will be relatively independent in both hardware and software in order to fulfill the design requirements. Obviously it means that both hardware and software will be designed separately as remote control part and remote monitoring part. In this chapter the design argumentation, validation and implementation are discussed in several aspects.

3.1. Major components

From argumentations in last chapter, the system based on the hybrid model has been decided to be implemented. To build the hybrid model involves major components such as PC, MCU, GSM/GPRS/EDGE terminals, and web camera. To choose the proper components is extremely important in the first stage. The components are selected based on the requirement of system design, and other considerations such as security and redundancy.

3.1.1. PC

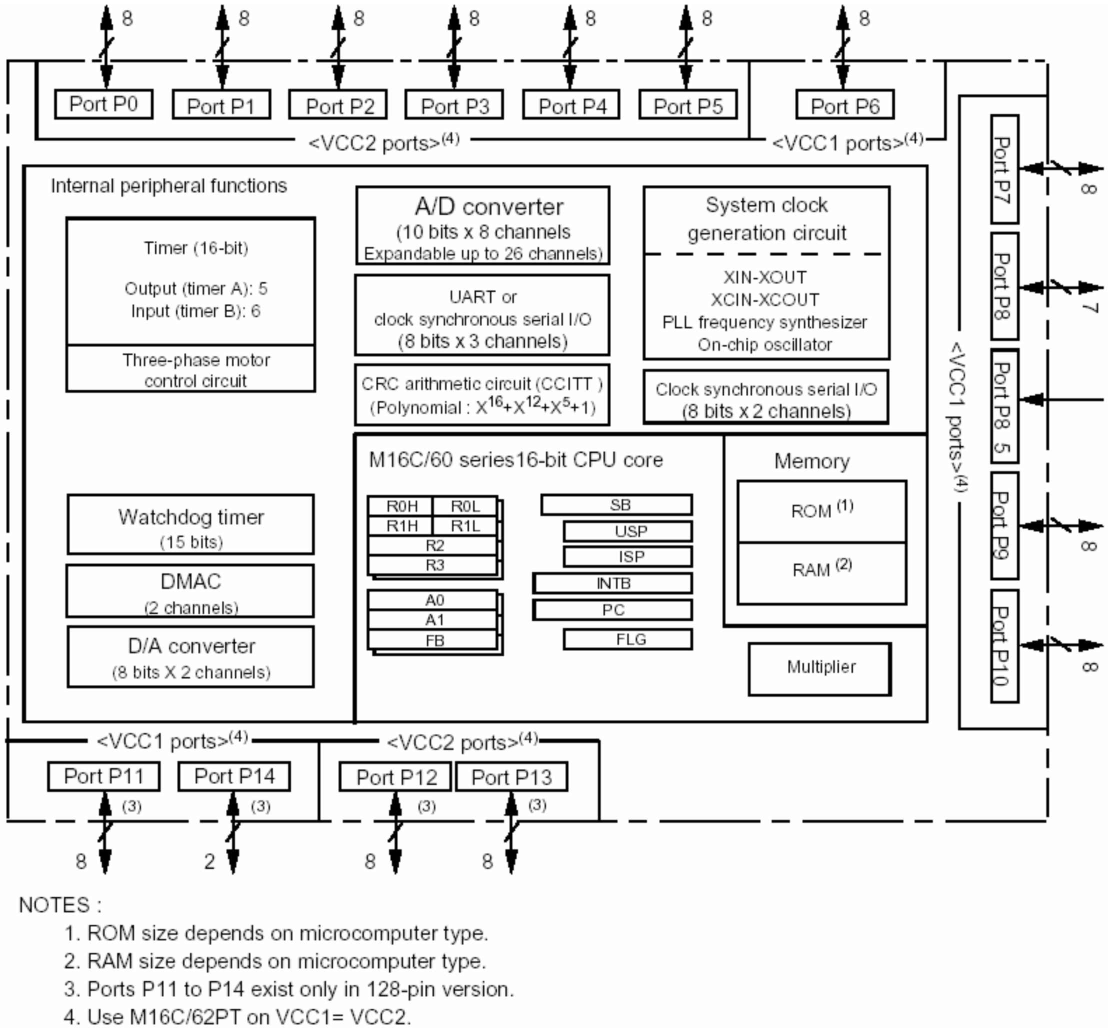
For the basic requirement of the PC, it shall have Personal Computer Memory Card International Association (PCMCIA) slots, serial port, parallel port and Universal Serial Bus (USB) port. The reason why it shall have PCMCIA slots is that the remote monitoring part relies on GPRS/EDGE data terminal with especially high-speed uplink and such data terminals available in the market all have PCMCIA interface. The serial port is for connection of a backup GSM terminal. The parallel port is for sending control bit and reading feedback bits interfacing with execution devices. The USB port is for connection with USB web camera. From the above requirements, a laptop is much more suitable than a desktop because of the integrated PCMCIA interface. Of course in practice, industrial PC would be required for real deployment of such power grid application. But for the prototyping, a laptop PC is sufficient. With other considerations such as reliability, durability and security, IBM ThinkPad T series laptop is absolutely the first choice.

IBM ThinkPad T series is designed to be the most secure notebooks available. On select T42 and T43 models are now even better with one integrated security solution out of the box. The combination of the Integrated Fingerprint Reader and the Embedded Security Subsystem is like having a security guard for the T series notebook. The Integrated Fingerprint Reader is built conveniently into the palm rest area of the notebook, making passwords available at the finger tip. Having to remember and enter multiple passwords is eliminated with a swipe of the finger, and security software is preloaded for an integrated solution out of the box. Such integrated security solution makes the T series notebook a highly secured PC. It even cannot be powered up for unauthorized access without entering the proper password. (IBM 2005)

3.1.2. MCU

For the basic requirement of the MCU, it shall have serial port for communication with the GSM terminal, and enough I/O ports for interfacing with the control and monitoring devices as well as necessary input/output devices. There are many microcontrollers available in the market which can fulfill these requirements. Renesas M16C/62 series microcontroller is selected, because of its high performance, powerful features, low cost, low power consumption, ease of use, and familiarity based on years of experience.

The Renesas M16C/62 – M30626FHPFP microcontroller serves as the central control unit for the designed MCU based remote control system. This microcontroller is packaged in a 100-pin plastic molded Quad Flat Package (QFP) and operates using sophisticated instructions featuring a high level of instruction efficiency. With 1 Mbytes of address space, it is capable of executing instructions at high speed. In addition, this microcontroller contains a multiplier and Direct Memory Access Controller (DMAC) which combined with fast instruction processing capability, makes it suitable for control of various office automation, communication, and industrial equipment which requires high-speed arithmetic/logic operations. M16C/62P is based on the M16C/60 Core and has 1 MB memory space. Maximum operating frequency is 24 MHz when using Phase-Locked Loop (PLL) Synthesizer. Figure 3.1 shows the functional block diagram of the M30626FHPFP chip. (Renesas 2003)


Port P0
Port P1
Port P2
Port P3
Port P4
Port P5
Port P6
<VCC2 ports>(4)
<VCC1 ports>(4)
Internal peripheral functions
Timer (16-bit)
Output (timer A): 5
Input (timer B): 6
Three-phase motor control circuit
A/D converter (10 bits x 8 channels Expandable up to 26 channels)
UART or clock synchronous serial I/O (8 bits x 3 channels)
CRC arithmetic circuit (CCITT) (Polynomial : X16+X12+X5+1)
System clock generation circuit
XIN-XOUT
XCIN-XCOUT
PLL frequency synthesizer
On-chip oscillator
Clock synchronous serial I/O (8 bits x 2 channels)
M16C/60 series16-bit CPU core
R0H R0L R1H R1L R2 R3 A0 A1 FB
SB USP ISP INTB PC FLG
Memory
ROM (1)
RAM (2)
Multiplier
Watchdog timer (15 bits)
DMAC (2 channels)
D/A converter (8 bits X 2 channels)
Port P7
Port P8
Port P8_5
Port P9
Port P10
Port P11
Port P14
Port P12
Port P13
8
7
2
(3)

NOTES :
1. ROM size depends on microcomputer type.
2. RAM size depends on microcomputer type.
3. Ports P11 to P14 exist only in 128-pin version.
4. Use M16C/62PT on VCC1= VCC2.

Figure 3.1 Block diagram of M30626FHPFP chip (Renesas 2003)

During the develop stage the 3DKM16C/62P 3 Diamonds Board which consists of an M30626FHPFP (M16C/62P) will be used to validate the design. A dedicated Printed Circuit Board (PCB) for the MCU will be redesigned for final implementation.

3.1.3. GSM/GPRS/EDGE terminals

For the purpose of redundancy design, more than one data terminal will be employed. From the argumentations in last chapter, the suggested model shall have at least two data terminals, primary and secondary. The primary one takes care of high-speed uplink/downlink data with relatively higher data throughput for the remote monitoring part as well as the remote control part under normal operational conditions. The secondary one takes care of conventional data communication as a first backup to the primary one, with relatively lower data throughput but higher reliability. Additional data terminals may be used if necessary as additional individual backups to the primary and secondary ones.

The data terminals will be selected from available equipments which have been already pre-selected based on certain criteria and have been already put in trial under various circumstances so that their characteristics and real world performance are somehow known already. These data terminal equipments are listed as follow.

1) PCMCIA data cards

- Nokia D211 Radio Card

The Nokia D211 is a multimode radio card that enables network access through GPRS, HSCSD, and wireless LAN networks. It is capable for mobile data connectivity through GPRS, HSCSD or wireless LAN, 'always-on' connection, access to Internet, with wireless connectivity up to 40.2 Kbit/s in GPRS networks, 43.2 Kbit/s in HSCSD networks, 11 Mbit/s in wireless LAN networks. (Nokia 2002)

- Option GlobeTrotter Universal Tri-band GPRS/GSM PC-Radio Card

The GlobeTrotter is an ultimate solution to provide high performance mobile wireless functionality, enabling users to make telephone calls, browse the Internet, send and receive emails, with SIM and Phonebook management seamlessly integrated. This Tri-band PC Data Card suitable for use on GSM networks worldwide with simultaneous GSM and GPRS registration. (Option 2005)

- Sierra Wireless AirCard 775

The AirCard® 775 is operating on EDGE and GSM/GPRS Networks, offering speeds up to three times faster than on GPRS networks. It is capable for worldwide use with Quad-band Operation, with typical speeds between 100~130 Kbit/s, capable of speeds up to 216 Kbit/s, and global roaming on EDGE, GSM/GPRS networks. (Sierra 2005)

2) GSM/GPRS terminal

- Nokia 30 GSM Connectivity Terminal

The Nokia 30 is a compact, highly advanced GSM Connectivity Terminal with a built-in SIM card reader, internal antenna and interfaces for connecting to a remote device. This makes it ideal as the communication link for a wide range of M2M applications. It can also be used as a normal wireless modem for connecting to the Internet. (Nokia 2002)

- Siemens MC35 Terminal

Developed primarily for the M2M market segment, the ultra-compact MC35 Terminal boasts an always-on connection and high-speed data transfer capabilities. The robust dual-band GSM unit with GPRS class 8 can be used in a wide range of areas including metering and remote maintenance, traffic systems, shipping & logistics, security, vending machines, and building technology. (Siemens 2005)

3) GSM/GPRS module

- Telit GM862-GPRS module

The Telit GM862 is a small lightweight and low power consumption device that allows digital communications services wherever there is a GSM network. It is the Telit Industrial product line of wireless telecommunications modules specifically designed and developed for M2M wireless applications such as remote meter billing, vending machines, automotive applications and fleet management, emergency services, security systems, environmental monitoring, POS terminals, handheld devices. Besides all, it has some unique features than any other wireless terminals. For example the Jammed Detection feature is able to detect the presence of an interference device such as a GSM Communication Jammer, and the Easy Scan feature scans all GSM base stations to get parameters such as Cell ID and Channel number which can be used not only for GSM cell locating but also for service functions. (Telit 2005)

Data Terminal Equipment	Key Features	Multi slot Class Mobile station Class	Approximate trail period and experience
Nokia D211	Dual band GSM 900/1800 MHz Support for GPRS, HSCSD, WLAN, and SMS	GPRS Multi slot Class 6, mobile station Class B	Half year, reliable, GPRS connection may occasionally drop
Option GlobeTrotter	Tri band GSM 900/1800/1900 MHz Support for GPRS, CSD, SMS, voice and fax	GPRS Multi slot Class 10, mobile station Class B	Over 2 years, very reliable, very seldom connection drop
Sierra Wireless AirCard 775	Quad band GSM 850/900/1800/1900 MHz Support for EDGE, GPRS, CSD, SMS, voice and fax	EDGE/GPRS Multi slot Class 12, mobile station Class B	Half year, reliable, GPRS connection may occasionally drop, and good performance with EDGE but the service is not always available depending on network resources and BER.
Nokia 30	Dual band GSM 900/1800 MHz Support for GPRS, HSCSD, CSD, SMS and USSD	GPRS Multi slot Class 6, mobile station Class B	Half year, very reliable, very seldom connection drop
Siemens MC35	Dual band GSM 900/1800 MHz Support for GPRS, HSCSD, CSD, SMS, USSD, voice and fax	GPRS Multi slot Class 8, mobile station Class B	Over 2 years, very reliable, very seldom connection drop
Telit GM862-GPRS	Dual band GSM 900/1800 MHz Support for GPRS, CSD, voice, SMS and fax	GPRS Multi slot Class 8, mobile station Class B	Over 2 years, very reliable with CSD, GPRS not tested

Table 3.1 Overview of various wireless data terminal equipments

Table 3.1 shows an overview of all the available data terminal equipments, their basic specifications and trial result for easy comparison and selection for the suitable devices.

The selection is based on the following criteria. The primary data terminal shall be capable to handle high data rate especially in uplink. For the primary data terminal, the reliability of packet switched connection is less important than data rate, as there is no existing data terminal which is 100% reliable that never drops the connection. The reliability shall be compensated from the redundancy design. That is to say if the connection drops, it shall be able to automatically switch to another mode and still maintain its responsibility. For the secondary data terminal, as it shall work partly as backup, the focus is more about its reliability with circuit switched connection. For both terminals, they shall be able to switch to circuit switched mode automatically when receiving a data call and suspend packet switched mode. This makes sure that the data call can always override the control when for example the GPRS connection is not responding. The mobile station class B is ideal for such purpose.

As the primary data terminal requires especially high data rate in uplink, therefore a maximum possible number of uplink slots is appreciated, and obviously multi slot class 12 is the choice which gives maximum 4 uplink slots. From the above listed devices, the Sierra Wireless AirCard 775 fulfils all the requirements. Besides it also supports EDGE, making it possible to support even up to 3 times data rate than GPRS. For the future development, a 3G UMTS data terminal shall be replaced as the primary terminal to support even high data rate. For the secondary data terminal, as it works with MCU, the choice is absolutely Telit GM862-GPRS module. Its design is optimised for interfacing with embedded system such as MCU, and it has advanced unique features which have great value to enhance the reliability and security. For the third backup data terminal, Nokia 30 GSM Connectivity Terminal is the best choice for its outstanding reliability and suitable multi slot class.

3.1.4. Web camera

The web camera is the input source of the remote monitoring part. It shall be a normal USB web camera that works flawlessly together with the PC based web camera server program. It shall support various video compression standards to minimize the bandwidth. It shall have sufficient resolution capability for future expansion. The purpose to require sufficient resolution of the web camera is to make the remote monitoring part have potential capability to broadcast higher quality video if the bandwidth is broadened, for example the employment of 3G data terminals and supporting networks. Such idea is to make the design always expandable for the future. Last but not least, it shall have proper protection for outdoor environment against weather conditions such as rain and snow, and ability to sustain extreme temperatures (but this requirement is skipped in prototyping). Logitech QuickCam Pro 4000 is selected based on the requirement and its own remarkable features, such as 640×480 video resolution with the advanced VGA CCD sensor and high-quality 1.3 mega pixel photo resolution with digital zoom, digital pan and tilt. (Logitech 2005)

3.2. Approach to the system design

3.2.1. The desired system

The remote control will be achieved based on a server-client program. The party to be able to accept user's control commands and be able to execute the control commands is defined as server, or remote control server. The other party where user sends control commands is defined as client, or remote control client. On server party there is a shell program so that the client can connect to the server with a terminal-like program and remotely execute the shell program. The shell program is actually a Human-Computer Interaction (HCI) of the remotely controlled device, with which user can interact with the real system. The client party is just an extension to this HCI.

The remote monitoring is similar to the remote control part. It will be also achieved based on a server-client program. The party to be able to monitor the execution of user's control commands and transmit the live video to user is defined as server, or remote monitoring server. The other party where user receives the live video from the scene to verify the execution of user's control commands is defined as client, or remote monitoring client. The server is able to monitor the process through a camera, add time stamp and stream the video over internet, or capture still pictures and keep updating at a relatively short interval. The client can view the streaming video or updating pictures and also check the time stamp to verify the validity of the source.

3.2.2. Reliability and security

The demanded system should be highly operational reliable. This will be achieved by utilizing redundant modular design and other measures i.e. the built-in feedback system. Although the main purpose of this remote control part as stated above is to accept the control commands and execute the control commands, however to design a built-in status feedback system in addition will be a great advantage. It is able to provide some lower level direct feedback to user, to verify the command execution results. Such kind of lower level feedback is certainly not sufficient to fulfill the visual monitoring requirements in the power grid application, as in the requirement it is stated that it must be visually verified, which is the reason to build another standalone remote monitoring system. However such implementation of lower level feedback is still a great benefit for elementary verification, especially to use with the combination of higher level visual verification from the remote monitoring system. Also in case of breakdown or unexpected situation, such implementation is greatly helpful to figure out the fault.

Another important issue to be considered is about the possible blocking of arriving network or dropping of connection. In case a call is blocked, although under rare situation this happens, the user is not able to access the system at all. Since the entire system is designed to be operated based on wireless communication network, there always existing a certain value of blocking probability. In reality under normal circumstance the service providers are not even able to guarantee a certain level of QoS, either there is never a solution to achieve zero blocking probability but only possible to minimize the blocking probability to approaching zero. This issue can be solved by employing hybrid communication means of packet switched/circuit switched access and multiple network service providers, say two physically individual network service providers are serving the same system, in case one is blocked it can automatically switch to another backup one etc, and then the blocking probability can be dramatically reduced. When using packet switched access, the connection may timeout and drop if the traffic is idle for a certain period. To prevent dropping connection due to timeout in packet switched mode, the system is designed to send small packets at regular time intervals i.e. ping to its DNS server, to keep the connection alive. The system is also designed in a way that it will always automatically reconnect once the connection is blocked or dropped.

Since such system should be highly secured, all communication must be secured by cryptographies. SSH/VPN is proposed as primary security solution when applicable, and extra cryptographies have to be implemented when SSH/VPN is not applicable. Besides, the system should have certain level of ability to identify and resist any sorts of hacker attack. Several solutions are proposed here to achieve the target.

To identify any possible hacker attack, first the remote system will always ask user to verify the current time after successful login. Since all the time stamp comes from the remote host, the time stamp is valid only if the current time on remote host is valid itself. The remote clock will be always synchronized to client party after user gives positive reply. If user checks the current time from remote host is different than the client computer, even small difference in seconds, may already imply that there might be system failure or hacker attack, because otherwise the clock should exactly match. Immediately after this step, second the remote system will always ask user to verify the current status plus time stamp. Since the user is always supposed to know and should be absolutely sure about current status. If status shows wrong end or stuck between two ends then it obviously implies that there is system failure or hacker attack, because otherwise the status should always match user's expectation. Third, during user command execution, there is a timer on remote host to count the time duration from the control command is sent until the controlled device reaches the target end, according to the reading value of feedback bits. If the operation is smooth, the time counted should never exceed a defined limit. If timeout is reached during the operation, then it may already imply that there might be system failure or hacker attack, because otherwise it should have finished already.

To resist any possible hacker attack, the system is designed so that under whatever situation the administrator of the system can always have possibilities to take over the control. This is achieved by using the hybrid hardware structures of PC and MCU with individual communication terminals, as well as hybrid communication means of packet switched and circuit switched. The principle that the administrator can always override any unauthorized access to system is that, the communication terminal used at server party is a Class B GPRS/EDGE data card, whenever there is incoming call, the always-on internet connection no matter in what status will be forced to suspend in order to respond to the incoming data call. Meanwhile, hackers are not possible to make the terminal busy in order to block incoming calls, because of the built-in equipment and user authentication features in the program, only with authorized Subscriber Identification Module (SIM) card and terminal equipment is able to access the remote system. The MCU based backup system provides another alternative for administrator to override unauthorized access to system under emergency situations. The GSM terminal connected to the server party is reserved only for incoming calls. Same as described before, hackers are not possible to make the terminal busy in order to block incoming calls, because of the built-in equipment and user authentication features in the program, only the user with authorized SIM card and terminal equipment is able to access the remote system.

As a brief summary, the major features which have been designed for enhancing reliability and security of the system are listed. For enhancing reliability: Redundancy design improves general system reliability. The built-in feedback with sensors provides an extra alternative for double verification of the disconnector status. Employing hybrid communication means and multiple network service providers dramatically reduces the blocking probability in communication. Keeping-alive and automatic-reconnection features prevent the possible disconnection from network. For enhancing security: All communications are secured by SSH/VPN or other cryptographies. The procedures of manual verification of current time, current status and timeout detection in the remote control program provide security measures to identify system failure or hacker attack. The abilities of overriding control, access control, and authentication for both user and equipment provide extra security measures against unauthorised access.

3.2.3. Design for redundancy and security

Since the system is required to have redundancy design to achieve high operational reliability and security, it is designed to use different means of remote control and monitoring through different physical communication channels and different hardware. This implies also the software has to be design for different platforms. But the idea is that no matter working under what kind of platform, the processes are always the same or very similar, and so are the user interfaces.

The means of communication are defined with following priorities.

1) 1st priority: PC-based server with connection through internet with GPRS/EDGE

- Principle

The server party is connected to GPRS/EDGE service which supposes to be always connected to internet. The client party initialize a connection to the server through SSH/VPN secured channel to execute the remote control program running on the server. The remote control program running on the server takes care of user authentication, acceptance and execution of control commands and acknowledgment of lower level feedback from the controlled device. The client party only needs a normal SSH/VPN client program with a preferably broadband internet enabled PC. Both SSH and VPN are proposed at this design stage, but finally a preferable solution on how to utilize these protocols will be made according to the implementation and testing results.

- Security solution

All data security during communication is ensured by SSH/VPN itself.

2) 2nd priority: PC-based server with connection through data call with CSD/HSCSD

- Principle

It serves as a primary backup alternative in case of the failure of normal communication stated in 1st means. It also serves as emergency overriding alternative if someone is trying to hack the remote system. At the client party, when the user finds trouble while trying 1st means, he will initialize the alternate program. This alternate client program is able to make a direct data call to the server party. Since the communication terminal used at server party is a Class B GPRS/EDGE data card, the current internet connection no matter in what status will be forced to terminate in order to respond to the incoming data call.

There is a relatively simple solution to achieve such backup system. The idea is to setup the server so that it's able to accept incoming connection, and to setup dial-up networking on the client party based on CSD/HSCSD. Once the client dials up to the server, the server automatically accepts the incoming connection. After user verification, the CSD/HSCSD connection is established. Then the client party can directly access the remote control program with SSH, which ensures the data security. This solution is absolutely technically feasible and doesn't need much effort to work it out, as with previous implemented remote control program there is almost no additional programming required rather than just some setup procedures. However, considering from system security point of view, such solution is not eligible at all since it has potential risk of being cracked. Attackers can easily paralyse the system just by looping of dial-up connections and keep the remote data terminal always busy so that it cannot accept any other incoming connection, since the fatal weakness of such system is that it can only accept one incoming connection at one time. To prevent such trouble from occurring, there must be some measures to be able to verify the caller ID and even the device ID, and reject any unauthorised incoming request from the beginning. Therefore it's necessary to design an application-specific program to fulfill the requirements, which is described in details as follow.

The remote control program running on the server is similar to the one in 1st means, takes care of user authentication, acceptance and execution of control commands and acknowledgment of lower level feedback from the controlled device. Besides that it has additional functions to accept data call and built-in data security with encryption / decryption related features such as random key generation and key exchange.

The main difference than 1st means is that there are added verification procedures during the initialization of communication. When it receives incoming data call, first the caller ID will be verified. If the caller ID matches the one in its database of authorized caller and equipment list, it will answer the data call and create terminal communication. Otherwise it will hang up the data call directly. Once the terminal communication is established between server and client, the client will then send its IMEI as second authentication for the server to verify. If the IMEI matches again the one in its database, it will continue to user authentication procedure. Otherwise it will again hang up the data call directly. After these successful authentication procedures, the following procedures are exactly the same as described in 1st means.

- Security solution

In such case of connection through data call, data security issues have to be taken into great consideration, since it's a customised solution which is not able to adopt any standard integrated data security solutions.

The authentications are done through two levels, equipment level and user level. The authentication of equipment means that user can only initialize a remote control session from authorized communication terminals. In our case the authentication of equipment includes SIM and IMEI verification.

First is SIM card with Personal Identification Number (PIN) code verification. SIM card is a smart card that operates a GSM phone. Each card is unique and carries the phone number and stored features that operate when inserted into a handset.

PIN code verification feature must be always on. Whenever the terminal is trying to connect to network services, it will always ask for PIN code. PIN code is the first protection against unauthorized usage of a SIM card. The user has to enter the correct PIN code before he gains full access to the SIM card. After this first verification, the terminal is able to connect to network provider and register for network services.

Send caller ID feature must be always on. Whenever the terminal initialize a call, the network operator will send the caller ID to the receiving terminal, and the receiving terminal will verify the caller ID. If the call ID matches the one in the authorized list, then the terminal will issue ATA command to answer the call and thus establish data terminal communication, else will issue ATH command to hang up the incoming call. This ensures operator can have access to the system only with the authorized SIM card and he must know the correct PIN code.

Second is server and client terminal's International Mobile Equipment Identity (IMEI) verification. The IMEI is a unique number given to every single mobile phone. IMEI numbers of cellular phones connected to a GSM network are stored in a database Equipment Identity Register (EIR) containing all valid mobile phone equipment. When a phone is reported stolen or is not type approved, the number is marked invalid.

The IMEI codes of server terminal and client terminal are retrieved every time at the program initialisation, by issuing AT+CGSN command (request product serial number identification) to the connected data terminals, and saved to a temporary variable. After successful verification of caller ID, the terminal answers the call and encrypted data communication is established. The server will first identify itself by sending its IMEI to the client. The client verifies the code and confirms that is the correct server. Then the client will also identify itself by sending its IMEI to the server. The server verifies the code and confirms that is an authorised client. Likewise, only if the IMEI codes of both parties match the corresponding ones in the authorized list, then the program will move on to welcome and user login procedure, else either party will issue ATH command to terminate the data call. After these successful verifications, the program will then move on to normal routines which are exactly the same as described in 1st means.

These basic verifications are the very beginning of authentications, however they are effective and should be able to prevent majority of unauthorized access to the system. The reasons are described as follow.

First, PIN code protection is one of the standard built-in features of SIM card to prevent unauthorized usage of SIM card.

Second, caller ID is identified and sent from telecom network operator and in principle it’s extremely difficult to reproduce fake caller ID unless someone has control of the network operator. The only known hacker attack is likely to duplicate the original SIM card to make an unauthorized clone. This is possible and relatively not so difficult, only if the original SIM card is unfortunately circulated to unauthorized parties, which is still rare to happen.

Third, IMEI is a unique number given to every single mobile station terminal. It is written in the EEPROM of the terminal device and not modifiable by the user. The 15-digit IMEI code is nearly impossible to crack by trails. The only known hacker attack is likely to generate a fake duplication of the IMEI from the original terminal device. This is possible but relatively difficult, only if the original IMEI of terminal device is unfortunately circulated to unauthorized parties, which is very rare to happen.

From above argumentation, the verification of SIM card and IMEI should be sufficient to prevent majority of unauthorized access to the system. To crack these verifications, hacker must have to obtain the original SIM card as well as the original IMEI of terminal device, which in combination would be extremely rare to happen.

These are add-on procedures for authentication which should be seamlessly integrated with the main program. Then the issue is data encryption during the terminal communication. From the above description it means that there should be a paired server-client program running on both parties, and they are physically different than the one used in 1st means but have very similar user interface and mostly same operation procedures. Data security in 1st means is ensured by SSH/VPN itself, but in 2nd means data security has to be built into this paired server-client program. In the original remote terminal program e.g. Telnet all the contents of the session including password and sensitive commands are sent unencrypted and therefore are open to sniffing of network traffic. So in our case the encryption before transmitting data and decryption after receiving data must be done when communicating through terminals. It ensures the data security in 2nd means that only encrypted data transmitting through unsecured open terminals. Although the GSM/GPRS air interface contains ciphering so no additional encryption is needed if leased lines are used after the radio access network, the reason why there need to be built-in encryption in this application will be discussed in Section 4.3.1.

The authentication and encryption method is proposed to be similar as SSH, using public key cryptography for authentication and secret key cryptography for ciphering of data. When the client program runs the first time, a pair of public key and secret key is formed at local computer. The public key is moved to the list of authorized keys of remote computer. Local computer sends remote computer its public key. If it is found in the list of authorized keys, remote computer creates a secret key and sends it to the client encrypted with client's public key. Local computer decrypts the session key with its secret key. After this session encrypted with secret key can start.

3) 3rd Priority: MCU-based server with connection through data call with CSD/HSCSD

It serves as a secondary backup alternative in case of the both failure of normal communication stated in 1st means and 2nd means. In addition it also serves as emergency overriding alternative if someone is trying to hack the remote system when the primary override fails.

All features in this means are exactly the same as those stated in 2nd means, except that the server or remote computer is a microcontroller or embedded industrial PC than normal PC.

	Hardware	Communication	Connection	Security
1st	PC +GPRS/EDGE Data card	Internet via GPRS/EDGE	IP addressed	SSH/VPN
2nd	PC +GSM terminal	Data call via CSD/HSCSD	Peer to Peer	Built-in
3rd	MCU +GSM terminal	Data call via CSD/HSCSD	Peer to Peer	Built-in

Table 3.2 Comparisons of the 3 alternatives

Table 3.2 shows comparisons for the above 3 alternatives. For the remote monitoring system, since the image or video transmission will be totally IP based, therefore it works only under 1st Priority of communication means. And the backup remote monitoring system uses same communication means but different network service providers to reduce blocking probability or connection drops. Besides communication means the proposed connection means for the remote monitoring system utilizes hybrid mode of broadcasting and peer-to-peer. At least two independent cameras serve respectively for broadcasting and peer-to-peer monitoring. Under normal circumstance, the user who is monitoring the control process should visually verify the updating images or live video from both two sources. The purpose to use such hybrid mode is that the broadcasting mode provides possibilities for easy access with standard web browser and flexibility to embed web functionalities, and to let not only the operator but also other authorised supervisors to monitor the control process when there is sufficient bandwidth (e.g. with 3G data terminals and network services), whereas the peer-to-peer mode is always eligible to satisfy the operator and to ensure the performance of video transmission when there is very limited bandwidth.

3.2.4. Session design

An approach session design of performing a remote control is described as following sequences. All communications travelling through SSH/VPN channels are security ensured. For other communications travelling through normal channels are secured by built-in cryptography. The remote monitoring session is different and will be described in later section.

1) Incoming connection established, welcome message and user login

```
/* show initial welcome message and login request */
Welcome to XXX
Login: admin
Password: *********

/* if username and password match then continue */
User admin authenticated, access to system granted.

/* else return beginning of step 1 */
Login failed, please try again.
/* end current session automatically when username and password
mismatch counted up to three times */
Bad login, session ended.
```

2) Manual verification of remote system status

```
/* ask user to verify the current time and date of remote system */
Current time and date is hh:mm:ss dd-mm-yyyy, correct? (yes or no)

/* if answered “yes” then continue, else give security warning */
WARNING: Server may have potential security defeat, are you sure to
continue? (yes or no)
/* if answered “yes” then continue, else end current session */
/* remark: this situation should be extremely rare unless hardware
failure or hacker attack */

/* ask user to verify the current status of remote system */
Current system status is □□□□□ OPEN @ hh:mm:ss dd-mm-yyyy, correct?
(yes or no)
/* ask user to verify the current status of remote system */
Current system status is ■■■■■ CLOSED @ hh:mm:ss dd-mm-yyyy, correct?
(yes or no)

/* if answered “yes” then continue, else give security warning */
WARNING: Server may have potential security defeat, are you sure to
continue? (yes or no)
/* if answered “yes” then continue, else end current session */
/* remark: this situation should be extremely rare unless hardware
failure or hacker attack */
```

3) Remote control and monitoring

```
/* user enters command to manipulate */
Enter your command: (OPEN or CLOSE)

/* if command given is different than current status then execute
command, give “executing” acknowledgment and start timing */
Executing...Current system status is ■■■□□ @ hh:mm:ss dd-mm-yyyy
/* remark: status is lively updated through reading the I/O ports
periodically until reaching the either end (OPEN or CLOSED) */
/* if timeout then give security warning, else continue */
WARNING: Operation timeout, server may have potential security defeat,
are you sure to continue? (yes or no)
/* if answered “yes” then continue, else end current session */
/* remark: this situation should be extremely rare unless hardware
failure or hacker attack */

/* operation accomplished and position locked to either end (OPEN or
CLOSED) */
Command executed successfully.
Current system status is set to ■■■■■ CLOSED @ hh:mm:ss dd-mm-yyyy
/* or */
Command executed successfully.
Current system status is set to □□□□□ OPEN @ hh:mm:ss dd-mm-yyyy

/* if command given is the same as current status then give “no
change” acknowledgment */
Set status is the same as current status, no change has been made, try
again? (yes or no)
```

```
/* if answered "yes" then return beginning of step 3, else end current
session */
```

4) Ending of current session

```
/* ask user's confirmation to end current session */
End current session? (yes or no)
/* if answered "yes" then end current session, else return step 3 */
```

The software design of remote control program is completely based on the above described procedures and the following flow charts shown in Figure 3.2 and Figure 3.3, which are respectively the remote control program at the server party and at the client party.

Figure 3.4 illustrates clearly how the respective actions are negotiated between client party and server party. The sequence diagram covers a complete remote control session including procedures of verification, encryption, control and feedback when using circuit switched access mode. The remote control session only involves user verification, control and feedback when using packet switched access mode, shown in dashed block, and leave the authentication and encryption to third party software i.e. SSH/VPN.

As for the security considerations, when using circuit switched mode there are a number of verification procedures as well as data encryption for securing the data transmission using unsecured communication channels. All these are built into the remote control program at both server and client parties. For an easier understanding, a table is attached in Appendix 2 which lists all details of the serial communication, i.e. strings transmitted and received at terminals of both parties.

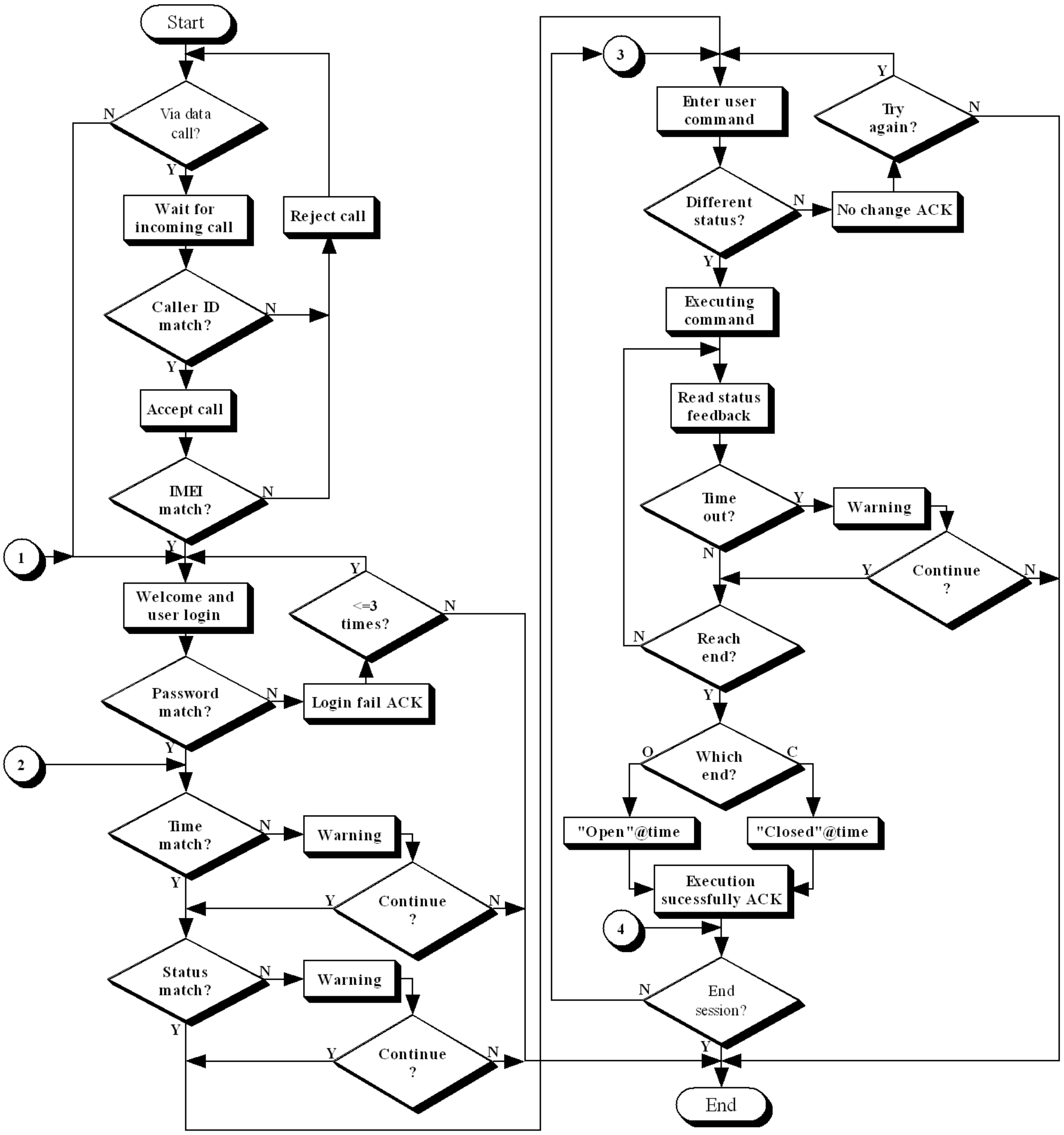


Figure 3.2 Flow chart of remote control system: server party

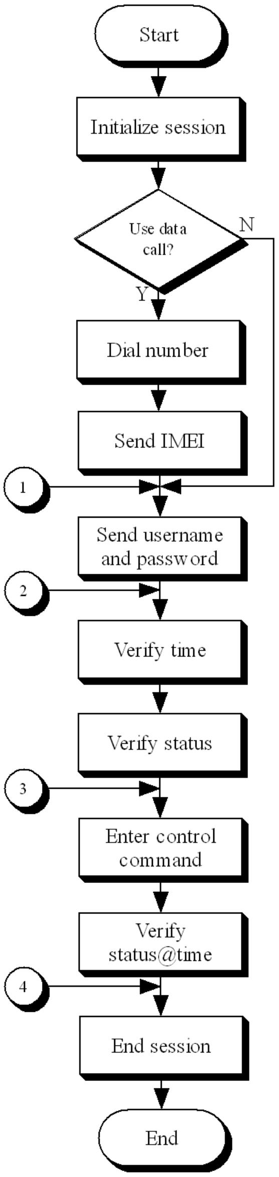


Figure 3.3 Flow chart of remote control system: client party

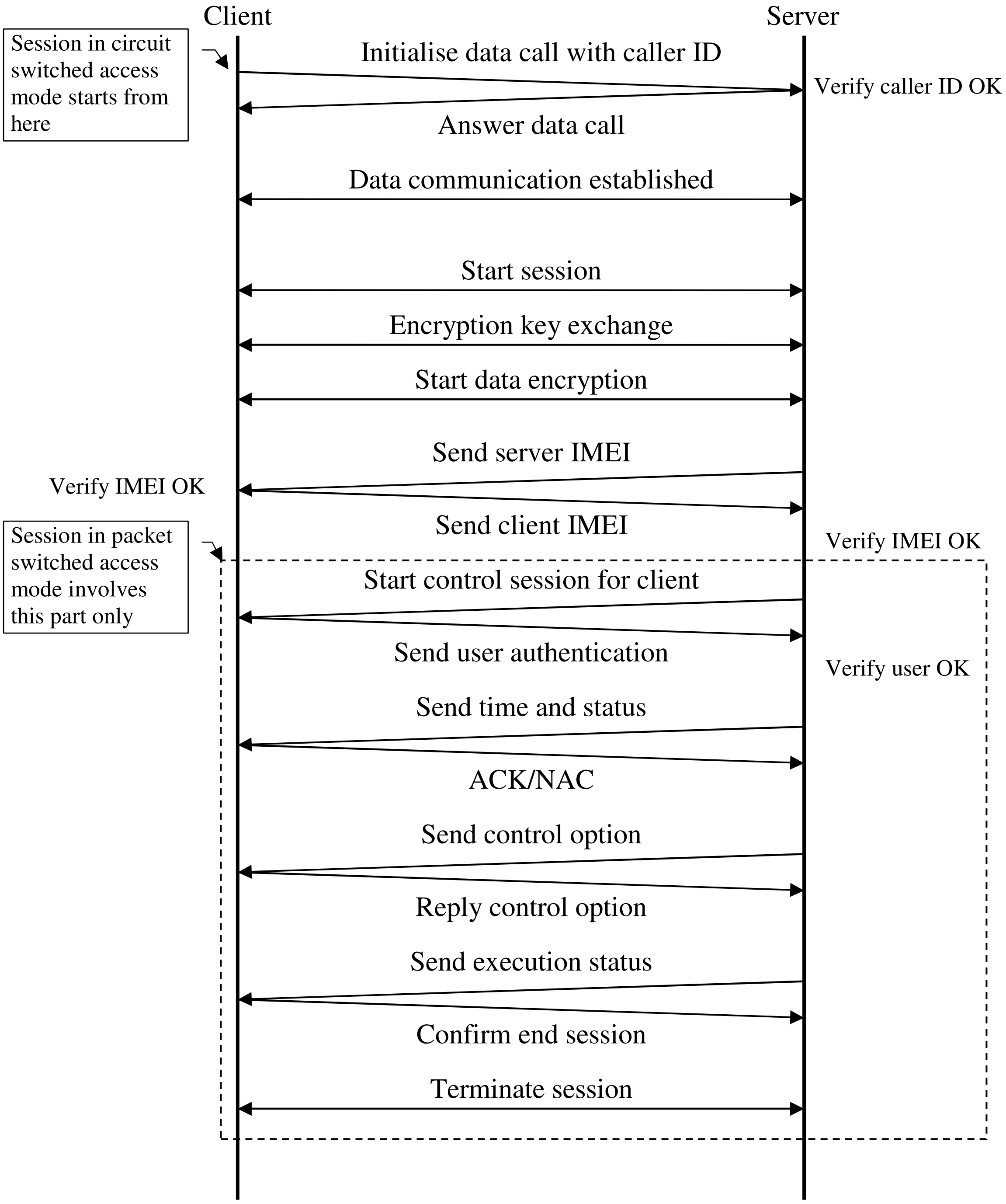


Figure 3.4 Sequence diagram of a remote control session between client and server

3.3. Functional entities implementation

From the argumentations described last chapter, the system modular structures have some variations and which variation to use is depended on the requirements. It's more realistic to implement some individual relatively complete and independent functional entities and then these can be combined together into different models to satisfy different kind of needs. Therefore the implementation mainly targets on PC based and MCU based entities. These entities can be used as standalone model, or can be combined together to form hybrid redundancy model, or can be duplicated to form parallel redundancy model, or can be in any other forms of redundancy models as desired. The entity mainly consists of communication module, processing module, control module and monitoring module. Hardware and software are implemented accordingly to each module.

3.3.1. PC based solution

This part takes care of both the remote control and remote monitoring based on PC solution. The implementation mainly involves these aspects: setup of communication terminal, setup of I/O port for remote control and implementation of related program, setup of web camera for remote monitoring and setup of related software.

1) Communication terminal

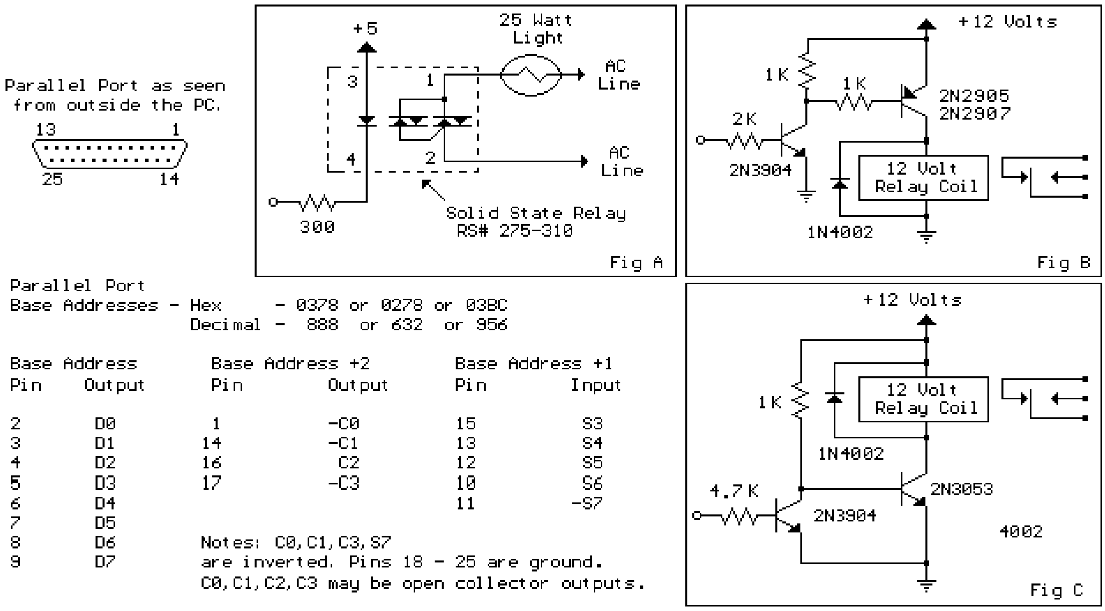
For the communication with data terminal equipment, this is done through serial port or PCMCIA interface emulated virtual serial port. The data terminal equipment is simply controlled by AT commands and communication is handled by server and client program. So there is no specific hardware implementation but purely software implementation for this part.

2) Remote control part

The remote control part needs both hardware and software implementation of interfacing between the PC and the controlled device. For a PC the interfacing of the controls and feedbacks with controlled device is done through the parallel port. A number of I/Os of the parallel port are used for sending control commands and receiving feedbacks. The following discusses in details how to write the commands to LPT port and read the feedbacks from LPT port.

- Writing data to the parallel port

Here a parallel port controlled relay interface is analysed. Below are three examples of controlling a relay from the PC's parallel printer port (LPT1 or LPT2). Figure 3.5A shows a solid state relay controlled by one of the parallel port data lines (D0-D7) using a 300 ohm resistor and 5 volt power source. The solid state relay will energize when a "0" is written to the data line. Figure B and C show mechanical relays controlled by two transistors. The relay in Figure 3.5B is energized when a "1" is written to the data line and the relay in Figure 3.5C is energized by writing a "0" to the line. In each of the three circuits, a common connection is made from the negative side of the power supply to one of the port ground pins 18-25. (Bowden 2005)



Parallel Port
Base Addresses - Hex - 0378 or 0278 or 03BC
Decimal - 888 or 632 or 956

Base Address		Base Address +2		Base Address +1	
Pin	Output	Pin	Output	Pin	Input
2	D0	1	-C0	15	S3
3	D1	14	-C1	13	S4
4	D2	16	C2	12	S5
5	D3	17	-C3	10	S6
6	D4			11	-S7
7	D5				
8	D6				
9	D7				

Notes: C0,C1,C3,S7 are inverted. Pins 18 - 25 are ground. C0,C1,C2,C3 may be open collector outputs.

Figure 3.5 A parallel port controlled relay interface (Bowden 2005)

- Reading data from the parallel port

The diagram in Figure 3.6 shows 5 switches connected to the 5 input lines of the parallel port. An external 5 volt power supply is used to provide high logic levels to the input pins when the switches are open. The 330 ohm resistors in series with the port connections provide some protection in case a connection is made to the wrong pin. The negative side of the power supply should be connected to the ground point of the parallel port, or any pin from 18 to 25. (Bowden 2005)

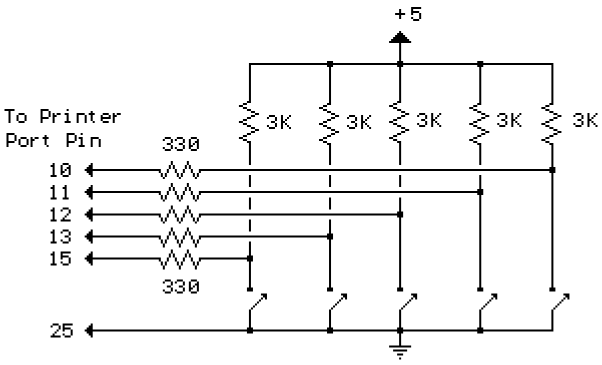


Figure 3.6 Connection diagram for feeding data to the parallel port (Bowden 2005)

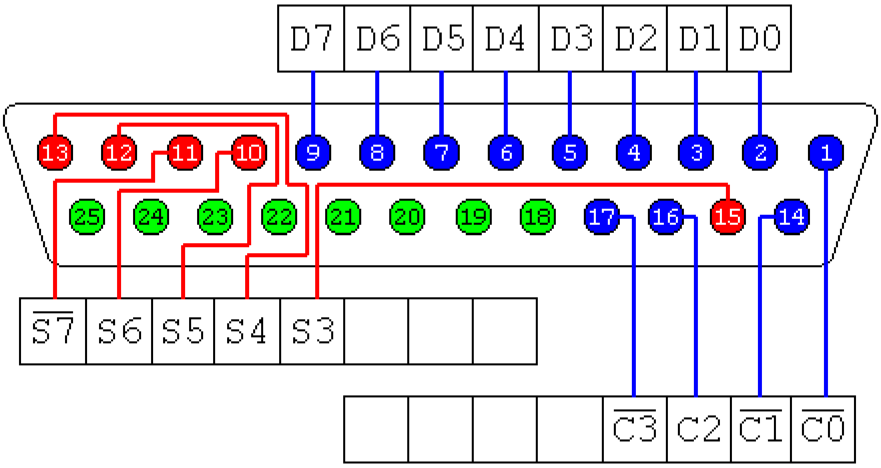


Figure 3.7 Layout of the parallel port pins (Hajer 2005)

- Accessing the port

There are three possible base addresses for the parallel port but LPT1 is usually at Hex 0378. Figure 3.7 shows the layout of port pins. Figure 3.8 shows I/O pin definitions of data port, status port and control port.

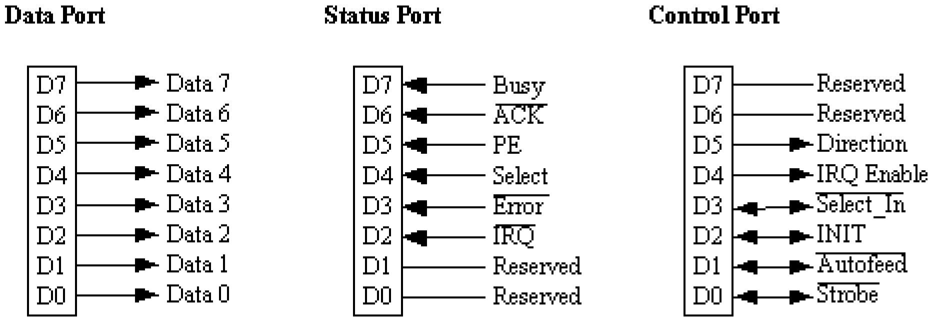


Figure 3.8 I/O pin definitions of the parallel port (Hajer 2005)

In Linux programming, to output a byte, call outb(value, port), for example:

```
/* Set the data signals (D0-7) of the port to all low (0) */
outb(0, BASEPORT);
/* Set the data signals (D0-7) of the port to all high (1) */
outb(255, BASEPORT);
```

Except the eight data lines, the parallel port also provides four control lines (C0, C1, C2, C3) that can be set high or low by writing data to the base address+2 so if the base address is Hex 0378 then the address of the control latch would be Hex 037A. Three of the control bits are inverted so writing a "0" to the control latch will set C0, C1, C3 high and C2 low.

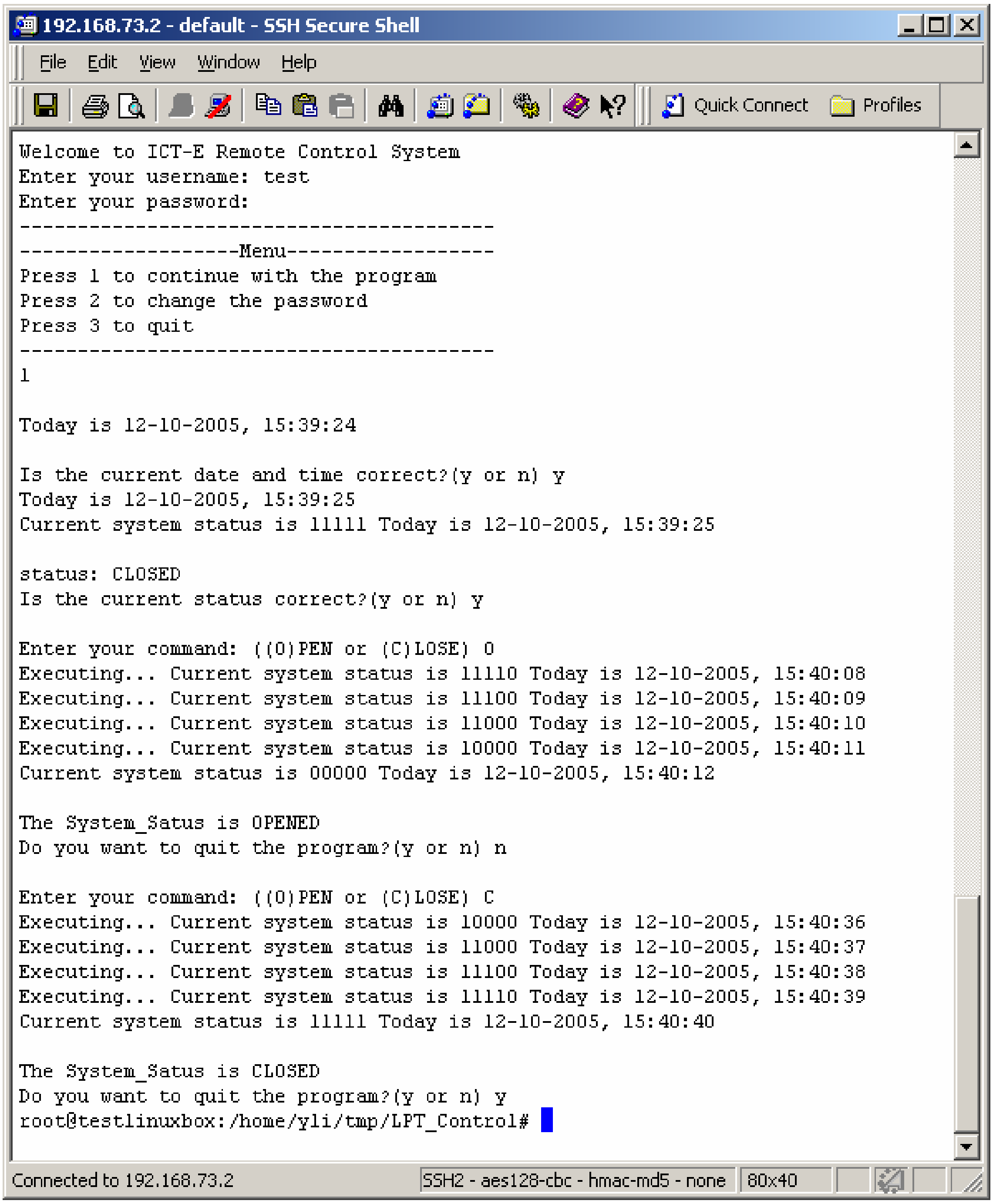
To input a byte (8 bits) from a port, call inb(port), it returns the byte it got, for example:

```
/* Read from the status port (BASE+1) and display the result */
printf("status: %d\n", inb(BASEPORT + 1));
```

The parallel port also provides five control lines (S3, S4, S5, S6, S7) that can read from the input and register data to the base address+1 so if the base address is Hex 0378 then the address of the status port would be Hex 0379. Status bit S7 is inverted so reading a "0" to will set S7 high. The state of the 5 lines is received as a single 8-bit number between 0-255. Each switch input represents a decimal value of 8, 16, 32, 64 and 128 which correspond to pins 15, 13, 12, 10 and 11. The last 3 bits (1, 2 and 4) are not used and should return a high level, so the value received with all switches open should be 1+2+4+8+16+32+64=127. If a switch is closed and the input is at ground, the value will be 0 except for pin 11 which is inverted and yields a value of 128 and 0 when high, so the value received when all switches are closed should be 1+2+4+128=135. The attached table in Appendix 3 shows the relationship between return value and real status.

The remote control program for both packet switched solution and circuit switched solution are based on exactly same principle as described above. The difference is that the packet switched solution works under SSH secure shell environment, whereas the circuit switched solution works under self-made terminal-like environment with built-in data security since the SSH is based on TCP/IP and cannot be utilized with terminal communication. The self-made terminal-like program is similar to SSH in principle, providing both authentication and encryption. Actually the core control program itself alone is designed for shell environment so it can be directly adopted into the packet switched solution. Then the circuit switched solution is an expansion to the core program which should add serial communication for modem control and built-in cryptography for authentication and securing data.

A prototype of the core control program has been developed for evaluation. It is design for remote control system based on PC or embedded PC running with Linux operating system. For testing purpose, it has been installed on a server running with Knoppix Linux system. Figure 3.9 shows a screenshot of a client session running from SSH Client. The screenshot gives some basic ideas about the core control program, which has been designed strictly according to the logics and functions defined in the flowchart as shown in Figure 3.2. The evaluation shows that the program has been able to meet all the desired specifications and requirements. The source code of this program is attached in Appendix 4.


192.168.73.2 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect
Profiles
Connected to 192.168.73.2
SSH2 - aes128-cbc - hmac-md5 - none
80x40

```
Welcome to ICT-E Remote Control System
Enter your username: test
Enter your password:
-----------------------------------------
-------------------Menu------------------
Press 1 to continue with the program
Press 2 to change the password
Press 3 to quit
-----------------------------------------
1

Today is 12-10-2005, 15:39:24

Is the current date and time correct?(y or n) y
Today is 12-10-2005, 15:39:25
Current system status is 11111 Today is 12-10-2005, 15:39:25

status: CLOSED
Is the current status correct?(y or n) y

Enter your command: ((O)PEN or (C)LOSE) O
Executing... Current system status is 11110 Today is 12-10-2005, 15:40:08
Executing... Current system status is 11100 Today is 12-10-2005, 15:40:09
Executing... Current system status is 11000 Today is 12-10-2005, 15:40:10
Executing... Current system status is 10000 Today is 12-10-2005, 15:40:11
Current system status is 00000 Today is 12-10-2005, 15:40:12

The System_Satus is OPENED
Do you want to quit the program?(y or n) n

Enter your command: ((O)PEN or (C)LOSE) C
Executing... Current system status is 10000 Today is 12-10-2005, 15:40:36
Executing... Current system status is 11000 Today is 12-10-2005, 15:40:37
Executing... Current system status is 11100 Today is 12-10-2005, 15:40:38
Executing... Current system status is 11110 Today is 12-10-2005, 15:40:39
Current system status is 11111 Today is 12-10-2005, 15:40:40

The System_Satus is CLOSED
Do you want to quit the program?(y or n) y
root@testlinuxbox:/home/yli/tmp/LPT_Control#
```

Figure 3.9 Screenshot of a prototype of the core control program

3) Remote monitoring part

The remote monitoring part for a PC has been decided to use ready made software designed for web camera broadcasting or peer-to-peer videoconferencing. The ready made software has sufficient functionalities which are good enough to be adopted into the application. To develop own software with more application specific features can be also considered as future development but not for the moment as this is beyond the scope of the thesis. For the web camera, it is connected with PC through USB port. The setup of web camera and video transmission either in broadcasting or peer-to-peer mode are completely controlled by related program. So there is no specific hardware implementation but purely software setups for this part.

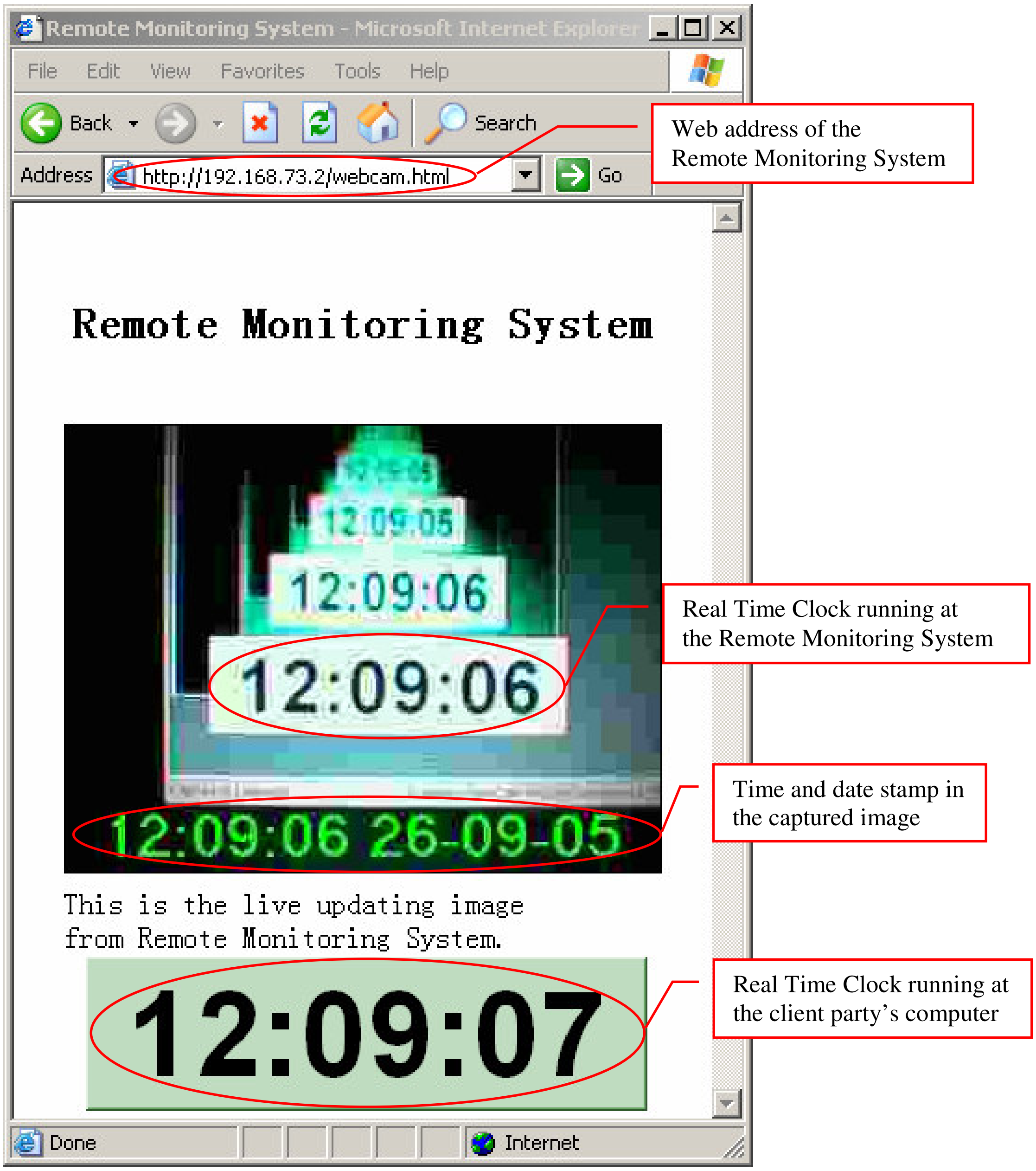
With the consideration of redundancy design, basically two different transmission means will both be employed, which are broadcasting mode and peer-to-peer mode to suit their respective circumstances. For the broadcasting mode, the advantage is that any authorised users are able to access the monitoring view simply with their web browsers, and it's web based application so that it's flexible to design with Java technology for instance to embed time stamp in the monitoring view which is very important functionality, etc, but the disadvantage is that its performance is poor with low bandwidth network which is unfortunately our case. For the peer-to-peer mode, the advantage is that the performance is good especially with low bandwidth network, but the disadvantage is that its lack of flexibility i.e. it requires own application to access the monitoring view, and user cannot add needed features for instance to embed time stamp in the monitoring view. They both have their own non-replaceable advantages. Therefore it's natural to utilize both of them simply to take their own advantages, e.g. flexibility of the broadcasting mode and the performance of the peer-to-peer mode.

In our application, normally, only one user is expected to access the monitoring view at one time. The key point of this remote monitoring application is the transmission of monitoring view through low bandwidth wireless communication network with an acceptable propagation delay. In other words the performance and reliability of transmission are weighted more than the video quality. To realise good performance of video transmission over low bandwidth wireless communication network has always been a challenge. The video hereby stated may refer to either streaming video or live updating pictures, since the Frame Per Second (FPS) can never achieve high value under such circumstance. With either one of the transmission modes stated above, broadcasting or peer-to-peer, normally the software support both streaming video and live updating pictures by auto-capturing at a predefined interval. The choice is made based on ensuring the best video performance while considering the video quality.

There are a number of existing software packages available for both broadcasting mode and peer-to-peer mode. Many of them are basically quite similar to each other. After some investigations, with broadcasting mode TinCam (Hiort-Lorenzen 2005) is selected for its consummate functionalities and with peer-to-peer mode Microsoft Portrait (Li 2005) is selected for its outstanding video performance under low bandwidth network. Performance testing has been done with various settings of TinCam and Microsoft Portrait to obtain the right settings.

With TinCam, to maximize the performance, the computer which runs TinCam has also been setup with Microsoft IIS server so that the captured images are saved directly to its local hard drive e.g. C:\Inetpub\wwwroot rather than uploaded to any third party servers, meanwhile the video device format has been set to use minimal colour bits (YUV9 9-bit) with 320×240 image size and JPEG quality has been set between 5~8%. With these settings the frame size can be reduced to 3~4 Kbytes which meets the minimal 1 FPS with the guaranteed minimal communication bit rate of 28.8 Kbit/s when there is only GPRS available. Applying these settings implies that the remote video transmission under majority of circumstances should be able to achieve 1 FPS as the bottom line. The testing results show that when using video streaming mode the video is smooth but the propagation delay is around 7~8 seconds which is not acceptable to fulfill the project requirements, while using auto-capture mode with its supported minimal capture interval of 1 second which generating video with 1 FPS the propagation delay is typically around 1~2 seconds which is able to fulfill the project requirements. Figure 3.10 shows a screenshot of the video display from the remote monitoring system in a client’s web browser, using TinCam auto-capture mode. The real time clock at the

Remote Monitoring System is captured as monitored activity to display on the screen in purpose to show the accordance of time stamp embedded in the image. In real usage the web camera is pointed directly to the monitored device, i.e. the disconnector. The large font clock at the bottom of the figure is the local real time clock running at the client party’s computer. From the time stamp the client can easily tell the propagation delay, in this case as shown in the figure, is only around 1 second.



Address: http://192.168.73.2/webcam.html

Remote Monitoring System

This is the live updating image from Remote Monitoring System.

Web address of the Remote Monitoring System

Real Time Clock running at the Remote Monitoring System

Time and date stamp in the captured image

Real Time Clock running at the client party’s computer

Figure 3.10 A screenshot from the remote monitoring system with TinCam

With Microsoft Portrait, to maximize the performance, the video bandwidth setting is set to 33.6 Kbps or less to meet the guaranteed minimal communication bandwidth when there is only GPRS available. Testing has been done with default capture settings using image size of 160×120 and frame rate of 10 FPS. The testing results show that the performance of video streaming with above settings is optimal. The video is clear, smooth and the propagation delay is typically under 1 second which is expected as an optimal solution to fulfill the project requirements. The major disadvantage for this solution as mentioned earlier is the lack of flexibility i.e. to embed time stamp in the video, however this can be solved with other alternatives e.g. to place a real time clock in the same monitored scene as shown in Figure 3.11. The figure shows a screenshot of the video display from the remote monitoring system at a client party's Portrait program. Similar to last test, the real time clock at the Remote Monitoring System is captured as monitored activity to display on the screen in purpose to let the client tell the propagation delay by comparing it to the large font clock at the bottom of the figure which is the local real time clock running at the client party's computer. In this case as shown in the figure the delay is even less than 1 second.

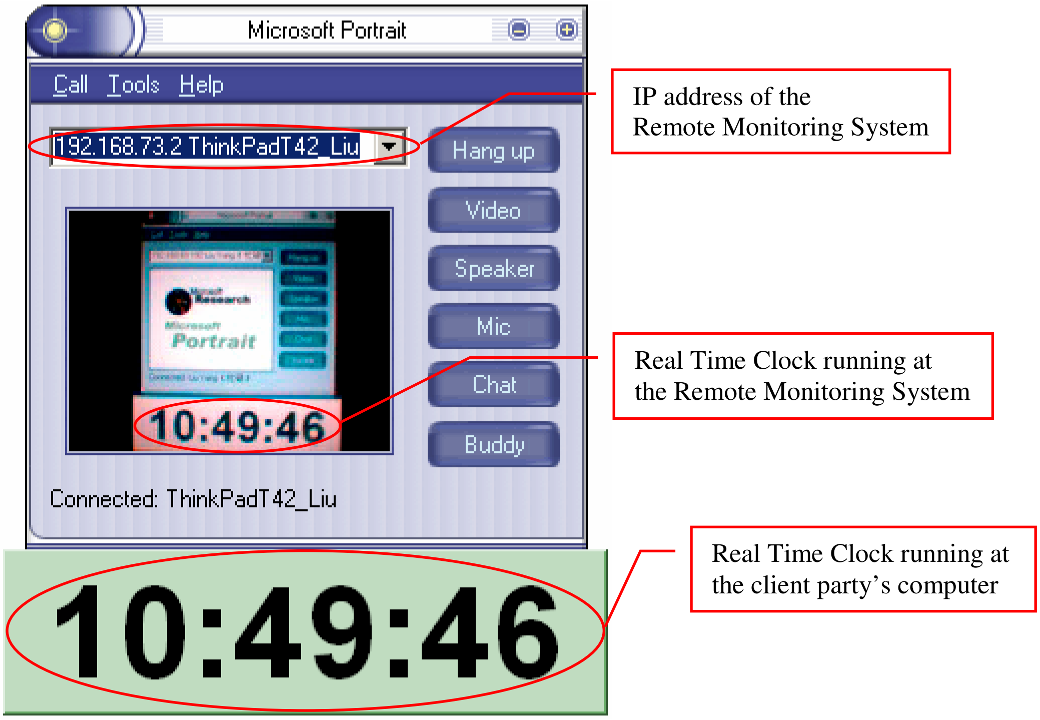

Microsoft Portrait
Call Tools Help
192.168.73.2 ThinkPadT42_Liu
Hang up
Video
Speaker
Mic
Chat
Buddy
10:49:46
Connected: ThinkPadT42_Liu
10:49:46
IP address of the Remote Monitoring System
Real Time Clock running at the Remote Monitoring System
Real Time Clock running at the client party's computer

Figure 3.11 A screenshot from the remote monitoring system with Microsoft Portrait

3.3.2. MCU based solution

This part at the moment takes care of only the remote control based on MCU solution, as a reliable backup to the PC part in case of failure. Due to technical limitations the remote monitoring based on MCU will be left as future development. The hardware and software implementation of MCU based solution is relatively much more complex than the PC based solution since it involves new hardware and software development e.g.: system architecture design and implementation of circuit including diagram and PCB, design and implementation of communication between MCU and GSM/GPRS data terminal and I/O interfacing for remote control, as well as future development proposals.

1) System architecture design

The overview design is illustrated by the block diagram in Figure 3.12. The Monitoring Module is planed for future development only and currently doesn't exist in the design and therefore is represented with dashed block. The LCD Displayer and Keypad are wrapped with dashed frame since they are for debug purpose only and detachable from the main PCB. They exist in prototyping, but in final design for security concerns they are attached only when necessary i.e. debugging. All the software functions in remote control part are kept exactly the same as PC based system. In fact the user cannot even notice the difference whether he is connected to a PC based or a MCU based remote control system.

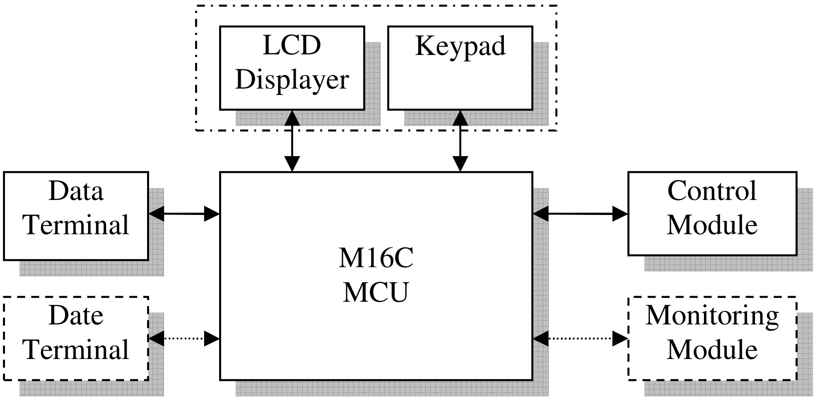


Figure 3.12 Block diagram of MCU based system overview design

The port connections between MCU and peripherals are described in details in Table 3.3.

Port 0	All 8 bits of Port 0 are used as data bus for the LCD displayer.
Port 3	Pin 3.1 is connected to the LCD Enable pin.
Port 5	Pins 5.0-4 are used as status feedback input bits which connected with sensors of Control Module. Pin 5.5 is used as output control bit which connected to Control Module to manipulate the disconnector. Pin 5.6 is connected to the LCD RS (Register Select) pin. Pin 5.7 is connected to the LCD R/W (Read/Write Select) pin.
Port 6	Pin 6.2 is connected to RxD of Data Terminal. Pin 6.3 is connected to TxD of Data Terminal.
Port 10	All 8 bits of Port 10 are used as data bus for communication with keypad. Pins 10.0-3 are used as inputs from the keypad to the MCU. Pins 10.4-7 are used as outputs from the MCU to the keypad.

Table 3.3 Port connections between MCU and peripherals

The circuit diagram and corresponding PCB layout are designed according to the above described structure and specifications. The design details are attached in Appendix 5 of this thesis.

2) Communication and I/O interfacing

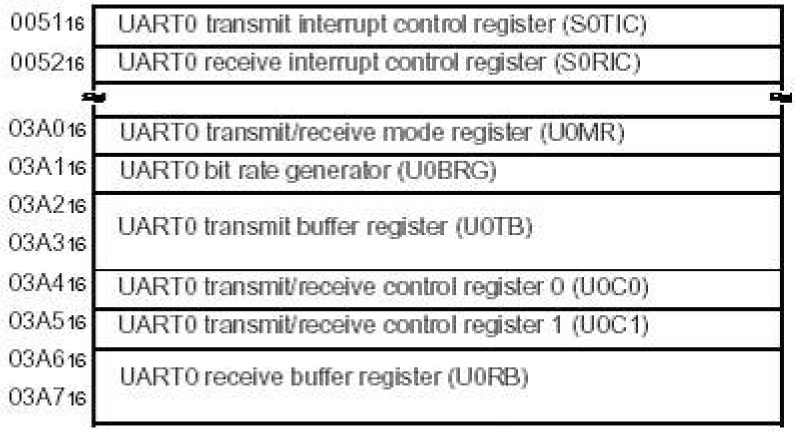
The implementation of serial communication between MCU (M16C) and GSM/GPRS data terminal (GM862) is relatively complex. Before connecting the GM862 module to the MCU, it’s necessary to study how the serial communicating is performed with the GM862 module through a PC terminal program, and then it’s much easier to program the M16C microcontroller to access the GM862 module according to related AT commands and retrieve corresponding responses.

The format of received signal has to be obtained by measuring with oscilloscope, because there are hidden characters in the responding message, e.g. carriage return and line feed at both ends (see Table 3.4), but can not be displayed in the terminal program. The format of responding message is very important to be studied before hand in order to program the UART communication of the MCU. Otherwise the MCU is not able to communicate with the GM862 module properly.

<CR><LF>	RING	<CR><LF>
<CR><LF>	+CLIP: "+358440244250",145,"",,"",0	<CR><LF>

Table 3.4 Layout of the incoming strings from the wireless data terminal

Then next step is the Special Functions Register (SFR) configurations for setup of the UART communication. The UART0 of M16C is selected to communicate with the GM862 module. There are 8 SFRs involved with UART0, 5 of them have to be set with precise values in order to have proper UART communication. Figure 3.13 shows the addresses and names of these 8 SFRs.



0051_{16}	UART0 transmit interrupt control register (S0TIC)
0052_{16}	UART0 receive interrupt control register (S0RIC)
$03A0_{16}$	UART0 transmit/receive mode register (U0MR)
$03A1_{16}$	UART0 bit rate generator (U0BRG)
$03A2_{16}$ $03A3_{16}$	UART0 transmit buffer register (U0TB)
$03A4_{16}$	UART0 transmit/receive control register 0 (U0C0)
$03A5_{16}$	UART0 transmit/receive control register 1 (U0C1)
$03A6_{16}$ $03A7_{16}$	UART0 receive buffer register (U0RB)

Figure 3.13 UART0 related SFRs (Renesas 2003)

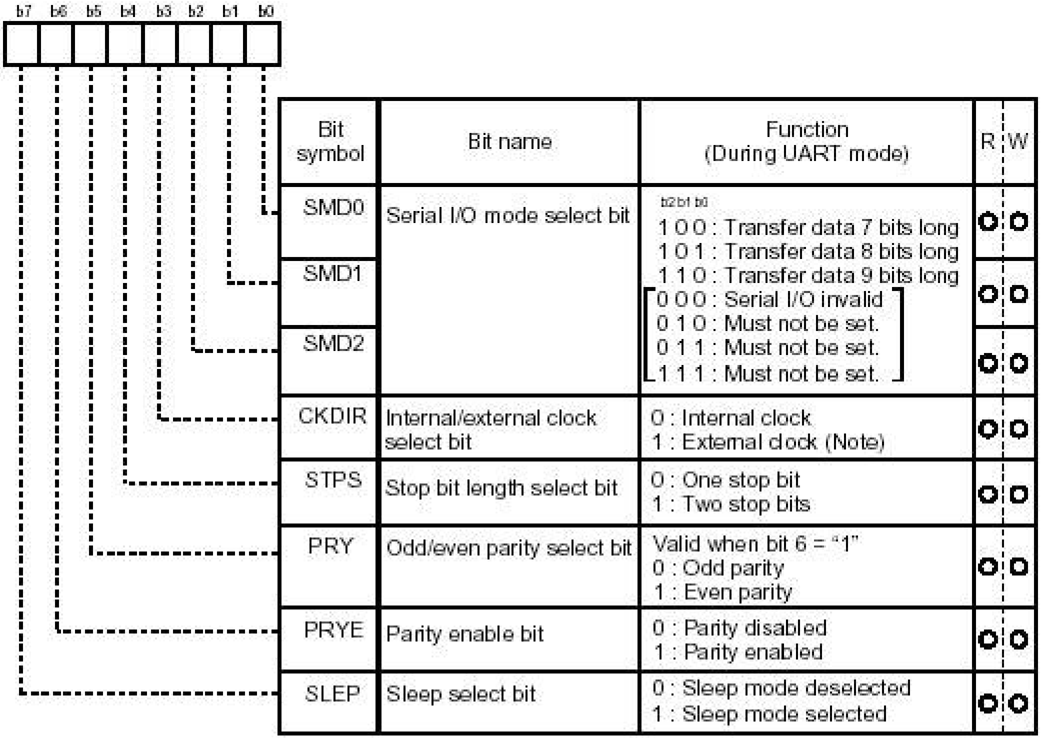
U0BRG – Bit Rate Generator Register

This 8-bit bit rate generator register configures the signal transmission rate. The value should be manually calculated from the following formula.

$$U0BRG = \frac{X_{in}}{16 \times Countsource \times Baudrate} - 1$$

The X_{in} denotes the crystal frequency. The parameter *Countsource* is used to dividing the main clock in order to alleviate the disparity and generate more exact baud rate as desired. In this program, the baud rate is 19200 bit per-second and the clock frequency is 24M, U0BRG = (24MHz/16/19200) - 1 = 77.125 (0x4D).

U0MR – Transmit and Receive Mode Register



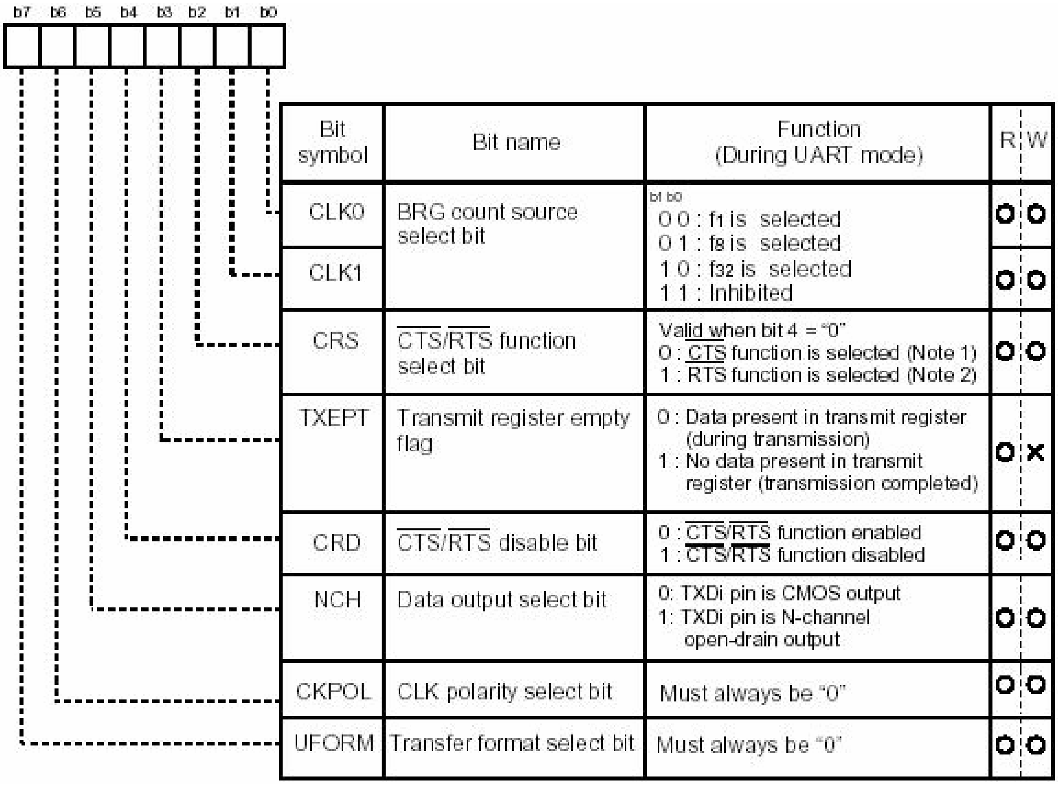
Bit symbol	Bit name	Function (During UART mode)	R	W
SMD0	Serial I/O mode select bit	b2 b1 b0 1 0 0 : Transfer data 7 bits long 1 0 1 : Transfer data 8 bits long 1 1 0 : Transfer data 9 bits long 0 0 0 : Serial I/O invalid 0 1 0 : Must not be set. 0 1 1 : Must not be set. 1 1 1 : Must not be set.	○	○
SMD1			○	○
SMD2			○	○
CKDIR	Internal/external clock select bit	0 : Internal clock 1 : External clock (Note)	○	○
STPS	Stop bit length select bit	0 : One stop bit 1 : Two stop bits	○	○
PRY	Odd/even parity select bit	Valid when bit 6 = "1" 0 : Odd parity 1 : Even parity	○	○
PRYE	Parity enable bit	0 : Parity disabled 1 : Parity enabled	○	○
SLEP	Sleep select bit	0 : Sleep mode deselected 1 : Sleep mode selected	○	○

Figure 3.14 U0MR configuration (Renesas 2003)

Figure 3.14 shows the configuration of U0MR. The settings of U0MR are 8-bit data, 1 stop bit, and no parity.

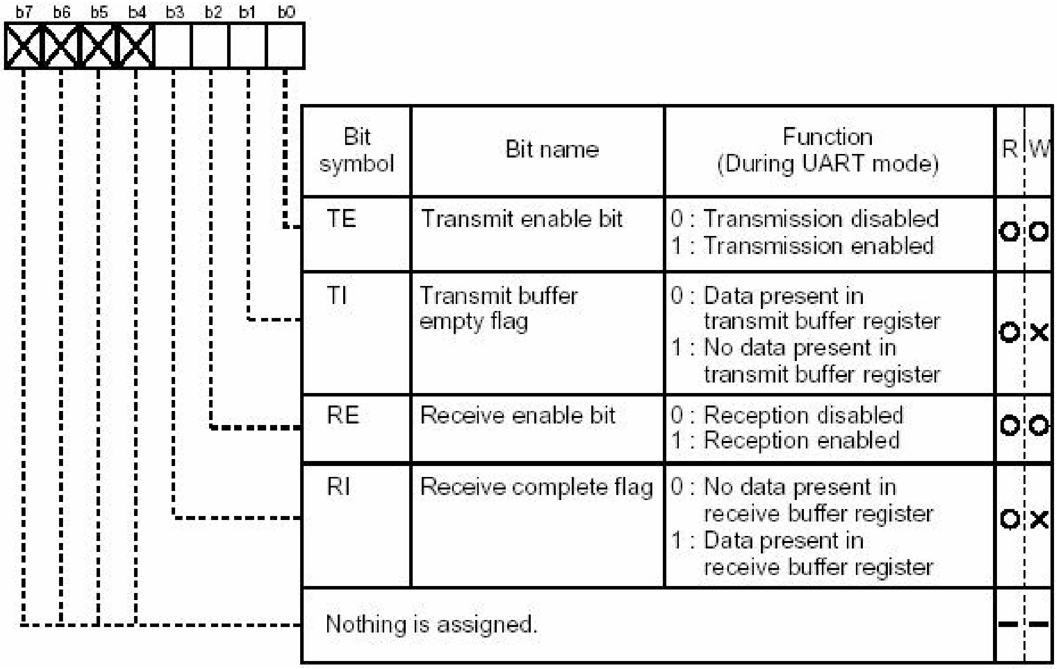
U0C0 & U0C1 – 2 Transmit and Receive Control Registers

The settings of U0C0 & U0C1 are based on count source selection and other functions, as shown in Figure 3.15 and Figure 3.16 respectively. The 3 different count sources, f1, f8 and f32, are compared to obtain best value for baud rate generation.



Bit symbol	Bit name	Function (During UART mode)	R	W
CLK0	BRG count source select bit	b1 b0 0 0 : f_1 is selected 0 1 : f_8 is selected 1 0 : f_{32} is selected 1 1 : Inhibited	○	○
CLK1			○	○
CRS	$\overline{\text{CTS}}$/$\overline{\text{RTS}}$ function select bit	Valid when bit 4 = "0" 0 : $\overline{\text{CTS}}$ function is selected (Note 1) 1 : RTS function is selected (Note 2)	○	○
TXEPT	Transmit register empty flag	0 : Data present in transmit register (during transmission) 1 : No data present in transmit register (transmission completed)	○	×
CRD	$\overline{\text{CTS}}$/$\overline{\text{RTS}}$ disable bit	0 : $\overline{\text{CTS}}$/$\overline{\text{RTS}}$ function enabled 1 : $\overline{\text{CTS}}$/$\overline{\text{RTS}}$ function disabled	○	○
NCH	Data output select bit	0: TXDi pin is CMOS output 1: TXDi pin is N-channel open-drain output	○	○
CKPOL	CLK polarity select bit	Must always be "0"	○	○
UFORM	Transfer format select bit	Must always be "0"	○	○

Figure 3.15 U0C0 configuration (Renesas 2003)



Bit symbol	Bit name	Function (During UART mode)	R	W
TE	Transmit enable bit	0 : Transmission disabled 1 : Transmission enabled	○	○
TI	Transmit buffer empty flag	0 : Data present in transmit buffer register 1 : No data present in transmit buffer register	○	×
RE	Receive enable bit	0 : Reception disabled 1 : Reception enabled	○	○
RI	Receive complete flag	0 : No data present in receive buffer register 1 : Data present in receive buffer register	○	×
Nothing is assigned.			—	—

Figure 3.16 U0C1 configuration (Renesas 2003)

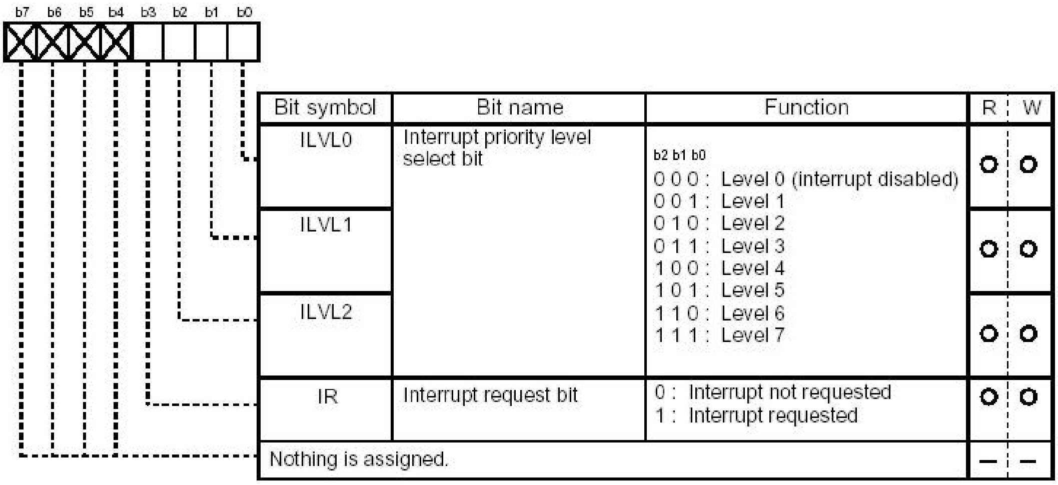
Table 3.5 compares the baud rates which are generated by different count sources f1, f8 and f32, and f1 generates the baud rate closest to 19200.

Count Source	U0BRG	Actual Baud Rate
f1	0x4D	19230.1
f8	0x26	19230.7
f32	0x12	19736.8

Table 3.5 Baud rates comparison

The CTS/RTS function is not necessary in this application, so it can be disabled. In M16C/62P, the transmission and reception are separately controlled by U0C1 register. They must be both enabled to have full duplex communication, and each of them has an individual serial interrupt register, namely S0TIC and S0RIC as shown in Figure 3.17.

S0TIC and S0RIC – Transmit and Receive Interrupt Control Register


b7 b6 b5 b4 b3 b2 b1 b0

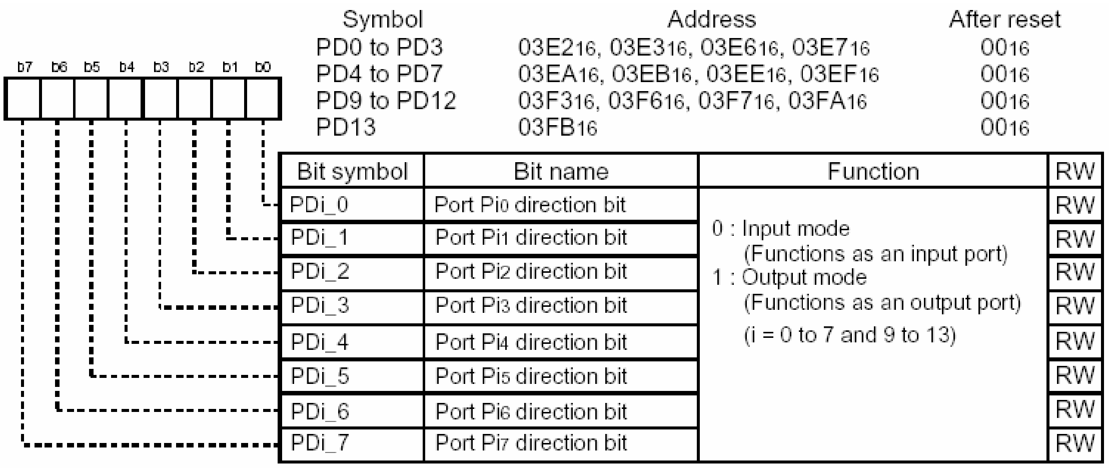
Bit symbol	Bit name	Function	R	W
ILVL0	Interrupt priority level select bit	b2 b1 b0 0 0 0 : Level 0 (interrupt disabled) 0 0 1 : Level 1 0 1 0 : Level 2 0 1 1 : Level 3 1 0 0 : Level 4 1 0 1 : Level 5 1 1 0 : Level 6 1 1 1 : Level 7	O	O
ILVL1			O	O
ILVL2			O	O
IR	Interrupt request bit	0 : Interrupt not requested 1 : Interrupt requested	O	O
Nothing is assigned.			–	–

Figure 3.17 S0TIC and S0RIC configurations (Renesas 2003)

When the serial communication part is properly programmed as above described, the microcontroller is able to receive strings from the data terminal, pick up the predefined commands to react to the I/O port and send feedback information to the data terminal.

The implementation of I/O interfacing for sending control bit and receiving feedback bits are relatively simple. The initialization of port is set by the port direction registers shown in Figure 3.18, to define the corresponding ports as input or output. After this is done, data can be directly read from and write to corresponding port registers shown in Figure 3.19.

PDi - Port Pi Direction Register

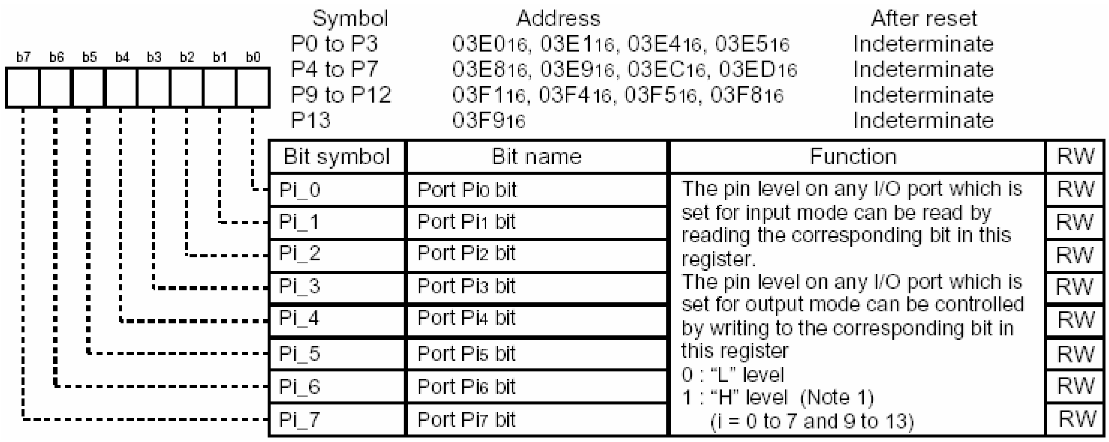

b7
b6
b5
b4
b3
b2
b1
b0

Symbol	Address	After reset
PD0 to PD3	$03E2_{16}$, $03E3_{16}$, $03E6_{16}$, $03E7_{16}$	00_{16}
PD4 to PD7	$03EA_{16}$, $03EB_{16}$, $03EE_{16}$, $03EF_{16}$	00_{16}
PD9 to PD12	$03F3_{16}$, $03F6_{16}$, $03F7_{16}$, $03FA_{16}$	00_{16}
PD13	$03FB_{16}$	00_{16}

Bit symbol	Bit name	Function	RW
PDi_0	Port Pi_0 direction bit	0 : Input mode (Functions as an input port) 1 : Output mode (Functions as an output port) (i = 0 to 7 and 9 to 13)	RW
PDi_1	Port Pi_1 direction bit		RW
PDi_2	Port Pi_2 direction bit		RW
PDi_3	Port Pi_3 direction bit		RW
PDi_4	Port Pi_4 direction bit		RW
PDi_5	Port Pi_5 direction bit		RW
PDi_6	Port Pi_6 direction bit		RW
PDi_7	Port Pi_7 direction bit		RW

Figure 3.18 PDi configuration (Renesas 2003)

Pi - Port Pi Register


b7
b6
b5
b4
b3
b2
b1
b0

Symbol	Address	After reset
P0 to P3	$03E0_{16}$, $03E1_{16}$, $03E4_{16}$, $03E5_{16}$	Indeterminate
P4 to P7	$03E8_{16}$, $03E9_{16}$, $03EC_{16}$, $03ED_{16}$	Indeterminate
P9 to P12	$03F1_{16}$, $03F4_{16}$, $03F5_{16}$, $03F8_{16}$	Indeterminate
P13	$03F9_{16}$	Indeterminate

Bit symbol	Bit name	Function	RW
Pi_0	Port Pi_0 bit	The pin level on any I/O port which is set for input mode can be read by reading the corresponding bit in this register. The pin level on any I/O port which is set for output mode can be controlled by writing to the corresponding bit in this register 0 : "L" level 1 : "H" level (Note 1) (i = 0 to 7 and 9 to 13)	RW
Pi_1	Port Pi_1 bit		RW
Pi_2	Port Pi_2 bit		RW
Pi_3	Port Pi_3 bit		RW
Pi_4	Port Pi_4 bit		RW
Pi_5	Port Pi_5 bit		RW
Pi_6	Port Pi_6 bit		RW
Pi_7	Port Pi_7 bit		RW

Figure 3.19 Pi configuration (Renesas 2003)

The above mentioned communication and I/O interfacing are the core routines of the coding for MCU based remote control.

3) Future development proposals

Due to the current technical limitations, the remote monitoring function based on MCU is proposed here and the real implementation will be left for future development. Basically the MCU based remote monitoring system will preferably employ some specialised embedded camera with built-in JPEG encoder than using normal USB web camera. This will eliminate the huge complexity of image processing tasks for the MCU and free it to focus on the broadcasting of images. The camera captures pictures at a predefined interval, encodes into JPEG format and transmits the image to the buffer of MCU. Then the MCU packs data and sends through IP packets. This proposal is based on the fundamentals from several proved projects such as wireless videoconferencing for mobile devices (Liu & Chen 2003) and wireless remote control and image capture (Telit 2005) etc. Therefore such proposal should be completely realisable.

The future development aims at a fully functional remote control and monitoring system which is entirely based on MCU or embedded PC. The motivation for providing such solution is that MCU based system is cheap and more reliable than PC based system.

3.3.3. Secured remote access

This part solves how to establish communication between client and server under different situations for remote access.

1) Remote control part

For the remote control program, the system no matter based on PC or MCU will use communication of either packet switched solution or circuit switched solution. A testing core program has been made to validate the feasibility of remote control through SSH secure shell. The idea is simple: the remote host is running Linux based operating system, in our case is Knoppix, and a program which designed to be able to read from and write to LPT port of the computer is residing on the host, and user can execute this program either from the host itself or remotely through SSH Secure Shell Client. This core program is able to evaluate both packet switched solution and circuit switched solution. Although from previous augmentation that the shell based remote control program for SSH implementation should be avoid to be used with circuit switched solution due to security considerations, however during the validation phase it's still viable to evaluate the communication performance between client and server.

As stated there are two different communication means, packet switched solution and circuit switched solution, are used in this application. Whether the proposed solution is eligible to work in reality as expected should be validated. Now let's analyse case by case. With circuit switched solution there won't be any access problem because it creates direct Point-to-Point Protocol (PPP) connection between the server and the client. While with packet switched solution, the server is constantly attached to its service provider via packet switched access. Normally the service providers use Dynamic Host Configuration Protocol (DHCP) server to assign dynamic IP address for every client as it connects. This implies at least two potential problems for the desired application. First, the assigned IP address is dynamic, which means that the server does not have a constant IP address. Although the server is supposed to be connected all the time, however once for some reason its connection drops and needs to reconnect, then its IP address will be changed and thus it will create unnecessary trouble for the client without being informed of changing IP address. Second, even worse problem, the assigned IP address is normally private address which can not be accessed from public internet. According to test, even clients which are connected to the same service provider cannot access the server either. Such situation happens only to the GPRS/EDGE service providers, which is believed to be caused by the wireless network infrastructure. Without solving these described problems, the packet switched solution will never work.

The solution is to use VPN to create tunnelling between the server and the client, and meanwhile setup of VPN gateway to fix the assigned IP address so that such barriers can be overcome. Figure 3.20 shows an example of VPN. In the example, the VPN connection first makes a call to an ISP. After the connection is established, the connection then makes another call to the remote access server that establishes the Point-to-Point Tunnelling Protocol (PPTP) or Layer Two Tunnelling Protocol (L2TP) tunnel. After authentication, the remote computer can access the corporate network, as shown in the following illustration.

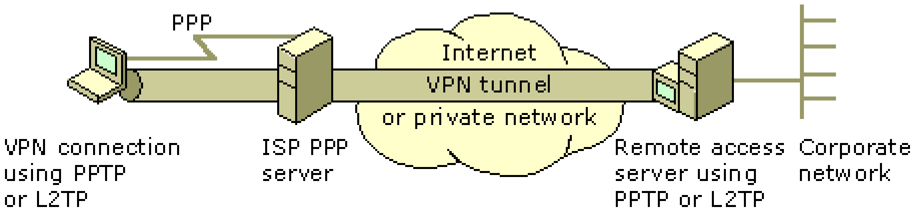
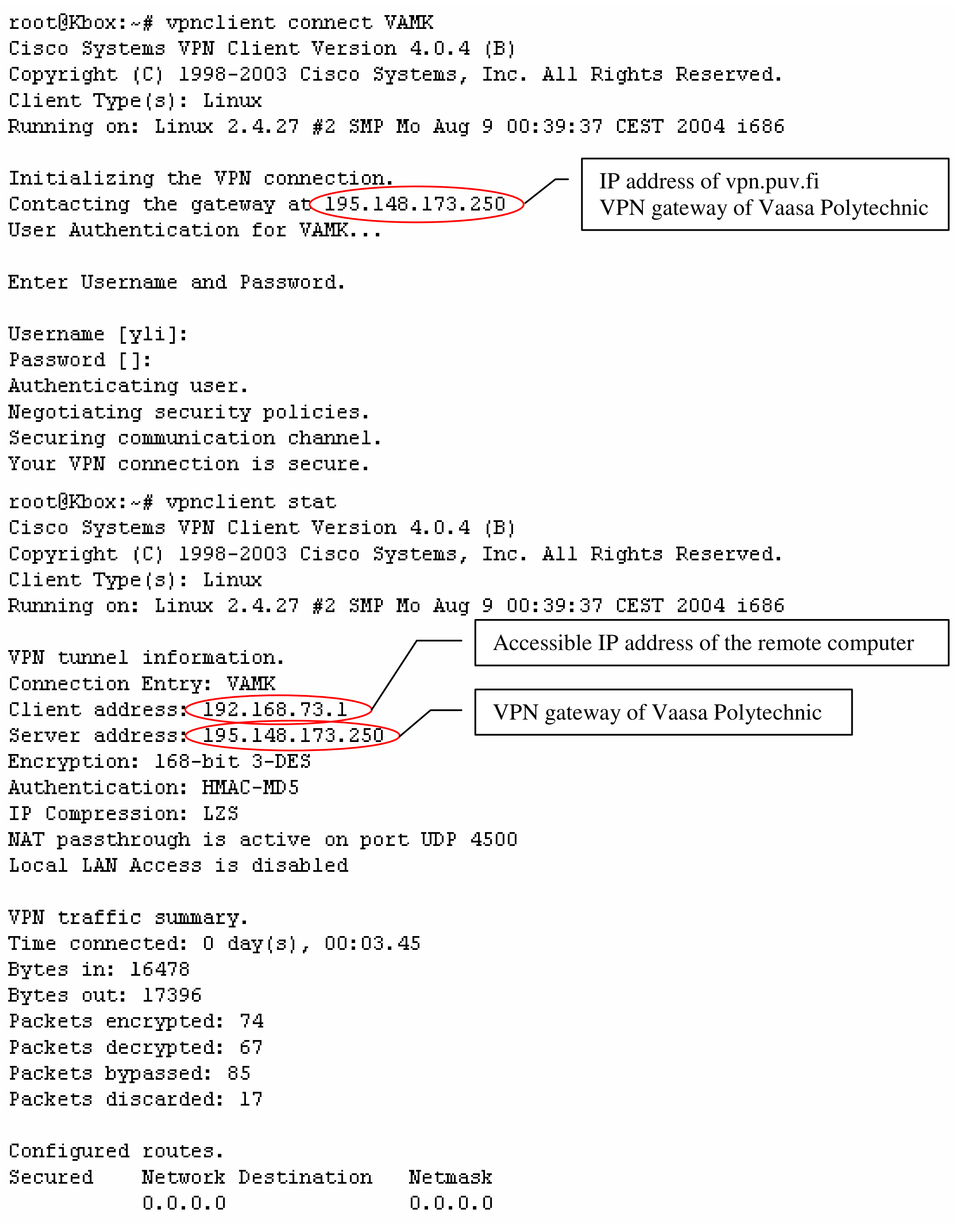

PPP
Internet
VPN tunnel
or private network
VPN connection using PPTP or L2TP
ISP PPP server
Remote access server using PPTP or L2TP
Corporate network

Figure 3.20 An example of VPN (Microsoft 2005)

A case study particularly for our application has been made. Since the test case has been done within the internal network of Vaasa Polytechnic, the illustration hereby uses this test case and its working environment as an example. Vaasa Polytechnic uses IPSec for its VPN connectivity, and Cisco Systems VPN Client is the client software that it uses. The secure remote communication is achieved by using the combination of L2TP and IPSec (L2TP/IPSec). L2TP is used to tunnel the data across a shared or public network such as the Internet and IPSec Encapsulating Security Payload (ESP) is used to encrypt data. The following explains in details about how VPN can solve the stated problems.

The screenshot in Figure 3.21 shows the how the Cisco Systems VPN Client creates an active VPN connection to Vaasa Polytechnic internal network through its VPN gateway vpn.puv.fi (195.148.173.250). After user authentication, the remote control system is assigned an IP address of 192.168.73.1, which can be fixed by binding its MAC address to the VPN gateway.

Figure 3.22 shows the IPconfig details of the remote control system and Figure 3.23 illustrates how the VPN makes the remote computer accessible with an inaccessible IP address by creating IPSec tunnelling. The remote computer first connects to its ISP, Sonera, with GPRS/EDGE connectivity and from the DHCP server gets a dynamically assigned IP address 10.101.X.X which is in reserved IP range and therefore inaccessible directly, then it makes a VPN connection to the VPN gateway of Vaasa Polytechnic and gets an fixed and accessible IP address 192.168.73.1 from Vaasa Polytechnic internal network so that it can be directly accessed from any client with IP address 192.168.69.X in the Vaasa Polytechnic internal network.



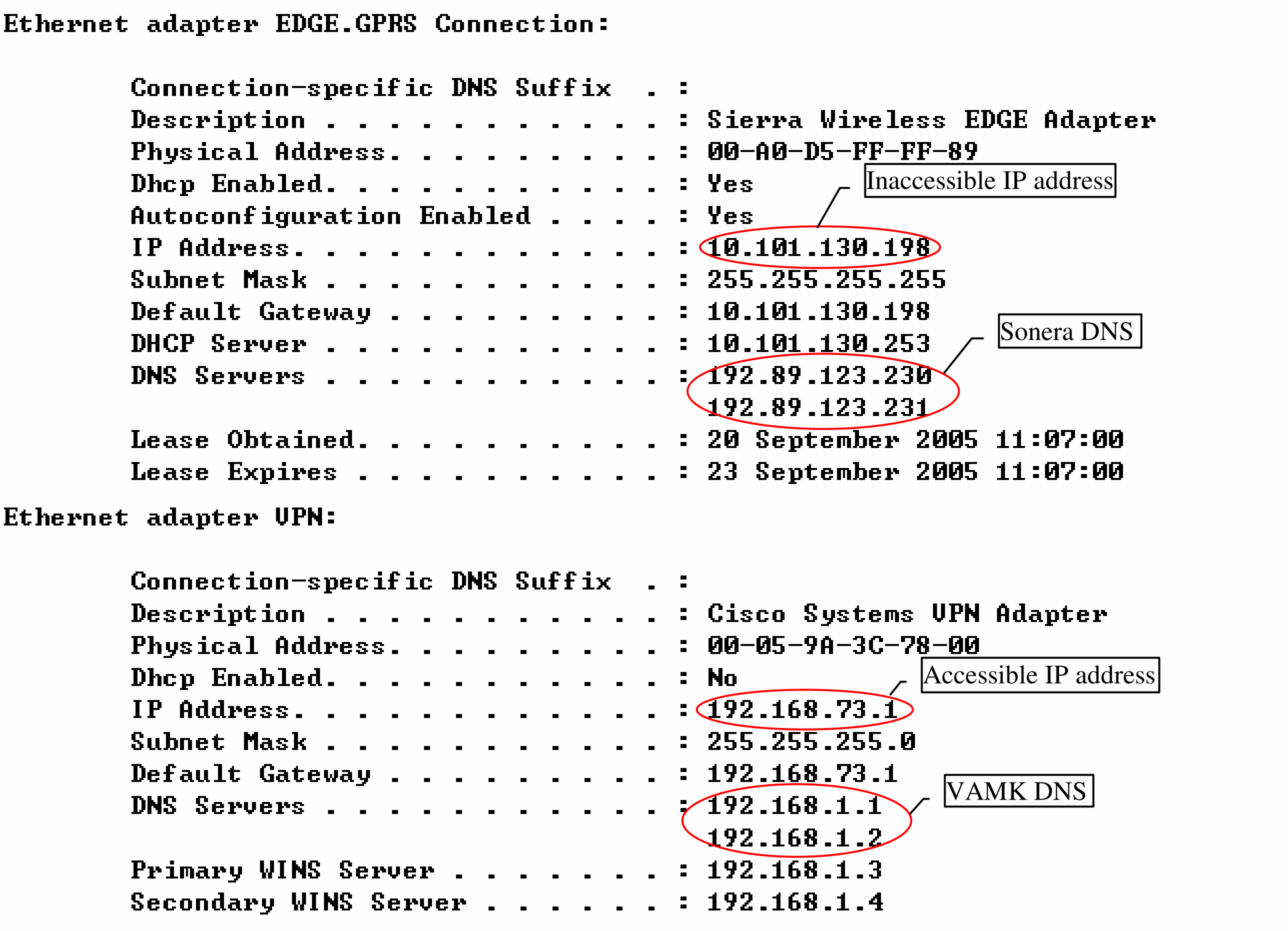
```
root@Kbox:~# vpnclient connect VAMK
Cisco Systems VPN Client Version 4.0.4 (B)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.27 #2 SMP Mo Aug 9 00:39:37 CEST 2004 i686

Initializing the VPN connection.
Contacting the gateway at 195.148.173.250
User Authentication for VAMK...

Enter Username and Password.

Username [yli]:
Password []:
Authenticating user.
Negotiating security policies.
Securing communication channel.
Your VPN connection is secure.
root@Kbox:~# vpnclient stat
Cisco Systems VPN Client Version 4.0.4 (B)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.27 #2 SMP Mo Aug 9 00:39:37 CEST 2004 i686

VPN tunnel information.
Connection Entry: VAMK
Client address: 192.168.73.1
Server address: 195.148.173.250
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: LZS
NAT passthrough is active on port UDP 4500
Local LAN Access is disabled

VPN traffic summary.
Time connected: 0 day(s), 00:03.45
Bytes in: 16478
Bytes out: 17396
Packets encrypted: 74
Packets decrypted: 67
Packets bypassed: 85
Packets discarded: 17

Configured routes.
Secured     Network Destination    Netmask
            0.0.0.0                0.0.0.0
```

IP address of vpn.puv.fi
VPN gateway of Vaasa Polytechnic

Accessible IP address of the remote computer

VPN gateway of Vaasa Polytechnic

Figure 3.21 An active VPN connection to VAMK with Cisco Systems VPN Client



```
Ethernet adapter EDGE.GPRS Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Sierra Wireless EDGE Adapter
        Physical Address. . . . . . . . . : 00-A0-D5-FF-FF-89
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.101.130.198
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 10.101.130.198
        DHCP Server . . . . . . . . . . . : 10.101.130.253
        DNS Servers . . . . . . . . . . . : 192.89.123.230
                                            192.89.123.231
        Lease Obtained. . . . . . . . . . : 20 September 2005 11:07:00
        Lease Expires . . . . . . . . . . : 23 September 2005 11:07:00
Ethernet adapter VPN:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Cisco Systems VPN Adapter
        Physical Address. . . . . . . . . : 00-05-9A-3C-78-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.73.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.73.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
                                            192.168.1.2
        Primary WINS Server . . . . . . . : 192.168.1.3
        Secondary WINS Server . . . . . . : 192.168.1.4
```

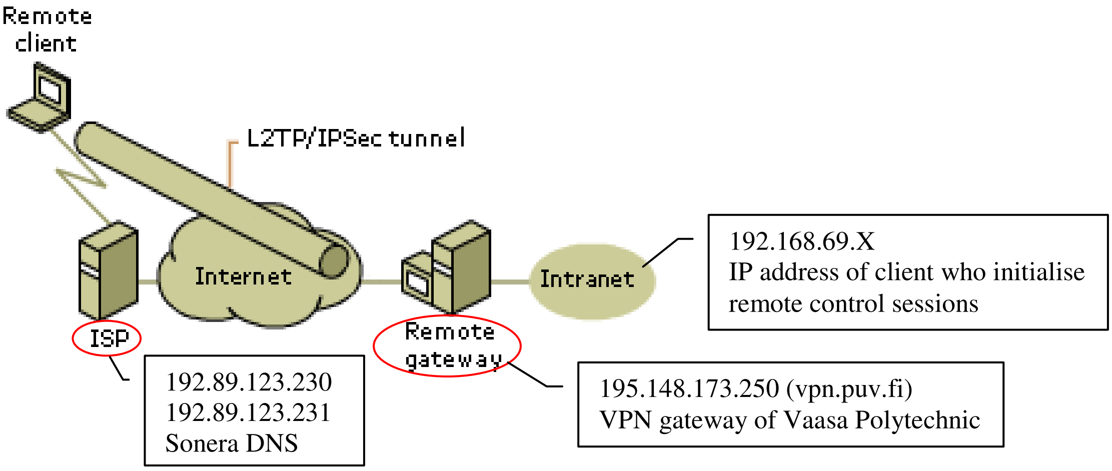
Inaccessible IP address

Sonera DNS

Accessible IP address

VAMK DNS

Figure 3.22 IPconfig details of the remote control system



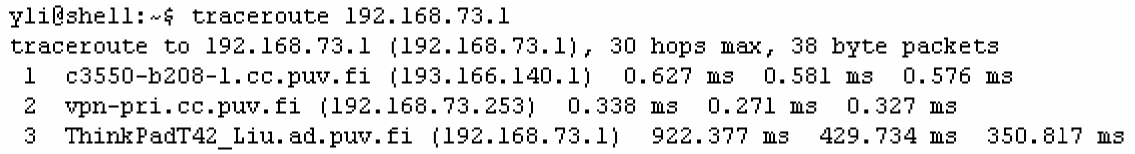
192.168.69.X
IP address of client who initialise remote control sessions

192.89.123.230
192.89.123.231
Sonera DNS

195.148.173.250 (vpn.puv.fi)
VPN gateway of Vaasa Polytechnic

Figure 3.23 Illustration of the VPN connection in the case study (Microsoft 2005)

Figure 3.24 shows the result of running “traceroute” from a client computer which is accessing the remote control system. By using VPN solution, the remote computer is now accessible, and meanwhile it can have a fixed IP address. It can be seen that the above mentioned two potential problems have been successfully solved.



```
yli@shell:~$ traceroute 192.168.73.1
traceroute to 192.168.73.1 (192.168.73.1), 30 hops max, 38 byte packets
 1  c3550-b208-1.cc.puv.fi (193.166.140.1)  0.627 ms  0.581 ms  0.576 ms
 2  vpn-pri.cc.puv.fi (192.168.73.253)  0.338 ms  0.271 ms  0.327 ms
 3  ThinkPadT42_Liu.ad.puv.fi (192.168.73.1)  922.377 ms  429.734 ms  350.817 ms
```

Figure 3.24 Traceroute result to access the remote control system

Since the testing case has been proved to be working very well, the ideas of executing remote shell program through SSH secure shell and using VPN to access the remote computer are accepted and kept for further development of the entire project. From the test case, the use of SSH to execute remote shell program as well as VPN tunnelling for IP access have been proved to be easy and effective, and also it is supposed to be very secure according to the design of SSH/VPN protocol. As conclusion SSH will be primary used for data security and VPN will be used only for IP access tunnelling when using with packet switched solution. In fact SSH has already covered end to end data security, therefore even no additional encryption is necessary to be setup in VPN client, although as extra IPSec has also provided strong cryptography (168-bit 3-DES) for the communication.

2) Remote Monitoring Part

For the remote monitoring program it has fewer options since only the packet switched solution is eligible. The communication for remote monitoring through packet switched solution is quite the same as used for remote control. Based on GPRS/EDGE connection the server creates VPN tunnelling to the same internal LAN as the client connects to, so that the client can directly access the server by addressing its IP address obtained from VPN gateway.

4. ANALYSIS AND IMPLEMENTATION FOR ENHANCED SECURITY

This chapter deals with the security issues of the remote control and monitoring system. The purpose is to implement enhanced security at all levels to prevent or resist possible known security attacks.

4.1. Security analysis

4.1.1. System security and data security

The remote control and monitoring system may face a lot of security threats during its operation. The main considerations are system security and data security.

System level security issues include the threat of intruders, network blocking, communication jamming, etc, and countermeasures for using various access control means, specific communication terminal design, etc. System security are implemented in both hardware and software level.

Data security includes e.g. the following topics: (Penttonen 2003)
- Confidentiality: Only those can read the data who are supposed to read it. Eavesdropping is as difficult as possible.
- Authentication: The sender of a message is who he claims to be.
- Integrity: Data remains unchanged, i.e. nobody can change it when it is moved across the network.
- Nonrepudiation: The receiver gets a certificate that the sender has done something, what he might want to deny later.
- Access: The access to a resource is controlled.
- Availability: The availability of service is guaranteed against attacks such as viruses.

The attacker has some methods against security:
- Interruption of service by destroying hardware, e.g., breaks against availability.
- Interception by some kind of eavesdropping breaks against confidentiality.
- Modification of message breaks against integrity of data.
- Fabrication of messages can be used to attack authenticity.

Data security will be implemented with various cryptographies. In our application there are different considerations for circuit switched access and packet switched access. For circuit switched access, the connection is established using CSD/HSCSD over wireless communication network and PPP available in most terminal software. Under normal circumstance the remote access server authenticates user with a password and typically no other special security mechanisms are deployed. The GSM network protects the user data over the air interface. Thus normally the wireless access will not require any extra security extensions and can be used just like a fixed dial-up modem. Data security of PPP connection is generally considered to be safe, but in application specific case data encryption is still necessary to be implemented, and the reasons will be discussed in subsequent section. For packet switched access using GPRS/EDGE instead of a telephony network it deploys the internet backbone as a gateway to the remote access server. The user data is transmitted from the cellular network via the insecure internet using IP, and the public internet is exposed to numerous security risks. One major security weakness is that, unlike in a point-to-point dial-up connection, internet packets are readable to anyone having access to the network. IP packets also tend to follow the same route, so the potential intruder most likely has an access to all IP packets. The wireless networks security functions for GPRS/EDGE alone is not enough to guarantee confidentiality. A highly reliable remote access system has to be created by combining wireless access with an end-to-end IP security solution. (Nokia 2002)

4.1.2. Security modelling and targeting

As overview the security problem can be described as following. A model for network security is captured in very general terms in Figure 4.1. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principles in this transaction, must cooperate for the exchange to take place. A logical information channels is established be defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, etc.

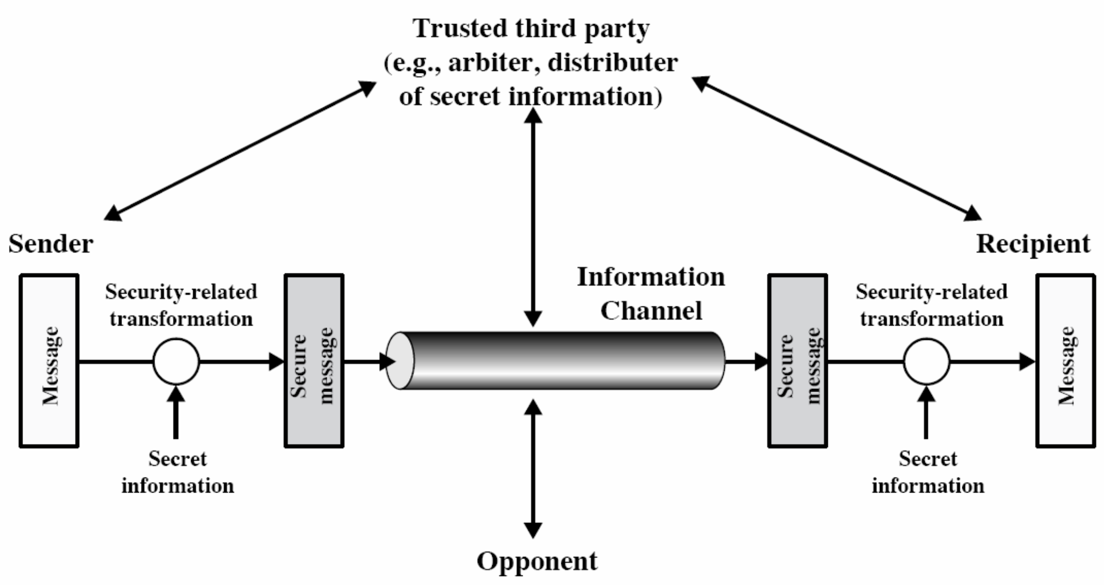


Figure 4.1 A model for network security (Stallings 2003)

This general model shows that there are four basic tasks in designing a particular security service (Stallings 2003):

- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- Specify a protocol to be used by the two principles that makes use of the security algorithm and the secret information to achieve a particular security service.

A complete security solution should offer the following critical functions to ensure the security of data and the system:

- Access control restricting unauthorised users from accessing the system
- Encryption preventing anyone from reading or copying data as it travels across the insecure internet
- Authentication ensuring that the data originates from the source that it claims

4.2. Implementation of system security measures

4.2.1. Hardware based security measures

The use of integrated Jam Detection and Easy Scan features of the Telit GM862 wireless GSM/GPRS terminal module provides hardware based security measures. (Telit 2005)

The Jam Detection feature allows the data terminal module to detect the presence of a disturbing device such as a communication jammer and give indication to the user and/or send a report of that to the network. This feature can be very important in our application which relies on the module for highly reliable and secured remote access via wireless communication network. In such application, the presence of a jammer device can compromise or even defeat the whole system reliability and functionality and therefore shall be recognised and reported either to the local system for countermeasure actions or to the network providing remote actions.

Easy Scan feature allows performing a quick survey through full band network. After scan is done the network information for every received Broadcasting Control Channel (BCCH) is available, i.e. C0 carrier assigned radio channel (BCCH), received level, bit error rate, number of valid channels, etc. which is very important information for future QoS analysis. It’s also useful for securing the application itself by constantly monitoring the network status, for example it will always know whether the received level is too low, whether the bit error rate is to high, how many base stations the operators have in the area where the application is located, etc.

4.2.2. Software based security measures

Software based security measures are mostly considered from access control and data encryption point of view. There are different security measures based on the communication mode of the remote control and monitoring system.

For the remote control system, it works in either packet switched mode or circuit switched mode. While working in packet switched mode, the data security relies on

SSH/VPN and system security relies on the executable rights of access control, since only users who have administrator privilege are able to run the control program which implies that attackers have even no chance to access the remote control program before they crack the Linux server. While working in circuit switched mode, the data security relies on built-in cryptography and system security relies on the verification of SIM and IMEI of two parties which is extreme unlikely to be achieved by attackers.

For the remote monitoring system, it works in either broadcasting mode or peer-to-peer mode. While working in broadcasting mode, the security relies on the web page access rights of the Microsoft IIS server defined by the server operating system, which implies that attackers have to crack the server in order to crack the system. While working in peer-to-peer mode, the security relies on Microsoft passport, which means that attackers have to crack Microsoft passport in order to crack the system. Either case is extreme unlikely to be achieved by attackers.

From above discussions it can be seen that the implemented security measures are able to provide powerful protections for the system from many aspects.

4.3. Implementation of data security measures

4.3.1. The need of data encryption

As discussed earlier, for packet switched access the user data is transmitted via the insecure internet using IP, obviously encryption is needed to ensure data security, and this is implemented directly with SSH/VPN solution, both of which use multiple strong cryptography algorithms to secure data.

But for circuit switched access the user data is transmitted from point to point which is normally considered to be secure, why there is still need for implementing encryption? The reason is that in our case the remote server is completely automated without any human operation, and therefore the security measures should be tighter for an unmanned server. As an assumption, consider a case of security attack on the server side. Since the remote server is unmanned, attackers can physically visit the site where the server is located. Then it's possible to replace the genuine server with a fake one by switching the serial cable from the terminal and therefore to eavesdrop data or fabricate fake response. Such attack is totally realisable due to the lack of server authentication and data encryption in circuit switched access mode, while in packet switched access mode such attack is not realisable thanks to SSH. Therefore in this application it's extremely necessary to implement data security measures similar as SSH when working in circuit switched access mode.

However, built-in data security implementation is only meant for the remote control application using PPP but not for other remote control or monitoring application. This is due to the nature that the remote control application is not designed for multi-user, but only one user can control while other users can just monitor.

4.3.2. Selection and implementation of encryption algorithms

The general ideas of symmetric encryption and asymmetric (public-key) encryption are illustrated in Figure 4.2 (Stallings 2003).

Consider the straightforward use of symmetric encryption (Figure 4.2a). A message *M* transmitted from source A to destination B is encrypted using a secret key *K* shared by A and B. If no other party knows the key, then confidentiality is provided: No other party can recover the plaintext of the message. In addition, B is assured that the message came was generated by A, and the message must have come from A because A is the only other party that possesses *K* and therefore the only other party with the information necessary to construct ciphertext that can be decrypted with *K*. Furthermore, if *M* is recovered, B knows that none of the bits of *M* have been altered, because an opponent that does not know *K* would not know how to alter bits in the ciphertext to produce desired changes in the plaintext. So the symmetric encryption provides authentication as well as confidentiality.

The straightforward use of public-key encryption (Figure 4.2b) provides confidentiality but not authentication. The source A uses the public key KU_b of the destination B to encrypt *M*. Because only B has the corresponding private key KR_b, only B can decrypt the message. This scheme provides no authentication because any opponent could also use B's public key to encrypt a message, claiming to be A.

To provide authentication, A uses its private key to encrypt the message, and B use A's public key to decrypt (Figure 4.2c). This provides authentication using the same type of reasoning as in the symmetric encryption case: The message must have come from A because A is the only party that possesses KR_a and therefore the only party with the information necessary to construct ciphertext that can be decrypted with KU_a. Assuming there is such structure, then this scheme does provide authentication. It also provides what is known as digital signature. Only A could have constructed the ciphertext because only A possesses KR_a. Not even B, the recipient, could have constructed the ciphertext. Therefore, if B is in possession of the ciphertext, B has the means to prove that the message must have come from A. In effect, A has "signed" the message by using its private key to encrypt. This scheme does not provide confidentiality. Anyone in possession of A's public key can decrypt the ciphertext.

To provide both confidentiality and authentication, A can encrypt M first using its private key, which provides the digital signature, and then using B's public key, which provides confidentiality (Figure 4.2d). The disadvantage of this approach is that the public-key algorithm, which is complex, must be exercised four times rather than two in each communication.

The encryption algorithm to be used in our application will follow the most popular form of classical communication security solutions, using public key cryptography for secure exchange of the secret key and then secret key cryptography for ciphering of data. Diffie-Hellman and Advanced Encryption Standard (AES) have been selected as encryption algorithms to be used in the data security solution of our application. Diffie-Hellman is one of the most widely used public key cryptography algorithms for secret key exchange, and AES is one of the well-know secret key cryptography algorithms as successor of Data Encryption Standard (DES). The following explains briefly about Diffie-Hellman and AES algorithms.

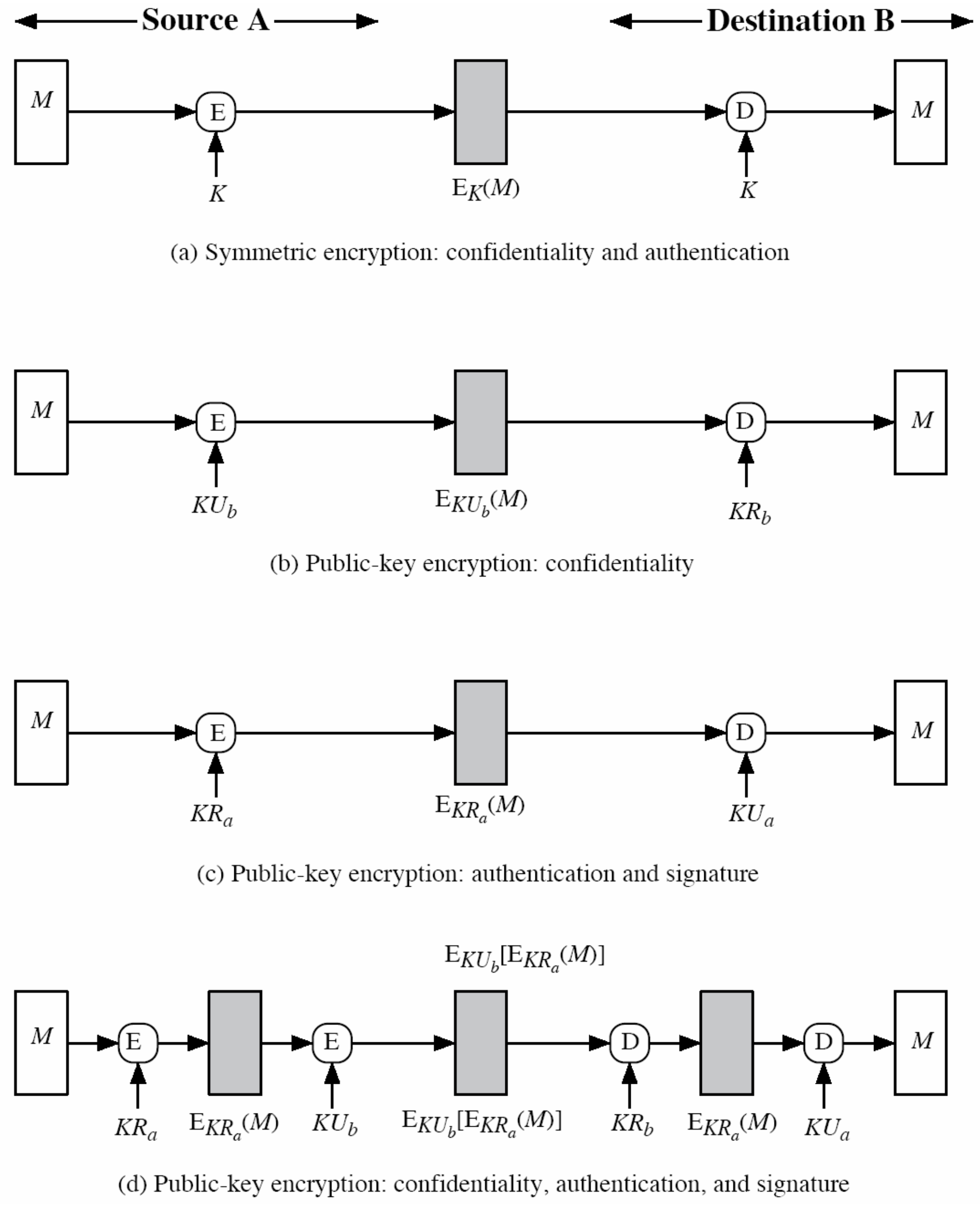

Source A
Destination B
M
E
K
$E_K(M)$
D
K
M
(a) Symmetric encryption: confidentiality and authentication
M
E
KU_b
$E_{KU_b}(M)$
D
KR_b
M
(b) Public-key encryption: confidentiality
M
E
KR_a
$E_{KR_a}(M)$
D
KU_a
M
(c) Public-key encryption: authentication and signature
$E_{KU_b}[E_{KR_a}(M)]$
M
E
KR_a
$E_{KR_a}(M)$
E
KU_b
$E_{KU_b}[E_{KR_a}(M)]$
D
KR_b
$E_{KR_a}(M)$
D
KU_a
M
(d) Public-key encryption: confidentiality, authentication, and signature

Figure 4.2 Message encryption (Stallings 2003)

Diffie-Hellman key exchange algorithm is to enable two users to exchange a key securely that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of the keys. Figure 4.3 shows a simple protocol that makes use of the Diffie-Hellman calculation. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt message on that connection. User A can generate a one-time private key X_A, calculate Y_A, and sent that to user B. User B responds by generating a private value X_B, calculating Y_B, and sending Y_B to user A. Both users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α and include those in the first message. (Stallings 2003)

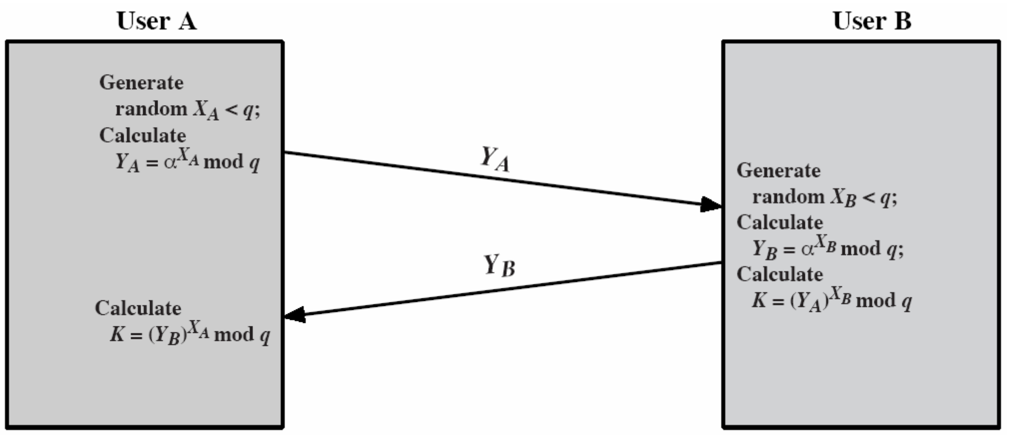

User A
Generate random $X_A < q$;
Calculate $Y_A = \alpha^{X_A} \bmod q$
Calculate $K = (Y_B)^{X_A} \bmod q$
Y_A
Y_B
User B
Generate random $X_B < q$;
Calculate $Y_B = \alpha^{X_B} \bmod q$;
Calculate $K = (Y_A)^{X_B} \bmod q$

Figure 4.3 Diffie-Hellman key exchange (Stallings 2003)

AES alias Rijndael is designed to have the following characteristics: resistance against all known attacks; speed and code compactness on a wide range of platforms; design simplicity. Figure 4.4 shows the overall structure of AES. The input to the encryption and decryption algorithms is a single 128-bit block. In published final standard, this block is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix. Similarly, the 128-bit key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words; each word is four bytes and the total key schedule is 44 words for the 128-bit key. Stallings (2003) has shown that AES does not use a Feistel structure but process the entire data block in parallel during each round using substitutions and permutation. The key that is provided as input is expanded into an array of forty-four 32bit words, w[*i*]. Four distinct words (128 bits) serve as a round key for each round as indicated in Figure 4.4. Four different stages are used, one of permutation and three of substitution:

- Substitute bytes: Uses an S-box, which defines a general reversible substitution, to perform a byte-by-byte substitution of the block;
- Shift rows: A simple permutation;
- Mix columns: A substitution that makes use of arithmetic over Galois field (2^8);
- Add round key: A simple bitwise XOR of the current block with a portion of the expanded key.

For both encryption and decryption, the cipher begins with an Add Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages. Only the Add Round Key stage makes use of the key. For this reason the cipher begins and ends with an Add Round Key stage. Any other stage, applied at the beginning or end, is reversible without knowledge of the key so would add no security. The Add Round Key stage is, in effect, a form of Vernam cipher (Stallings 2003) and by itself would not be formidable. The other three stages together provide confusion, diffusion, and nonlinearity, but by themselves would provide no security because they do not use the key. We can view the cipher as alternating operations of XOR encryption (Add Round Key) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on. This scheme is both efficient and highly secure. Each stage is easily reversible. For the Substitute Bytes, Shift Rows, and Mix Columns stage, an inverse function is used in the decryption algorithm. For the Add Round Key stage, the inverse is achieved by XORing the same round key to the block, using the result that $A \oplus A \oplus B = B$. As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm. This is a consequence of the particular structure of AES. Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext. Figure 4.4 lays out encryption and decryption going in opposite vertical directions. At each horizontal point (e.g., the dashed line in the figure), State is the same for both encryption and decryption. The final round of both encryption and decryption consist of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible. (Stallings 2003)

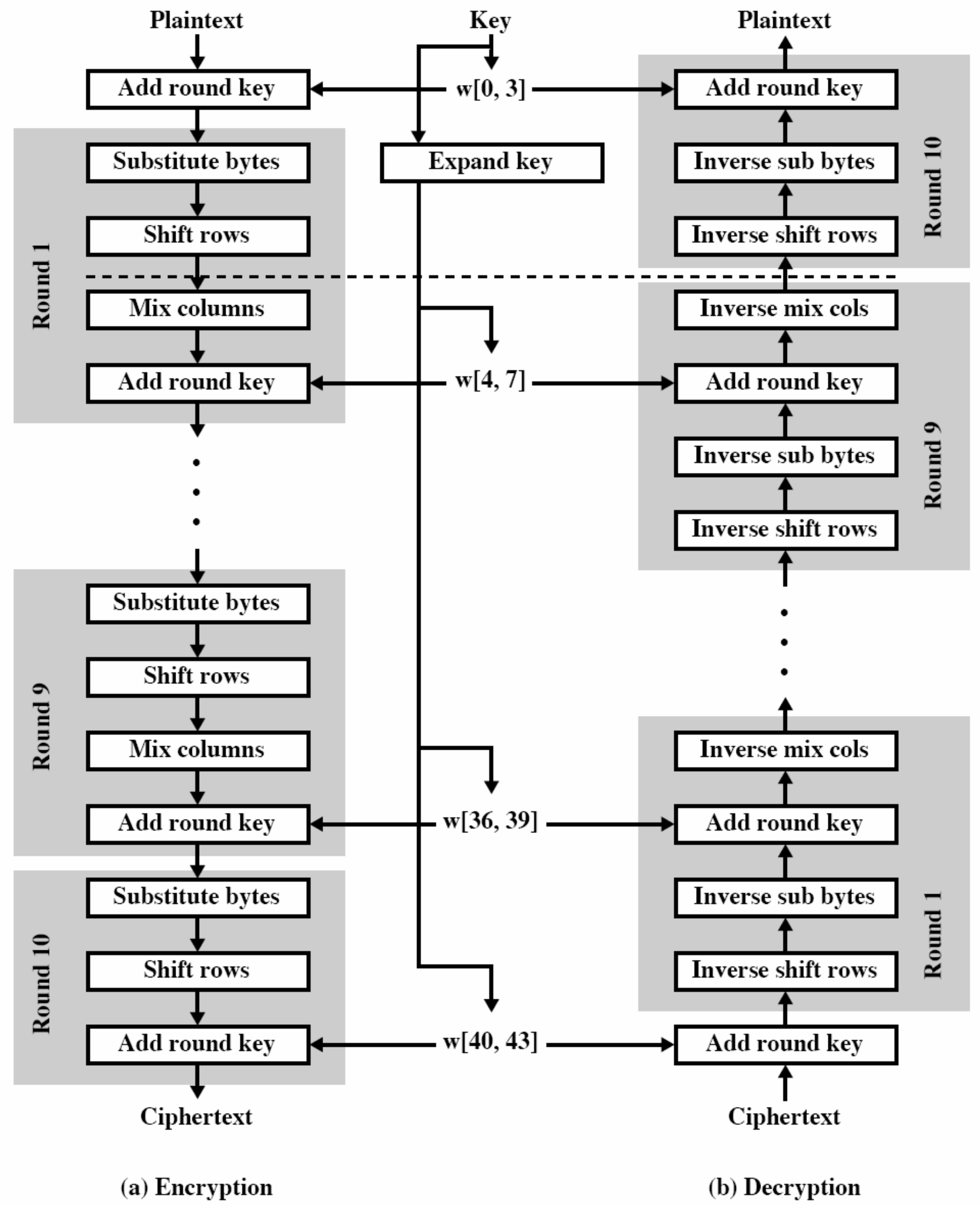


Figure 4.4 AES encryption and decryption (Stallings 2003)

Both Diffie-Hellman and AES algorithms have to be implemented in C language so that they can be integrated seamlessly into the remote control program which is designed to run under Linux platform. The coding of the algorithms mainly follows available decent implementations from internet resources, i.e. AES in C code by Gladman (2005).

5. PERFORMANCE ANALYSIS FOR THE WIRELESS COMMUNICATION

This chapter studies the performance of the developed remote control and monitoring system in wireless communication networks, by using analytical methods and numerical evaluation. The main objective is to evaluate the performance of obtained QoS, e.g. the overall blocking probability and the average queuing time for this particular system, with hybrid communication means of EDGE/GPRS/GSM.

5.1. Background of the performance analysis

The initial method of data transmission in GSM is circuit switching, which reserves the traffic channel for the entire communication time, and wastes the radio resource when data traffic occurs in bursts with long silent intervals. In the development of GSM phase 2+, GPRS over the GSM has been specified to increase the utilization efficiency of the radio resource. The physical channels unused by circuit switched services are allocated dynamically to the GPRS according to the actual needs for packet transfers. In the study here, from network resource allocation point of view a GSM CSD call is assumed to be equivalent to a GSM voice call and therefore the evaluation is done for voice to represent CSD performance.

Based on (Nogueira, Baynat, Eisenmann, 2005) GPRS is an overlay on GSM networks that allows end-to-end IP-based packet traffic from the terminal to e.g. the Internet. EDGE is an improvement over GPRS whereby the modulation scheme on radio is modified to allow higher throughputs thanks to advanced power amplifier and signal processing technologies. In a GPRS (or EDGE) cell, traffic is split between voice (on circuit) and data (on packet). Data uses a few dedicated circuits which are decomposed into 20 ms blocks carrying elementary packet traffic. EDGE uses adaptive modulation and coding, thus it differs from the GPRS that it can also adapt the modulation scheme, and due to the fact that in many occasions EDGE service is not available due to high BER or limitation of network resources, therefore only the GPRS/GSM performance is considered as the worst case analysis here.

Earlier studies of GPRS performance (Bianchi, Capone, Fratta, Musumeci 1995) and (Turina, Beming, Schster, Anderson 1996) focus on the protocol behaviour with a fixed number of channels used for data transmission. However, the number of channels available to GPRS is a random variable depending on the voice traffic and the voice channels' occupancy, thus the service statistics is a movable boundary Markov process (Wieselthier & Ephremides 1995). The analysis of GPRS performance is a complicated problem especially as multiple classes of quality of service and multiple classes of users are supported in GPRS. In the study here, the GPRS performance, e.g., the blocking probability and average queuing time, in the variable resource is evaluated by an approximation method. Only single slot GPRS is assumed in this study for the ease of analysis, and on the other hand it's sufficient to evaluate the performance of worst case scenario.

For the developed prototyping wireless remote control and monitoring system, it has been designed to utilize hybrid communication means in order to improve its reliability performance of wireless communication. Figure 5.1 illustrates a single terminal model of improved reliability performance with reduced blocking probability. Let P_{Bp} donate the blocking probability of using packet switched access i.e. EDGE/GPRS and P_{Bc} donate the blocking probability of using circuit switched access i.e. CSD/HSCSD. Consider the model shown in Figure 5.1. Assume that a remote access attempt firstly tries to connect with packet switched access with blocking probability $P_{Bp} = 0.05$, if it is blocked then secondly tires to connect with circuit switched access with blocking probability $P_{Bc} = 0.01$, if it is again blocked then we consider that this remote access attempt has failed due to the blocking from network. It can be easily obtained that the overall blocking probability of such system is $P_{Bp} \cdot P_{Bc} = 0.05 \times 0.01 = 5 \times 10^{-4}$, which is already very small. Even this is for using single terminal case, and the overall blocking probability will be further reduced with double redundant terminal case (with physical independent network service providers), which can be estimated as $(P_{Bp} \cdot P_{Bc})^{2} = 2.5 \times 10^{-7}$. From description in Section 3.2.2., the system is designed in a way that it will always automatically reconnect in case the connection is blocked or dropped. Therefore the overall blocking probability discussed here is also applicable to evaluate the blocking probability of the system for regaining access to the network.

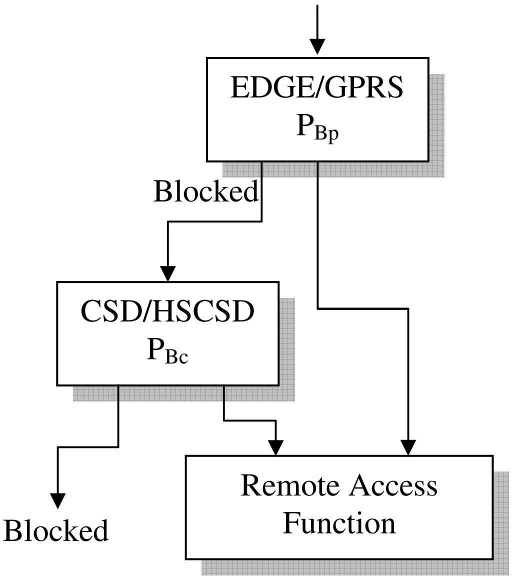


Figure 5.1 Hybrid model with reduced blocking probability

5.2. Principles of the radio resource allocation for GPRS

GPRS is designed to support from intermittent and burst data transfers to occasional transmission of large volume of data. The GPRS and GSM circuit switched services share the same radio resource. Whenever a channel is not used by circuit switched services, it may be utilized by GPRS. The allocation of physical channels for GPRS can be based on the needs for actual packet transfers which is referred to as "capacity on demand" principle. When the Packet Data Channels (PDCHs) shared by all GPRS users are congested due to the GPRS traffic load and more resource available in the cell, the network can allocate more physical channels as PDCHs. The GPRS does not require permanently allocated PDCHs. The operator can decide to dedicate permanently or temporarily some physical channels for GPRS traffic. However, the HSCSD service supports as well multiple slot services and has higher priority to access the physical channels. As the introduction of HSCSD service into the GSM system, it might be difficult to guarantee the quality of service of GPRS if no channel is dedicated to GPRS.

The number of allocated PDCHs in a cell can be increased or decreased according to demand. In order to implement this principle, a load supervision function, which monitors the load of the PDCHs and the number of allocated PDCHs in a cell can be increased or decreased, must be used in the system. Upon resource demand for circuit switched services, some PDCHs must be released as soon as soon as possible. The release can have two alternatives:

1) Immediate Release: the GPRS user is forced to stop its transmission until resource is available for GPRS again and the channel released by GPRS is allocated to circuit switched services.
2) Delayed Release: the GPRS user can continue its transmission up to some frames or until the ending of packet transmission, before the channel is allocated to circuit switched services.

For the study here, the immediate release is assumed in order to investigate the relation between the average interruption time and interrupting probability and the GPRS traffic. If the average interruption time and interrupting probability are low, the delayed release protocol can be considered to simplify the system. (Ni & Häggman 1999)

5.3. Performance evaluation

5.3.1. System model

According to (Ni & Häggman 1999), for a system with *m* physics channels, m_v channels are shared by voice and data services and m_d channels are dedicated to data, as shown in Figure 5.2. In the pool of m_v channels, when channels are not used by voice services, those channels are used for GPRS transmission. The voice services own preemptive priority over GPRS, i.e., whenever channels used by the GPRS service are needed by voice services, the GPRS transmission in those channels is stopped until some channels are available for GPRS. The users with interrupted service have higher priority for resource allocation than those in queue.

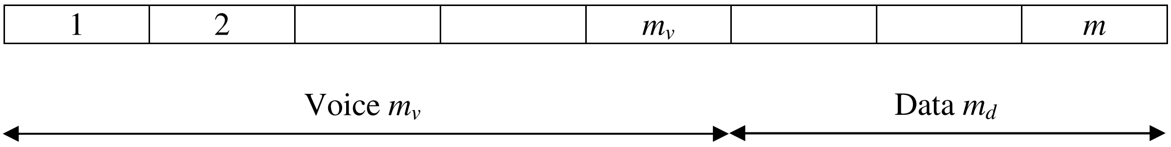


Figure 5.2 Illustration of radio resource structure allocated to GSM and GPRS

Assume that voice users' arrival is a Poisson process with a rate of λ_v and the call service time is exponentially distributed with a mean of $1/\mu_v$. All GPRS users share the physical channels unused by the voice services. The arrival of GPRS users is assumed to be a Poisson process with rate λ_d and the service time is exponentially distributed with a mean of $1/\mu_d$. The maximum number of users accepted into the system (in service and queue) is *N*. GPRS calls are served according to the first in first out principle. The arriving GPRS user is allowed to transmit data if a sufficient number of free channels is available; otherwise it is queued or blocked.

5.3.2. An approximation method for performance evaluation

The voice services are independent of GPRS. Because GPRS is mainly designed to transmit intermittent and burst data, the service time of GPRS is rather smaller than that of voice services. As an approximation, the decomposition technique can be used to analyze the GPRS performance (Ghani & Schwartz 1994). The essential of this technique is to use the voice services probability distribution to describe the interaction of voice services to GPRS. Thus, the GPRS performance in the dynamically variable resource is obtained by combining this distribution with the performance in a fixed resource. (Ni & Häggman 1999)

For the voice services, the probability of *n* users in service (no queuing) is:

$$r_n = r_0 (\frac{\lambda_v}{\mu_v})^n \frac{1}{n!}, n = 0,1,..., m_v \tag{5.1}$$

$$\text{where } r_0 = \left[\sum_{n=0}^{m_v} (\frac{\lambda_v}{\mu_v})^n \frac{1}{n!} \right]^{-1}$$

For voice services there are always m_v channels available no matter how many channels are occupied for data services. Since voice services always have higher priority than data services, data users will be forced to suspend their connections and give resources to the voice users. Therefore the blocking probably for voice services is the probability that all m_v channels are occupied by voice users, which is:

$$P_v = r_0 (\frac{\lambda_v}{\mu_v})^{m_v} \frac{1}{m_v!} \tag{5.2}$$

The channels unused by the voice services may be used for the data services. The probability of x channels available for the data services is equal to that of m_v-x channels used by voice services and is obtained as by (Eq. 5.1):

$$g(x) = r_0 (\frac{\lambda_v}{\mu_v})^{m_v - x} \frac{1}{(m_v - x)!}, x = 0,1,..., m_v \tag{5.3}$$

For the transmission of single slot GPRS in a fixed number of C channels, the average queuing time can be obtained from the *M/M/C/N* queuing system, where N is the maximum number of data users in the network (in service and in queue). The steady-state probability p_n is:

$$p_n = \begin{cases} p_0 \frac{\rho^n}{n!}, n < C \\ p_0 \frac{\rho^n}{C!C^{n-C}}, C \leq n \leq N \end{cases} \tag{5.4}$$

where n is the number of users in the system, $\rho = \lambda_d / \mu_d$, and

$$p_0 = \left[1 + \sum_{n=1}^{C-1} \frac{\rho^n}{n!} + \sum_{n=C}^{N} \frac{\rho^n}{C!C^{n-C}} \right]^{-1}$$

A new arrival is accepted into the system only if the number of data users in the network is below the maximum accepted number N. Otherwise, the new arrival is blocked. The blocking probability is:

$$P_N(C) = p_0 \frac{\rho^N}{C!C^{N-C}} \tag{5.5}$$

The average number of user in the system is obtained as:

$$W(C)=\sum_{n=1}^{N} np_n = p_0(\sum_{n=1}^{C}\frac{\rho^n}{(n-1)!}+\frac{C^C}{C!}\sum_{n=C+1}^{N}\frac{n\rho^n}{C^n}) \tag{5.6}$$

Combining (Eq. 5.3) with (Eq. 5.5) and (Eq. 5.6), the average blocking probability and average queuing time of single slot GPRS in a dynamically varied resource are obtained as following expressions respectively:

$$\overline{P_d}=\sum_{x=0}^{m_v} g(x)P_N(x+m_d) \tag{5.7}$$

$$\overline{T_d}=\frac{1}{\lambda_d(1-\overline{P_d})}\sum_{x=0}^{m_v} g(x)W(x+m_d)-\frac{1}{\mu_d} \tag{5.8}$$

Combining (Eq. 5.2) with (Eq. 5.7), the overall blocking for this particular system with single terminal is obtained as:

$$\overline{P}=P_v\overline{P_d}=r_0(\frac{\lambda_v}{\mu_v})^{m_v}\frac{1}{m_v!}\cdot\sum_{x=0}^{m_v} g(x)P_N(x+m_d) \tag{5.9}$$

5.3.3. Numerical evaluation results

In the numerical evaluation, 4 carriers, i.e., 4×8=32 channels in a cell are assumed, from which 1 channel m_d is reserved for data and 31 channels m_v are shared by circuit switched services and data. When a new circuit switched call arrives, if no free channel is available and the number of circuit calls in service is below 31, one of data calls is suspended in order to allocate one channel to the new circuit call. When resources are available, the interrupted data calls have higher priority to be allocated resource than the queuing calls. The maximum number of users allowed into network N is 40.

Figure 5.3 shows the blocking probability of voice services and data services and Figure 5.4 shows the overall blocking probability of hybrid GPRS/CSD. From the figures it can be seen that such hybrid GPRS/CSD communication means is very effective in reducing the overall blocking probability.

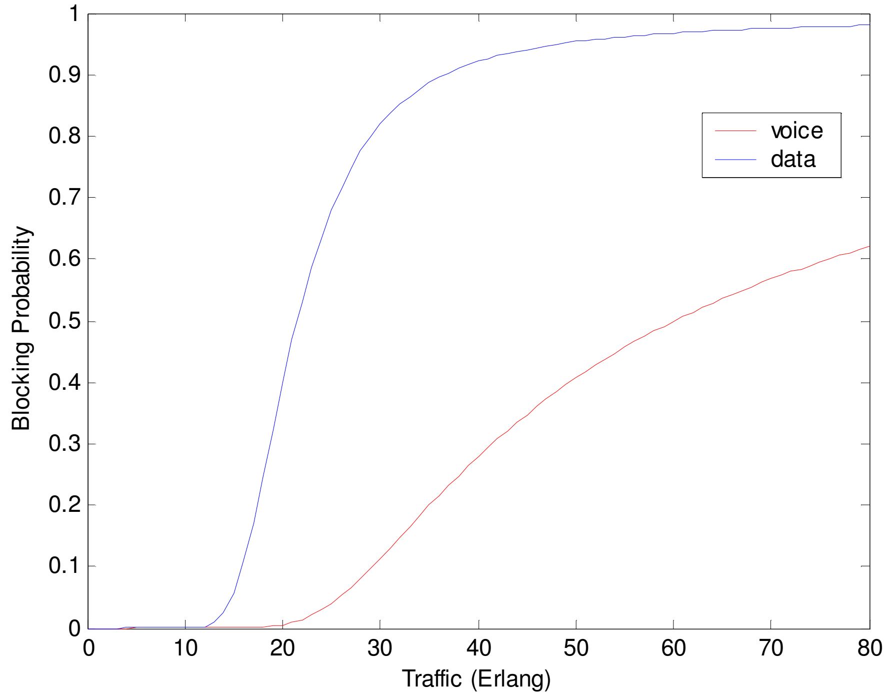


Figure 5.3 Blocking probability of voice services and data services

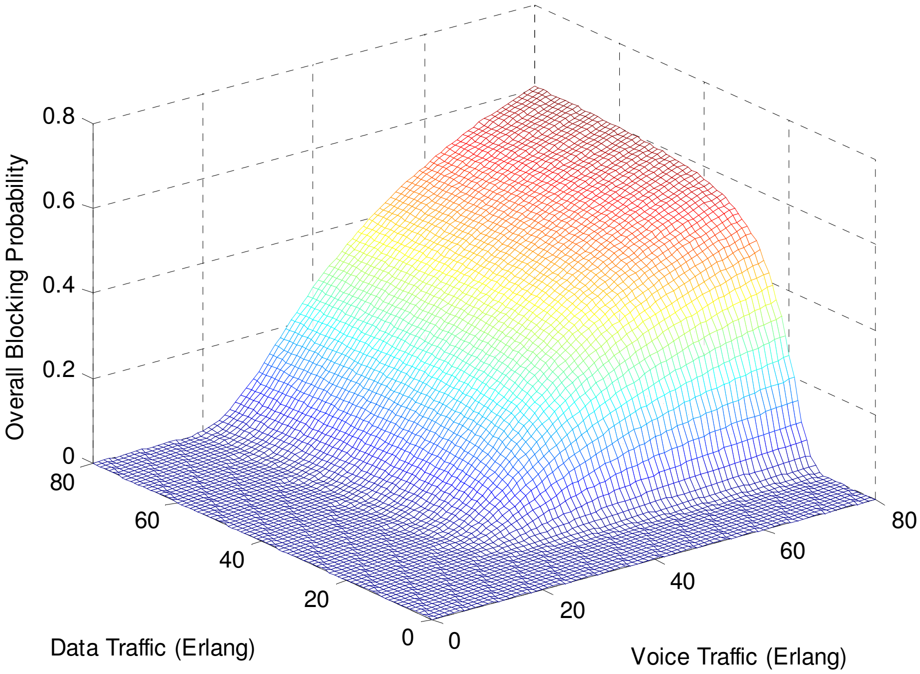


Figure 5.4 Overall blocking probability of hybrid GPRS/CSD

6. CONCLUSION

In this thesis work, a prototyping development towards a secured wireless remote control and monitoring system with redundancy has been carried out as a pilot of the industrial ICT-E project. The objective is to develop new low cost communication and control concepts for medium voltage devices that would enable the electrical grid operators to benefit from the advantages of the remote monitoring, diagnostics, and control by making such solutions economically feasible. Therefore the design and implementation of the prototype have been based on the idea of utilizing current available commercial wireless communication networks with considerations of not compromising the required performance of reliability and security.

As the major difference from a traditional remote control and monitoring application, the demanded system relies on completely wireless communication network, and the reliability and security issues are mostly concerned. A number of the state of art communication technologies including commercial communication networks and civilian communication networks for military use have been reviewed and their eligibilities to be employed in this project have been analyzed. To achieve the reliability and security requirements over wireless links, besides the development of a traditional remote control and monitoring application, various redundant modular structures as well as various levels of security measures e.g. access control for system security and cryptography for data security have been designed and implemented. Furthermore the redundancy design of the system modular structures has been theoretically analysed to evaluate the system reliability performance, and the reliability performance in wireless communication network has been analytically evaluated.

The prototype application developed in this thesis work has successfully met the desired requirements of providing a reliable, secure and economical solution for the wireless remote control and monitoring system using current available wireless communication networks. As a pilot of the ICT-E project, this thesis work has given fundamental and practical overview of the perspective future for utilizing commercial wireless communication technologies in remote control and monitoring applications. The future development to consummate functionalities and improve performances of such system and deploy such applications into real industrial use would be promising, based on the contribution of this thesis work.

REFERENCES

Andersson, Christoffer (2001). *GPRS and 3G Wireless Applications*. John Wiley & Sons, Inc, New York, USA.

Berrou, C.; Glavieux, A.; Thitimajshima, P. (1993). “Near Shannon limit error-correcting coding and decoding: Turbo-codes”. Proceedings of 1993 IEEE International Conference on Communications, (ICC93), Vol. 2, 23-26 May 1993, pp. 1064-1070.

Bhobe, A. U.; Perini, P. L. (2001). “An overview of smart antenna technology for wireless communication”. Proceedings of 2001 IEEE Aerospace Conference, Vol. 2, 10-17 March 2001, pp. 2/875-2/883.

Bianchi, G.; Capone, A.; Fratta, L.; Musumeci, L. (1995). “Packet data service over GSM networks with dynamic stealing of voice channels”. Proceedings of 1995 IEEE Global Telecommunications Conference, Vol. 2, 13-17 Nov. 1995, pp. 1152-1156.

Bowden, Bill. “Parallel Port Relay Interface” and “Reading Data from the Parallel Port” [online]. Bowden's Hobby Circuits [cited 17.08.2005].
<URL: http://ourworld.compuserve.com/homepages/Bill_Bowden/>

Eberspächer, Jörg; Vögel, Hans-Jörg; Bettstetter, Christian (2001). *GSM Switching, Services and Protocols, Second Edition.* John Wiley & Sons, Ltd, Chichester, England.

El Mahdy, Galal (2001). *Disaster Management in Telecommunications, Broadcasting and Computer Systems*. John Wiley & Sons, Ltd, Chichester, England.

IEEE (2005). “IEEE 802 LAN/MAN Standards Committee” [online]. IEEE Standards Working Group Areas [cited 11.10.2005]. <URL: http://grouper.ieee.org/>

Ghani, S.; Schwartz, M. (1994). “A decomposition approximation for the analysis of voice/data integration”. *IEEE Transactions on Communications*, Vol. 42, No. 7, July 1994, pp. 2441-2452.

Gladman, Brian (2005). “AES Code Implementation” [online]. Brian Gladman's Home Page [cited 27.09.2005]. <URL: http://fp.gladman.plus.com/>

Goldsmith, A. J.; Wicker, S. B. (2002). “Design challenges for energy-constrained ad hoc wireless networks”. *IEEE Wireless Communications*, Vol. 9, Issue 4, Aug. 2002, pp. 8-27.

Hajer, Matthijs (2005). “LPT Port Interface Description” [online]. Matthijs' Electronics Pages [cited 17.08.2005]. <URL: http://home.planet.nl/~m.f.hajer/>

Hiort-Lorenzen, Simon (2005). *TinCam WebCam Software* [online]. TinCam website [cited 28.06.2005]. <URL: http://www.tincam.com/>

Holma, Harri and Toskala, Antti (2001). *WCDMA for UMTS Radio Access for Third Generation Mobile Communications*. John Wiley & Sons, Ltd, Chichester, England.

IBM (2005). “ThinkPad T40 Series Product Information” [online]. IBM Personal Computer Division [cited 10.05.2005]. <URL: http://www.pc.ibm.com/>

Jäntti, Riku and Luoma, Kari (2005). “ICT of Electric distribution network” [internal document]. Oy Merinova Ab.

Li, Jiang (2005). *Microsoft Portrait* [online]. Microsoft Research [cited 28.06.2005]. <URL: http://research.microsoft.com/~jiangli/portrait/>

Liu, Yang and Chen, Jie (2003). “A Wireless Videoconferencing Approach towards 3G Mobile Network Services”. Proceedings of 2nd International Workshop on Embedded Systems, Internet Programming and Industrial IT, Kiel, Germany.

Logitech (2005). “QuickCam Pro 4000 Product Specifications” [online]. Logitech Inc. [cited 18.05.2005]. <URL: http://www.logitech.com/>

Microsoft (2005). “Virtual private network (VPN) connections overview”. Help and Support Center, Windows XP Professional. Microsoft Corporation.

MOD (2005). *Defence Science & Technology Information Sheets* [online]. Ministry of Defence of the United Kingdom [cited 08.06.2005]. <URL: http://www.mod.uk/>

Ni, S.; Häggman, S. (1999). "GPRS performance estimation in GSM circuit switched services and GPRS shared resource systems". Proceedings of 1999 IEEE Wireless Communication and Networking Conference (WCNC'99), Vol.3, 21-24 Sept. 1999, pp. 1417-1421.

Nogueira, G.; Baynat, B.; Eisenmann, P. (2005). "Asymptotic behavior of a GPRS / EDGE network with several cells controlled by a global capacity limit". Proceedings of XIth International Symposium on Applied Stochastic Models and Data Analysis (ASMDA), May 2005.

Nokia (2002). *Nokia 30, Nokia D211 User's Guide and Data Security Guide* [online]. Nokia Corporation [cited 12.05.2005]. <URL: http://www.nokia.com/>

Option (2005). "GlobeTrotter Specifications" [online]. Option Wireless Technology [cited 12.05.2005]. <URL: http://www.option.com/>

Penttonen, Martti (2003). *Data Security 2003* [online]. University of Kuopio [cited 20.07.2005]. <URL: http://www.cs.uku.fi/~penttone/secu2003/>

Razavilar, J.; Rashid-Farrokhi, F.; Liu, K. J. R. (1999). "Software radio architecture with smart antennas: a tutorial on algorithms and complexity". *IEEE Journal on Selected Areas in Communications*, Vol. 17, Issue 4, April 1999, pp. 662-676.

Renesas (2003). *Renesas M16C/62 Group (M16C62P) Hardware Manual* [online]. Renesas Technology [cited 08.08.2005]. <URL: http://www.renesas.com>

Safwat, A. M.; Mouftah, H. (2005). "4G network technologies for mobile telecommunications". *IEEE Network*, Vol. 19, Issue 5, Sept.-Oct. 2005, pp. 3-4.

Shannon, C. E. (1949). *The Mathematical Theory of Information*. University of Illinois Press (reprinted 1998).

Sharma, G.; Kumar, G. S. (2005). “Moving towards HSUPA: a complete 3.5G wireless system”. Proceedings of 2005 IEEE International Conference on Personal Wireless Communications (ICPWC 2005), 23-25 Jan. 2005, pp. 174-177.

Siemens (2005). “MC35i Terminal Datasheet” [online]. Siemens Communications - Wireless Modules Portal [cited 12.05.2005]. <URL: http://www.siemens.com/wm>

Sierra (2005). “AirCard 775 Datasheet” [online]. Sierra Wireless, Inc. [cited 12.05.2005]. <URL: http://www.sierrawireless.com/>

Stallings, William (2003). *Cryptography and Network Security, 3rd Edition*. Prentice Hall, Pearson Education, Inc, New Jersey, USA.

TEKES (2002). *Information Technology and Electric Power Systems*, *TESLA Technology Programme 1998-2002* [online]. TEKES, The National Technology Agency [cited 05.05.2005]. <URL: http://www.tekes.fi>

TEKES (2003). *DENSY – Distributed energy systems 2003-2007* [online]. TEKES, The National Technology Agency [cited 05.05.2005]. <URL: http://www.tekes.fi>

Telit (2005). *Telit GM862 Product Description* [online]. Telit Communications S.p.A. [cited 12.05.2005]. <URL: http://www.gm862.com/>

Trivedi, Kishor S. (2002). *Probability and Statistics with Reliability, Queuing and Computer Science Applications 2nd Edition*. John Wiley & Sons, Inc, New York, USA.

Turina, D.; Beming, P.; Schoster, E.; Andersson, A. (1996). “A proposal for multi-slot MAC layer operation for packet data channel in GSM”. Proceedings of 1996 5th IEEE International Conference on Universal Personal Communications (ICUPC’96), Vol. 2, 29 Sep.-2 Oct. 1996, pp. 572-576.

Wieselthier, J. E.; Ephremides, A. (1995). “Fixed- and movable-boundary channel-access schemes for integrated voice/data wireless networks”. *IEEE Transactions on Communications*, Vol. 43, Issue 1, Jan. 1995, pp. 64-74.

APPENDICES

Appendix 1. ICT of Electric distribution network

Project description (Jäntti & Luoma 2005)

This project will focus on the telecontrol and remote monitoring of medium voltage devices such as switches and disconnectors. Typically the amount of data needed in remote control of such devices has been very small. Traditionally in case of disconnectors, only the contact information, open/closed, is transmitted. Using concurrent mobile technology also a picture of the disconnector's state could be transmitted eliminating the need of the maintenance crew to visit the site to visually verify that the disconnector is really in open position before grounding the line. The time constant of the disconnector is in the order of magnitude of seconds, thereby tolerating up to one second communication delays. This suggests that even GSM/GPRS networks could in some cases be utilized in telecontrol applications. Of course, there are many control loops, in which the delay requirements are very strict, in which case commercial radio access networks are not fast and reliable enough. Even in those cases, they could, however, be utilized as a auxiliary back up systems or in part of some quality loop setting parameters for the local fast control loops.

- Objectives

This project focuses on the information and communication technology (ICT) needed to control the future energy systems. The objective is to study what are the current and expected communication requirements for distance monitoring and remote control applications in electrical networks and whether the current ICT technology can meet them. Both technical and economical feasibility will be investigated. This task has the following objectives.

1) Service and business concepts

The objective is to find out what the relevant processes and needs of the end-users are and how the overall end-to-end service concept should be organized. The concept should answer questions like: What are the roles of different stakeholders - how should own the distance monitoring and remote control system? What kinds of agreements are needed among the players?

2) Review of state of the art and find barriers

The objective is to review the possibilities and restrictions of the novel wireless communication networks and communication and control protocols. Also the barriers preventing utilization of these technologies will be investigated. The barriers include technological, quality of service (QoS) related barriers and economical, equipment and data transmission cost related, barriers.

3) Distance monitoring and remote control technology

The objective is to find out what are the communication requirements for distance monitoring and remote control applications and how these could be met by using concurrent or upcoming information and communication technology by using off-the-shelf or upcoming ICT solutions and network services.

- Tasks

The tasks of this project mainly involve the followings.

1) End-user processes and needs

In this task, the relevant processes of the distribution network operators are reviewed and their needs for distance monitoring investigated.

2) Mapping of the communication requirements and finding barriers

This task is to be done in co-operation with energy cluster, grid operators and equipment manufactures. The output of this task is a set of constraint against which the different ICT technologies will be compared.

3) Review of state of the art in wireless networks and networking

The key points in this task are the operation costs and availability of different services among their quality of service (QoS) properties. The first two factors advocate the use of commercial radio access networks. Hence, in this task we will focus on GSM/GPRS, EDGE, and UMTS networks which will be compared against other possibilities. Telia-Sonera has demonstrated that GPRS network can be used for distance metering electricity consumption in the consumer end. The critical question here is whether the QoS requirements of the transmission network control applications could be met using M2M communication in commercial networks. In addition network security issues will be investigated and different protocols reviewed. Also the reliability of the networks will be addressed.

Especially, we will evaluate the new signalling opportunities of the recently introduced IP Multimedia Subsystem (IMS) which allows the use of session initiation protocol SIP based signalling in GSM/GPRS and UMTS networks. Here once again, we will consider the QoS constraints in terms of delay and reliability. Also other telenetwork based signalling approaches will be considered such as MMS-messaging and simple circuit switched call based signalling. For instance, MMS based signalling could be used to transmit video picture of the disconnector state. Circuit switched call based signalling could provide more reliable way to indicate simple on-off information than GPRS based transmission in case of network congestion. The opportunities of TETRA networks already discussed in the TESLA program will be kept in mind as comparison.

4) Review of state of art in control protocols

There exist standardized protocols for telecontrol applications such as the IEC 870-5 protocol which can run even over IP-networks (see IEC 870-5-104). Also some general purpose automation schemes, such as OPC, and proprietary protocols, such as Modbus, could be used together with IP-networks that then in turn could run over the wireless access networks e.g. GPRS). The choice of protocol will be mostly dictated by the needs of the applications determined in task 2.

5) Development of new concepts for distance monitoring and remote control

Based on the review and system model a new concept is developed for distance monitoring and remote control. This task is a case study.

6) Security and safety issues

Controlling disconnector state is critical for the safety of the technician working in the field. Nowadays he or she must physically visit the disconnector and verify the disconnector state visually. He will also lock the control switch of the disconnector so that nobody could switch it on accidentally during the maintenance operation. Developing a digital control strategy that is reliable enough and which could be trusted by the field technicians is a critical issue. In this task safeguards and safe operation principles will be developed. In order to do so, safety critical control methods used in process industry will be benchmarked.

Since the control of disconnectors is safety critical all digital transactions must be secured. Origin of the control messages should be authenticated, the use of control actions authorize and the integrity of control messaging secured against security attacks. For this reason different virtual private network (VPN) solutions will be considered.

7) Development of new service and management concepts

This task is parallel to the previous one focusing on the business aspects.

Appendix 2. Serial communication details of client party and server party

Local Client			Remote Server		
TxD	RxD	Action	TxD	RxD	Action
`AT`	`OK`	Verify “OK”	`AT`	`OK`	Verify “OK”
`AT+CREG?`	`+CREG: 0,1`	Verify 2nd number is “1”	`AT+CREG?`	`+CREG: 0,1`	Verify 2nd number is “1”
`AT+CSQ`	`+CSQ: 10,0`	If 1st number is too small or 2nd number >0 then give warning	`AT+CSQ`	`+CSQ: 10,0`	If 1st number is too small or 2nd number >0 then give warning
`AT+CGSN`	`354592000636751`	Save to variable IMEI_C	`AT+CGSN`	`354592000636348`	Save to variable IMEI_S
`AT+CLIP=1`	`OK`	Verify “OK”	`AT+CLIP=1`	`OK`	Verify “OK”

`ATD0442726524`	`OK`	Verify “OK”, wait for “CONNECT”		`RING`
				`+CLIP: "+358440244250",145,””,,””,0`
					Verify Caller ID

	`CONNECT 9600`	Verify “CONNECT”	`ATA (or ATH)`	`CONNECT 9600`	Verify “CONNECT”
Y_A	Y_B	Start key exchange, generate random X_A, calculate Y_A and K	Y_B	Y_A	Start key exchange, generate random X_B, calculate Y_B and K
Encrypted message	Encrypted message	Start encryption with K	Encrypted message	Encrypted message	Start encryption with K

Appendix 3. Look up table for reading of the LPT port

Return value	Bit value								Real status				
	B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3
135	128	0	0	0	0	4	2	1	0	0	0	0	0
143	128	0	0	0	8	4	2	1	0	0	0	0	1
151	128	0	0	16	0	4	2	1	0	0	0	1	0
159	128	0	0	16	8	4	2	1	0	0	0	1	1
167	128	0	32	0	0	4	2	1	0	0	1	0	0
175	128	0	32	0	8	4	2	1	0	0	1	0	1
183	128	0	32	16	0	4	2	1	0	0	1	1	0
191	128	0	32	16	8	4	2	1	0	0	1	1	1
199	128	64	0	0	0	4	2	1	0	1	0	0	0
207	128	64	0	0	8	4	2	1	0	1	0	0	1
215	128	64	0	16	0	4	2	1	0	1	0	1	0
223	128	64	0	16	8	4	2	1	0	1	0	1	1
231	128	64	32	0	0	4	2	1	0	1	1	0	0
239	128	64	32	0	8	4	2	1	0	1	1	0	1
247	128	64	32	16	0	4	2	1	0	1	1	1	0
255	128	64	32	16	8	4	2	1	0	1	1	1	1
7	0	0	0	0	0	4	2	1	1	0	0	0	0
15	0	0	0	0	8	4	2	1	1	0	0	0	1
23	0	0	0	16	0	4	2	1	1	0	0	1	0
31	0	0	0	16	8	4	2	1	1	0	0	1	1
39	0	0	32	0	0	4	2	1	1	0	1	0	0
47	0	0	32	0	8	4	2	1	1	0	1	0	1
55	0	0	32	16	0	4	2	1	1	0	1	1	0
63	0	0	32	16	8	4	2	1	1	0	1	1	1
71	0	64	0	0	0	4	2	1	1	1	0	0	0
79	0	64	0	0	8	4	2	1	1	1	0	0	1
87	0	64	0	16	0	4	2	1	1	1	0	1	0
95	0	64	0	16	8	4	2	1	1	1	0	1	1
103	0	64	32	0	0	4	2	1	1	1	1	0	0
111	0	64	32	0	8	4	2	1	1	1	1	0	1
119	0	64	32	16	0	4	2	1	1	1	1	1	0
127	0	64	32	16	8	4	2	1	1	1	1	1	1

Appendix 4. C source code for the prototyping core control program

```
<lpt_cont.h>

#ifndef LPT_CONT_H
#define LPT_CONT_H
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>
#include <asm/io.h>
#include <termios.h>
#include <time.h>
#include <pthread.h>
#define BASEPORT 0x378 /* lp1 */
#define BUFFERLENGTH 30

// lpt_cont
int getch();
void readpasswd();
void delete_keybuffer();
int compare(char *string1, char *string2);
int *calculate_binary(int d_number);
void get_time();
int access_LPT();
void printb(int array[]);
void sys_status();
void switch_on_output();
void switch_off_output();
void *timemeasure();

// lpt_auth
void encrypt(char *message, int len);
void decrypt(char *message);
void username_passwd_string(char *user_name, char *user_passwd);
int write_to_file();
int read_from_file();
int check_user_passwd(char *decrymessage, char *decrym_file);

#endif
```

```
<lpt_auth.c>

#include "lpt_cont.h"
char msg[30];
char encry_msg[30];
char decry_msg[30];
int length = 0;
int userlength;
int passwdlength;

void encrypt(char *message, int len)
 {
  char temp_array[30];
  strcpy(temp_array, message);
  int p;
  int temp;

  for(p = 0; p < len; p++)
  {
    temp = (int) temp_array[p];
    temp = temp + 89;
    encry_msg[p] = (char) temp;
  }
 }

void decrypt(char *message)
 {
  char temp_array[30];
  strcpy(temp_array, message);
  int message_len = strlen(temp_array);
  int p;
  int temp;

  for(p = 0; p < message_len; p++)
  {
    temp = (int) temp_array[p];
    temp = temp - 89;
    decry_msg[p] = (char) temp;
  }
 }

int check_user_passwd(char *decrymessage, char *decrym_file)
 {
     char temp1[30];
     char temp2[30];
     strcpy(temp1, decrymessage);
     strcpy(temp2, decrym_file);

     if(!strcmp(temp1, temp2))
      return 1;
     else
      return 0;
 }

void username_passwd_string(char *user_name, char *user_passwd)
 {
  int w;
  int y = 0;
  userlength = strlen(user_name);
  passwdlength = strlen(user_passwd);
  length = userlength + passwdlength;

  for(w = 0; w < 30; w++)
  {
    if(w < userlength)
      msg[w] = user_name[w];
    if(w >= userlength)
    {
      msg[w] = user_passwd[y];
      y++;
    }
  }
 }

int write_to_file()
 {
     FILE *fp;

     if((fp = fopen("passwd.txt", "w")) == NULL)
     {
       fprintf(stderr, "\nFile can not be opened");
       return 0;
     }
     if(fputs(encry_msg, fp) == EOF)
     {
       fprintf(stderr, "\nFile: WRITE ERROR");
       return 0;
     }
     fclose(fp);

     return 1;
 }

char buffer2[BUFFERLENGTH];

int read_from_file()
 {
     FILE *fp;
     // open file
     if((fp = fopen("passwd.txt", "r")) == NULL)
     {
         fprintf(stderr, "\nFile can not be opened\n");
         return 0;
     }
     // read lines
     while (!feof(fp) )
     {
         fgets(buffer2, BUFFERLENGTH, fp);
     }
     fclose(fp);
     return 1;
 }
```

```
<lpt_cont.c>

#include "lpt_cont.h"

char internal_password[15];
int state = 0;

int getch()
{
      struct termios oldt, newt;
      int ch;
      tcgetattr( STDIN_FILENO, &oldt );
      newt = oldt;
      newt.c_lflag &= ~( ICANON | ECHO );
      tcsetattr( STDIN_FILENO, TCSANOW, &newt );
      ch = getchar();
      tcsetattr( STDIN_FILENO, TCSANOW, &oldt );
      return ch;
}

void readpasswd()
{
      int x;

      for(x = 0; x < 15; x++)
      {
            internal_password[x] = 0;
      }

      char character;
      int t = 0;

      while ((character != 10))                // ASCII CODE for ENTER
        {
           character = getch();

             if(character == 127)
           {
            if(t > 0)
            {
                  t--;
            internal_password[t] = 0;
            }
           }
           else
           {
            if(character != 10)
            {
                  internal_password[t] = character;
                        t++;
            }
           }
        }
}

void delete_keybuffer()
{
 char waste[255];
 gets(waste);
}

int compare(char *string1, char *string2)
{
  char temp1[15];
  char temp2[15];
  int s;

  for(s = 0; s < 15; s++)
  {
   temp1[s] = string1[s];
   temp2[s] = string2[s];
  }

  int z = 0;
  int r = 0;
  int w = 0;

 while(temp1[r] != 0)
        r++;

  while(temp2[w] != 0)
        w++;

  if(r != w)
        return 0;

  while(temp1[z] != 0 && temp2[z] != 0)
  {
    if(temp1[z] != temp2[z])
      return 0;

      z++;
  }

  return 1;
}

int temp_array_new[5];

int *calculate_binary(int d_number)
{
      int j;

      for(j = 0; j < 5; j++)
      {
       temp_array_new[j] = 0;
      }

      int temp = d_number - 7;
      int temp_array[] = {256,128,64,32,16,8};

      int i;

      for(i = 0; i < 5; i++)
      {
            if(temp < temp_array[i] && temp >= temp_array[i+1])
            {
                  temp_array_new[i] = 1;
                  temp = temp - temp_array[i+1];
            }
      }

      if(temp_array_new[0] == 1)
            temp_array_new[0] = 0;
      else
            temp_array_new[0] = 1;

      return temp_array_new;
}

char buffer[50];

void get_time()
{
      time_t now;
      struct tm *pointer;

      // determine the current time
      time(&now);

      // convert the time_t-value in the structure of the type tm
      pointer = localtime(&now);

       strftime(buffer, 80, "Today is %d-%m-%Y, %H:%M:%S", pointer);
}

int access_LPT()
{
      /* Get access to the ports */
      if (ioperm(BASEPORT, 3, 1)) {perror("ioperm"); exit(1);}

      /* Set the data signals (D0-7) of the port to all low (0) */
      outb(0, BASEPORT);

      /* Sleep for a while (100 ms) */
      usleep(100000);

      /* Read from the status port (BASE+1)*/
      state = inb(BASEPORT + 1);

      /* We don't need the ports anymore */
      if (ioperm(BASEPORT, 3, 0)) {perror("ioperm"); exit(1);}

      return state;
}

void printb(int array[])
{
 int j;
 for(j = 0; j < 5; j++)
 {
  printf("%d", array[j]);
 }
}

void sys_status()
{
      calculate_binary(state);
      get_time();
      printf("Current system status is ");
      printb(temp_array_new);
      printf(" ");
      puts(buffer);
}

void switch_on_output()
{
      /* Get access to the ports */
      if (ioperm(BASEPORT, 3, 1)) {perror("ioperm"); exit(1);}
      outb(0, BASEPORT+2);

      /* We don't need the ports anymore */
      if (ioperm(BASEPORT, 3, 0)) {perror("ioperm"); exit(1);}
}

void switch_off_output()
{
      /* Get access to the ports */
      if (ioperm(BASEPORT, 3, 1)) {perror("ioperm"); exit(1);}

      outb(2, BASEPORT+2);

      /* We don't need the ports anymore */
      if (ioperm(BASEPORT, 3, 0)) {perror("ioperm"); exit(1);}
}

int tm = 0;
int tlock = 0;

void *timemeasure()
{
  sleep(30);
  printf("\ntimeout");
  tlock = 1;
  char timeout_warning;
  do
  {
     timeout_warning = ' ';
     printf("\nDo you want to continue?(y or n) ");
     scanf("%s", &timeout_warning);
  }
  while(timeout_warning != 'y' && timeout_warning != 'n');
   if(timeout_warning == 'n')
      tm = 1;
   else
    tlock = 0;
  return NULL;
}
```

```
<lpt_main.c>

#include "lpt_cont.h"

int count = 0;

// lpt_cont
char username[15];
extern char internal_password[15];
extern int temp_array_new[5];
extern char buffer[50];
extern int state;
extern int tm;
extern int tlock;

// lpt_auth
extern char msg[30];
extern char encry_msg[30];
extern char decry_msg[30];
extern int length;
extern char buffer2[BUFFERLENGTH];

// for timeout
time_t begin, end;
struct tm *pointer;
char *c, buffer1[80];
double duration;

int main()
{
 switch_off_output();

 do
 {
      strcpy(username, " ");

      printf("\nPress Ctrl+C at any time to break");

      printf("\nWelcome to ICT-E Remote Control System");

      printf("\nEnter your username: ");
      scanf("%s", &username);

      delete_keybuffer();

      printf("Enter your password: ");
      readpasswd();

      username_passwd_string(username, internal_password);

      if(read_from_file())
      {
            decrypt(buffer2);

            if(!check_user_passwd(decry_msg, msg))
            {
                  count++;
                  printf("\nLogin failed\n");

                  if(count == 3)
                  {
                        printf("\nLogin failed 3 times.\n");

                        return 0;
                  }
            }
      }

      else
       return 0;
 }
 while(!check_user_passwd(decry_msg, msg));

 char menu_choice = ' ';

 do
 {
      printf("\n----------------------------------------");
      printf("\n------------------Menu------------------");
      printf("\nPress 1 to continue with the program");
      printf("\nPress 2 to change the password");
      printf("\nPress 3 to quit");
      printf("\n----------------------------------------");
      printf("\n");

  scanf("%s", &menu_choice);

  if(menu_choice != '1' && menu_choice != '2' && menu_choice != '3')
      printf("\nwrong input");
 }
 while(menu_choice != '1' && menu_choice != '2' && menu_choice !=
'3');

 if(menu_choice == '1')
 {
  char date_time;
  char warning;
  char system_status;

  printf("\n");
  get_time();
  puts(buffer);

  do
  {
    date_time = ' ';
    printf("\nIs the current date and time correct?(y or n) ");
    scanf("%s", &date_time);
  }
  while(date_time != 'y' && date_time != 'n');

  if(date_time == 'n')
  {
   do
```

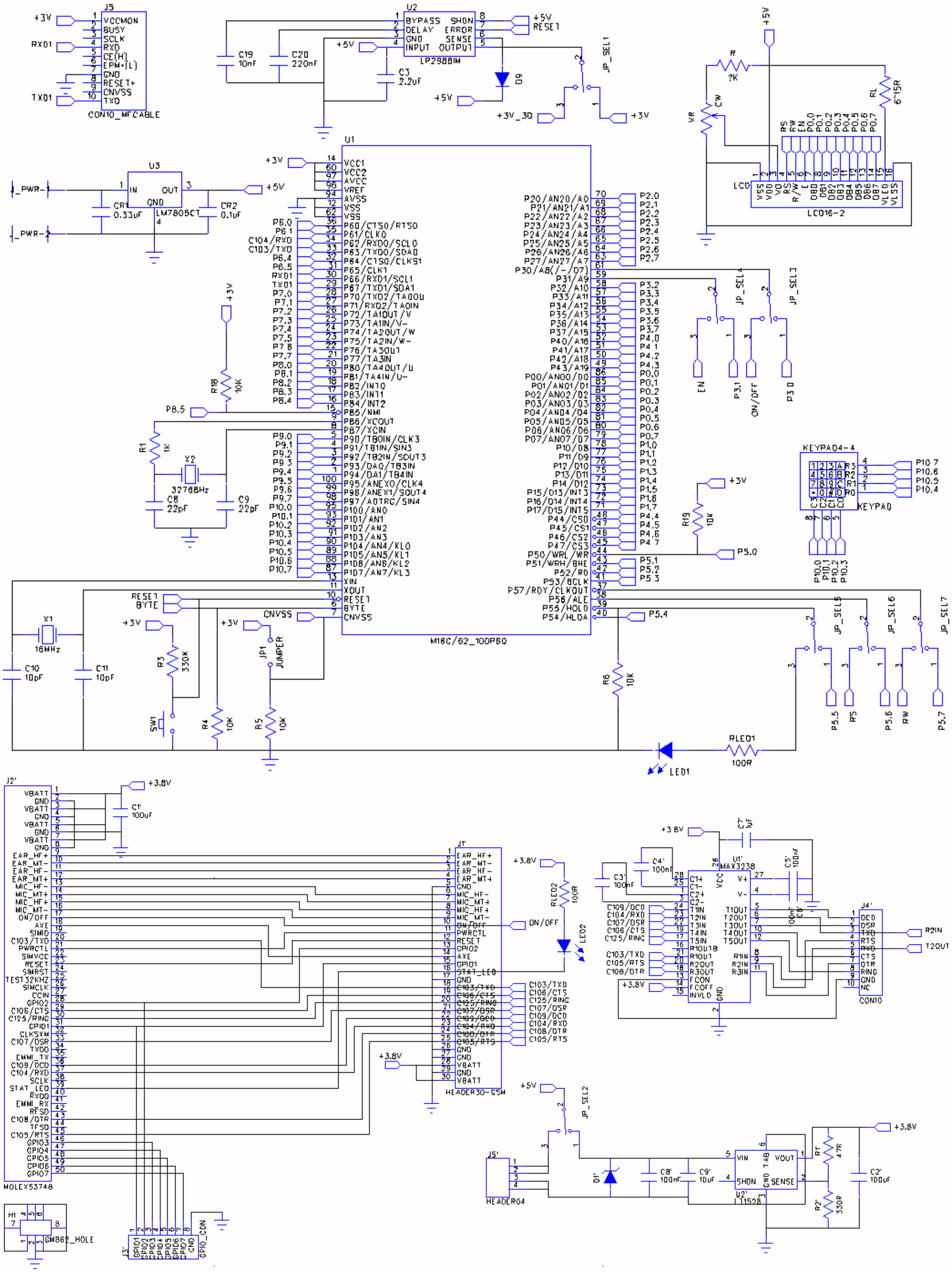
```
    {
      warning = ' ';
      printf("\nWARNING: Server may have potential security defeat, are
you sure to continue?(y or n) ");
      scanf("%s", &warning);
    }
    while(warning != 'y' && warning != 'n');
  }

  if(warning == 'n')
    return 0;

  else
  {
      access_LPT();

      get_time();
      puts(buffer);

      if(state == 135)
      {
            sys_status();
            printf("\nstatus: OPENED ");
      }

      else if(state == 127)
      {
            sys_status();
            printf("\nstatus: CLOSED ");
      }

      else
      {
            sys_status();
            printf("\nThe current system status is not correct\n ");
            return 0;
      }

      do
      {
            printf("\nIs the current status correct?(y or n) ");
            scanf("%s", &system_status);
      }
      while(system_status != 'y' && system_status != 'n');

      if(system_status == 'n')
      {
            do
            {
                  warning = ' ';
                  printf("\nWARNING: Server may have potential
security defeat, are you sure to continue?(y or n) ");
                  scanf("%s", &warning);
            }
            while(warning != 'y' && warning != 'n');

            if(warning == 'n')
```

```
           return 0;
    }
}

while(1)
{
    delete_keybuffer();
    char command;
    int lock = 0;

    do
    {
          command = ' ';
          printf("\nEnter your command: ((O)PEN or (C)LOSE) ");
          scanf("%s", &command);
    }
    while(command != 'O' && command != 'C');

    pthread_t p;

    // system is closed
    if(command == 'O' && state == 127)
    {

          switch_on_output();

          pthread_create(&p, NULL, timemeasure, NULL);

          while(state != 135 && tm != 1)
          {
            if(tlock != 1)
            {

                 // start measure time
                begin = time(0);

                access_LPT();

                if(state == 119 && lock == 0)
                  lock = 1;

                if(state == 103 && lock == 2)
                  lock = 3;

                if(state == 71 && lock == 4)
                  lock = 5;

                if(state == 7 && lock == 6)
                  lock = 7;

                if(lock == 1 || lock == 3 || lock == 5 || lock == 7)
                {
                 printf("Executing... ");
                 sys_status();
                 lock++;
                }
            }
```

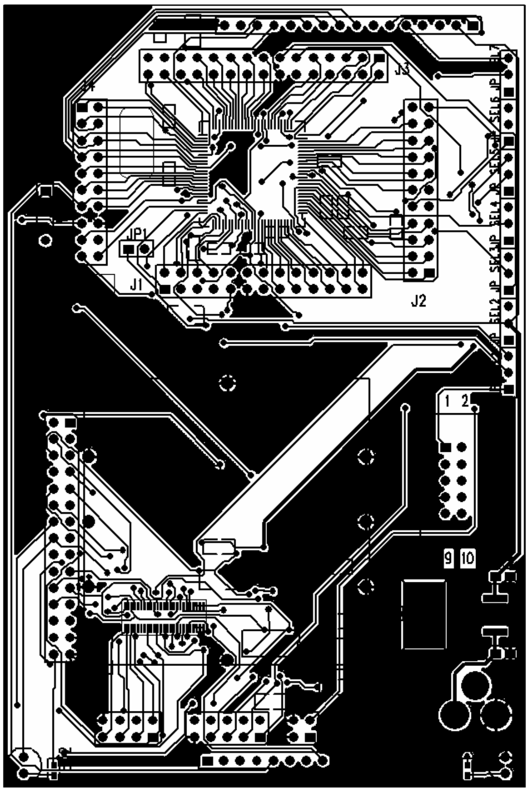
```
      }

      if(state == 135)
      {
       sys_status();
       printf("\nThe System_Satus is OPENED ");
       switch_off_output();
       pthread_cancel (p);
      }

      pthread_join (p, NULL);

      if(tm == 1)
       return 0;
}

// system is opened
else if(command == 'C' && state == 135)
{
      switch_on_output();

      pthread_create(&p, NULL, timemeasure, NULL);

      while(state != 127 && tm != 1)
      {
        if(tlock != 1)
        {
            access_LPT();

            if(state == 7 && lock == 0)
              lock = 1;

            if(state == 71 && lock == 2)
              lock = 3;

            if(state == 103 && lock == 4)
              lock = 5;

            if(state == 119 && lock == 6)
              lock = 7;

            if(lock == 1 || lock == 3 || lock == 5 || lock == 7)
            {
             printf("Executing... ");
             sys_status();
             lock++;
            }
        }
      }

      if(state == 127)
      {
            sys_status();
            printf("\nThe System_Satus is CLOSED ");
            switch_off_output();
            pthread_cancel (p);
      }
```

```
            pthread_join (p, NULL);

            if(tm == 1)
             return 0;
      }

      else
      {
            char system_status_error;

            do
            {
                  system_status_error = ' ';
                  printf("\nThe set status is the same as the current
status. No change has been made. ");
                  printf("\nDo you want to try it again?(y or n) ");

                  scanf("%s", &system_status_error);
            }
            while(system_status_error != 'y' && system_status_error !=
'n');

            if(system_status_error == 'n')
             return 0;

            else
             continue;
      }


      char quit_program;

      do
      {
            quit_program = ' ';
            printf("\nDo you want to quit the program?(y or n) ");
            scanf("%s", &quit_program);
      }
      while(quit_program != 'y' && quit_program != 'n');

      if(quit_program == 'y')
       return 0;
  }
}

else if(menu_choice == '2')
{
 char conf_name[15];
 char temp_passwd[15];

 do
 {
      strcpy(username, " ");

      printf("\nPress Ctrl+C at any time to break");
      printf("\nWelcome to ICT-E Remote Control System");

      printf("\nEnter your new username: ");
      scanf("%s", &username);

      delete_keybuffer();

      printf("Enter your new password: ");
      readpasswd();

      strcpy(temp_passwd, internal_password);

      strcpy(conf_name, " ");

      printf("\nConfirm your username: ");
      scanf("%s", &conf_name);

      delete_keybuffer();

      printf("Confirm your password: ");
      readpasswd();

      if(strcmp(username, conf_name) != 0 || strcmp(temp_passwd,
internal_password) != 0)
            printf("username or password does not match");
}
while(strcmp(username, conf_name) != 0 || strcmp(temp_passwd,
internal_password) != 0);

      username_passwd_string(username, internal_password);
      encrypt(msg, length);

      if(write_to_file())
         printf("\npassword/username has/have been changed!!!\n");


      else
       printf("\npassword/username could not be changed!!!\n");
}

else
 return 0;

  return 0;
}
```

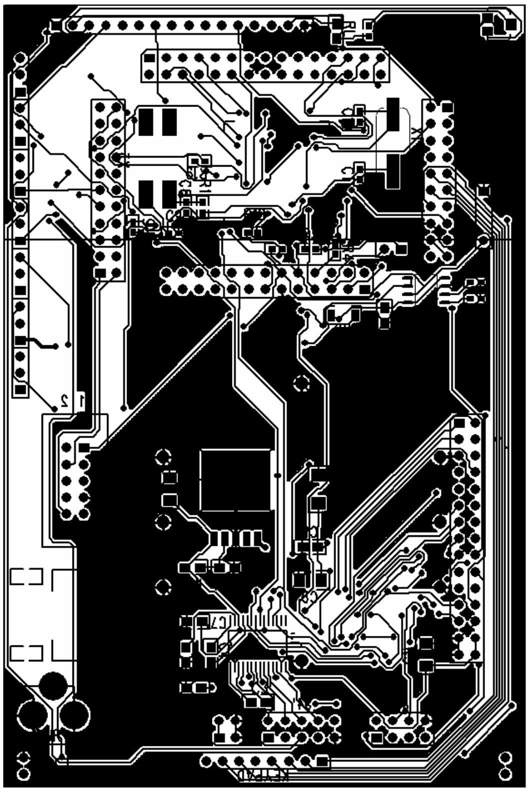
Appendix 5. Design of circuit diagram and PCB layout for MCU based system



Circuit diagram



Top layer PCB



Bottom layer PCB