OPTIMISATION OF UHF RADIO SCADA SYSTEMS FOR ELECTRICAL DISTRIBUTION NETWORKS

Pierre Delport

Thesis presented in partial fulfilment for the degree of

Master of Engineering Sciences

at the

University of Stellenbosch

Supervisor : Dr. H.J. Vermeulen

April 2006

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my own original work, and has not previously, in its entirety or in part, been submitted at any university for a degree.

………………………..

P. Delport

15 December 2005

Abstract

This thesis presents the results of an investigation to establish methods to improve the performance of area radio based communication systems for Supervisory Control and Data Acquisition (SCADA) systems. The considerable scale on which an area radio network is used as a telecommunication network is quite unique to South Africa due to a lack of high bandwidth telecommunication systems in rural areas.

Research was done to establish Key Performance Indicators (KPIs) to measure the performance of the area radio telecommunication systems. Two KPIs were chosen, namely Remote Terminal Unit (RTU) availability and Control Success Rate (CSR). These KPIs were trended over a three-year period to measure the effectiveness of measures taken to improve the systems. Two measures were implemented, namely to change the RTU radios, antennas and coaxial feeder cables and to redesign the communication systems in such a way to restrict multiple RTU protocols on the same area radio telecommunication network.

The installation of new digital radios together with low loss coaxial cable and specific antennas improved the RTU availability from 96.87 % for the year 2002 to 99.17 % for the year 2004, which realised in an increase of 2.83 % for 432 installed RTUs. This measure, however, did not influence the CSR. The implementation of the newly designed communication networks had a significant influence on the control success rate of the SCADA systems and the KPI increased from 77.65 % for the year 2002 to 78.76 % for the year 2003 and 80.88 % for the year 2004. A drastic increase in performance was observed after the restriction of multiple RTU protocols on the same network during May 2004, where the value for twelve months prior to September 2005 was measured at 84.38 %.

The utilisation of area radio telecommunication networks was measured for two operational networks and it was found to be well within the specifications of international accepted standards. One of these networks comprised of three repeaters and 84 installed RTUs and an average utilisation of 17 % and a peak utilisation of 25 % was measured. The other network had an installed base of 4 repeaters and 15 installed RTUs's and an average utilisation of 3 % and a peak utilisation of 8 % was measured. This compares favourable with the IEEE standard 999-1992 [20], which recommends a channel utilisation of between 40 % and 60 %.

Keywords : Key performance indicators, Radio telecommunication networks, Remote terminal unit

Opsomming

Hierdie tesis verteenwoordig die resultate van navorsing wat gedoen is om metodes te formuleer wat die prestasie van 'n area radio telekommunikasie stelsel kan verbeter tussen 'n Toesigbeheer en Data Versameling (TBEDV) meesterstasie en afstandbeheerstels. Die groote van die geografiese area wat deur die area radio telekommunikasie netwerk gedek in Suid Afrika word is uniek as gevolg van die tekortkominge aan goeie en goedkoop hoë bandwydte telekommunikasie stelsels in die afgesonderde landelike gebiede.

Navorsing is gedoen om Sleutel Prestasie Indikators (SPI's) te definieer om die prestasie van area radio telekommunikasie netwerke te meet. Twee SPI's is gekies, naamlik Afstandbeheer Beskikbaarheid (AB) en Suksesvolle Beheer Bevele (SBB). Die tendens van die twee SPI's is oor 'n tydperk van drie jaar bestudeer om te bepaal of die geimplementeerde maatreëls suksesvol was om die prestasie van die stelsels te verbeter. Twee maatreëls is geimplemnteer, naamlik om die radios, antennas en koaksiale antenna kabels te vervang by plekke met swak prestasie en om die telekommunikasie netwerke te herontwerp sodat die gebruik van verskillende kommunikasie protokols op een area radio telekommunikasie network beperk sal word.

Die installasie van nuwe digitale radios tesame met lae verlies kaoksiale kabels en die gebruik van spesifike antennas het die AB verbeter van 96.87 % vir die jaar 2002 tot 99.17 % vir die jaar 2004. Dit kom neer op 'n verbetering van 2.83 % vir 'n totaal van 432 afstandbeheer stelle. Hierdie maatreel het egter nie die SBB enigsens verbeter nie. Die implementasie van die herontwerpte telekommunikasie stelsels het egter 'n groot positiewe impak gehad op die SBB. Hierdie SPI het verbeter van 77.65 % aan die einde Desember 2002 tot 80.88 % aan die einde van Desember 2004. Die implementering van die nuwe telekommuikasie stelsels was gedurende Mei 2004 en die sukses oor 'n twaalf maande tydperk is eers werlik opmerkbaar aan die einde van September 2005, waar dit verbeter het na 84.38 % vir die twaalf maande voor September 2005..

Die benutting van twee operasionele area radio telekommunikasie netwerke is gemeet om te bepaal of dit voldoen aan nasionale sowel as internasionale spesifikasies. Die een netwerk se topologie het bestaan uit 3 radio herleiers en 84 afstandbeheer stelle en het 'n gemiddelde gemete benutting van 17 % en 'n piek benutting van 25 % gehad. Die ander netwerk se topologie het bestaan uit 3 radio herleiers met 20 afstanbeheer stelle en het 'n gemiddelde gemete benutting van 3 % het 'n piek benutting van 8 % gehad. Dit val binne die IEEE standaard 999-1992 [20] wat 'n benutting van tussen 40 % and 60 % aanbeveel.

Sleutelwoorde : Sleutel prestasie indikators, Radio telekommunikasie netwerke, Afstandbeheerstelsel

Contents

Section **Page**

List of symbols

ALP	Application Layer Protocol
ANSI	American National Standards Institute
ANSI-HSSP	The American National Standards Institute's Homeland Security Standards Panel
ARC	Auto Re Close
BER	Bit Error Rate
b/s	Bits per second
CASM	Common Applications Services Model
CBM	Condition Based Maintenance
CD	Collusion Detection
CSMA	Carrier Sense Multiple Access
CSR	Control Success Rate
dB	Decibel
DC	Direct Current
DLL	Data Link Layer
DNP3	Distributed Network Protocol version 3
DOL	Data Object Library
DOM	Design out Maintenance
DRTU	Distribution Remote Terminal Unit
DS	Direct Sequence
EPA	Enhanced Performance Architecture
EPRI	Electric Power Research Institute
ERP	Effective Radiated Power
ETSI	European Telecommunications Standards Institute
EV	Estel Variant
FBM	Failure Based Maintenance
FCC	Federal Communications Commission
FH	Frequency Hopping
GOMSFE	Generic Object Models for Field Equipment
ICASA	Independent Communications Authority of South Africa
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
KEPCo	Kansas Electric Power Cooperative
KPI	Key Performance Indicator
MDS	Microwave Data Systems
MODEMS	Modulator / Demodulators
NRTC	the National Rural Telecommunications Cooperative
PLC	Power Line Carrier
PMRTU	Pole Mount Remote Terminal Unit
PTT	Press To Talk
RBE	Report by Exception
RCM	Reliability Centred Maintenance
RF	Radio Frequency
RTF	Run to Failure
RTU	Remote Terminal Unit
SABRE	South African Band Re-planning Exercise
SCADA	Supervisory Control and Data Acquisition
SEF	Sensitive Earth Fault
TBM	Time Based Maintenance
TCP/IP	Transmission Control Protocol and Internet Protocol
UBM	Used Based Maintenance
UHF	Ultra High Frequency
UPS	Uninterruptible Power Supply
UCA	the Utility Communications Architecture
U.S	United States
W	Watt

List of figures

List of tables

1. Project description and motivation

1.1. Overview

Supervisory Control and Data Acquisition (SCADA) is a process control system that enables a system operator to monitor and control processes distributed among various remote sites. A properly designed SCADA system saves time and money by eliminating the need for service personnel to visit each site for inspection, data collection and logging or to make adjustments. Real-time monitoring, system modifications and troubleshooting as well as increased equipment life and automatic report generation are just a few of the benefits that come with modern SCADA systems.

In South Africa, the local electricity utility ESKOM, uses SCADA systems mainly for the following:

- Supervising and control of Power Generation (Power Stations).
- Supervising and control of Electrical Networks (Transmission and Distribution).

The SCADA master stations are situated at various control centres where control personnel supervise and manage the electrical network on a 24 hour basis. At these centres alarms from the remote sites are received and acted upon. Controls are dispatched to open or close breakers and to tap transformers manually. Measured analogue values are also displayed at the SCADA master, including variables such as voltage, current and frequency measurements from remote sites.

All SCADA systems need to be optimised to ensure a reliable system that will meet the demands of the power utility personnel and electrical consumers. Where problems occur, one will often find the following generalized statements and complaints:

- The SCADA system never works when needed.
- Breakers do not close when the controls are dispatched.
- The SCADA system is unreliable.

Most of these complaints are normally based on perceptions due to one or two incidents that stood out over a period of time. Quite often it is found that the complainants do not understand how the system functions and are just making general statements. It is therefore important that all personnel involved must be well trained and have the knowledge to assess the performance of the system. Optimisation of the system should be conducted on a continuous basis. Over time the reliability of the system will increase as SCADA personnel learn the SCADA system details and achieve a better understanding of the system.

1.1.1. A brief history

SCADA began in the early 1960s as an electronic system operating as input and output transmissions between a master station and a remote station. Each master was connected to its own remote. The master station would receive data through a telemetry network and then display this on a panel which was a big wall that housed lights to present alarm and other conditions. Analogue values were presented by analogue electro – mechanical meters. Controls were initiated by pressing switches on the panel. The whole plant that was supervised by the system was graphically presented on the panel.

In the early 1970s, Distributed Control Systems (DCS) were developed to control separate remote subsystems and in the 1980s, with the development of the microcomputer, process control could be distributed among remote sites. Further development enabled DCS to use programmable logic controllers, which have the ability to control sites without taking direction from a master.

In the late 1990s, SCADA systems were built with DCS capabilities and systems were customized based on certain proprietary control features built in by the designer. Recently, with the Internet being utilized more as a communication tool, SCADA and telemetry systems are using automated software with certain portals to download information or control a process. This however also introduced the security risk in the form of cyber attacks and software viruses. Engineered SCADA systems today not only control processes but are also used for measuring, forecasting, billing, analyzing and planning. Modern SCADA system must meet a whole new level of control automation while interfacing with obsolete equipment yet remain flexible enough to adapt to future developments

SCADA systems are used mainly in industrial processes: e.g. steel making, power generation (conventional and nuclear) and distribution and chemistry. The configuration of a typical RTU will vary from a few Input/Output (I/O) points to several 10 thousands I/O points. The topology of a typical SCADA system is shown in Figure 3.1. There will be some Man Machine Interface (MMI) which is typical a Visual Display Unit (VDU) or computer monitor, keyboard and mouse. The MMI is connected to the SCADA master, which is connected to some communication system. The communication medium may be copper wire, microwave radio, area radio, optical fibre cable or a standard Local Area Network (LAN). This communication network enable the SCADA master to communicate with the Remote Terminal Units (RTUs) which is connected to the plant which is monitored by the SCADA master.

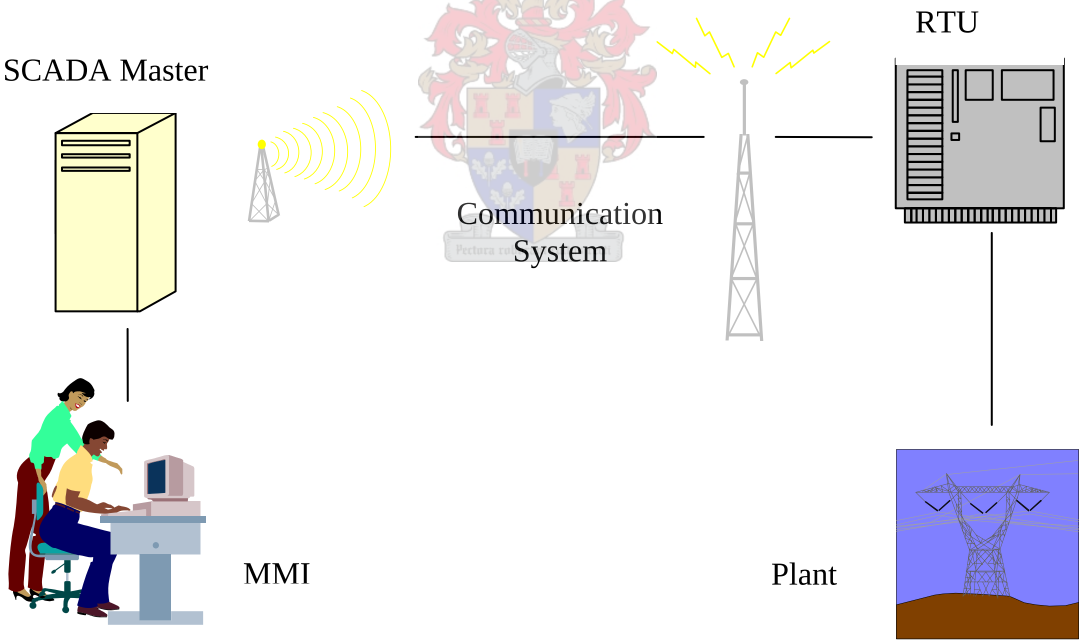


Figure 1.1. Basic SCADA System Topology.

The SCADA system will have the following basic messages between the SCADA Master and RTU:

- Control execute (e.g. execute control, raise or lower transformer taps).
- Control return message (e.g. the control executed successful).
- Analogue change of state (e.g. analogue change from 456 A to 478 A).
- Digital input change of state (e.g. alarm on/off).
- Resynchronise RTU (reset all parameters e.g. time).

The SCADA system assists the control personnel to supervise the system which they need to control. It supplies them with the necessary information to manage the network and give them the ability to run the network at its optimum. Operating personnel will be able to act on alarms received by the MMI and select controls to execute. These controls will include opening and closing of breakers at the sub stations and raising or lowering taps of transformers. When a critical alarm is received at the control centre the operating personnel may dispatch service personnel to investigate at the site and take corrective action. Information coming from the SCADA master also assists the network optimisation personnel to forecast the load on the electrical network as well as planning future network expansion.

1.2. Factors affecting the performance of a SCADA system

1.2.1. Introduction

Any one of the following factors will affect the performance of a typical SCADA system:

- Operating personnel competency.
- Integrity of the SCADA database.
- Failure of the SCADA master.
- The availability of the telecommunication network.
- The condition of the Remote Terminal Unit (RTU) at the remote sites.
- The condition of the plant that is supervised by the SCADA system.

The remainder of this section gives a brief discussion of the abovementioned aspects.

1.2.2. Operating personnel competency

Incorrect controls being dispatched will affect the performance of the control success rate. A good example is when a control is dispatched to a Remote Terminal Unit (RTU) during an interrogation cycle or when a RTU has just been reset. This may cause the SCADA master to time out due to the delay in communication between the RTU and master. The incorrect interpretation of alarms and analogues received at the control centre may also affect the integrity of the system.

1.2.3. Integrity of the SCADA database

If the database is not setup correctly it may cause the controls not to execute or the control may be sent out to the wrong RTU of device. For example Breaker 1 will open instead of Breaker 2. If the digital inputs coming from the RTUs are not programmed correctly the incorrect alarm or analogue value may be displayed.

1.2.4. Failure of SCADA master

The SCADA master may fail due to hardware failure of subsystems such as the server and communication equipment (e.g. local area network, modems, etc) and cable and wiring faults. In practice it is also possible that data corruption on the SCADA master servers may occur. It is therefore important to have a warm standby system available to take over the functions in the case of a failure. This will ensure a high availability of the SCADA system.

1.2.5. The availability of the telecommunication network

Controls will not execute if the telecommunication system are down or if there are a high amount of noise present on the system. No alarms or analogues will be received from the RTU at the Master. This will lead to delayed restoring time of the electrical network which will affect electricity sales and will influence customer satisfaction.

The weather condition at a specific time could affect the communication network as adverse weather conditions may degrade the performance of the telecommunication network and messages to and from the SCADA master will be corrupted or delayed. During adverse weather conditions there will also be much more state changes from the RTU to the master due to trips, alarms and analogue changes. This will cause the network to overflow with communication data and will result in data loss or delayed information. It is possible that alarm conditions of breaker trips are only received at the SCADA master hours after it was initiated at the RTU.

1.2.6. The condition of the RTU at the remote sites

The performance of the SCADA system will be affected if there are any hardware failures at the RTU or if the RTU is not setup and programmed correctly. A power failure at the RTU will also affect the system. It is therefore very important that adequate battery power backup is installed at the RTU and that the Direct Current (DC) system is maintained at regular intervals. Antenna alignment as well as the physical condition of the coaxial cable at the RTU are also contributing factors to the performance of the SCADA system.

1.2.7. The condition of the plant that is supervised by the SCADA system

Controls dispatched to the RTU will fail if the breaker that must be operated in the field is faulty. The same will account for a situation where the physical electrical line is broken and lying on the ground. The protection system will inhibit the execution of the control if there is any fault condition on the electrical network. This will cause a control fail message at the control centre.

1.3. Optimisation of SCADA systems

It is important to measure the performance of the SCADA system in order to determine if there are any problem areas that can be improved on. Figure 1.1 shows a block diagram of a typical performance measurement cycle. The first step is to define a Key Performance Indicator (KPI) and set a target to achieve. The measured performance indicator is then compared with the set target. An investigation should follow if the target is not achieved. A report coming from the investigation should propose changes that may be implemented to enhance the performance of the system. After implementation the performance must be evaluated again and if necessary the target may be adjusted accordingly. If the target is achieved it must be re-evaluated to determine if the target is meaningful and if necessary the target should be adjusted accordingly. This performance measurement cycle should be a continuous process.

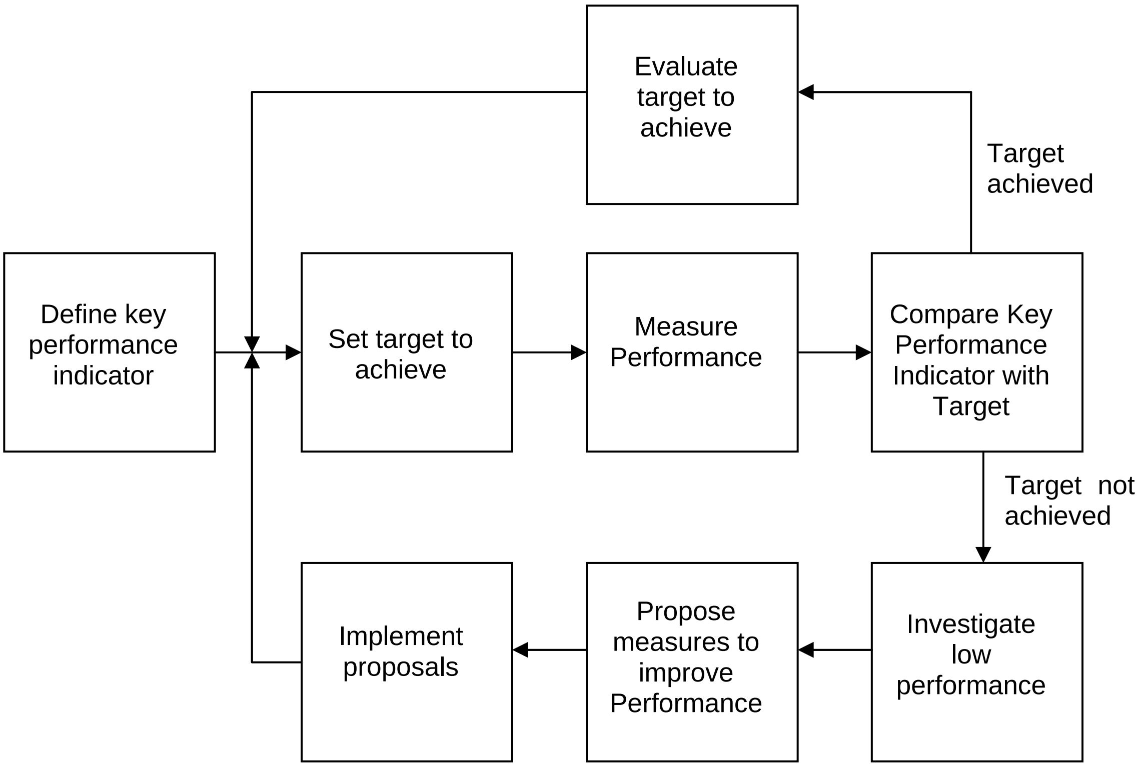


Figure 1.2. Block diagram of a performance measurement cycle.

The communications link is a critical element in any SCADA network. A reliable, cost-effective means for transporting data must be employed if the full benefits of SCADA are to be realized. At the power stations the communication medium between the SCADA Master and Remote Terminal Units (RTUs) covers relatively short distances and is hard wired with either twisted pair copper wire or optical fiber cable. Both these mediums are highly reliable.

For transmission and distribution systems the communication links typically employs optical fiber cabling, Ultra High Frequency (UHF) radio, microwave transmission and Power Line Carrier (PLC) systems. PLC systems are the least used and are currently being phased out. PLC systems will therefore not be considered in this investigation. The optical fiber cables and microwave systems are highly reliable and are managed by bandwidth management systems that auto reroute communications in case of fading, node failure or data loss. Error correction and packet switching are used that results in availability of close to 100% on these systems.

The area radio systems where all RTUs communicate through UHF repeaters are not always reliable, especially in adverse weather conditions and with high data traffic load. However, radio links present an attractive option to many users because it offers reasonable high availability, eliminates the ongoing payment of access fees, and allows users to have direct control over their systems. It is often the chosen medium when one or more sites are outside the coverage area of microwave and optical fiber systems and where continuous monitoring of data is required.

1.4. Research objectives

1.4.1. Overview

With the current expansion of the electrical network and associated SCADA systems it has become necessary to track the performance of the SCADA systems. This raises the following key research questions:

- How can the performance UHF area radio SCADA networks be measured?
- How can the factors contributing to weak performance be identified?

Initial studies have shown that the area radio network is currently the worst performing communication type. Therefore, the aim of this investigation is to perform an in-depth study of the current UHF area radio SCADA telecommunication network and identify the parameters that can be changed to improve the performance of the system. The key question defined above gives rise to the following detailed research objectives:

- Define Key Performance Indicators (KPIs) to monitor performance.
- Develop a data mining tool to measure the KPIs.
- Measure SCADA system performance.
- Measure the network and repeater utilisation.
- Determine RTU message types per network.
- Determine maintenance philosophies and procedures.

The remainder of this section discusses the abovementioned research objectives in more detail.

1.4.2. Define key performance indicators

Performance indicators need to be defined in order to track the performance of the RTUs, communication protocols, repeaters and networks. International, local and self-defined indicators will be studied to establish the best practice for this specific project.

1.4.3. Data mining tool

There is a need for a data-mining tool to supply and trend the performance indicators to measure the SCADA system performance. Detail specifications for the tool will be defined and the tool will be developed. Ideally the data should be captured and stored in a database with a user-friendly interface. Relevant queries and reports will be developed to assist with the performance measurement.

The above data will be analysed on the SCADA master that will supply availability information with regards to specific RTUs. The availability per RTU, RTU type and RTU protocol can be measured from the above mentioned data. This data must be captured and analysed over a period of time to measure the performance of the system more accurately.

The physical configuration of the communication systems needs to be established and captured into the data-mining tool. This includes the list of communication networks, radio repeaters and the RTU names per repeater. This configuration will assist us to calculate the performance per network, repeater and per RTU.

1.4.4. Measure the SCADA system performance

The performance data generated by the SCADA master will be imported into the data mining tool weekly and relevant queries and reports will be generated. The performance tool will supply detail performance of the SCADA system with reference to parameters such as RTU type and protocol, individual repeater network performance and network.

Due to refurbishment projects SCADA systems change over time. RTUs get replaced due to reasons such as the need to upgrade outdated technology, unacceptable performance levels of equipment, national contract awarded change from one company to another and the expansion at the site (more functionality or I/O points needed at the site). RTU protocols are normally company specific and some companies use non-open protocols. This will mean in practice that more that one protocol will be used on the same communication network. Some protocols are more robust that other and will force itself over another. This will result in data loss on the network.

Research will be done to establish the influence that different protocols will have on the performance of a network. If necessary the networks will then be redesigned in such a way that only one protocol will be used on a system. The performance of the single protocol network will then be compared with the performance of the multiple protocol networks.

The physical distance between the RTU and the repeater will affect the signal strength at both ends and thus will influence the performance of the network. The maximum power output of the repeater is fixed as defined by the Independent Communications Authority of South Africa (ICASA). The only changes that can be implemented are the following:

- Distance between RTU and repeater.
- Antenna type at the RTU.
- Coaxial antenna cable type at the RTU.
- Coaxial antenna cable length at the RTU.
- Receive radio sensitivity at the RTU.

The signal strength at the RTUs will be investigated and compared with manufacturer standard and ESKOM national standards. The strength of radio signals in a well-designed SCADA system must exceed the minimum level needed to establish basic communication. This excess strength is known as the fade margin, and it compensates for variations in signal level, which may occur from time to time due to foliage growth, minor antenna misalignment, or changing atmospheric losses

1.4.5. Measure the network and repeater utilization

Research will be done to establish the utilisation per repeater and network. This measurement is the percentage of time that the network is busy per 24 hours. This data must be stored in a SQL database that will assist with data mining. Due to the expansion of the SCADA networks there is need to know how new RTUs will affect the current telecommunication system. If a certain network is already used at its optimum any more traffic on the network will negatively influence the performance of the network.

For this project two networks will be chosen where the usage will be captured and analysed for at least one month to establish network utilisation. These values will be compared with national and international recommended network utilisation values. This will assist with determining the maximum number of RTU configuration for that specific network and to establish a standard for other networks.

1.4.6. Determine remote terminal unit message types per network

The combination of this measurement and the network usage as described above will assist with network expansion and also with the setup of current RTUs, repeaters and networks. The same networks will be used to capture all messages and store this information in a SQL database. This data will make it possible to calculate the percentage of usage per message type and then derive a standard setup for specific RTU types, for example the analogue message updates times.

RTUs will only transmit an *analogue update* message to the SCADA master when there is a change to the current analogue value. Analogue updates to the SCADA master will be continuous or very frequent at a site where analogue values change quite often, for example a furnace or at traction sub stations. This excessive analogue update will result in the data congestion of the telecommunication network. To minimise analogue updates to the SCADA master an analogue update window or also called jitter factor is programmed into the analogue inputs of the RTU. This will define a window in which an analogue may change or drift before an analogue update message will be transmitted to the SCADA master and thus reduce the number of updates. This parameter is user definable and assists with traffic reduction on the communication systems.

With the knowledge of analogue percentage of the communication traffic it will be possible to optimise the analogue window values. This will also assist with future expansion as a calculation can be done to determine beforehand how the system will be influenced by the new analogues that will be added to the current network.

1.4.7. Determine maintenance philosophies and procedures

The information coming from the investigations and performance data will assist to establish RTU specific maintenance philosophies and procedures. Over time, any communications system requires a degree of preventive maintenance to ensure peak operating efficiency. Periodic checks of master and remote sites should be made to identify and correct problems before they become threats to system operation.

Practice has shown that power supplies and battery failures, poor cable connections and signal strength problems cause most RTU failures. It will thus only make sense to specifically maintain these areas on a regular basis. Signal strength problems are mainly causes by poor antenna installations, the accurate alignment of directional antennas and the coaxial feeder cable. These cables degrade due to weather and high temperature conditions and quite often it is found that water has seeped into the cable, which has a detrimental effect on the impedance of the coaxial cable and will result in the loss of signal strength.

2. Literature study

The literature study focuses on a number of issues, namely

- Supervisory Control and Data Acquisition (SCADA) standards organizations.
- Protocol standards.
- Performance measurement of SCADA systems.
- Design of SCADA systems on area radio networks.
- Network utilisation.
- Maintenance philosophies of SCADA systems.
- Conclusions.

The remainder of this chapter discusses each of the aspects in detail and compare ESKOM standards with international standards.

2.1. Supervisory control and data acquisition standards organizations

There are many organizations involved in the standardization of Supervisory Control and Data Acquisition (SCADA) systems. This section details some of these organizations and the roles they play. [21]

2.1.1. The Institute of Electrical and Electronics Engineers

The IEEE Standards Association (IEEE-SA) is a membership organization that produces electrical and Information Technology (IT) related standards that are used internationally. The IEEE has been involved in standardizing technologies for many years. The two standards that have been published by the IEEE with respect to SCADA systems are discussed below: [21]

IEEE Std 999-1992 – IEEE Recommended Practice for Master/Remote SCADA Communications. This recommended practice applies to the use of serial digital transmissions by SCADA systems having geographically dispersed terminals. These types of systems typically utilize dedicated communication channels, such as private microwave channels or leased telephone lines, which are limited to data rates of less then 10,000 b/s.

IEEE Standard 1379-2000 – IEEE Recommended Practice for Data Communications between Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IED's) in a Substation. This recommended practice presents a uniform set of guidelines for communications and interoperation of IED's and RTUs in an electric utility substation. This recommended practice does not establish an underlying communication standard. Instead, it provides a specific limited subset of two existing communication protocols and encourages understanding and timely application.

2.1.2. American National Standards Institute

The American National Standards Institute (ANSI) is a private, non-profit organization that administers and coordinates the United States (U.S.) voluntary standardization and conformity assessment system [21]. The Institute's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.

The mission of The American National Standards Institute's Homeland Security Standards Panel (ANSI-HSSP) is to identify existing consensus standards, or, if none exists, assist the Department of Homeland Security (DHS) and those sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security. The ANSI-HSSP promotes a positive, cooperative partnership between the public and private sectors in order to meet the needs of the nation in this critical area.

Established by ANSI in February 2003, the ANSI-HSSP's scope is to catalog, promote, accelerate and coordinate the timely development of consensus standards within the national and international voluntary standards systems intended to meet identified homeland security needs, and communicate the existence of such standards appropriately to governmental units and the private sector. The panel will initially focus its activities on responding to the most immediate standards needs of DHS.

2.1.3. Electric Power Research Institute

The Electric Power Research Institute (EPRI) was founded in 1973 [21] as a non-profit energy research consortium for the benefit of utility members, their customers, and society. Their mission is to provide science and technology-based solutions of indispensable value to global energy customers by managing a far-reaching program of scientific research, technology development, and product implementation.

With expertise in a wide spectrum of scientific research, technology development, and product application, EPRI [21] is able to offer solutions that cut across traditional boundaries, taking advantage of the latest advances in many fields. EPRI provides the knowledge, tools, and expertise you need to build competitive advantage, address environmental challenges, open up new business opportunities, and meet the needs of your energy customers.

EPRI has developed The Utility Communications Architecture (UCA) [21] to integrate communications for "real-time" utility operations for SCADA systems. The UCA is the only existing protocol that provides interoperability among different monitoring and control equipment and interconnectivity among databases for utility operations. The UCA Version 2 specification has been recently published by the Institute of Electrical and Electronic Engineers (IEEE) Standards Board as technical report TR1550 [23]. EPRI takes great pride that the UCA technology has been published by the IEEE. In addition, UCA is in review by the International Electrotechnical Commission (IEC) to become the international standard for integrated utility operations. The new UCA Version 2 includes four parts that are published in two volumes, as follows: [21]

Part 1: Introduction. Gives an overview of the UCA Version 2. This document presents a background, philosophy, and applications of UCA to provide a basic understanding of UCA.

Part 2: Profiles. Presents the profiles and protocols for various communication media, including local area networks, radio, optical fiber network, and telephone; including guidelines on the use of the Internet protocols in a UCA context.

Part 3: Common Applications Services Model (CASM). Describes models for device behavior from a UCA communications perspective; it also defines the language, services, semantics, and applications of UCA.

Part 4: Generic Object Models for Field Equipment (GOMSFE). Presents a detailed list of device object models for a wide range of substation and distribution field equipment, including breakers, relays, sectionalizes capacitor controllers, Remote Terminal Units (RTUs), and other Intelligent Electronic Devices (IEDs).

2.1.4. International Electrotechnical Commission

The International Electrotechnical Commission (IEC) Technical Committee 57 Working Group 03 (TC57 WG03) was chartered to develop protocol standards for telecontrol, teleprotection, and associated telecommunications for electric utility systems, and it has created IEC 60870-5 [21], a group of five utility-specific protocol standards. IEC 60870-5 specifies a number of links, frame formats, and services that may be provided at each of three layers. IEC 60870-5 uses the concept of a three-layer Enhanced Performance Architecture (EPA) reference model for efficiency of implementation in devices such as RTUs, meters, relays, etc. used in SCADA systems.

IEC 60870-5 specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer EPA reference model for efficient implementation within RTUs, meters, relays, and other IEDs. Additionally, IEC 60870-5 defines basic application functionality for a user layer, which is situated between the OSI application layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers. The following descriptions provide the basic scope of each of the five documents in the base IEC 60870-5 telecontrol transmission protocol specification set. Standard profiles are necessary for uniform application of the IEC 60870-5 standards. Such profiles have been and are being created. The Standard 101 profile is described in detail following the description of the applicable standards.

IEC 60870-5-1 (1990-02) [21] specifies the basic requirements for services to be provided by the data link and physical layers for telecontrol applications. In particular, it specifies standards on coding, formatting, and synchronizing data frames of variable and fixed lengths that meet specified data integrity requirements.

IEC-60870-5-2 (1992-04) offers a selection of link transmission procedures using a control field and optional address field; the address field is optional because some point-to-point topologies do not require either source or destination addressing.

IEC 60870-5-3 (1992-09) specifies rules for structuring application data units in transmission frames of telecontrol systems. These rules are presented as generic standards that may be used to support a great variety of present and future telecontrol applications. This section of IEC 60870-5 describes the general structure of application data and basic rules to specify application data units without specifying details about information fields and their contents.

IEC 60870-5-4 (1993-08) provides rules for defining information data elements and a common set of information elements, particularly digital and analog process variables that are frequently used in telecontrol applications.

IEC 60870-5-5 (1995-06) defines basic application functions that perform standard procedures for telecontrol systems, which are procedures that reside beyond layer 7 (application layer) of the ISO reference model. These utilize standard services of the application layer. The specifications in IEC 60870-5-5 (1995-06) serve as basic standards for application profiles that are then created in detail for specific telecontrol tasks.

Each application profile will use a specific selection of the defined functions. Any basic application functions not found in a standards document but necessary for defining certain telecontrol applications should be specified within the profile. Examples of such telecontrol functions include station initialization, cyclic data transmission, and data acquisition by polling, clock synchronization, and station configuration.

2.1.5. DNP3 users group

The development of Distributed Network Protocol version 3 (DNP3) was a comprehensive effort to achieve open, standards-based interoperability between substation computers, RTUs, IEDs (Intelligent Electronic Devices) and master stations (except inter-master station communications) for the electric utility industry for SCADA systems [1],[21]. Also important was the time frame; the need for a solution to meet today's requirements. As ambitious an undertaking as this was, the objective was achieved. Since the inception of DNP, the protocol has also become widely utilized in adjacent industries such as water/waste water, transportation, and the oil and gas industry.

DNP3 is based on the standards of the International Electrotechnical Commission (IEC) Technical Committee 57, Working Group 03, who have been working on an OSI 3 layer “Enhanced Performance Architecture” (EPA) protocol standard for telecontrol applications. DNP3 has been designed to be as close to compliant as possible to the standards, as they existed at time of development with the addition of functionality not identified in Europe but needed for current and future North American applications (e.g. limited transport layer functions to support 2K block transfers for IEDs, RF and fiber support). DNP3 has been selected as a Recommended Practice by the IEEE C.2 Task Force; RTU to IED Communications Protocol.

DNP3 was developed by Harris, Distributed Automation Products. In November 1993, responsibility for defining further Distributed Network Protocol version 3 (DNP3) specifications and ownership of the DNP3 specifications was turned over to the DNP3 Users Group, a group composed of utilities and vendors who are utilizing the protocol [21].

DNP3 is an open and public protocol. In order to ensure interoperability, longevity and upgradeability of protocol, the DNP3 User Group has taken ownership of the protocol and assumes responsibility for its evolution. The DNP3 User Group Technical Committee evaluates suggested modifications or additions to the protocol and then amends the protocol description as directed by the User Group members.

Complete documentation of the protocol is available to the public. The four core documents that define DNP3 are: Data Link Layer Protocol (DLL) description, transport functions, Application Layer Protocol (ALP) description, and Data Object Library (DOL) (referred to as the "Basic 4 Document"). The User Group also has available to members the document "DNP3 Subset Definitions" which will help implementers identify protocol elements that should be implemented [21].

2.2. Protocol standards

2.2.1. International protocols

As mentioned in 2.1. the following international standards currently defines RTU protocols:

- IEC 60870.
- Distributed Network Protocol version 3 (DNP3).
- Modbus.

For the purpose of this investigation only IEC 60870 [2] and DNP3 [1] will be discussed as Modbus is strictly more for programmable logic controllers rather than RTUs. Both standards are well defined and governed by some organisation. The IEC set the standard for IEC 60870 and the DNP users group governs the DNP3 protocol. The IEC (International Electrotechnical Commission) published the first standard in 1988 and the following parts were covered [2]:

- Basic concepts.
- Environmental characteristics.
- General principles of data integrity.
- A three-layer stack architecture.
- Data link service.
- Application functions.
- Data formats.
- Application objects.
- Testing.

The IEC 60870-5-1 to IEC 60870-5-5 series of standards [2] present general definitions for communication protocols, while the IEC 60870-5-101 presents a profile for an Electric Power SCADA protocol. It was first published in 1995 and the updated second edition in February 2003. The IEC 60870-5-104 was published in 2000 [2] and describes the transport of IEC 60870-5-101 application data over network transports such as TCP/IP. This used mainly for substation automation where all the SCADA, Protection, metering and other intelligent substation devices are connected onto one bus. The IEC 60870-5-101 and IEC 60870-5-104 standards are widely adopted in Europe, the Middle East and Latin America.

While the IEC 60870-5-101 is specifically an electric power-orientated protocol, Distributed Network Protocol version 3 (DNP3) is a more generic SCADA protocol. DNP3 was developed by a Harris controls division and was placed as public domain in 1993. A DNP3 users group was formed to assume technical responsibility for the extension and enhancement of the protocol. DNP3 is well supported in North America, Australia and shares the electrical market in Asia, Africa and South America.

Of the two protocols, only the DNP3 protocol is implemented on the ESKOM SCADA networks. In the Western region this was only done during the end of 2004 and this protocol is currently the worst performing protocol on the UHF area radio network in the region. This may be due to teething problems. Both standards do not define the usage of Ultra High Frequency (UHF) area radio networks, but rather expect a good wideband communication network. The ESKOM networks are configured as Report By Exception (RBE) also known as unsolicited reporting where only status changes in the field will be reported to the SCADA Master. This technology improves the efficiency of the networks as they save network usage. Both protocols support RBE.

DNP3 supports “unsolicited reporting” [1] where a RTU report events without being polled by the MASTER. The IEC 60870-5-101 [2] also supports an “unsolicited” reporting mode, but only with a dedicated point to point communication channel.

2.2.2. Protocols used by ESKOM

ESKOM currently use the following protocols for RBE and unsolicited reporting.

- DNP3.
- EV (Estel Variant – ESKOM protocol).
- INTRAC (Motorola proprietary protocol).
- MDLC (Motorola proprietary protocol).

INTRAC and MDLC are currently being phased out and the investigation will only focus on EV and DNP3.

EV [4], [5], [6] is the only protocol specifically designed for UHF area radio networks due to a unique need in ESKOM distribution. EV was designed from the ESTEL protocol which is a solicited reporting protocol also using RBE. The ESTEL protocol was also designed by ESKOM, but is an open protocol. It was however only used by ESKOM. None of the above protocols specify the following:

- Maximum of RTUs per communication line.
- Performance measurement of RTUs.
- Communication design specifications.
- Preferred communication type.

2.3. Performance measurement of SACDA systems

2.3.1. Performance measurement used in the ESKOM distribution system.

Two documents were found within ESKOM describing performance measurement on SCADA systems. The ESKOM distribution standard [8] (SCSASACE2) describes the following two performance indicators, namely RTU Availability (RTU Avail) and Control Success Rate (CSR).

RTU availability measures in percentage the amount of time that the master polled the remote and if the remote responded successfully to the poll. This will test the Master, communication equipment and the remote. The formula for RTU availability is described by the relationship [8]

$$\text{RTU Avail} = \frac{No.\,of\ successful\ RTU\ responses\ to\ polls}{Total\ no.\,of\ RTU\ polls} \times 100\%. \qquad (2.1)$$

Control success rate measures in percentage the number of controls that was initiated by the master and of which the master received an “execute successful message” from the remote. The formula for RTU availability is described by the relationship [8]

$$\text{CSR} = \frac{Total\ no.\,of\ controls\ despatched - Total\ no.\,of\ unsuccessful\ controls}{Total\ no.\,of\ controls\ despatched} \times 100\%. \qquad (2.2)$$

RTU availability will give a good indication of the condition of the communication equipment, while CSR will also measure the performance of the SCADA master, control personnel, the RTU and the plant in the field.

2.3.2. Performance measurement used in the ESKOM transmission system.

The ESKOM transmission standard is currently in draft form [9] and describes two Key Performance Indicators (KPIs), namely Control System Availability Index (CSAI) and Control Command Dependability Index (CCDI).

The purpose of the Control System Availability Index (CSAI) is to indicate the reliability of the Control System in relation to the ratio of the total number of hours that service was available, to the total number of hours it was demanded or needed. These measures will be affected at RTU level. The formula for CSAI is described by the relationship [9]

$$\text{CSAI} = \frac{(D-E)-I}{(D-E)} x100\% \qquad (2.3)$$

where D denotes the total number of hours control system was demanded, I denotes the total number of hours of interruption and E denotes the total hours of outages.

The purpose of Control Command Dependability Index (CCDI) index is to measure the success rate of Control Commands being issued. Any control cards failures and configuration inaccuracies resulting in control command issued not being successful will be counted against the CCDI. The formula for CSAI is described by the relationship [9]

$$\text{CCDI} = \frac{S-Q}{S} x100\% \qquad (2.4)$$

where S denotes the total number of controls issued and Q denotes the total number of controls failed after being issued.

In both cases the two performance indicators are describing the same measurement and will be good indicators to use.

2.3.3. International standards

Performance measurement is defined in the paper "Quality Of Service In The NOMOS TMN System" [11], which was presented at the international conference on "Power Sector Telecommunication System for the 21st Century" in Nueva Delhi India (January 1997).

The following KPIs are defined in the paper: [11]

- Availability.

  This information is obtained from the availability log of their SCADA system

- Mean Time Between Failures (MTBF).

  The MTBF information is also obtained from the availability log.

- Mean Time to Repair (MTTR).

A work management system is needed to obtain this information to measure the MTTR. All work that technical personnel do on the equipment must be logged on the system with all relevant information. The most important information is the following:

- Date and time of the failure.
- Reference number of the fault.
- Name of the site at which work was done.
- Detail information regarding failed equipment at the site.
- Arrival time at site.
- Date and time that work was started at the site.
- Date and time that the failure was cleared at the site.
- Detail of the work done at the site.

The time to repair is calculated from the date and time that the failure cleared and the date and time that work was started at the site. The data from the work management system should also correspond to the failures in the availability log.

Two journals were found that described performance measurement on SCADA systems, namely:

- ESTELLE: A method to analyze automatically the performance of telecontrol protocols in SCADA systems [24].
- A framework for the specification of SCADA data links [25].

The authors of the paper on the ESTELL technique of measuring performance [24] describes methods to automatically calculate and measure the performance of SCADA systems. The ESTELL technique analyzes the performance of SCADA protocols and compares this with analytical and measured results. It does not measure the performance of the SCADA system as whole, but rather focus on the performance of individual SCADA protocols. This technique will work well for protocol designers and with new protocols implementations; however it will not work for this specific thesis as it is not possible to choose between protocols as standard SCADA protocols already have been implemented in ESKOM. A better solution will be to measure the performance of the current SCADA systems and try to implement measures to improve the overall performance of the low performance telecommunication networks, radio repeaters and RTUs.

The framework for the specification of SCADA data links [25] focus on the performance of the telecommunication system between the front end processor at the SCADA master and the RTU at the sub station. The effect of the bit error rate (BER) of a communication link is discussed and it was found that the performance of a telecommunication network will degrade when the BER exceeds 1 error in 10^4 (a BER of 10^{-4}) [25]. It is also stated that it is possible that the SCADA master will not detect the low performance or performance degrading of a telecommunication network, as this will rather be picked up by analyzing the performance of the system by a third party. For this thesis it will be impossible to measure BER on the ESKOM

SCADA telecommunication lines as all lines are constantly in use by the SCADA system and cannot be taken out of service for a period of time to measure the BER.

The time delay or status update time from when a status change occurred at the RTU and the time that the status change was received at the SCADA master was also measured [25]. This measurement will give a good indication of the data traffic congestion on a telecommunication network as this time will increase with high network utilization. It is however not possible to measure this time due to the setup of the current r*eport by exception* networks as implanted by ESKOM. The Estel Variant (EV) protocol does not allow the *change of state* messages to be time stamped at the RTU and only the SCADA master will stamp the time of data reception, which make the calculation impossible. ESKOM also did not implement time stamping of the *change of state message* with the DNP3 protocol on the *report by exception* telecommunication networks, although the protocol does allow this function.

The control response time was also measured and is defined as the time measured from when a control was executed at the SCADA master until the master have received a successful execute message from the RTU [25]. This time will vary between different protocols as each protocol defines a secure control differently. The EV protocol for example will first transmit a *control select* message and will wait for a reply from the RTU and will then follow with *control execute* message. The RTU will then reply with an *execute successful* message, but the SCADA master will only accept the control to be successful when a *status change* message is received from the device that the control was executed on. The SCADA master will see a c*ontrol execute* as failed if this time is exceeded beyond a predefined time even if the control was successful.

The data to calculate the control response time with should be available from the SCADA master. This data is however stored in a log file and not in a data table, which make it difficult for mathematical calculations and to run data queries on. The SCADA master does however log the amount and detail of control failures and manual investigations on these control failures should supply the number of failures due to telecommunication related timeouts. This will be measured in the chapter 5 which focuses on control success rate.

2.4. Telecommunication system design standards

2.4.1. ESKOM standards documents

Two documents were published with regards to design standards pertaining to design standards, namely “Telecommunications Guideline: Antenna Selection for Telecontrol RTU Applications” [17] and “Telecommunications: High-Level User Requirements for Telemetry Communications in Distribution” [18]. Telecommunications Guideline: Antenna Selection for Telecontrol RTU Applications” [17] focus mainly on antenna type, signal strength, earthling, coaxial cables and connectors, while Telecommunications: High-Level User Requirements for Telemetry Communications in Distribution [18] describes the user requirements for an area radio telecommunications system. The documents are discussed in more detail as below.

2.4.2. Antenna types

Different antenna types such as whip antennas, dipoles and corner reflector antennas are discussed [17] and it is recommend that whip antennas should only be used indoors where the signal strength is good. Dipoles should be used for normal used and a stacked dipole should be used where high gain is required. Corner reflectors should be used with RTUs with very low signal levels and in areas with lots of Radio Frequency (RF) interference.

2.4.3. Signal levels

The signal levels should be measured to the nearest repeater an should not exceed the design threshold of -90dBm, while the Effective Radiated Power (ERP) should not exceed the Independent Communications Authority of South Africa’s (ICASA) regulation of 20 W [17]. The relationship between the power measured at the antenna, the gain of the antenna and the ERP is shown in the following Table 2.1.

Note that the gain of the antenna is measured in dBd and not dBi. This differs sometimes from manufacturer to manufacturer. The formula to convert between dBi and dBd is

$$\text{dBi} = \text{dBd} + 2.15.$$

Table 2.1. Effective Radiated Power derived from the relationship between the power measured at an antenna and the gain of the antenna. [17]

	Gain of Antenna (dBd)									
Power at the Antenna (W)	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	1	1	2	2	3	3	4	5	6	8
1.5	2	2	2	3	4	5	6	8	9	12
2	2	3	3	4	5	6	8	10	13	16
2.5	3	3	4	5	6	8	10	13	16	20
3	3	4	5	6	8	9	12	15	19	24
3.5	4	4	6	7	9	11	14	18	22	28
4	4	5	6	8	10	13	16	20	25	32
4.5	5	6	7	9	11	14	18	23	28	36
5	5	6	8	10	13	16	20	25	32	40

The maximum allowed output power at the radio equipment and the maximum allowed ERP as defined by ICASA is shown in table 2.2.

Table 2.2. ICASA maximum output power regulation for UHF double frequency. [17]

UHF Double Frequency Maximum		
Radio Equipment	Maximum Output Power (W)	Maximum ERP (W)
Base and Mobile output power	20	20
Repeater output power	20	80

2.4.4. Earthing

All antennas at substations and pole-mounted switchgear devices should be earthed in accordance with the relevant standards. This is very important in areas with high lightning activity to minimize equipment damage during adverse weather conditions.

2.4.5. Coaxial cables and connectors

The document recommends the use of coaxial cable with minimal losses. The values as depicted in Table 2.3. may be used to establish the best cable for the maximum cable distance. It is not recommended to use RG 58 cable due to the high losses. It is preferred to use RG 213 for up to 5 m lengths in poor communications areas [17]. For connectors it is recommended to use high quality waterproof N-Type connectors and the use of BNC or TNC-type connectors should be restricted to radio equipment that is manufactured with these connectors [17].

Table 2.3. Radio Frequency power attenuation caused by coaxial cable loses in dB/100m at a frequency of 410 MHz. [17]

Coax Cable	dB/100m @ 410MHz
½” Foam	4.9
½” Flex	7.6
LMR 400	8.6
RG213/4	17
RG 58	34.7

2.4.6. User requirements for an area radio SCADA communication system

Technical bulletin 04TB-037 published October 2004 [22] describes the usage of antennas for RTU Ultra High Frequency (UHF) area radio communication as well as the radio output power. The Independent Communications Authority of South Africa (ICASA) is enforcing the adoption of international band plan conventions through the South African Band Re-planning Exercise (SABRE). In terms of SABRE, Eskom needs to swap the transmit and receive frequencies of all its Ultra High Frequency (UHF) repeaters and mobile radios.

A major benefit of SABRE is that it offers Eskom a good opportunity to re-design its UHF radio band to optimize the area radio network for SCADA usage. Based on extensive research [22] it was determined that the changes in Table 2.4. would optimally reduce co-channel interference and therefore improve reliability. The changes have been accepted by both ESKOM Distribution and Eskom Telecommunications, and subsequently new frequencies / channels have been allocated to all existing repeaters.

Table 2.4: SABRE changes to the UHF area radioband. [22]

	Pre-SABRE organization of the UHF radio band	**Post-SABRE organization of the UHF radio band**
Cell pattern	7-cell primary and 3-cell secondary pattern	12-cell primary pattern
Cell radius	35 km	30 km
No. of telecontrol channels	30 used	48 with an additional 12 channels reserved for special applications
Ideal re-use distance between co-channel repeaters	160 km	180 km
Worst-case re-use distance between co-channel repeaters	55 – 92 km	137 km

A major concern surrounding SABRE is that the advantage gained from reduced co-channel interference, could effectively be undone through the incorrect application of Remote Terminal Unit (RTU) antennas [22]. To understand the problem it is necessary to review the Radio Frequency (RF) propagation characteristics of the different UHF antennas used in Eskom. This is shown in Table 2.5. Note that a level of -90 dBm defines useable coverage, whereas a level of -115 dBm (the cut-off level) is used to define total coverage. The difference in coverage area between useable coverage and total coverage, is the area where the radio signal is too weak for reliable data transmission (i.e. < -90 dBm), but still sufficiently strong (i.e. > -115 dBm) to cause co-channel interference. Actually the co-channel interference cut-off level is -120dBm, but for practical reasons a less stringent cut-off level of -115dBm has been used.

From Table 2.5 [22] it is apparent that the total forward and reverse range for any given antenna is at least 5 times larger than the corresponding useable range. In other words, a 5 W mobile radio has the potential to cause co-channel interference at a distance approximately 5 times further than the distance at which the repeater receive level is at -90 dBm or better. This is significant and one of the main factors that could negatively affect radio network reliability, especially during peak traffic periods.

Table 2:5 Characteristics of commonly used RTU antennas. [22]

Characteristics	**3-element yagi**	**7-element yagi**	**12-element yagi**	**Corner reflector**	**Half-wave dipole (on pole)**	**Folded dipole (on pole)**	**Loaded Whip**
Antenna Gain (dBd)	4.94	8.95	11.51	7.54	3.17	2.57	4.00
Antenna Gain (dBi)	7.09	11.10	13.66	9.69	5.32	4.72	6.15
Co-ax losses (typical)	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Net antenna gain (dBi)	6.09	10.10	12.66	8.69	4.32	3.72	5.15
EIRP (W)* (Legal maximum limit is 32.73 W)	20.32	51.16	92.25	6.98	13.52	11.78	16.37
Net antenna gain (dBd)	3.94	7.95	10.51	6.54	2.17	1.57	3.00
ERP (W)* (Legal maximum limit is 20W)	12.39	31.19	56.23	22.54	8.24	7.18	9.98
ERP (dBm)*	40.93	44.94	47.50	43.53	39.16	38.56	39.99
Useable range* (i.e. distance in forward direction at which a level of -90dBm is achieved)	26	34	40	31	23	22	24
Total range* (i.e. distance in forward direction at which the cut-off level of -115dBm is achieved)	134	174	207	159	119	114	126
Ratio of Total range : Useable range*	5.2	5.1	5.2	5.1	5.2	5.2	5.3
Distance at which the cut-off level (-115dBm) is achieved in the reverse direction (134° - 226°)*	40	58	64	32	66	76	126
Front-to-back range ratio (at -115dBm)	3.35	3.00	3.23	4.97	1.80	1.50	1.00

* Radio transmitting at high power (i.e. 5 W)

According to principles contained in the British MPT1411 [22] specification, highly directional antennas should be used at RTUs, while the transmit power of the RTU radios should be adjusted to achieve the minimum required level at the repeater and thereby minimize interference. Given the factors that are prevalent in South Africa, such as the high cost of directional antennas, the frequency of theft, and the complexity in managing the transmit powers of all installed radios, a combination approach to radio transmit power and antenna selection is necessary.

Following from extensive analysis of RF propagation and antenna characteristics; a frequency re-use distance of 155km, an ideal re-use distance of 180 km, and a worst-case re-use distance of 137 km can be arrived at by using Table2.5. Therefore it is recommended that [22] the maximum RTU radio transmit power is 5 W. Any radio currently transmitting at a higher level should be turned down to 5 W. For RTU radios transmitting at the normal level of 5 W the following is recommended [22] :

- High-gain omni-directional antennas (e.g. loaded whips) should never be used.
- Normal-gain omni-directional antennas (e.g. half-wave dipole or folded dipole antennas) should not be used outside the UHF cell, i.e. not further than 30 km from the repeater it is working to.
- 3-Element Yagi antennas can be used any distance from a repeater, up to a maximum of 40 km.
- Corner reflectors may only be used at distances greater than 30 km from a repeater.
- For RTUs further than 40 km from a repeater, path profiles should be done to all co-channel repeaters within a 180 km radius to determine the level of interference. Based on the results a Corner Reflector, 7-element Yagi, or in extreme cases, a 12-element Yagi may be used.

If in terms of the above criteria, if an existing antenna is incorrect or if the signal level at any RTU is better than -80 dBm, then the RTU radio should be set to transmit on low power, i.e. 1 W. Any antenna could then be used, although it should be considered that at 1 W the maximum forward range would be less than 30 km. If adequate range can not be achieved when the radio is set to 1 W, then the radio transmit power should be adjusted to a level between 1 W and 5 W that results in a repeater receive level of -90 dBm.

2.4.7. International standards

Jean Tourrilhes describes the following design issues on his personal website [15]:

The use of radio spectrums is regulated in all countries by telecommunication regulation organizations of which the most prominent are the Federal Communications Commission (FCC) for North America and the European Telecommunications Standards Institute (ETSI) for Europe. The usage of radio frequencies as well as frequency bandwidth for TV and radio broadcasting are defined and allocated to users by these organizations. This is done for commercial, private users as the military.

The *Industrial*, Scientific and Medical (ISM) bands are allocated for users to use more flexable than other radio bands. The frequencies allocated to these bands are at 900 MHz and 2.4 GHz. These frequencies are unlicensed and free to use without having to register or to pay anything

There is however a set of rules imposed to avoid problems on these frequencies which needs to be considered during the design stage of a telecommunication system that will be used on these frequencies. The communication system use Spread Spectrum techniques to make full use of all the available bandwidth and frequencies of the radio channels. This is also to ease congestion on the different channels that are in the specific frequency band and to equalize bandwidth utilization between the different channels. Direct Sequence (DS) or Frequency Hopping (FH) techniques are allowed as methods to optimize spread spectrum on the ISM band.

The Spread Spectrum rules are as follows but may vary between country and FCC allocations : [15]

- Direct Sequence systems must spread their signal at least 11 times.
- Frequency Hopping systems stay on a channel a maximum of 0.4 s and use 75 channels at minimum in each 30 s period.
- FCC allocates both the 900 MHz and 2.4 GHz band with 1 W maximum power.
- ETSI allocates only the 2.4 GHz band with 100 milliwatt maximum power (900 MHz is used for GSM cell phones in Europe).
- The 2.4 GHz band is available worldwide and the regulations are mostly compatible between the different authorities (usually 80 MHz of bandwidth between 2.4 GHz and 2.48 GHz).
- The Spread Spectrum rules originally allowed around 2 Mb/s maximum bit rate (both FH and DS),
- Direct Sequence people managed to find a loophole and now offer 11 Mb/s systems

The main exception is Japan which has some additional constraints. Care must be taken if a high response time is needed by the user as these bands may be highly utilized by other users.

In the United States of America the National Rural Telecommunications Cooperative (NRTC) purchased the 220 MHz frequency at an FCC auction. It promotes the 220 MHz specifically for electric utility SCADA systems and being a member of the NRTC has the benefit of using this frequency without having to wait for license approval from the FCC [15].

A good example of a company to make use of this benefit is The Kansas Electric Power Cooperative (KEPCo) who needed to improve their SCADA capability. KEPCo has a generated capacity combination of two-thirds home-generated power and one-third purchased power under contracts with other utilities [15].

The installation setup and commissioning of the system was done before the summer of 2001 due to the savings on time with the application of radio frequency usage. The system comprised of approximately 300 RTU's which used remote radios as communication medium. The master station as well as 32 radio repeater sites were installed and a combination of 10 communication technologies were used to communicate between the SCADA master and RTUs. The Kansas Lyntegar's 220 MHz system was used in conjunction with the MDS 2710 radios. A total of 38 substations across the entire supervised geographical area were supervised by the complete SCADA system [15].

Bill McGinnis of Alexander Utility Engineering in San Antonio, Texas, designed the system and the backbone telecommunication system consisted of multiple radio repeaters with the longest path independent of repeaters reaching roughly 80km [15].

Lyntegar belongs to United Telecomm, a group of Texas coops that jointly purchased 220MHz rights for Texas, Arizona, New Mexico, and Oklahoma through NRTC and Cooperative Wireless [15].

Microwave Data Systems (MDS) published a whitepaper called “**Proper Planning Improves Reliability in Radio-based SCADA Systems”** on their website [16] and focused on the following points:

- Basic site selection requirements.
- Evaluating communication path quality.
- Antennas and coaxial antenna cables.
- Direction of transmission reception.
- Antenna mounting considerations.
- Spread spectrum systems.
- Maintaining system performance.

More in-depth investigation will be done later in the paper with regards to the above points. Although all the mentioned issues by Jean Tourrilhes, NRTC and MDS are very relevant it only take care of only one problem and that is if the RTU will operate a specific geographical position.

It does not take into account what impact the addition of another RTU will have on the current SCADA network. That is currently the major problem on all area radio based SCADA network. We first need to establish what the loading of the current network is and what does the traffic consist of. We need more detailed information with regards to the percentage of the data that is related to the different types of data messages. In order to calculate the impact that a new RTU will have on a SCADA system the above information is needed.

2.5. Network utilization

DNP3 is assumed as the SCADA protocol in terms of NRS037 [18]. Another reason for using DNP3 in the model is that DNP3 messages are on average far longer (in terms of the number of bytes transmitted) than any of the other SCADA protocols currently used by Eskom. It therefore presents the worst-case scenario, which makes the model valid for any combination of existing SCADA protocols.

The following communication parameter assumptions are being made to calculate network utilization on an area radio based SCADA network [18]:

- Each byte consists of 8 data bits + 1 start bit + 1 stop bit = 10 bits.
- The Constant Redundancy Check (CRC) overhead length is 2 bytes for every 16 bytes of data, plus 2 bytes for the last few bytes that do not make up a complete group of 16 bytes.
- Each DNP3 message header length is 10 bytes.
- The transport layer and application layer overhead length per unsolicited response is 5 bytes.
- The total overhead per DNP3 message is calculated as the sum of the CRC, the DNP message header, the transport layer and the application layer.
- The average acknowledge reply message length is 3 bytes (excluding overhead).
- The average single analogue message length is 14 bytes (excluding overhead).
- The average single control message length is 18 bytes (excluding overhead).
- The average single control message reply length is 28 bytes (excluding overhead).
- The average single status message length is 12 bytes (excluding overhead).
- To assist with effective channel access, DNP3 defines a minimum and maximum back-off time, before accessing the communications channel. The RTU’s minimum back-off time is set to the propagation time (i.e. latency) to allow the SCADA Master Station to get first access to the channel (SCADA master station back-off time = 0s). This is usually about half the required PTT warm-up time. The maximum back-off time is typically 10 times the minimum time, to allow for the decreased likelihood of collisions. To assist with effective channel access, DNP3 defines a minimum and maximum back-off time, before accessing the communications channel. The RTU’s minimum back-off time is set to the propagation time (i.e. latency) to allow the SCADA Master Station to get first access to the channel (SCADA master station back-

off time = 0s). This is usually about half the required PTT warm-up time. The maximum back-off time is typically 10 times the minimum time, to allow for the decreased likelihood of collisions.

- Therefore, on average RTUs will choose a back-off time of [min. time + (max. time – min. time) x 0.5], but since the quickest RTU (i.e. shortest back-off time) will always access the channel first, it has been decided to use [min. time + (max. time – min. time) x 0.1] as the average time to access the channel.
- Due to the synchronized reporting that results from a power network disturbance, the first round of RTU transmissions will fail due to multiple collisions. This will have the effect of delaying the first successful messages by the minimum retry time, which is typically 5 seconds.

The following RTU parameter assumptions are being made to calculate network utilization on an area radio based SCADA network [18]:

- An average RTU consists of 16 analogues inputs, of which the average analogue reports 24 times per day.
- An average RTU consists of 20 controls outputs, of which the average control is used 1 times per day.
- An average RTU consists of 40 status inputs, of which the average status reports 1 times per day.
- The average RTU has 4 integrity polls per day.
- Each integrity poll request is 10 bytes in length bytes (no overhead).
- Each integrity poll response is 826 bytes in length (including overhead).
- In a disturbed scenario, 10% of the inputs change simultaneously and must be reported within 60 seconds as per a requirement from the control centre. In the context of unsolicited report-by-exception communications, this means that all the RTUs need to report 10% of their database and receive the appropriate acknowledgement from the SCADA master station within 60s. In a solicited report-by-exception environment it means that the SCADA master station must be able to poll and receive a response (containing 10% of the database)

from all the RTUs within 60s.

Based on the above assumptions we can assume that each RTU and SCADA master transaction involves 2030 bits in 60 seconds during a disturbed scenario and the number of bits transmitted can be presented by the relationship [18]

Number of Bits transmitted = (RTU response + SCADA master station reply) x no. of bits per byte

Each RTU and SCADA master transaction involves two PTT warm-up delays as the communications channel needs to be accessed twice, as well as the RTU's average back-off delay. Therefore the transaction time per RTU and SCADA master transaction is presented by the relationship [18]

Transaction time = (No. of Bits transmitted / Data bit rate of channel) + (PTT Delay x 2) + RTU average back-off time.

The capacity of the telecommunication system, in terms of the maximum number of RTUs that can be supported, while still meeting the 60 s user requirement is then calculated by the relationship [18]

Capacity = (60s – retry time / Transaction Time) x Effective transfer capacity of the system

where the effective transfer capacity of the system is deemed to be 35 %. [18]

This is the midpoint between the recommended channel utilization for SCADA channels and Ethernet respectively:

- IEEE standard 999-1992 [20] recommends that the utilization for a SCADA communications channel should be considered as being between 40% and 60 %. However, for disturbance conditions it recommends that the lowest value (i.e. 40%) be used. Because this value applies to all types of communications channels, including microwave and optical fiber cable networks, it is considered to be optimistic for radio-based communication systems.

- Ethernet networks are known to have a practical transfer capacity of roughly 30 %. [19] However, Ethernet has the advantage over shared radio systems, because in addition to the CSMA (Carrier Sense Multiple Access) technique to minimize collisions, it also supports CD (Collision Detection), and is therefore able to detect when collisions occur. Because of this attribute, and the fact that its latency is much shorter than for radio systems, the 30 % capacity is also considered optimistic for radio systems during disturbance conditions.
- Therefore a transfer capacity of 35 % has been selected as a pragmatic, optimistic, value for shared radio systems. [18]

Calculating the capacity of shared communications systems as a function of different data bit rates and varying PTT delays yields the following table (Table 2.5). Please note the use of a logarithmic scale on the X-axis to emphasize the effect that the PTT warm-up time has on system throughput. The values in Table 2.6 can also be presented graphically as in Figure 2.1.

Table 2:6. Capacities of unsolicited RBE systems as a function of different Data Bit Rates and PTT Delays. [18]

PTT warm-up time (ms)	**Ave Back off Time (ms)**	**Data bit Rate (bits/s)**		
		1200	**4800**	**9600**
1000.0	950.0	4	6	6
500.0	475.0	6	10	11
250.0	237.5	8	17	20
125.0	118.8	9	24	33
62.5	59.4	10	32	49
31.3	29.7	11	37	63
15.6	14.8	11	41	75
7.9	7.4	11	43	82
3.9	3.7	11	44	86
2.0	1.9	11	45	89

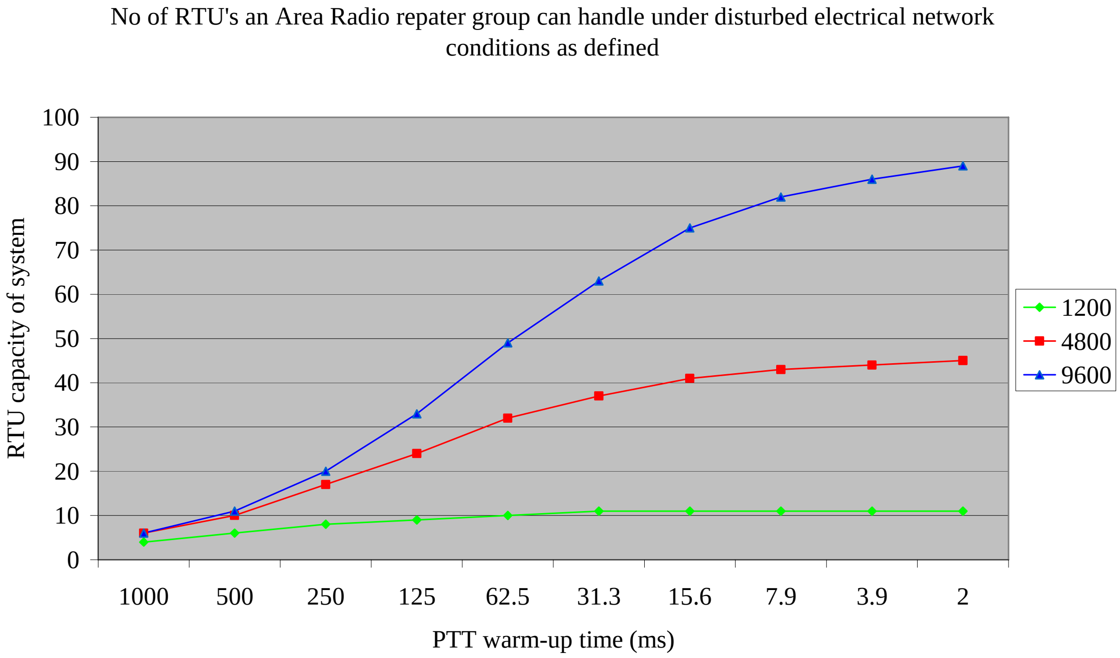


Figure 2:1. Capacity of unsolicited RBE systems as a function of different Data Bit Rates and PTT Delays. [18]

Based on the above model the conclusion can be drawn that a radio-based unsolicited report-by-exception communication system should at least support a data throughout rate of 9600 bps, with a maximum PTT warm-up delay of 50 ms in order to meet the user requirements stated in Table 2.6. It is thus not possible for a 1200 bps or 4800 bps communications network to meet the requirements [18].

As discussed earlier we can use the network utilization of an Ethernet LAN network as a reference for the network utilization of an area radio network. The following information with regards to an Ethernet LAN network utilization is published by 3-COM on their website [19].

As general guidelines, your network is healthy under these conditions:

- Utilization is running up to 15 % most of the time.
- Utilization is peaking between 30 % and 35 % for a few seconds at a time, with large gaps of time between peaks.
- Utilization is peaking at 60 % for a few seconds, with large gaps of time between peaks. However, in this instance, locate the reason for the peak. Determine if the problem might get worse or if you can isolate it.

A network will start showing signs of degraded performance if the 30 % utilization peaks start occurring very close together. These theoretical values will be compared with data from two live networks in the “Network Utilization” chapter.

2.6. Remote terminal unit maintenance standards

2.6.1. ESKOM distribution standard

ESKOM distribution technology has published a maintenance philosophy [12] for maintenance on RTUs. This document describes the maintenance intervals, maintenance types per RTU type.

The maintenance philosophy describes the following maintenance types:

- Breakdown maintenance (Failures).
- Condition based maintenance (CBM).
- Preventative maintenance (PM).

The maintenance types are defined as follows in the document: [12]

Breakdown maintenance is also known as “Run to Failure (RTF)” or “Failure Based Maintenance (FBM)” and the philosophy is to wait until the equipment fail and then restore the faulty plant as quickly as possible. Condition based maintenance is described as Reliability Centered Maintenance (RCM) and is done when the performance of the equipment is falling below the established standard [12]. Preventative maintenance is described as Used Based Maintenance (UBM) or Time Based Maintenance (TBM). [12]

Of the three types only breakdown maintenance is described correctly in the document. Condition based is described incorrectly as CBM may also be done as used based maintenance or time based maintenance. In other words the condition of the plant may be inspected and maintained if necessary after a certain usage or on a specific time cycle. The same philosophy may be used with preventative maintenance, which may also be time based or it may be done after a certain number of usage or operations (UBM).

The reference to RCM is also not correct as RCM in itself is a tool that can be used to assist you with defining your maintenance strategy. The use of RCM will assist with the evaluation of the plant and then give direction to use either breakdown maintenance, condition based maintenance or preventative maintenance.

Reference should also be done to Design out Maintenance (DOM). The focus of DOM is to improve the design of the plant in order to eliminate or reduce maintenance. It is important to evaluate this policy on technical and economical aspects. It may be possible to eliminate all failures, but the cost may prove to be too high.

The document focuses on the following maintenance:

- The RTU itself.
- The telecommunication system.
- The power supply system.

Maintenance of the telecommunication system and RTU is important and will improve the reliability of the SCADA system if it is done properly.

2.6.2. International maintenance standards

The American Public Transport Association [14] published a Standard for SCADA System Inspection, Testing and Maintenance in July 2004. The document deals with various aspects including the following:

- Requirements.
- Training.
- Materials.
- Tools.
- Safety.
- Inspection, testing and maintenance procedures.
- Correction of deficiencies.
- Documentation.

This is also a very generic document and refers to manufacturer maintenance documentation, thus using the prescribed maintenance procedures of the equipment manufacturers. The following maintenance standard was published on the website of EPCOR, an energy providing company from Canada. It focused on the following: [14]

- Requirements of the SCADA system:
  Requires accurate communications with control and master station personnel. The system must monitor substation events for control, during RTU down times.

- General maintenance:
  Cleaning and dusting of internal parts
  In the case of excessive hardware change counts must be corrected.
  Card edges sockets and control blocking switches are cleaned and sprayed.

- Analogue board calibration:
  All analogue inputs must be tested by applying a constant current to the analogue input terminals of the analogue boards. The digital counts of the analogue to digital converter on the boards must be compared with the supplied constant current at the analogue inputs. The analogue board must be calibrated if the digital count does not correspond with the analogue value as injected into the analogue input.

- Battery and other DC voltage maintenance:
  Take accurate voltage checks of all DC supply systems and compare to manufacturer specifications.
  Batteries must be tested for voltage and current with a load test over time and temperature.
  All cells and battery connections must be cleaned thoroughly.

- Communication line maintenance:
  A tone generator must be used to inject a tone at a specified level at one end of the communication line and compared with the measured value at the other

end of the communication line. All communication equipment must be calibrated if the level is not in the specified range.
Bit error rate tests on the communication line will supply accurate information with regards to the condition of the system in total.
Data checks must be done for aging or line degradation.

These points are generic, but are virtually the same as the standard currently used by ESKOM distribution. Le Truong from UTSI [13] describes periodic maintenance on SCADA systems and focus on the following:

- What type of maintenance need to be done.
- Reasons companies chose to do maintenance.
- Reasons companies chose not to do maintenance.
- Outcome of maintenance.

In the document all of the above points focus on SCADA masters and not on RTU maintenance and thus is not valid for this research project.

2.7. Conclusion

The Ultra High Frequency (UHF) radio network used by ESKOM is rather unique in the sense that most other countries rely on very secure wideband communication networks for SCADA systems. Optical fiber cables, microwave communication links and hard wire connections are freely available in other countries and UHF radio links are used less frequently than in South Africa.

Some utilities in North America do use radio repeater technology, but this is done on digital radio networks that use spread spectrum techniques (either direct sequence or frequency hopping). Frequencies are controlled by the FCC and in most cases it is a license free system. This may have an impact on security of data and the systems may also be congested due to that fact that it is public domain.

2.7.1. SCADA standards organizations

There are many international standards organizations, but only two of them define RTU protocol specifications, namely the IEC and the DNP3 users group. The two published standards are not compatible, although both standards are open standard protocols. There is a need for one international standard for all RTU protocols, which will ensure better interfacing between SCADA masters and different RTU makes and models.

2.7.2. Protocols standards

While SCADA protocols are more open today, there is no clear consensus of which protocol is best. IEC 60870-5 series and DNP3 have many similarities but are not 100 % compatible. Only manufacturer propriatotory protocols were implemented in the past by ESKOM due to the lack of international standards on RTU protocols. ESKOM is starting to follow international trends by adopting the DNP3 protocol. It must be said however that DNP3 is not really designed to work at its optimum over our UHF radio networks. It should however work well on the wideband optical fiber and microwave networks. Current manufacturer specific and ESKOM specific protocols are being phased out.

2.7.3. Performance measurement

RTU performance is measured in ESKOM and is used to improve the current systems. Performance indicators are very similar to other international standards.

2.7.4. Telecommunication design

Current ESKOM telecommunication designs for RTU systems are not based on scientific studies, but rather on assumptions. Detail studies should be done on the current telecommunication system during the planning phase of a new RTU. This should include current network utilization and the theoretical impact of the new additions on the network. The telecommunication network should be redesigned if the investigation proves a future utilization of beyond 40 %. Antenna and cable selection standards are in place and are currently being reviewed to conform to ICASA standards.

2.7.5. Network utilisation

IEEE standard 999-1992 [20] recommends that the channel utilization for a SCADA communications channel should be considered as being between 40% and 60 %. This is however aimed at broadband communication networks, for example microwave and optical fiber cable networks, and is considered to be optimistic for radio-based communication systems. Local area network manufacturers specify a network utilization of between 30 % and 40 % and are more realistic for radio-based communication systems as in theory the Ethernet local area networks are very similar to area radio communication systems. Both systems “listen” on the network for idle time and then transmit the data and both systems use some type of error detection for data security.

2.7.6. Maintenance standards

Maintenance standards are in place in ESKOM and correspond well with international standards. Not many standards are published internationally and companies rather rely on the RTU manufacturers to prescribe maintenance standards. All maintenance standards rely on performance measurement of the systems. Performance information should influence maintenance cycles and philosophies. The ESKOM Distribution RTU maintenance document should be revised as some of the definitions are not correct.

3. Communication systems and KPI research.

3.1. Introduction

The research for this thesis focuses on the following:

- Communication system configurations for SCADA systems used by Eskom Distribution.
- SCADA Key Performance Indicator (KPI) research.
- RTU availability analysis.
- Control success rate analysis.
- Communication channel utilisation research on area radio communication systems.
- RTU installation and maintenance standards.

The communication system configurations for SCADA systems used by Eskom Distribution and the KPI research will be discussed in the remainder of this chapter.

3.2. Communication systems

There are currently two basic communication system protocols used by ESKOM, namely solicited and unsolicited. The unsolicited communication system is also known as Report by Exception (RBE).

In the case of a solicited communication system the RTUs are multi-dropped on a communication network and are continuously polled by the master. On average all RTUs are polled roughly every three to ten seconds, depending on the number of RTUs on the communication system. These systems require microwave, optical fibre or power line carrier (PLC) communication. Although these systems do provide a very reliable and high bandwidth, it is also a very expensive and is not always feasible in remote areas. This telecommunication configuration is mainly used at bigger sub stations that need very high communication availability and bandwidth.

Figure 3.2. shows a block diagram of a typical continuously polled system. All the RTUs are multi dropped on one communication line which in practice this means that all the RTUs will receive the same information coming from the SCADA master.

Each RTU will have a unique address and will only respond to a command coming from the SCADA master when it recognises its own address. The SCADA master will sequentially poll the RTUs one by one and the RTUs will respond back in the same polling sequence. All state changes at the site will be transmitted back to the SCADA master only after the specific RTU has received a poll with its unique address from the SCADA master. The system does not use a token, but this configuration is very similar to the Arcnet topology used in the Local Area Network (LAN) environment as all RTUs have an equal chance to communicate with the SCADA master

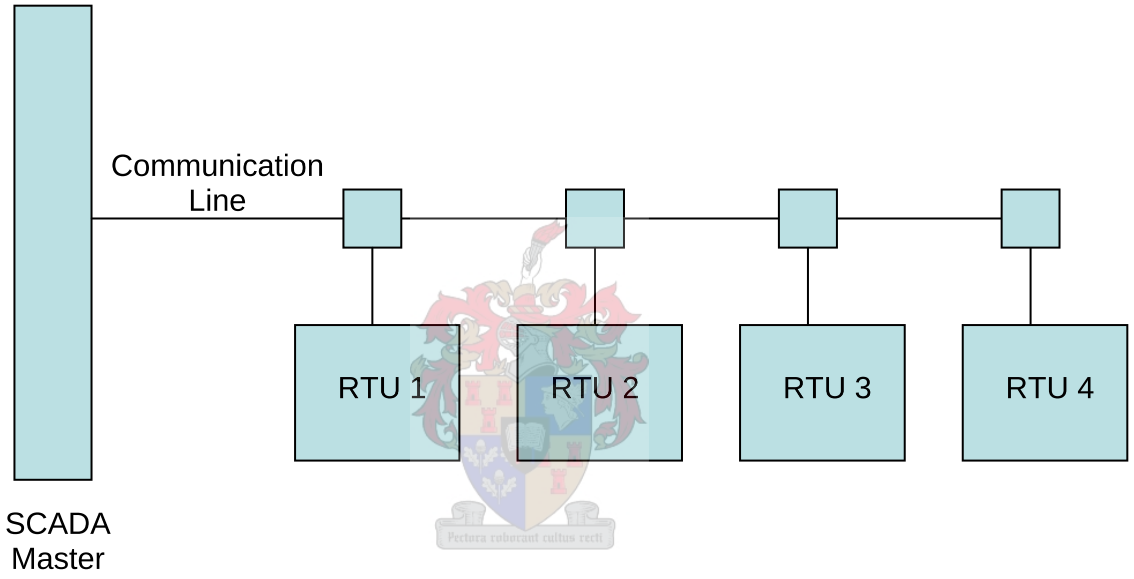


Figure 3.1. Block diagram of a typical continuously polled system (solicited protocol).

The unsolicited or Report by Exception (RBE) communication system normally use an UHF area radio based system. This consists of radio repeaters which will cover specified geographical areas and a group of RTUs which will communicate with the master via the radio repeaters. These radio repeaters are then connected to the wide band radio network to form a communication network. This system is cheap, but lacks the bandwidth and response times. It is mainly used in rural areas where dedicated communication is not readily available. The RTUs are not continuously polled and rather work on report by exception. With every change of state at the remote terminal unit there will be an update transmitted to the SCDA master. The RTU will first do a Carrier Detect (CD) or also known as *channel busy* to establish if the radio channel is available before it will transmit the data to the SCADA master. This configuration is very similar to the Ethernet topology in Local Area Network (LAN) environment.

The RTUs are however polled at certain intervals to test the availability of the RTU. These intervals are configured depending on the loading of the network and specific repeater. The specific protocol used by the RTU will also have an impact on the poling cycle. In less densely populated areas this interval can be from once every four hours and may go up to once every seven hours in more densely populated areas. The RTU will contact the SCADA master when a change of state occurs at the remote site which may be an alarm condition that change, breaker indication that change or a change in analogue value. This will prompt the RTU to transmit the new value to the SCADA master to update the database.

The block diagram in Figure 3.3. shows a very simple Ultra High Frequency (UHF) area radio based communication system. There are two radio repeaters connected on the telecommunication system. RTU 1, 2, 3 and 4 are configured to work via radio Repeater A and RTU 5, 6 and 7 works via Repeater B. In practice there may be up to 7 repeaters on one communication line and up to 100 RTUs configured per repeater. This does impact on the network utilisation and will affect the RTU availability and the success rate of controls sent out from the SCADA master. In practice it is possible for two or more RTUs to start transmitting data messages at the exact same time, which will lead to data corruption. A Constant Redundancy Check (CRC) is done by the SCADA master and all RTUs continuously to detect any corrupt data messages. In the case of a CRC error both RTUs will back off for a random time and will then re-transmit the data.

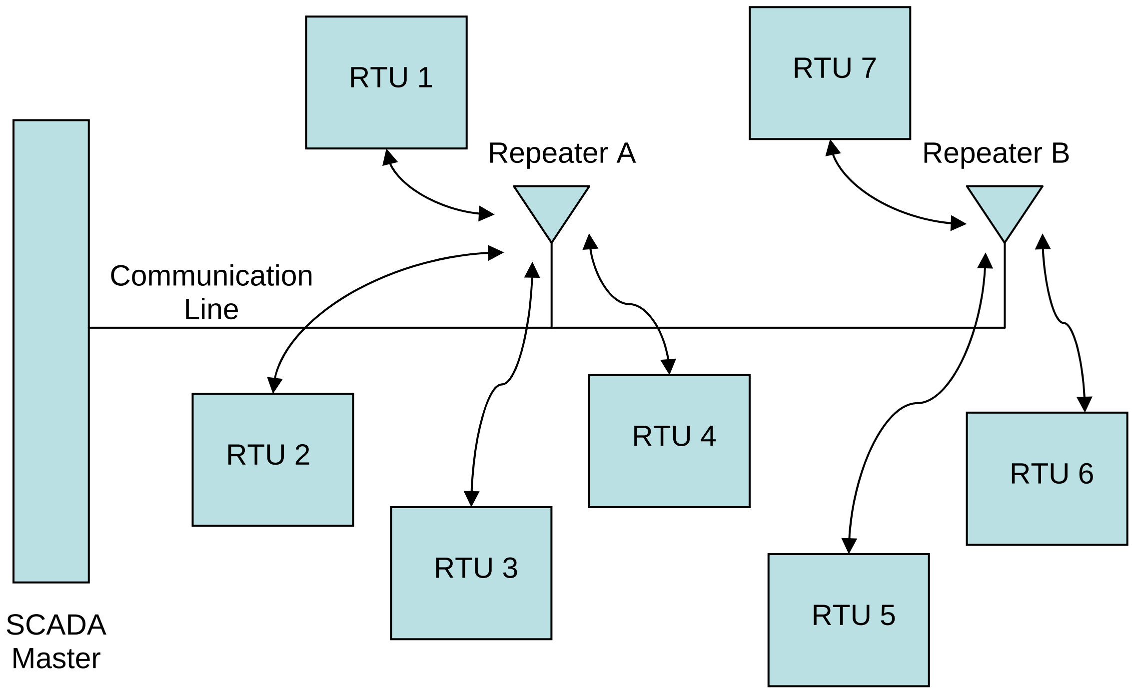


Figure 3.2. Block diagram of a typical area radio based system (unsolicited protocol).

3.3. Key performance indicators

To ensure a reliable SCADA system we need to measure the performance of the system. We need to define Key Performance Indicators (KPIs) which will indicate if the system is performing to its defined design. A KPI must be easy to measure, easy to obtain and must be appropriate for the system. Targets to achieve must be set to measure the KPIs. This will give an indication whether we can improve or not.

The following constraints is published in the document “Telecommunications: High-Level User Requirements for Telemetry Communications in Distribution” [18] by Dieter Gutshow.

- Due to the half-duplex nature of the communication system, only one device can communicate at any given time.
- Data collisions occur because of the time delay between when an RTU asserts the channel and the other RTUs become aware of this assertion. This is a function of the time taken for an RTU to open the repeater squelch plus the time taken for all the other repeaters in the group to open the squelch on the radios of all the other RTUs. The probability of collisions increases as this time increases and as the number of RTUs wanting to transmit increases.

- Relatively long Press to Talk (PTT) warm-up times (500ms to 1000ms) are needed for the communications equipment to reach a suitable operating state to send data reliably. This plays a significant role in determining the number of RTUs that a repeater group can service.
- Under normal power network conditions the communication system is lightly loaded and the number of collisions is low. However collisions increase sharply as the number of data transactions increase in response to disturbances on the electrical power network. This increase in the number of collisions severely limits the throughput when the channel is busy.
- The analogue nature of the communication system means that audio levels need to be adjusted correctly across the entire system to ensure correct operation. This is often not achieved because standards are not implemented, and/or because end-to-end system tests are not performed after maintenance activities. The end result is distortion of data signals which result in degraded performance.
- Another disadvantage of the analogue nature of the present system is that the total noise and distortion contribution of all portions of a communication link impacts on the Bit Error Rate (BER). This is in contrast with a digital system that allows regeneration at each link interface, which significantly improves BER.
- The current radio repeaters, RTU mobile radios and some links do not support remote management.

The listed constraints that impact on the functionality and performance of the SCADA system are as follows: [18]

- Relatively long Press to Talk (PTT) delays reduce the amount of “airtime” that is available for data transmissions.
- Data collisions are mitigated through collision avoidance algorithms and transmission retries that are implemented on the RTUs. Data collisions and the required collision avoidance methods limit the maximum throughput.
- Due to limited amounts of available “airtime”, RTUs are configured to report data in an unsolicited report-by-exception fashion to limit both the number of

transmissions and the volume of data transmitted.

- System throughput becomes severely compromised during periods of peak data traffic. This means that data often gets delayed beyond its useful life, which negatively affects the ability of the control centre to monitor and control the power network.
- Due to the above problems, the SCADA system cannot be expanded to existing/new substations on repeater networks which experience congestion from time-to-time. To overcome this constraint new repeaters and backbone links have to be deployed at additional cost to the business.
- RTUs are currently forced to report voltage, current and power value changes on large changes in excess of 10% rather than on much smaller changes in the order of 1% – 2% changes that are required by the control centre and network optimization departments to effectively manage the power network. This is because the existing communication system is unable to handle the large amounts of data that would result from frequent analogue value updates.
- Because of the above mentioned capacity constraints, portions of the communication system cannot be utilized for enhanced SCADA applications such as Distribution Automation which would typically require more RTU transactions. It therefore prevents the implementation of solutions to improve overall power network reliability and customer satisfaction.
- SCADA performance is degraded because of inadvertent adjustment of audio levels and/or the cumulative degradation of BER across multiple links.
- Because the radio repeaters, mobile radios and some links are not proactively managed, faults or loss of service goes unnoticed by the service provider, until reported by the customer. This results in extended loss of SCADA functionality.

Key Performance Indicators (KPIs) are the tools that allow a business to measure the quantity and quality of a service being delivered. In the context of a SCADA network KPIs are fundamental in assessing the overall performance of the network in terms of business efficiency, financial savings and customer satisfaction. Another benefit from well-defined and clearly understood KPIs are performance benchmarks which allow different operational divisions to aim for the same goals, whilst allowing management to compare apples with apples.

The process starts by considering some quantitative measurements for the strategic objectives of the business. To avoid possible confusion that could be brought about by too large number of indicators, it is suggested that the absolute minimum number of KPIs that will allow proper performance assessment be developed.

3.3.1. RTU availability

Two KPIs were chosen to measure the performance of the SCADA system, namely RTU availability and Control Success Rate (CSR). The reasons for choosing these two KPIs were that both are easy to calculate, the data to calculate the indicators are easily available and both KPIs give a good high level indication of the SCADA system performance.

RTU availability measures in percentage the number of times that the master polled the remote and if the remote responded successfully to the poll. This will test the Master, communication equipment and the remote. The formula for RTU availability is described by the relationship [8]

$$\text{RTU Avail} = \frac{No.of\ successful\ RTU\ responses\ to\ polls}{Total\ no.of\ RTU\ polls} \times 100\ \%. \qquad (2.1)$$

Only the number of polls and number of successful responses are used to calculate the RTU availability. This data will however limit further investigations into the causes of failures as well as system anomalies. The following data is necessary to do more in depth investigations into RTU availability:

- Date and time of message.
- RTU name.
- Percentage available per RTU.
- Percentage fail per RTU.
- Percentage disabled per RTU.

A RTU can also be disabled at the SCADA master. This is used when a site is decommissioned or out of service for a certain time. This will also be used when a communication system is inactive or failed for a certain period of time and it will be irrelevant to poll the RTU during that time. To obtain an accurate RTU availability figure these disabled cases should be omitted and not seen as failures.

It was decided to get the data in a comma delimited file (CSV) format from the SDADA master. This will make it easy to import into a database table with the correct format. The file must have a header that consists of the date range of data. The sum of the percentages must add up to 100 %. Due to the rounding of the percentages it was found that the sum will sometimes be +/-0.1 % from 100 %. For this reason a column *other* was introduced where the difference between the sum and 100% will be stored. This percentage is however too small to affect the accuracy of the analysis.

3.3.2. Control success rate

Control success rate measures in percentage the number of controls that was initiated by the master and of which the master received an *execute successful message* from the remote. The formula for RTU availability is described by the relationship [8]

$$\text{CSR} = \frac{Total\,no.\,of\ controls\,despatched - Total\,no.\,of\ unsuccessful\ controls}{Total\,no.\,of\ controls\,despatched} \times 100\ \%. \qquad (2.2)$$

RTU availability basically only measure the performance of the communication equipment, while CSR may be influenced by the control personnel, SCADA master, communication equipment, RTU and the plant in the field. It is thus a more comprehensive indicator. All controls with a CSR which does not conform to the target needs to be investigated to establish the causes that contribute to the poor performance.

The number of controls sent out and the number of control failures over a certain period of time are needed to calculate the control success rate. This data is however limited and it will be impossible to analyze the exact causes of the failures. The following data is needed to do a meaningful data analysis study:

- Date and time of the dispatched control.
- Site to where the control was dispatched.
- The device that was selected for the control the control (e.g. Farmers 1 Breaker).
- Type of control dispatched (e.g. close, open).
- Control message generated by the SCADA master (control failed, control successful).
- User who dispatched the control.
- Desk from where control was initiated.

3.4. Data mining tool

3.4.1. Introduction

It was decided to produce the data on an average per week per RTU basis to minimise the quantity of the data. A query was written to extract the data from the SCADA master and importing the data file into Microsoft Excel. The data and trending graphs were drawn within Excel for the first analysis. This method is however cumbersome and with a file in excess of 700 lines per week, it soon became clear that Excel could not handle the vast amount of data. The first real database was developed in Microsoft Access and was later ported to MS SQL Server due to better data security on MS SQL Server. There were also limitations on the graphical side and it was decided to get a professional software development company to do the development for a full software tool. Figure 3.4. depicts a block diagram of the RTU monitor and SCADA system topology. The SACDA master and other SCADA terminals are interfaced via a secure SCADA local area network. This is done for security reasons to reduce cyber attacks and virus contamination. A query is run on one of the engineering terminals to extract the relevant data from the SCADA master database. This data is then imported into the RTU monitor database with the RTU monitor user interface. All other data mining and reporting is done with the user interface running on a standard personal computer.

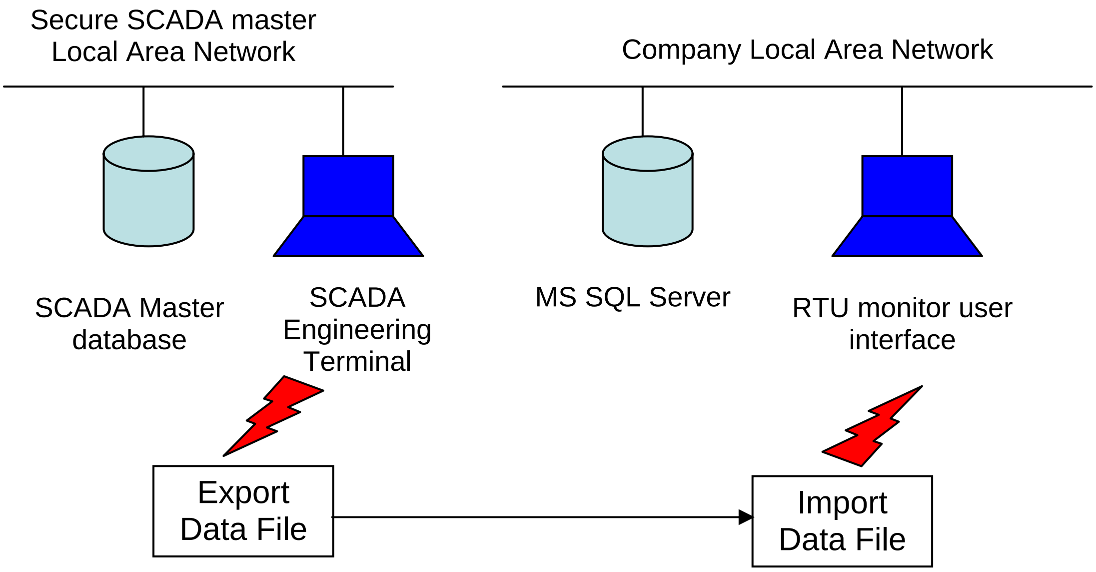


Figure 3.3. Block diagram of the RTU monitor and SCADA system topology.

3.4.2. Data mining tool specifications

Specifications were compiled for a data-mining tool and a request to tender was send to software development companies. A tender was awarded, the software tool was developed and the first commercial version was implemented during 2002. The current version can use either MS SQL Server or Access as a server. The user interface is designed to import RTU availability files created from the SCADA master as well as control files. The detail technical specifications are discussed in the remainder of the chapter.

3.4.3. Importing of data

The following specifications were specified with regards to the importing of data from the SCADA master.

- The system must be able to import RTU results from a uniform comma-delimited text file.
- The system must be able to ignore the results from a list of RTUs designated as test RTUs.
- The system must be able to ignore the results from a list of RTUs designated as decommissioned RTUs.
- The system must be able to ignore the results from a list of new RTUs that are still to be commissioned.

- When the disabled % for an RTU is 100%, the disable flag for that RTU must automatically be set to true.
- When importing results for a new RTU, the system must automatically create a new RTU in the database, and allow the configuration for the new RTUs to be entered.
- The system must be able to import the controls send out by the SCDADA master and alarms received by the SCADA master per day per shift from a uniform delimited text file.

3.4.4. Data entry

The system will contain data entry forms to maintain the following data:

- SCADA networks detail.
- Repeaters names and configuration.
- RTU names and configuration.
- RTU types (i.e. the RTU Protocol used).
- RTU availability results.
- RTU configuration history (Data is automatically appended when an RTU's configuration is changed.).
- Controller success rate.
- Controller success rate KPI.
- Controls send and alarms received by controllers, per day per shift.

3.4.5. Reports

The system will contain reports to print the following information:

- Availability per RTU.
- Availability per RTU Type.
- Availability per repeater.
- Availability per SCADA network.
- RTU configuration history.
- Average RTU availability.
- Alarms received list.

- Controls send list.
- Control success rate per RTU.
- Control success rate per RTU type.

3.4.6. Graphs

The system will contain graphs to display the following information:

- Availability per RTU type (Each RTU type is displayed on a separate line graph).
- Availability per RTU (A line graph with a trend line per RTU).
- Availability per RTU type (A line graph with a trend line per RTU Type).
- Availability per repeater (A line graph with a trend line per repeater).
- Availability per SCADA network (A line graph with a trend line per SCADA Network).
- Average availability per RTU (A bar chart per RTU).
- Average availability per RTU type (A bar chart per RTU type).
- Average availability per repeater (A bar chart per Repeater).
- Average availability per SCADA network (A bar chart per SCADA network).
- Control success rate (A line chart with an average KPI line).
- A bar chart showing the percentage of RTUs above and below a specified %.
- Control failure analysis (A pie chart showing the success and failures per type of failure.
- Alarms received (A bar chart with a trend line).
- Controls send (A bar chart with a trend line).

3.4.7. Security

The system will be able to control access to data entry forms and reports, using the latest available security system. Secure logon to the database will be provided and the system administrator will manage all security issues and access rights to individual users.

3.4.8. Operating system and development language specifications

Access Basic was chosen to develop the user interface (front end) and MS SQL Server 2000 as the database (back end). The transport protocol on the LAN is TCP/IP and an MS SQL open database connectivity (ODBC) driver was used to interface the front end to the database. These languages were chosen because it was quick to develop, easy to administrate SQL Server and also relatively cheap compared to other database servers.

3.4.9. Data file formats

An example of the RTU availability file is shown in Table 3.1. This data is extracted from SCADA master and then imported into RTU Monitor. The file is in a comma-delimited format and starts with a header, which contains the date and time range for availability data. The data include the type of RTU protocol, the RTU name, the percentage of the available time, the percentage of the failed time and the percentage of the disabled time. The data name *other* field denotes the percentage that cannot be specified by any of the other categories. This normally has to do with the rounding of the values to two decimal places after the comma.

Table 3.1. Example of RTU availability data extracted from SCADA master.

RTU AVAILABILITY STATISTICS FOR PERIOD 26-SEP-2005 00:00:00 TO 3-OCT-2005 00:00:00					
TYPE	NAME	ON	FAILED	DISABLED	OTHER
PMRTU	18TH_AVE	100	0	0	0
PMRTU	8TH_AVE	100	0	0	0
ESTEL	ACACIA	99.95	0	0	0.05
PMRTU	ACKERMAN	100	0	0	0
ESTEL	AGGENE_E	99.87	0.05	0	0.08
ESTEL	AIRPRT_E	99.95	0	0	0.05
DNP	AL1R2834	70.69	6	23.31	0
DNP	AL1R875	0	0	100	0

Table 3.2. shows an example of the control file extracted from the SCADA master. The file is $ delimited. The *date* and *time* field is the exact date and time that the SCADA master executed the control. The *site* field is populated with the name of the site that the control was dispatched to and the *device* field is populated with the device that was selected to execute the control. The *control* field depicts the type of control that was selected.

The *message* field is the message that was generated by the SCADA master when the control was initiated and includes the return message after the control was executed. The message may also be a control fail message. The control fail message will however not indicate the cause of the failure. This may be caused by numerous plant failures at the site. A good example is a feeder of which the conductor has broken off and is lying on the ground. The protection system will inhibit such controls due to the high risk to human life and the environment. In cases like this the SCADA master will not necessary be aware of plant failures in the field and will try to execute the control. These cases will have to be investigated individually to establish the cause of failure. The control failure causes will be discussed in more detail in chapter 5.2. A list of SCADA master generated control messages is shown in Table 3.3. The *initiator* field is populated with the name of the operator that executed the control and the desk field is populated with the terminal from which the control was executed. In practice it does happen that different control personnel execute the same control from different terminals within a short space of time to the same device. This will inevitably cause a control failure and the data from the log file will assist with the investigation as the sequence of events from both controls will be available.

Table 3.2. Example of control data extracted from SCADA master.

Date and Time	**Site**	**Device**	**Control**	**Message**	**Initiator**	**Desk**
16/08/2004 10:20:52	KHYLTS_D	11A_RING_BKR	TRIP	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 10:26:33	KHYLTS_D	11A_RING_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 10:31:28	TEST_SUB	BELHAR1_BKR	TRIP	CONTROL EXECUTE	CONTROL	SAWK08
16/08/2004 12:46:19	BRENTWD	11KV_BSEC2_BKR	TRIP	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 12:51:05	BRENTWD	11KV_BSEC2_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 14:42:18	MULDRSVL	TRACT_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK02
16/08/2004 16:27:57	_BOWER	OVERH2_RC260	CLOS	CONTROL EXECUTE	ENGINEER	SAWK08
16/08/2004 18:02:53	DEZALZE	FARM1_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK02

Table 3.3. Control message examples generated by the SCADA master.

Message	Description
CONTROL EXECUTE	Control was dispatched
CONTROL FAILED, BLOCK COMMS FAILURE	Control Failure
CONTROL FAILED, RTU COMMS FAILURE	Control Failure
CONTROL FAILED, UNKNOWN ERROR	Control Failure
CONTROL MESSAGE CORRUPTED	Control Failure
CONTROL SUCCESS	Control Successful Executed
CONTROL TIMED OUT	Control Failure
FRONT-END CONTROL REPLY TIMEOUT	Control Failure
RADIO CHANNEL BUSY	Control Failure
RTU FAILED TO EXECUTE CONTROL	Control Failure

3.4.10. RTU monitor software data model

The graphical outlay of the RTU monitor data model is shown in Figure 3.5 and depicts the tables and fields as created in the database for RTU availability. Figure 3.6 depicts the tables and fields as created in the database for control success rate.

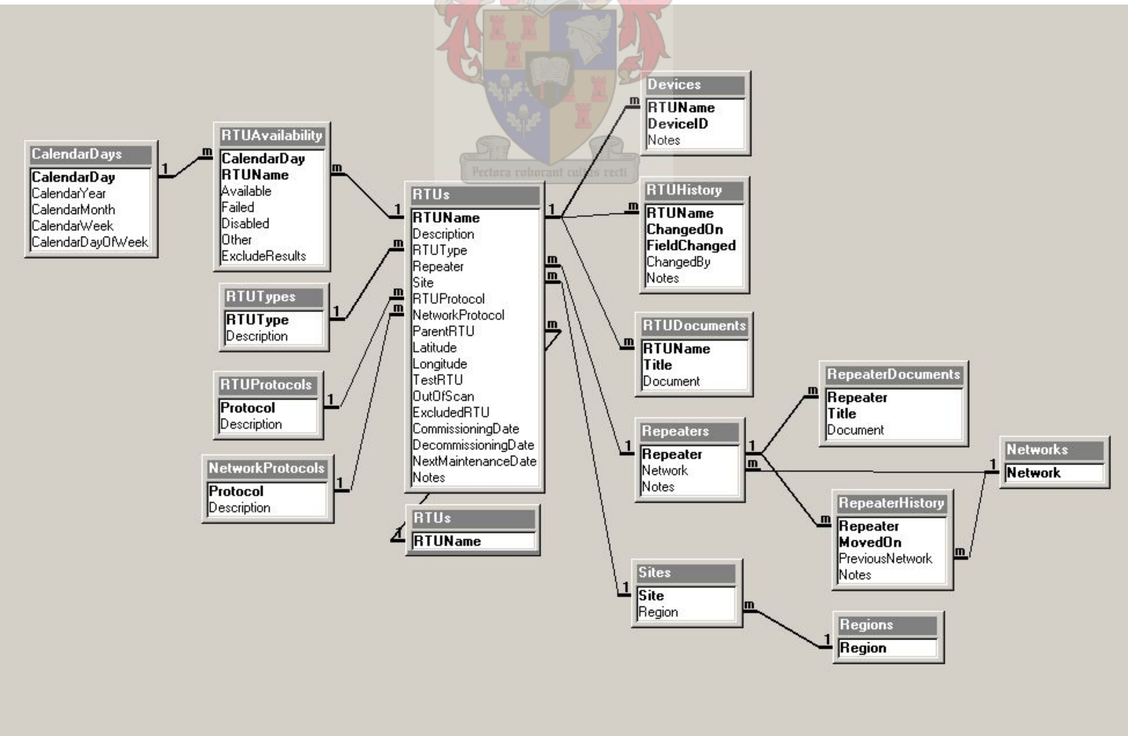


Figure 3.4. Graphical layout of RTU monitor data model for RTU availability.

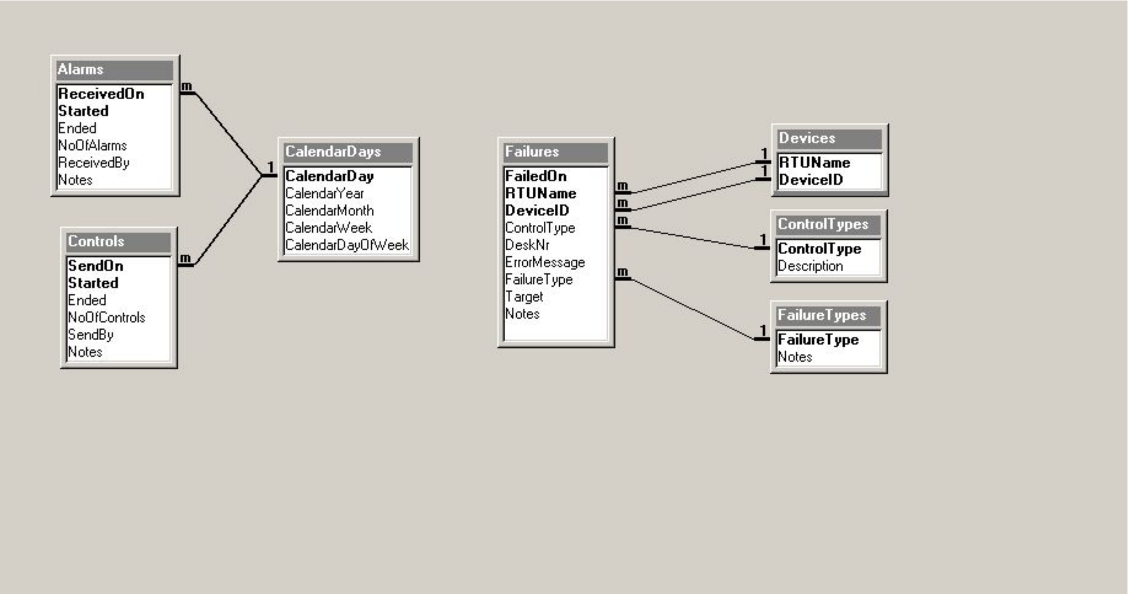


Figure 3.5. Graphical layout of RTU monitor data model for RTU control success rate.

4. RTU availability analysis

4.1. Data analysis for year 2002

The configuration of the communication systems was established and the RTU monitor software tool was populated with the relevant data. This includes the list of communication systems, repeaters and Remote Terminal Units (RTUs). The RTU specific data includes the commissioning dates, protocols, installation types and manufacturers.

RTU availability data was extracted from the SCADA Master with script files and imported into the RTU Monitor software tool with data from 1999. For this project only the data from January 2002 to December 2004 was analysed. The list of communication systems and the installed numbers or RTUs as at the end December of 2002 is shown in Table 4.1. The “4 Wire E & M” and “X21” communication systems are solicited communication systems as explained in 3.2 and thus do not use area radios as a telecommunication medium. A total of 37 repeaters were installed at that stage which serviced 220 RTUs.

Table 4.1. Installation numbers of RTUs per communication system end December 2002.

Communication System	Repeater	RTU's	Protocol
4 Wire E & M	0	22	Solicited
X21	0	27	Solicited
Tygerberg	3	54	Unsolicited
Peninsula	4	44	Unsolicited
Winelands	9	35	Unsolicited
West Coast	8	46	Unsolicited
New South	13	41	Unsolicited

The installation numbers of RTU addresses per RTU protocol type is shown in Table 4.2. Some RTU types or protocols use more that one address per RTU. In practice that may be up to 15 addresses per RTU. The RTU use only one MODEM and antenna as shown in the functional block diagram of a multiple address RTU in Figure 4.1. The reason for choosing to show it per address is that the SCADA master sees each individual address as a RTU which it needs to interrogate, which result in a higher figure of perceived RTUs. This does increase the traffic on the communication system as there are more interrogations done on the cyclic interrogation cycle, as would have been the case if all RTUs use only one address per RTU.

Table 4.2. Installation numbers for per RTU protocol at the end of December 2002.

RTU / Protocol Type	**Installed base per RTU address**
ERTU	32
PUTU	20
PMRTU / EV	152
INTRAC	237

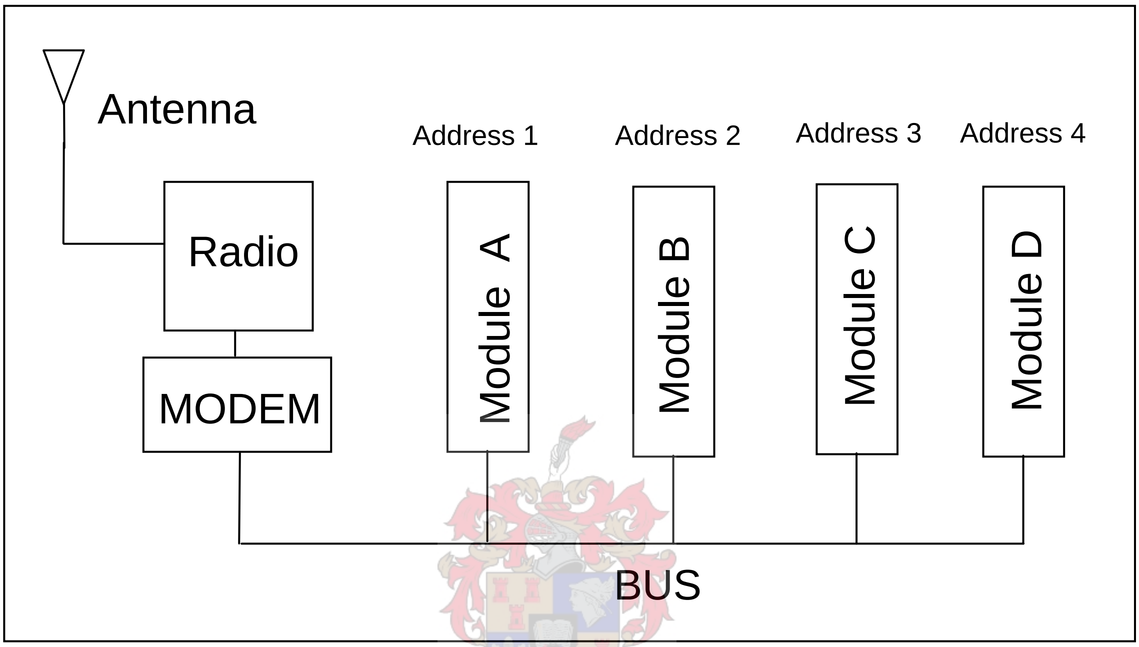


Figure 4.1. Functional block diagram of a multiple address RTU.

The functional block diagram of a single address RTU is shown in Figure 4.2. In this case module A is programmed with a single address and does the decoding for the other modules. Module A acts as a master Central Processing Unit (CPU) and communicates with the other modules either on an integration bus or by some other communications medium. In this case the master module will store all the relevant state changes information and will upload the data to the SCADA master.

The single address topology is preferred to the multiple addresses because it uses less bandwidth and it is easier to configure the RTU. It is also easier to analyse the RTU performance under fault conditions.

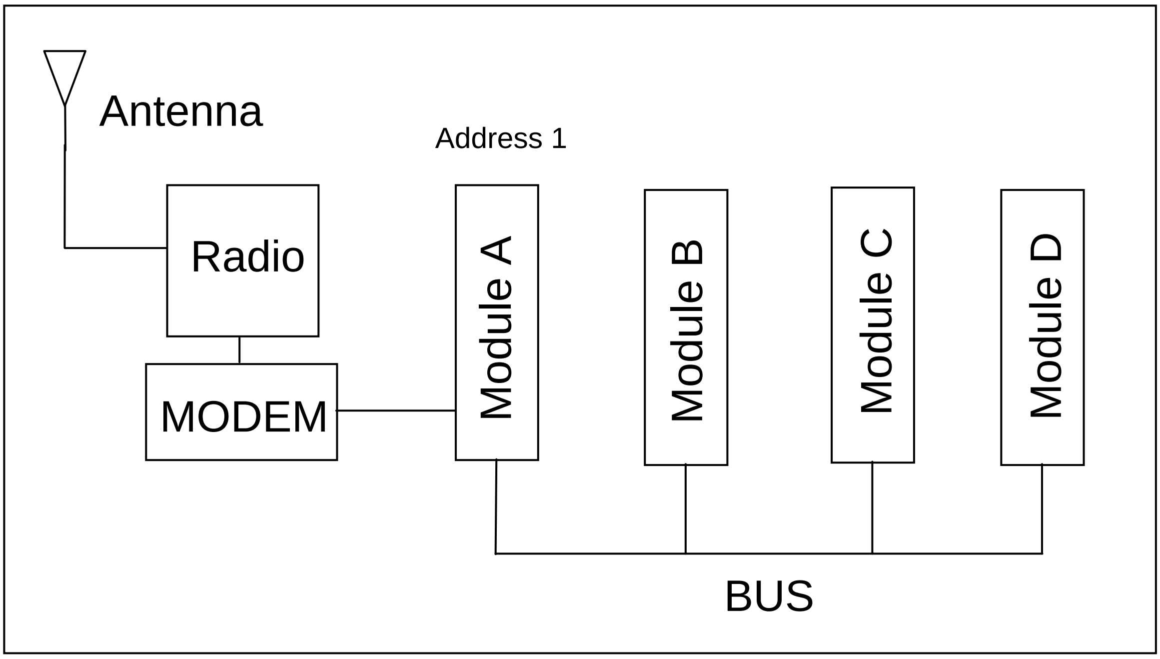


Figure 4.2. Functional block diagram of a single address RTU.

The Remote Terminal Unit (RTU) availability data per protocol was trended for the year 2002 as in Figure 4.3. The performance of the different protocols was compared and it was found that the Pole Mount Remote Terminal Unit (PMRTU) and INTRAC protocols were the worst performers. Both the PMRTU and INTRAC protocols are unsolicited or report by exception protocols, which use area radio communication systems. It was decided to compare the availability performance of RTU types, the availability of repeaters and the availability of individual RTUs with each other to establish the cause of the poor performance.

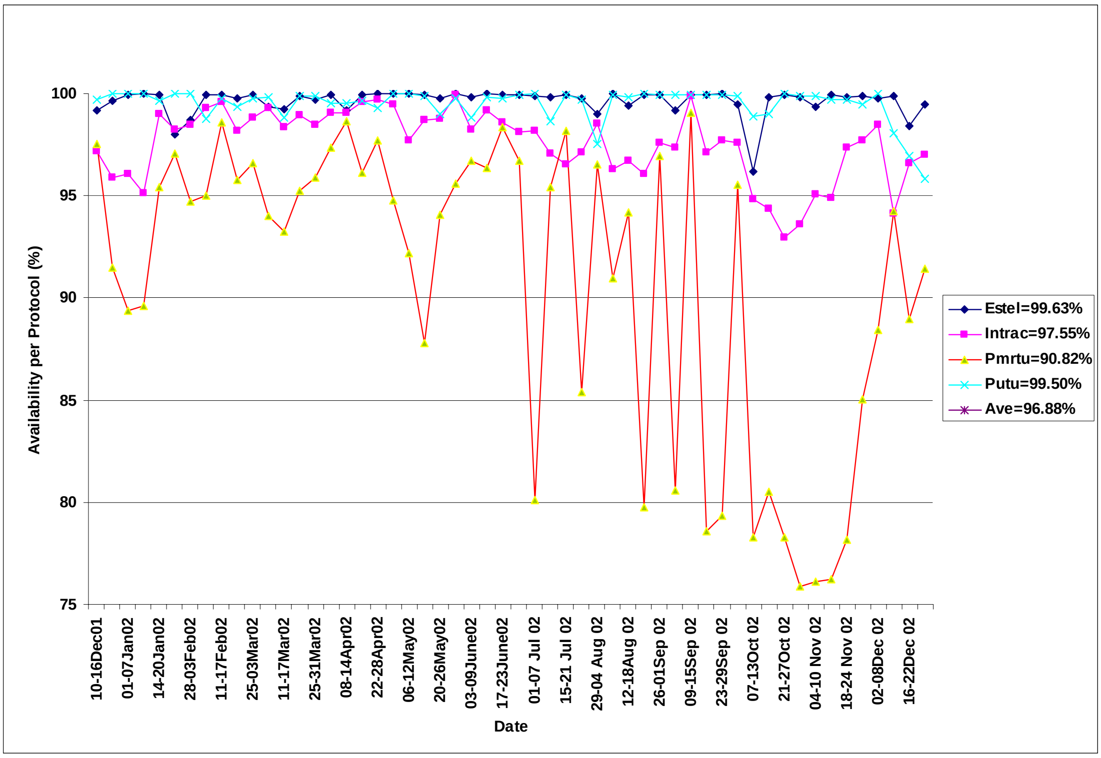


Figure 4.3. Western Region RTU availability for 2002 per RTU protocol.

4.1.1. Availability comparison between RTU types

The availability of the different RTU types was compared to see if there was a specific trend between them. This was done because more than one RTU type used the same protocol. In this case the IST Distribution Remote Terminal Unit (DRTU), IST Pole Mounted Remote Terminal Unit (PMRTU) and CONLOG PMRTU all used the PMRTU protocol. The results of the analysis are shown in Table 4.3.

From the analysis it was found that CONLOG PMRTU was the worst performer with IST PMRTU second and the IST DRTU the third worst performer. It was decided to refurbish all CONLOG PMRTU’s with IST PMRTU’s or upgrade the reclosers with NULEC reclosers. The NULEC reclosers are manufactured with integrated RTUs that use DNP3 as a communication protocol. The decision was also based on manufacturer support for the product as the manufacturing of the CONLOG PMRTU was discontinued. The CONLOG PMRTU installation numbers came down from 54 at the end of the year 2002 to 10 at the end of the year 2005. The IST PMRTU has also lately been discontinued and will also be replaced with NULEC reclosers.

Table 4.3. RTU Performance comparisons per RTU Type for 2002.

RTU Type	Available%	Failed%	Disabled%	Other%
IST ERTU	99.66	0.33	0	0.01
TELKOR PUTU	99.5	0.42	0.01	0.07
Motorola MOSCAD	99.15	0.66	0.14	0.05
Motorola INTRAC	97.14	2.39	0.45	0.03
DRTU(IST DRTU)	95.96	3.18	0.6	0.17
IST PMRTU	93.29	5.85	0.52	0.34
CONLOG PMRTU	91.13	7.53	1.23	0.11

4.1.2. Causes for low RTU availability

The following causes were identified for the low availability:

- Type of radio at the RTU.
- Type of antenna at the RTU.
- Feeder coaxial cable between radio and antenna.
- Load on network (network utilization).
- Polling intervals from the SCADA master.
- Type of RTU protocol on the network.
- Condition of the RTU battery and charger.

The different causes are discussed in more detail below.

4.1.3. Type of radio at the RTU

Radio types with the lowest performance were identified and it was established that they were analogue radios. As a result the analogue radios with MODEMS were replaced with digital radios that came with an integrated MODEM in the radio. The radio is interfaced to the RTU with a standard RS232 interface.

4.1.4.Type of antenna

All RTUs with low performance in bad reception areas were identified and the installed low gain antennas were replaced with high gain antennas because of the higher gain offered by the specific design (e.g. corner reflector antennas). This increased the receive signal strength and ultimately improves the performance of the system.

A guideline for antenna selection for Telecontrol RTU applications were published during November 2003 [17] , which recommended specific antennas, feeder coax cable and connectors.

4.1.5. Feeder cable between radio and antenna

Feeder cables were checked to be within specification according to the standards as recommended [17]. The radio performance of a site can quickly be verified by following measurements:

- Signal strength at the radio antenna input.
- Transmit power level at the radio output.
- Reverse power level at the radio output.

4.1.6. Network utilisation

There were no tests done on network utilisation in the early stages of the project. At that stage there were no measurement tool available and it was decided to focus on the other factors and see if there will be any improvement in performance. The first network utilisations investigations were done towards the end of 2005 and are described in the network utilisation chapter later.

4.1.7. Polling intervals from SCADA master

RTUs on unsolicited networks are polled at certain intervals during the day by the SCADA master. These cycles may vary from every two to eight hours depending on the size of the communication network. Networks with a high installed RTUs capacity are polled less often than smaller networks to compensate for traffic congestion. In practice it may happen that a scheduled poling cycle may start before the previous cycle is completed due to high communication traffic load. Policies on cyclic polling intervals from the SCADA master were reviewed and changed on problematic communication networks.

4.1.8. Type of RTU protocol on network

Some RTU protocols are more robust that others and transmit over another message which will result in corrupted data. A good example is the Estel Variant (EV) protocol compared with the Intrac protocol. When a control is initiated from the SCADA master to a EV RTU all other EV RTUs will back off and wait until a control execute message is transmitted by the selected RTU. This will allow maximum bandwidth to the selected RTU and will result in a higher control success rate.

The Intrac protocol on the other hand will transmit any state of change at the RTU to the SCADA MASTER regardless of any other traffic on the communication system. If the two protocols are on the same communication line this may result in a delay with the control execute message from the EV RTU. This again will cause the SCADA master to timeout the control and will be seen as a control failure.

The policy to use only one RTU protocol on one communication system was accepted and implemented. This sounds simple, but is not always possible in practice. Normally the capital outlay to implement such a policy is not always feasible. In some cases this will mean that a new communication system and a new repeater needs to be installed to service only two RTUs.

The communication systems were reconfigured to keep the mixing of protocols on the same network to the absolute minimum. The result can be seen in the Table 4.8 and Table 4.9. The installed repeater base increased by 20 from the end of the year 2002 to the end of the year 2004 and the number systems increased by 6 during the same period. Some communications systems were split while others were combined in order to optimise the networks.

4.1.9. The condition of the RTU battery and charger

A good battery and effective charger at the RTU are essential. The RTU draws approximately 10 amps when transmitting and the capacity of the battery must also allow the RTU to operate for at least 12 hours when there is a mains power failure at the site. This is to assist operating personnel with the monitoring, assessment and restoring of the failed network.

A policy to periodically test the RTU batteries and chargers was implemented and all batteries are to be replaced every two years. It is important to disconnect the charger from the battery when a load test is done and an appropriate load must be connected to the battery to establish the battery’s capacity.

4.2. Data analysis for year 2003

The list of communication systems and the installed numbers or RTUs as at the end December of 2003 is shown in Table 4.4. A total of 47 repeaters were installed at that stage which serviced 245 RTUs. The network enhancing implementations as described in 4.1.2 were continued during 2003. The availability trends in Figure 4.4 shows an increase in RTU availability performance from 96.87 % average for all protocols at the end of December 2002 to 98.35 % at the end of December 2003. The big dip in performance during April 2003 was due to a complete communication system that was down and was not due to any RTU radio or antenna failures and may be discarded.

Table 4.4. Installation numbers of RTUs per communication system end December 2003.

Communication System	Repeater	RTU's	Protocol
4 Wire E & M	0	22	Solicited
X21	0	41	Solicited
Tygerberg	3	67	Unsolicited
Peninsula	4	45	Unsolicited
Winelands	9	36	Unsolicited
West Coast	8	46	Unsolicited
New South	13	41	Unsolicited
North Cape	10	10	Unsolicited

Table 4.5. Installation numbers for per RTU protocol at the end of December 2003.

RTU / Protocol Type	Installed base per RTU address
ERTU	38
PUTU	16
PMRTU / EV	168
INTRAC	227

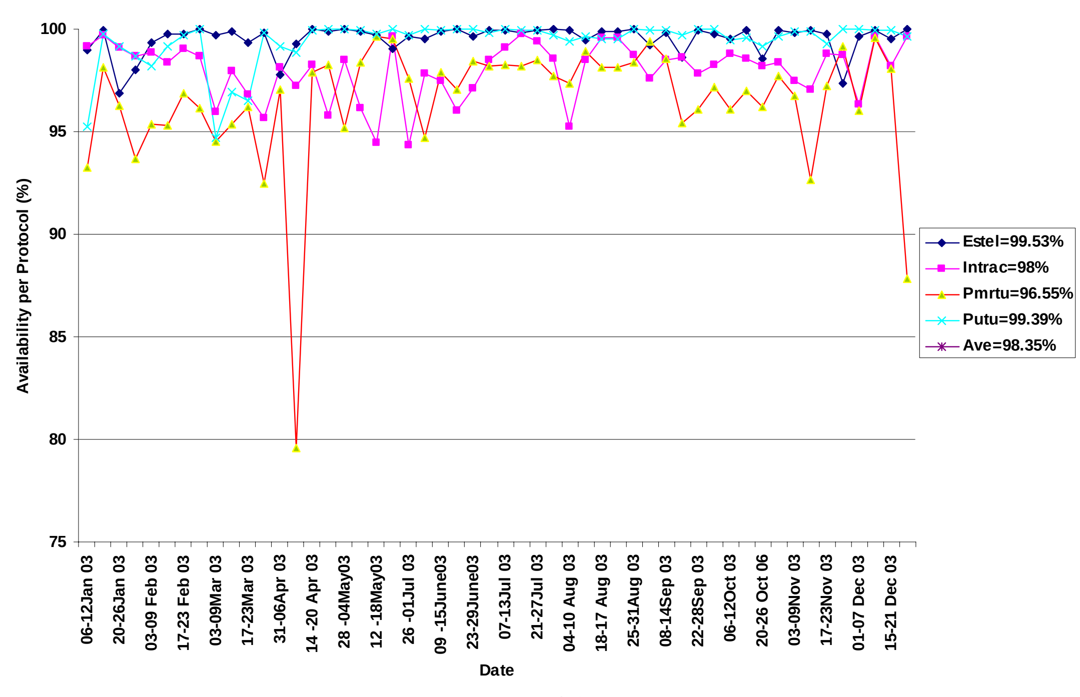


Figure 4.4. Western Region RTU availability for 2003 per RTU protocol.

4.3. Data analysis for year 2004

The main focus during 2004 was to redesign the communication systems as such. The installed telecommunication systems were reconfigured and some systems were split into more than one new telecommunication system. The list of configured telecommunication systems is shown in Table 4.6. There was an increase of 5 radio telecommunication systems from the beginning of January 2003 to the end of December 2004. A total of 57 repeaters were in commission and a total of 262 RTUs were in service. The main focus of the newly designed telecommunication systems was to minimise the usage of multiple protocols per telecommunication system as far as possible and to reduce the number of repeaters per telecommunication.

The reason for that is to minimise traffic per communication system during control messages. A good example is the Estel Variant (EV) protocol which is designed in such a way that all RTUs on a communication network will back off when they receive a *control select* message that was directed to one of the RTUs on the network. The other RTUs will store any state changes that occurred at the site during this time in a buffer and will only transmit this information to the SCADA master after the originally selected RTU has transmitted a *control execute* message to the SCADA master.

This will leave the communication channel open for the one RTU to execute the control and transmit an *execute successful* message to the master. Control timeouts are minimised in this way at the SCADA master. These failures occur when the *execute successful* message is only received after a predefined time has expired at the master after the control was selected. Other protocols like the Motorola Intrac are more robust and will not back off when they receive a *control select* message. They will immediately transmit a change of state and will thus take up valuable bandwidth on the communication system which may result in control timeout failures.

Table 4.6. Installation numbers of RTUs per communication system end December 2004.

Communication System	**Repeater**	**RTU's**	**Protocol**
4 Wire E & M	0	30	Solicited
X21	0	38	Solicited
Tygerberg	1	65	Unsolicited
Peninsula	3	25	Unsolicited
Kanonkop	1	10	Unsolicited
Helderberg	4	17	Unsolicited
West Coast	8	46	Unsolicited
South Coast	15	45	Unsolicited
Karoo	7	13	Unsolicited
North Cape	10	11	Unsolicited
Rooiberg Northern Cape	2	14	Unsolicited
Prieska Northern Cape	2	16	Unsolicited
Komsberg Northern Cape	4	13	Unsolicited

Table 4.7. Installation numbers for per RTU protocol at the end of December 2004.

RTU / Protocol Type	**Installed base per RTU address**
ERTU	48
PUTU	16
PMRTU / EV	170
INTRAC	231
DNP3	61

The result of changes in the telecommunication systems can be seen in Figure 4.5. From February 2004 on the RTU availability for all the RTU protocols was at an average of above 97 %. The average availability changed from 96.87 % in 2002 to 99.17 % in 2004. This is an increase of 2.83 % for 432 RTUs.

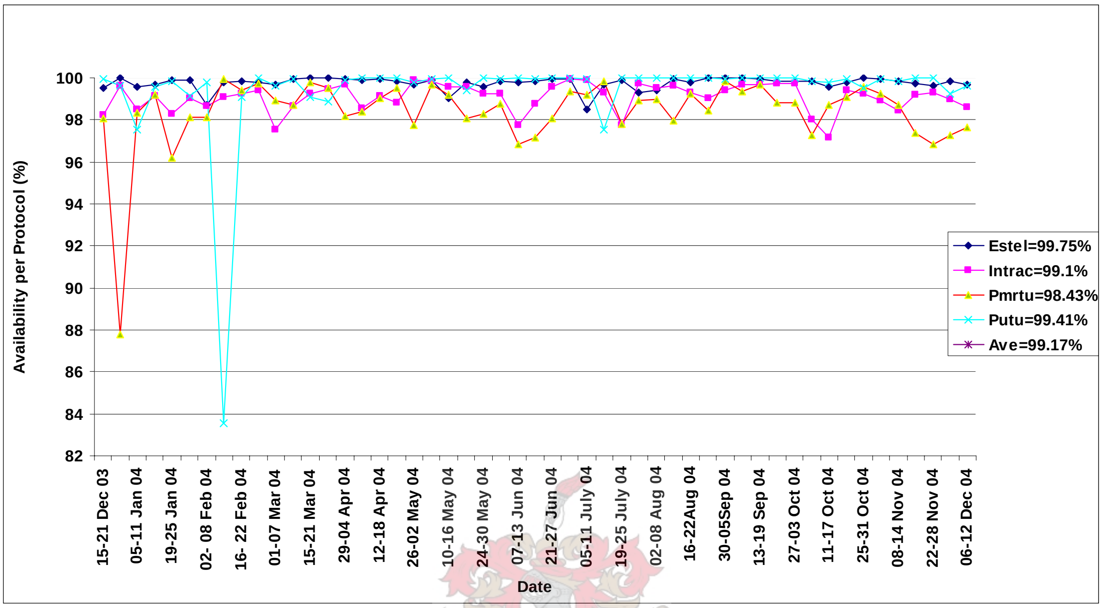


Figure 4.5. Western region RTU availability for 2004 per RTU protocol.

The numbers in Table 4.8 and Table 4.9 depict the changes to the telecommunication systems from December 2002 to December 2004. The installed repeater numbers as shown in Table 4.8 shows the increase from 37 in 2002 to 57 in 2004, which is an increase of 20 repeaters. The numbers in Table 4.9 depict the increase of 6 telecommunication systems from December 2002 to December 2004.

Table 4.8. Increase in repeaters per year.

Year	Repeaters
2002	37
2003	47
2004	57

Table 4.9. Increase in communication networks per year.

Year	Systems
2002	7
2003	8
2004	13

4.4. Specific RTU case study

Khayalitsha Sub Station is a good example of a site that was identified as a RTU with an unacceptable low RTU availability during 2002. The radio and antenna was replaced during August 2002 and average availability increase from 91.21 % for the first six months of the year 2002 to 98.56 % for the last six months of the year 2002. The availability trend for the Khayalitsha RTU is shown in Figure 4.6.

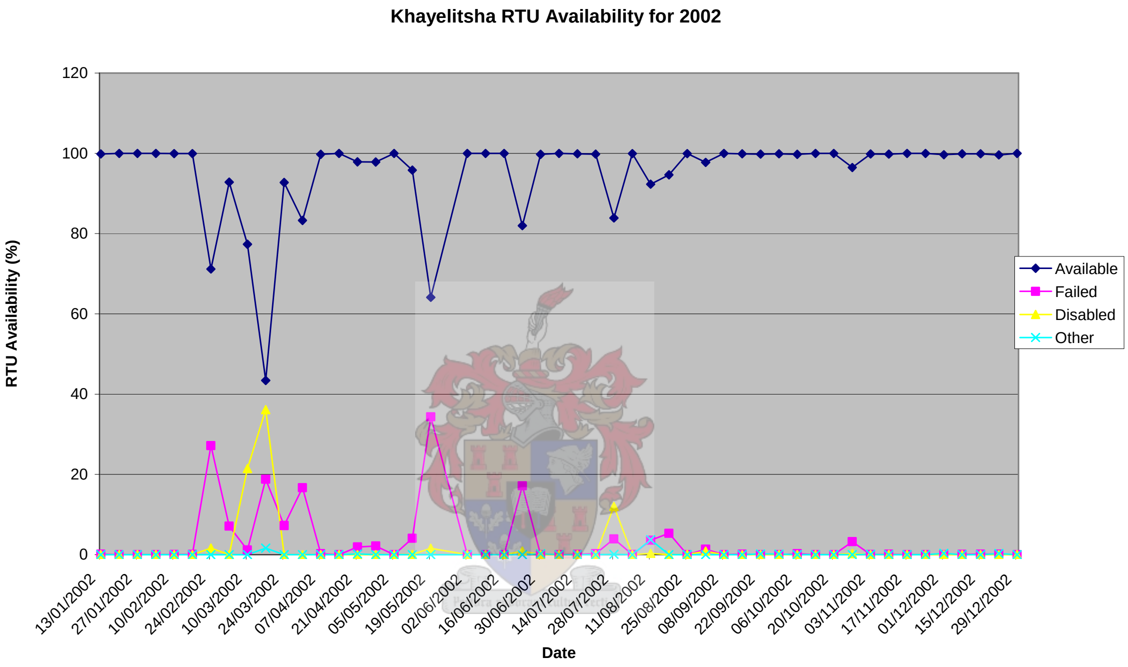


Figure 4.6. RTU availability at Khayelitsha sub station for year 2002.

4.5. DNP3 availability analysis

The first Distributed Network Protocol version 3 (DNP3) Remote Terminal Unit (RTU) installation in Western Region was done during January 2005. Data was captured and analysed to compare the availability data of DNP3 with the other protocols. The information coming from the analysis is displayed in Figure 4.7 and the results showed that DNP3 is currently the worst performing protocol of all unsolicited protocols. The average RTU availability for DNP3 from January 2005 up to June 2005 was 96.9 %. This low performance was perceived as teething problems due to the new technology.

From July 2005 there was an increase in RTU availability for DNP3 of 1.4% to 98.3% at the end of August and at that stage it was thought that the teething problems have been sorted out as the DNP3 performance was on par with the other area radio based protocols. The performance of the performance of DNP3 however declined again by 1.7 % between September and October 2005 and was measured at an average of 96 % for the two months. The average performance measured for DNP3 from January 2005 up to October 2005 was 97.21 %, which is 1.43 % lower that the average RTU availability for all protocols.

The low RTU availability performance for DNP3 is of great concern as this is seen as the new standard that needs to be implemented for Eskom Distribution. A thorough investigation needs to be done to establish the cause of the low RTU availability performance of the DNP3 installations.

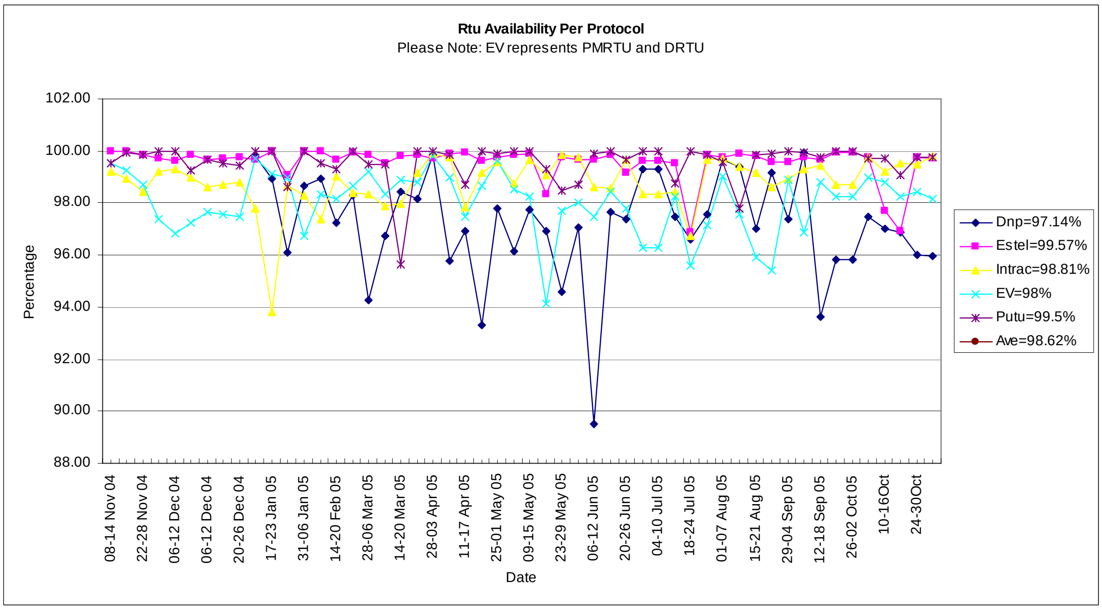


Figure 4.7. Western region RTU availability for 12 Months up to October2005 per RTU protocol.

5. Control success rate

With the RTU Availability at an acceptable percentage it was decided to concentrate on the Control Success Rate (CSR). Data pertaining to CSR was collected from Dec 2001, but the data at that stage was very basic and only supplied the number of controls sent out and the number of failures. This data was used to trend the CRS graphically, but was too limited to do any further analysis on. The data available was used calculate and trend the CSR and it was decided to use only the data from January 2002 up to December 2004, which is the same range that was used for the RTU availability analysis.

A new query was written to extract the data from the SCADA master towards the end of 2004 and the specifications for RTU Monitor were changed and developed by the software company. This data was used to investigate the control failure causes later in this chapter. The following data required was extracted from the SCADA master as from the end of 2004:

- Date and Time that the control was dispatched and executed..
- Site to which the control was dispatched.
- The device where the control was sent to (e.g. Farmers 1 Breaker).
- Type of control dispatched (e.g. Close, Open).
- Control message generated by the SCADA master (e.g. Control Failed, Control Successful).
- User who dispatched the control.
- Desk from where the control was dispatched.

The data as depicted in Table 5.1. is an example of the data produced from the query.

Table 5.1. Control data format example.

Date and Time	**Site**	**Device**	**Control**	**Message**	**Initiator**	**Desk**
16/08/2004 10:20:52	KHYLTS_D	11A_RING_BKR	TRIP	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 10:26:33	KHYLTS_D	11A_RING_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 10:31:28	TEST_SUB	BELHAR1_BKR	TRIP	CONTROL EXECUTE	CONTROL	SAWK08
16/08/2004 12:46:19	BRENTWD	11KV_BSEC2_BKR	TRIP	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 12:51:05	BRENTWD	11KV_BSEC2_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK03
16/08/2004 14:42:18	MULDRSVL	TRACT_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK02
16/08/2004 16:27:57	_BOWER	OVERH2_RC260	CLOS	CONTROL EXECUTE	ENGINEER	SAWK08
16/08/2004 18:02:53	DEZALZE	FARM1_BKR	CLOS	CONTROL EXECUTE	CONTROL	SAWK02

5.1. Control failure analysis.

The Control Success Rate (CSR) data for 2002 were captured and trended in the graph shown in Figure 5.1 and the average CSR for the year 2002 was calculated at 77.65 %. The CRS ranged from 62 % up to 92 % during the year and no trend could be established between known factors such as season and weather. At that stage only limited data pertaining to control failures causes were available. Investigations done on the limited data available indicated that some of the failures were caused by repeated controls that were executed by the control personnel to devices at substations after breakers have tripped. When this was investigated it was found that control personnel were not always aware of alarms or flags coming in from the RTUs indicating that it was impossible to execute a control. This was either due to limited information coming from the RTUs or in some cases due to a lack of system knowledge. Specific training procedures for the control personnel were put in place to eliminate this problem.

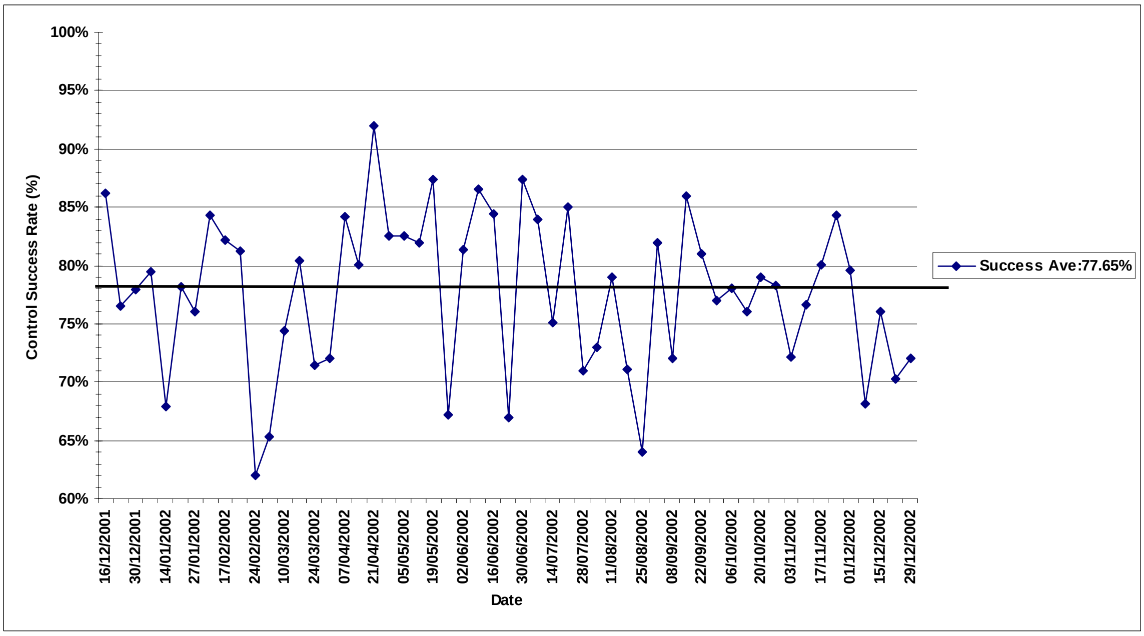


Figure 5.1. Controllers Control Success Rate for Western Region 2002.

The Control Success Rate (CSR) data for the year 2003 were captured and trended in the graph shown in Figure 5.2. The CSR trend for the year 2003 compares very well with the CSR trend for the year 2002. This implicates that the changes in the telecommunication systems as described in Chapter 4 had no or little effect on the CSR. As in 2002 there were no data available to establish control failures during 2003.

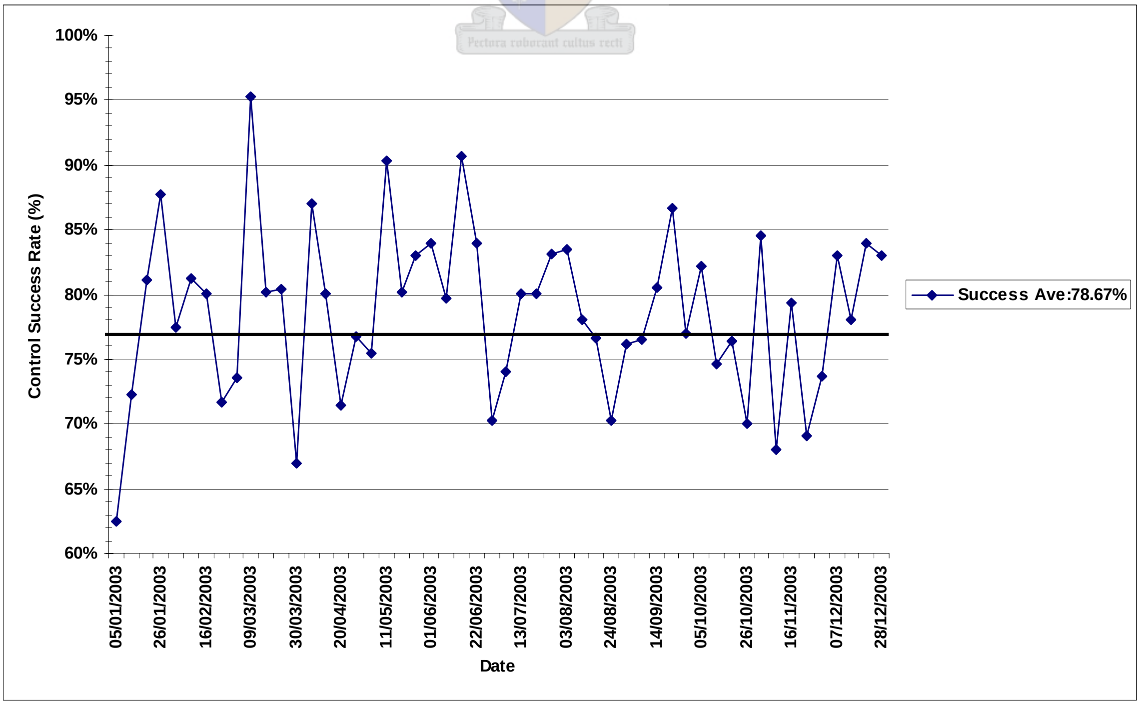


Figure 5.2. Controllers Control Success Rate for Western Region 2003.

From this one can conclude that the changing of antennas and radios that had a major effect on the RTU availability from middle 2003 on did not influence the CSR at all. More had to be done to increase the control success rate.

As discussed in Chapter 4 the main focus during 2004 was to redesign the communication systems as such. Current telecommunication systems were reconfigured into more that one system and new telecommunication systems were commissioned. The main focus of the newly designed telecommunication systems was to minimise the usage of multiple protocols per telecommunication system as far as possible and to reduce the number of repeaters per telecommunication system.

The reason for that is to minimise traffic per communication system during control messages. For example the Estel Varian (EV) protocol is designed in such a way that all RTUs on a communication network will back off when they receive a *control select* message that was directed to one of the RTUs on the network. The other RTUs will store any state changes that occurred at the site during this time in a buffer and will only transmit this information to the SCADA master after the original selected RTU has transmitted a *control execute* message to the SCADA master.

Up to May 2004 there was no visible change in the average control success rate (CSR). The implementation of the networks optimisation was done during May 2004 and from there on the CSR was remarkably better. From this we can conclude that the usage of more than one protocol on the same network was a major contributor to the low CSR. The control success average for the year 2004 was 80.88 %, which was 2.21% better than for the year 2003. The increase in control success rate was only visible after May 2004 and the result will only be realized in the value for twelve months prior to June 2005 which was 84.38 %. There was thus an increase of 5.62 % from December 2003 to June 2005. The graph in Figure 5.3 shows the increase in CSR after May 2004.

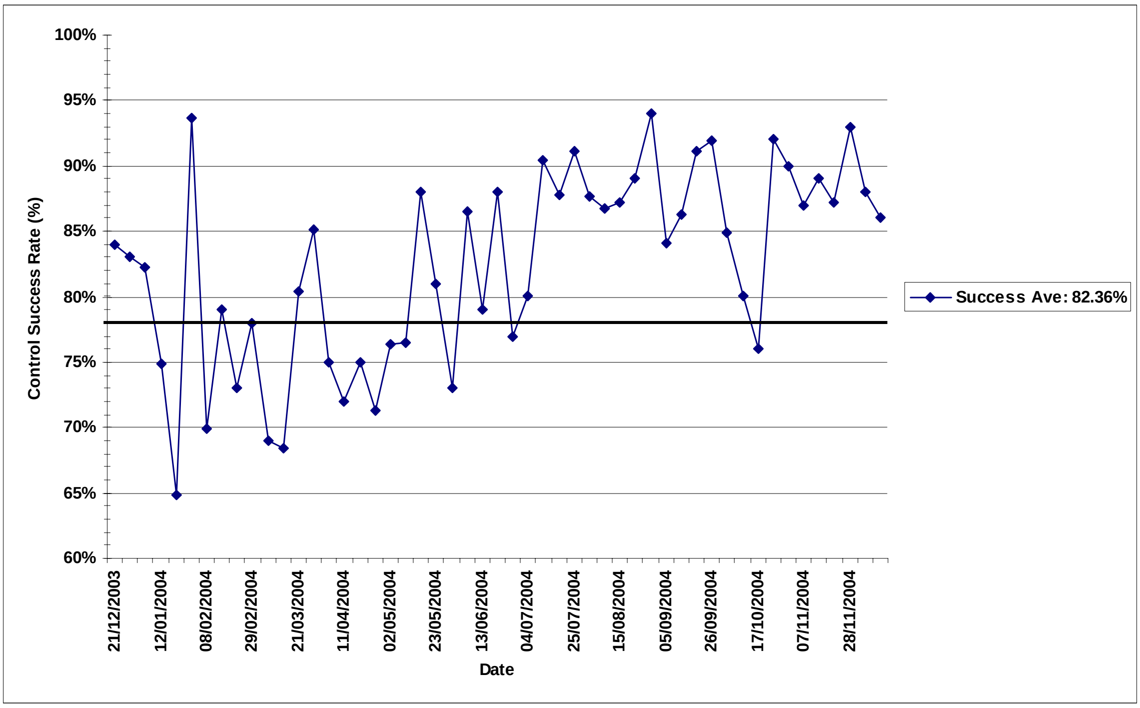


Figure 5.3. Controllers Control Success Rate for Western Region 2004.

5.2. Failure causes

Data from January 2002 to December 2004 was analyzed to establish the main control failure causes. These causes were defined as follows:

- Plant failure.
- Communication or plant failure.
- Communication delayed indication.
- Communication failure.

5.2.1. Plant failure

These are defined as all failures due to HV plant failure causes. This include breaker failures, damaged structures and poles, trees on lines, broken feeders, cables, isolators and fuses. The complete list is shown in Table 5.2.

5.2.2. Communication or plant failure

In some cases there is not enough information available to distinguish between a plant or communication failure. With these cases they are classed as *Communication or Plant Failures*.

5.2.3. Communication delayed indication

A timer is set at the SCADA master when the SCADA master initiates a *control* message to a RTU. If a *control execute successful* reply is not received from the selected RTU within a pre-defined time the control will be classed as a failure even if the control was executed at the site. These are normally caused by traffic congestion on the communication system.

5.2.4. Communication failure

Communication failures are defined as all failures due to a failed communication system. This includes the communication line, MODEMS, radios, antennas, repeaters, antenna feeder cable or it may also be a due to a power failure. The control failure causes for the year 2002 up to the year 2004 were investigated and are displayed in Figures 5.4, Figure 5.5. and Figure 5.6. The comparison between the three years is displayed in Figure 5.7.

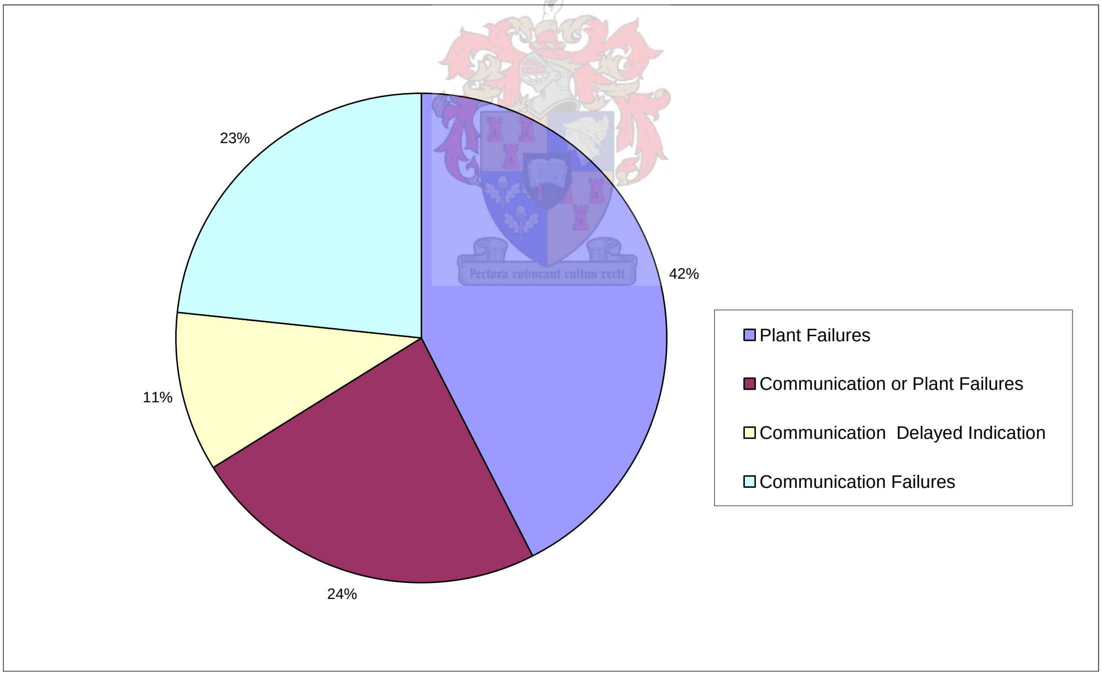


Figure 5.4. Control failure causes for 2002.

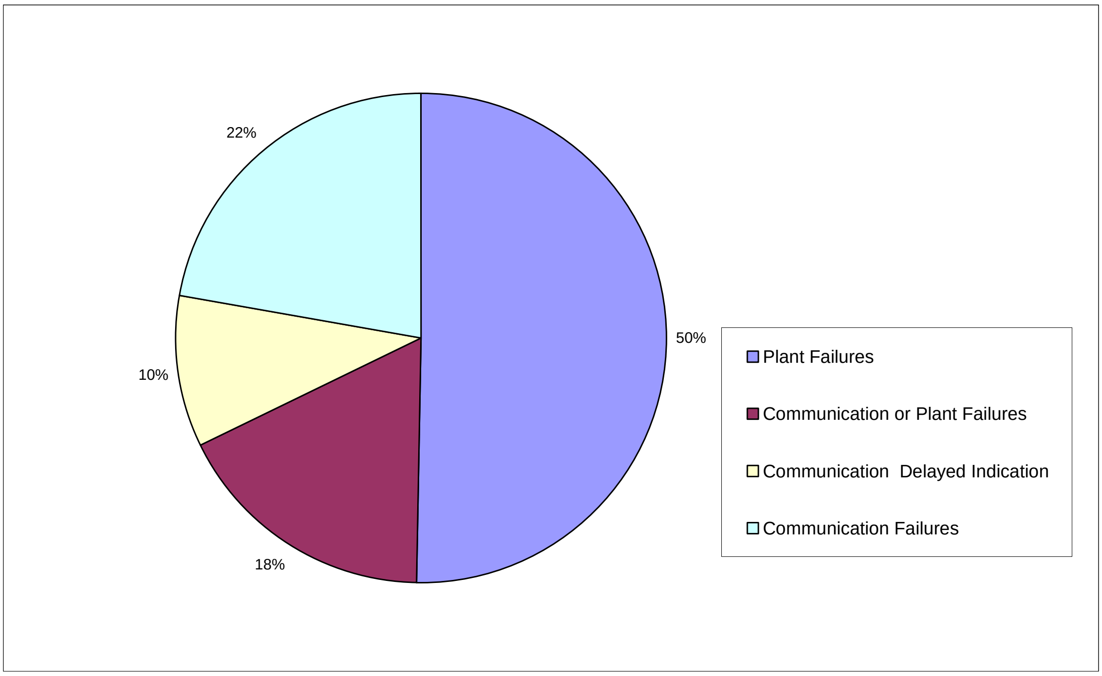


Figure 5.5. Control failure causes for 2003.

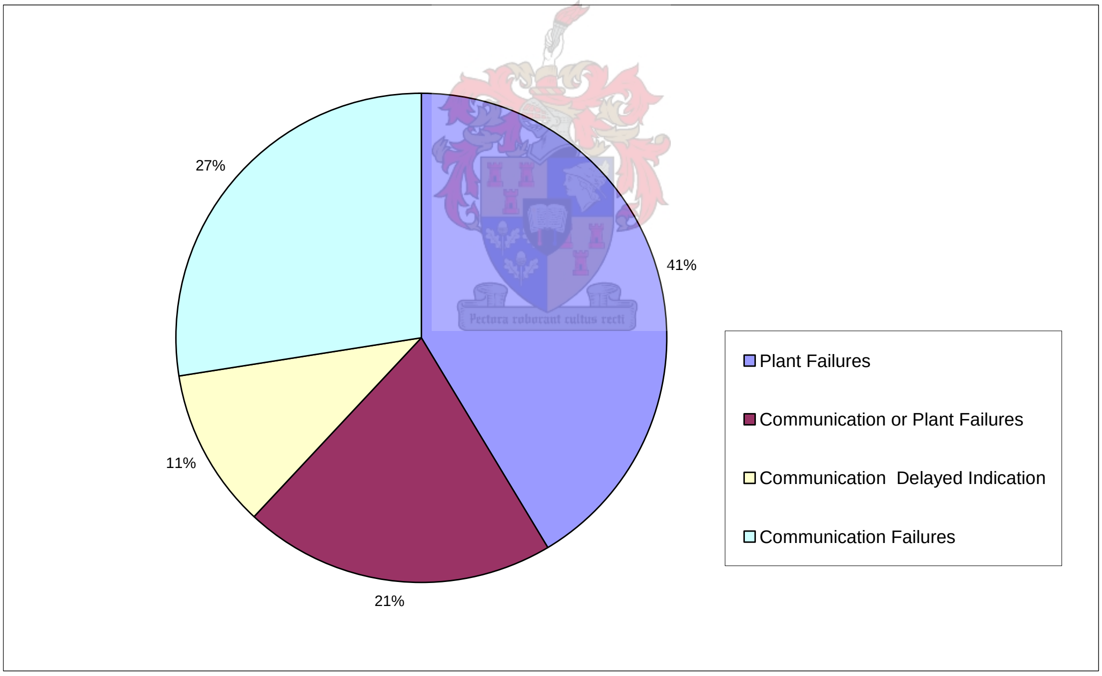


Figure 5.6. Control failure causes for 2004.

It is interesting to note that the trends are very similar every year. More information is needed for an in-depth study. The trends for the different causes over the three years are shown in Figure 5.7. This is displayed on an average per week. From this one can conclude that plant failures are the biggest cause for control failures per year and need to be investigated further.

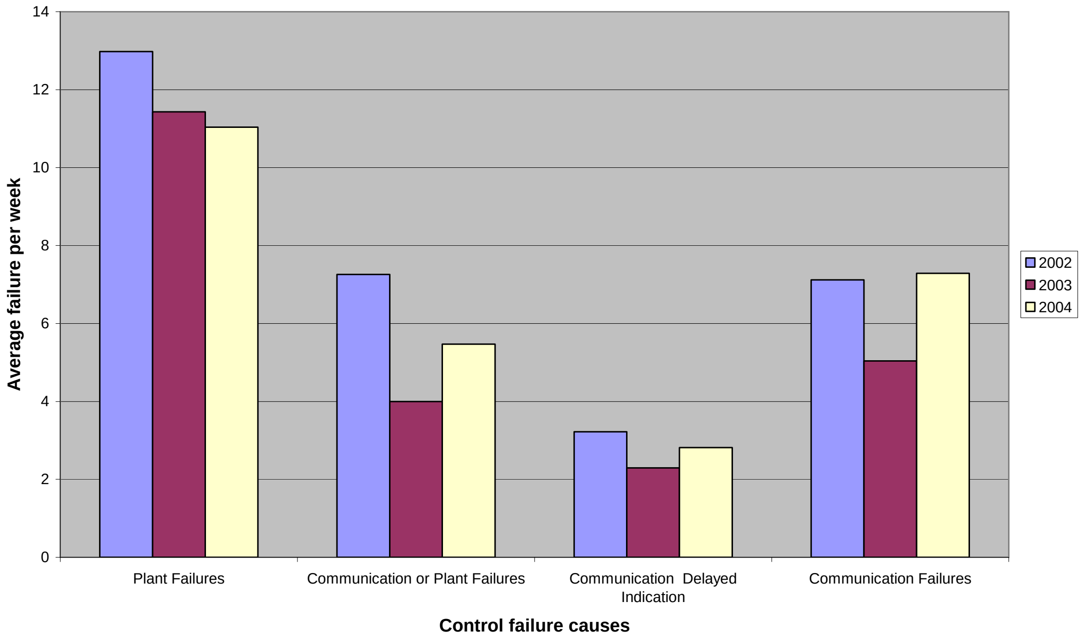


Figure 5.7. Control failure cause comparison per year.

5.3. Plant failures analysis

The individual plant failures were investigated and the different causes are shown in Table 5.2. In the investigation it was found that the biggest contributing factor to the plant failures was Sensitive Earth Faults (SEFs).

Control fails caused by SEFs can be explained as follows. Figure 5.8. shows an example a sensitive earth fault on a power line. The breaker at the sub station will operate, but will not try to Auto Re Close (ARC) due to the SEF flag that was set at the protection equipment.

This will also inhibit the RTU to close the breaker remotely from the SCADA master. This is done as a safety measure to inhibit power restoration in the case of a broken wire lying on the ground and for example has melted the ground and does not cause a high current fault. If this feeder is then reenergized it will cause a potential hazardous condition for any living being that may come in contact with the feeder on the ground.

The correct procedure will be for the controller at the control centre to dispatch a field team to patrol the feeder and do a physical search for any irregularity. If there are no physical damage or after the damage is restored the field team must manually reset the SEF flag. Only then the control personnel will be able to close the breaker remotely from the SCADA master or the field team at the site can initiate a manual close on the protection equipment panel.

A parameters set for a breaker to trip on SEF is low current for a long period. This is approximately between 4 and 7 A for a time period of 5 s. These setting will differ between geographical areas and feeder schemes.

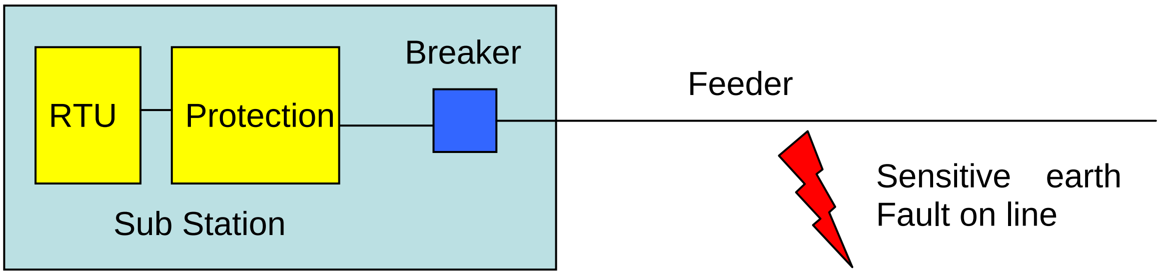


Figure 5.8. Graphical explanation of sensitive earth fault.

The data in Table 5.2. is also graphically displayed in Figure 5.9. It clearly shows the high percentage of SEF related control failures. All causes that occurred less than 10 times for the year was lumped into the “other” bracket but their detail can all be seen in Table 5.2.

Table 5.2. Number of failure causes for 2004 per failure cause type.

Plant failure cause	Number of failures	Plant failure cause	Number of failures
Bird	8	Overhead Line	3
Breaker	4	Phase fault	4
Bushings	3	Pole	5
Cable	8	Pole	2
Conductor	26	Protection Fail	6
Fire	7	Reclose lock out	26
Fuse	67	Sensitive Earth Fault	167
High Voltage	2	Springtimer	1
Isolator	10	Theft	5
Jumper	35	Tower	2
Lighting	7	Transformer	4
Line	6	Tree	17
Link	6	Vehicle	7
Overcurrent	24	VT fail	6

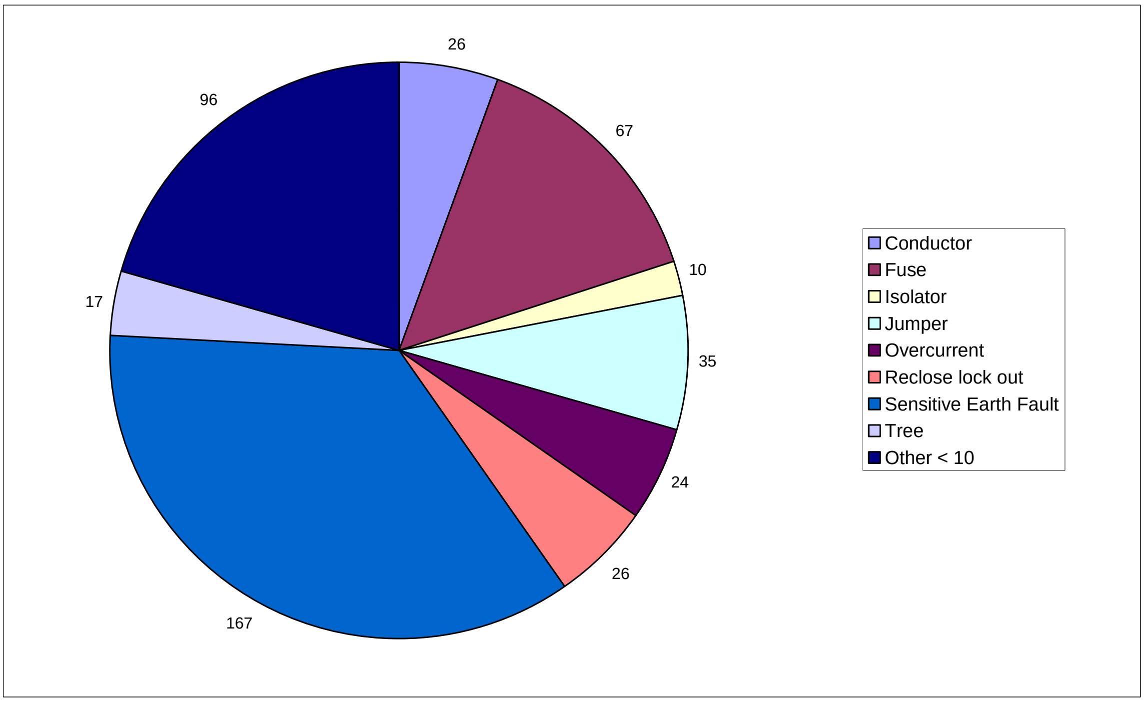


Figure 5.9. Plant failure causes that caused control failures for 2004.

The current data available on the log sheets are not enough to do a more comprehensive study. More in-depth research needs to be done on the SEF caused control failures, as there may be a solution to minimize these failures. There may be a significant change in control success rate if the SEF related failures could be kept to a minimum.

5.4. RTUs with low control success rate

The data from the query as described in the beginning of the chapter assisted with the identification of specific sites with low performance. A study was done to identify the RTUs with the worst control success rate on data captured from September 2004 up to August 2005 and the results are published in Table 5.3. A total of eight sites were identified with a control success rate of 0 % and on further investigation it was found that all RTUs were CONLOG PMRTU's. This does not necessarily mean that the CONLOG PMRTU is the worst performer as other factors may have caused the control success rate, for example the site may be in a geographical area where the area communication is also bad or it may be due to equipment failure.

Not enough time was available to investigate the causes of the low success rate at the identified sites. It is recommended that all sites need to be investigated individually as there may be various contributing factors to the low control success rate. Three of the sites in Table 5.3. have subsequently been decommissioned, namely DR3_R280, DR3_R284 and LG2_R348. The CONLOG PMRTU's were replaced by IST PMRTU's , while the RTU protocol was also changed from Estel Variant (EV) to DNP3 on the new installations. The performance of the new RTUs need to be evaluated over the next six months to establish if there are any change to the performance of the control success rate.

Table 5.3. RTUs identified with 0% control success rate.

RTU Name	**Controls Send Out**	**Controls Successful**	**Failed Returns**	**Control Success Rate (%)**
AL2_R520	5	0	5	0
DR3_R280	23	0	23	0
DR3_R284	26	0	26	0
GYDO1	2	0	2	0
HU1_R14	3	0	3	0
LG2_R348	14	0	14	0
MN2_R88	5	0	5	0
RT1_R421	3	1	3	0

6. Network Utilization

6.1 Introduction

The following network study was done to establish the network utilization on two networks. For this exercise it was decided to analyse only Remote Terminal Units (RTUs) which use the Estel Variant (EV) protocol due to time constraints and also due to the fact that there are currently only a few DP3 RTUs in the Cape Peninsula area. The majority of RTUs currently are EV protocol.

Two networks which were both accessible from Stellenbosch were chosen and on which the majority of RTUs were using the EV protocol, namely Tygerberg network and Helderberg network. The Tygerberg network topology had 3 repeaters which serviced 84 RTUs and the Helderberg network 4 repeaters that serviced 22 RTUs. The Tygerberg network was also the biggest network in the Western Region, where the Helderberg network the smallest at that stage.

Two corner reflector antennas were installed on the roof of the Engineering Faculty at the University of Stellenbosch and connected to two TAIT 2015 digital radios. This is the same antennas and radios that are installed at most of the RTU sites. Low loss RG 213 coaxial cable was used to minimise losses due to the long distance between the antennas and radios. The TAIT radios are manufactured with a RS232 port which made it easy to connect to a serial port on a standard personal computer (PC). The data was parsed live into a database on the PC and a small user interface was developed to do data analysis and graphical trends. The block diagram in Figure 6.1. shows the setup that was used to capture and analyse the data from the two networks.

It was decided to use MySQL as a server because the software is freeware and do not require any licence fees. The operating system used was Windows 2000 Professional and the user interface was written and compiled in Delphi.

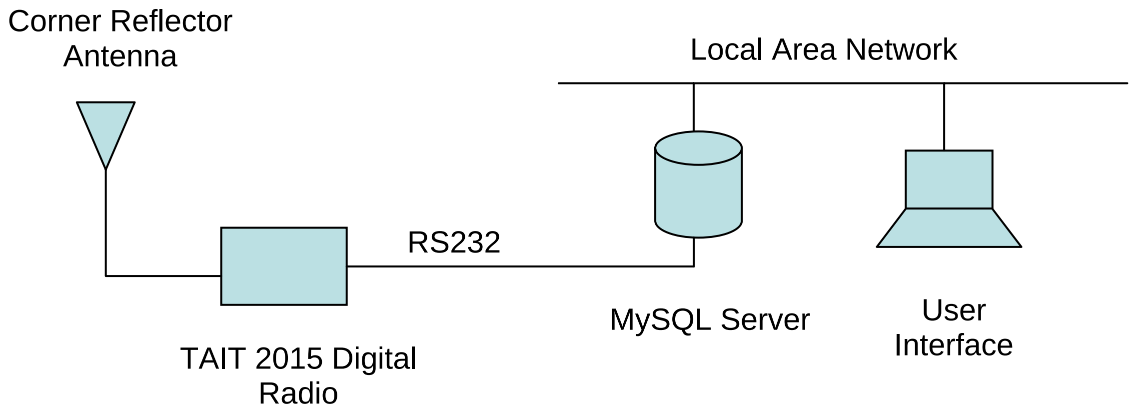


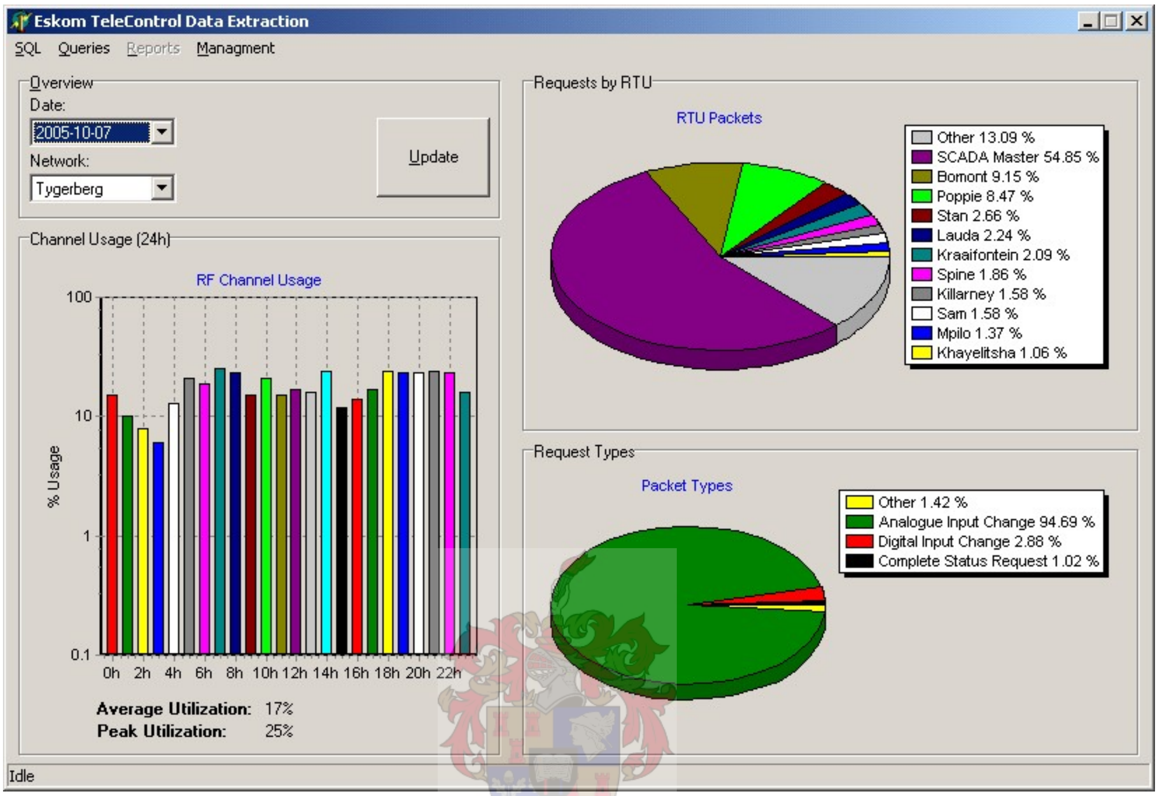
Figure 6.1. Block diagram of area radio network analysis setup.

6.2. Tygerberg network data analysis

The data for the day of 7 October 2005 was analysed and the different graphs are presented in Figure 6.2. The Tygerberg communication system had an average utilisation of 17 % and a peak utilisation of 25 % for the day. This compares well with the recommended value of 40 % specified by the IEEE standard 999-1992 (Recommended channel utilisation for a SCADA communication network) [20] and is also well within the Ethernet specified capacity of 30 % [19]. It is also within the recommended value of 35 % by the ESKOM user requirement document DSP0009 [18].

Two sites were standing out with higher that average utilisation when the site utilisation was analysed, namely Bomont and Poppie. The results can be seen in the utilisation pie chart per RTU in Figure 6.1. The utilisation for Poppie was measured at 8.47 % and the utilisation for Bomont was measured at 9.15 %. Both sites were situated in industrial areas and were thus subjected to high changes in load due to the starting of pumps and other heavy machinery, which will caused continuous fluctuations in analogue values. The RTUs at such sites will tend to transmit more analogue updates to the SCADA master and will thus increase the network utilisation.

It is also interesting to note that of the Supervisory Control and Data Acquisition (SCADA) message request types the *analogue input change* type occupied the most of the network activity measured at 94.69 % *with digital input change* second at 2.88 %. The *complete status request* type was measured at 1.02 %. This is normal as the request is only done up to four times per day and is used by the SCADA master to cyclically interrogate the RTUs at a pre-defined times to establish if the RTUs are still operational. It is these requests that are used to determine the RTU availability data as discussed earlier.



Date: 2005-10-07

Network: Tygerberg

Average Utilization: 17%

Peak Utilization: 25%

Idle

Figure 6.2. Tygerberg network utilisation for 7 October 2005.

The data from Bomont was analysed and is graphically presented in Figure 6.3. It was established that most of the data was generated by only two analogues inputs, namely analogue 20 and 21. The *analogue input change message* type was measured at 99.85 %, which was much higher that the average for the complete Tygerberg network, which was measured 94.69 %. A work order was created on the work management system and a technician was dispatched to investigate the abnormal analogue activity at the site. It was found that the RTU was configured correctly and the unusual number of updates was due to high activity on the customer site which influenced the analogue changes. These were mainly due to electrical pumps connected to the power network.

The only option to lower the analogue updates will be to change the analogue jitter factor as described in 1.4.6. that is programmed into the RTU. The current standard in the ESKOM Western region is 80 counts out of a full-scale count of 2048, which translates into a 4 % jitter or delta update window. The only solution in this case will be to change the current jitter factor from the standard to a higher value. The number of packet per hour as shown in Figure 6.3 also depict that there were less activity just after 20h00, but high activity starts again after midnight.

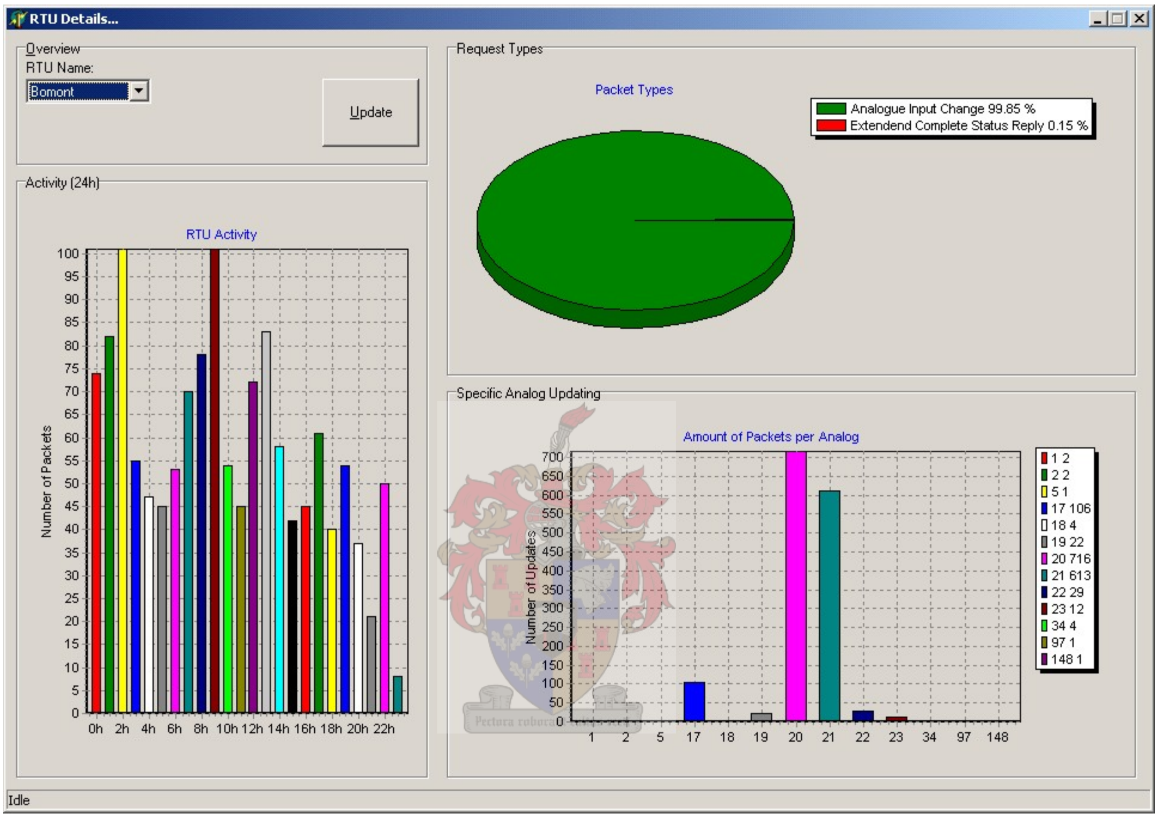

RTU Name: Bomont

Figure 6.3. Bomont network utilisation for 7 October 2005.

The utilisation for Bomont was trended over a period of three weeks and the results are shown in Figure 6.4. The measured utilisation values ranged from 7.8 % to 18.2 % with an average of 9.95 %. This is clearly too high for one single RTU and measures should be taken to reduce radio network traffic from the site. As discussed earlier this can only be done with the change of analogue delta windows.

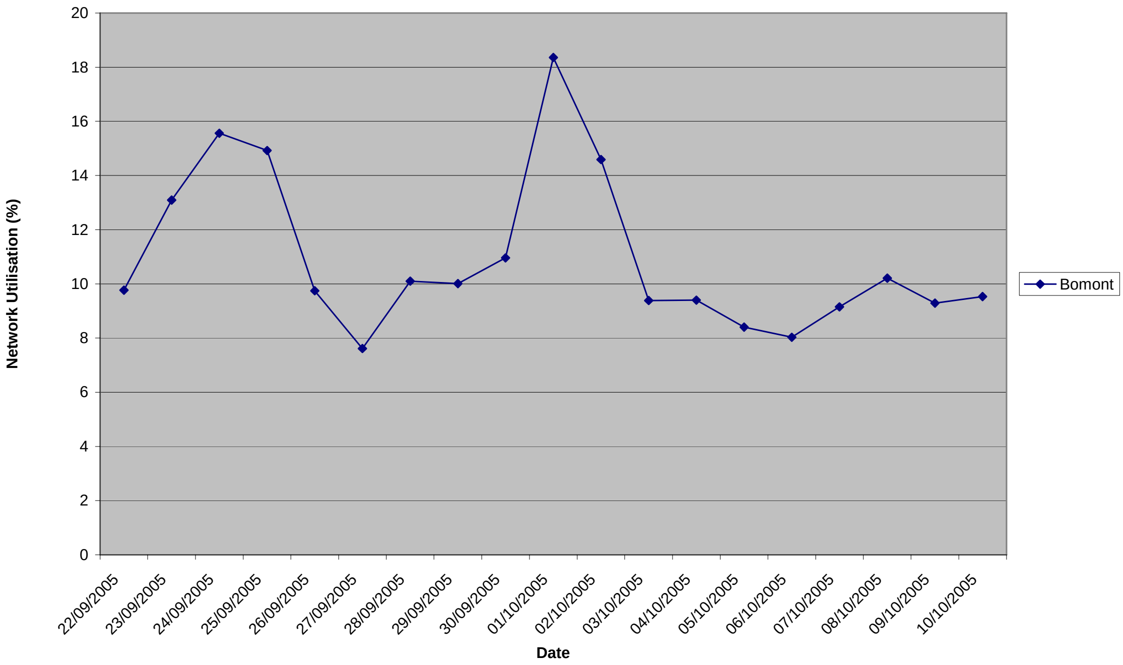


Figure 6.4. Bomont network utilisation trended over a three-week period.

The data from Poppie was also analysed and is graphically presented in Figure 6.5. It was found that the data was generated by only two analogues, namely analogue 17 and 19. The *analogue input change* message type was also measured at 99.84 %, which is as in the case of Bomont much higher that the average for the complete Tygerberg network, which were measured at 94.69 %. The number of packet per hour as shown in Figure 6.5. also depicts that the activity at the site starts after 8h00 in the morning and slows down after 22h00 the evening.

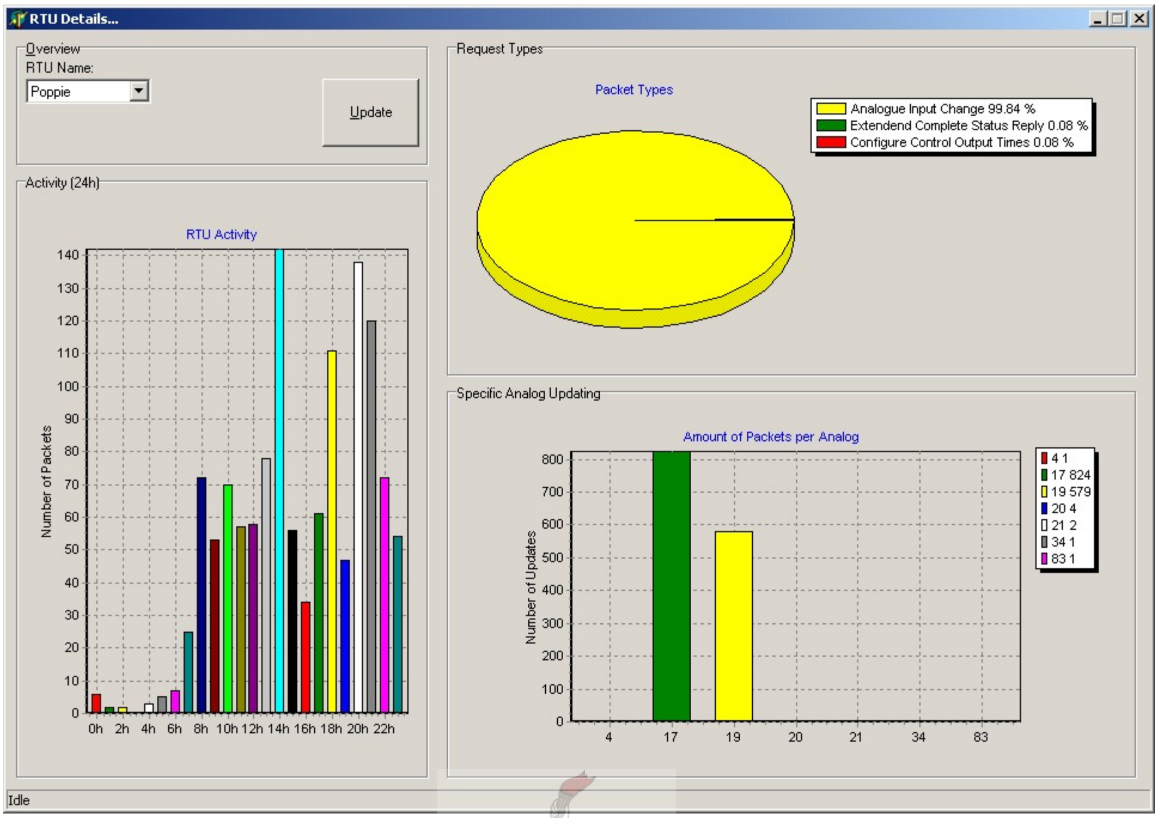

RTU Name: Poppie

Figure 6.5. Poppie network utilisation for 7 October 2005.

The utilisation for Poppie was trended over a period of three weeks to compare this with the results from Bomont. The results are shown in Figure 6.6. The values ranged from 7.8 % to 18.2 % with an average of 9.95 %. The high network utilisation in Figure 6.6. from 26 September 2005 to 29 September 2005 was observed and investigated. It was found that there was abnormal activity at the sub station during that time in the form of new plant commissioning which resulted in above normal switching. This increased the network utilization due to the extra controls being executed, analogue updates as well as digital input changes. From this we can conclude that Poppie is functioning within acceptable specifications.

The radio network utilisation for Tygerberg network was also trended over a three week period to establish if any abnormal activities occurred during this time. The results are presented in Figure 6.7. The average utilisation for the three weeks is 18.42 % and the average of peak values is 31 %. From this we can conclude that even being the most complex network, the Tygerberg network utilisation is still within ESKOM and International specifications for area radio SCADA networks.

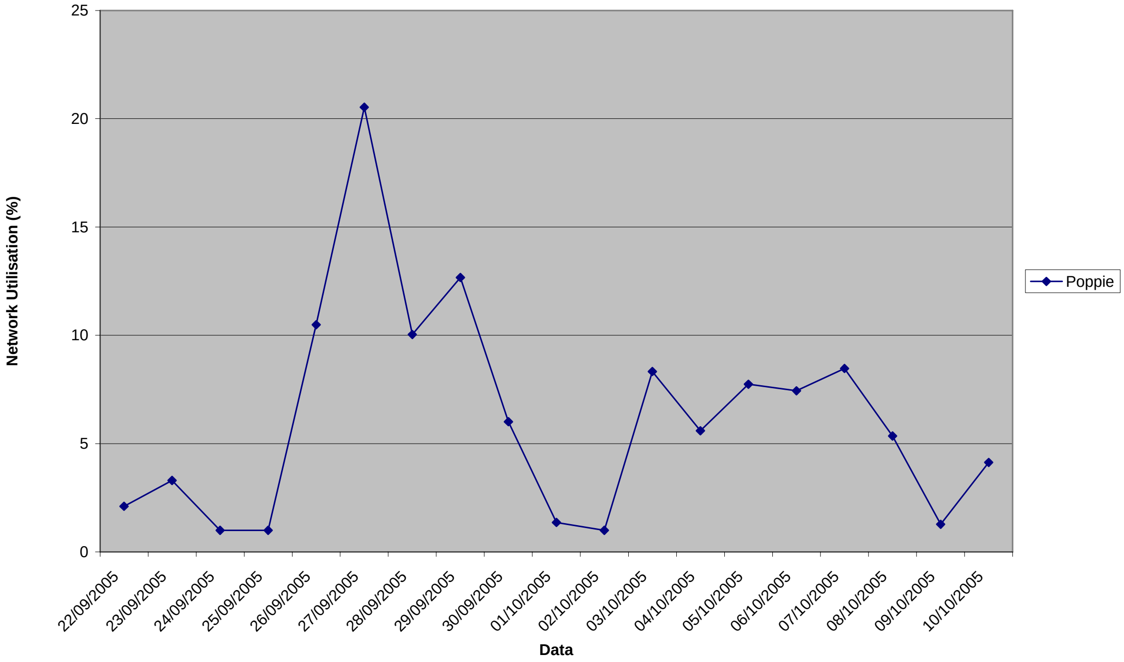


Figure 6.6. Poppie network utilisation trended over a three week period.

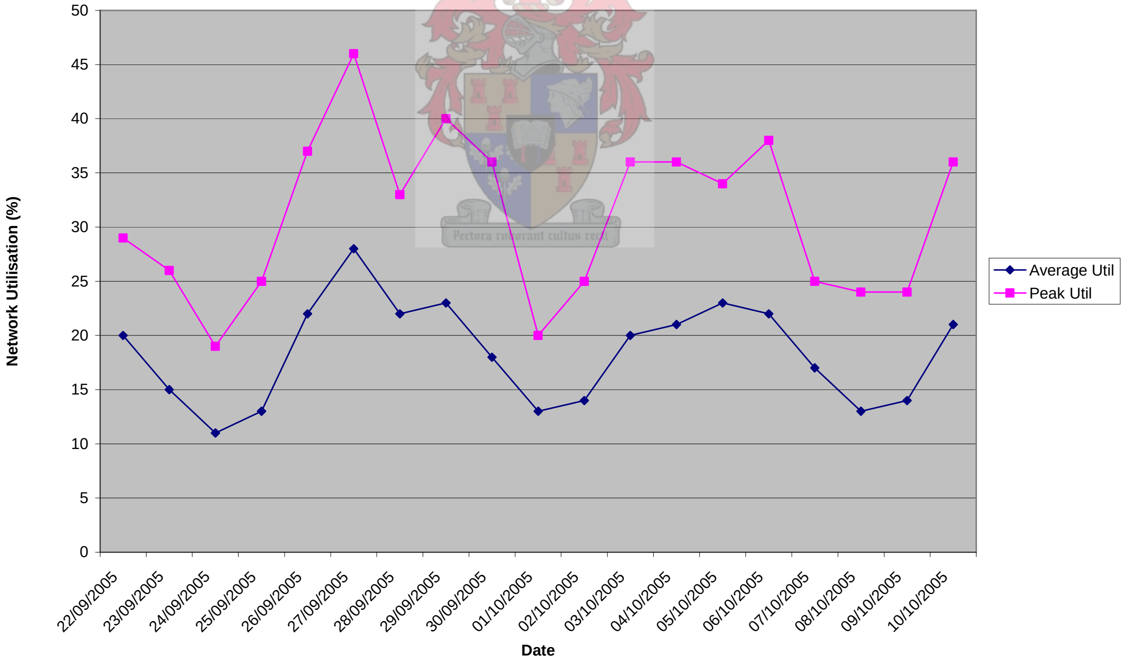
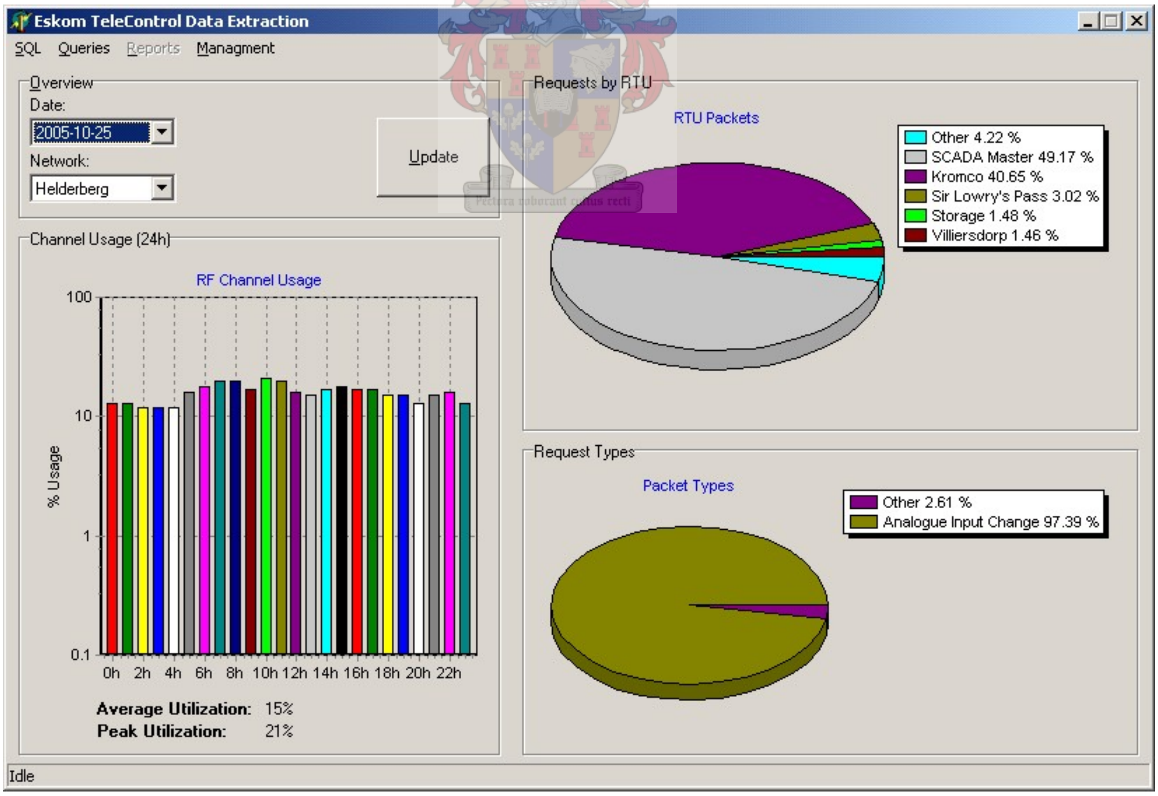


Figure 6.7. Tygerberg network utilisation trended over a three week period.

6.3. Helderberg network data analysis

From the data in for the Helderberg communication network was analysed and an average utilisation of 15 % was measured with a peak value of 21%. The data analysis for Helderberg is depicted in Figure 6.8. As in the case with Tygerberg it compares well with the recommended value of 40 % specified by the IEEE standard 999-1992 (Recommended channel utilisation for a SCADA communication network) [20]. It is also well within the Ethernet specified capacity of 30 % and well within the recommended value of 35 % by the ESCOM user requirement document DSP0009 [18].

The utilisation of the Helderberg communication was further analysed and it was found that Kromco sub station was standing out with an above average measured utilisation of 49.17 %. The data is shown in the *Requests by RTU* pie chart in Figure 6.8. The data of Kromco was further analysed and the detail information can be seen in Figure 6.9.



Date: 2005-10-25

Network: Helderberg

Average Utilization: 15%

Peak Utilization: 21%

Figure 6.8. Helderberg network utilisation for 25 October 2005.

The graphs in Figure 6.9. shows that all the analogues are updating more than normal. The a*nalogue input change* message type was also at 99.8 %, which is much higher that the average for the complete Helderberg network of 97.38 %. A work order was created and a technician was dispatched to investigate the site. An analysis tool was connected to the RTU and it was found that the RTU was transmitting analogue update values every 10 seconds to the SCADA master. The RTU configuration was analysed and it was found that the jitter factor (or analogue delta window) was set to 8 counts instead of the standard of 80 counts.

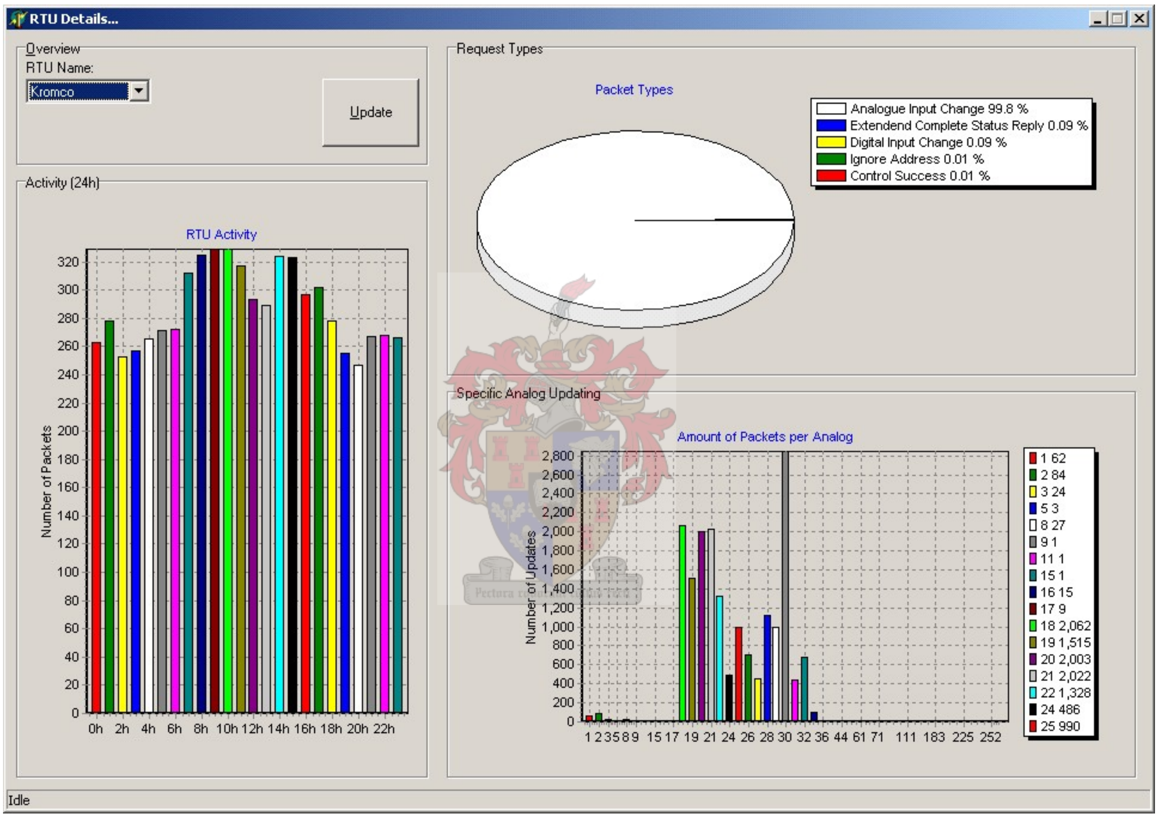
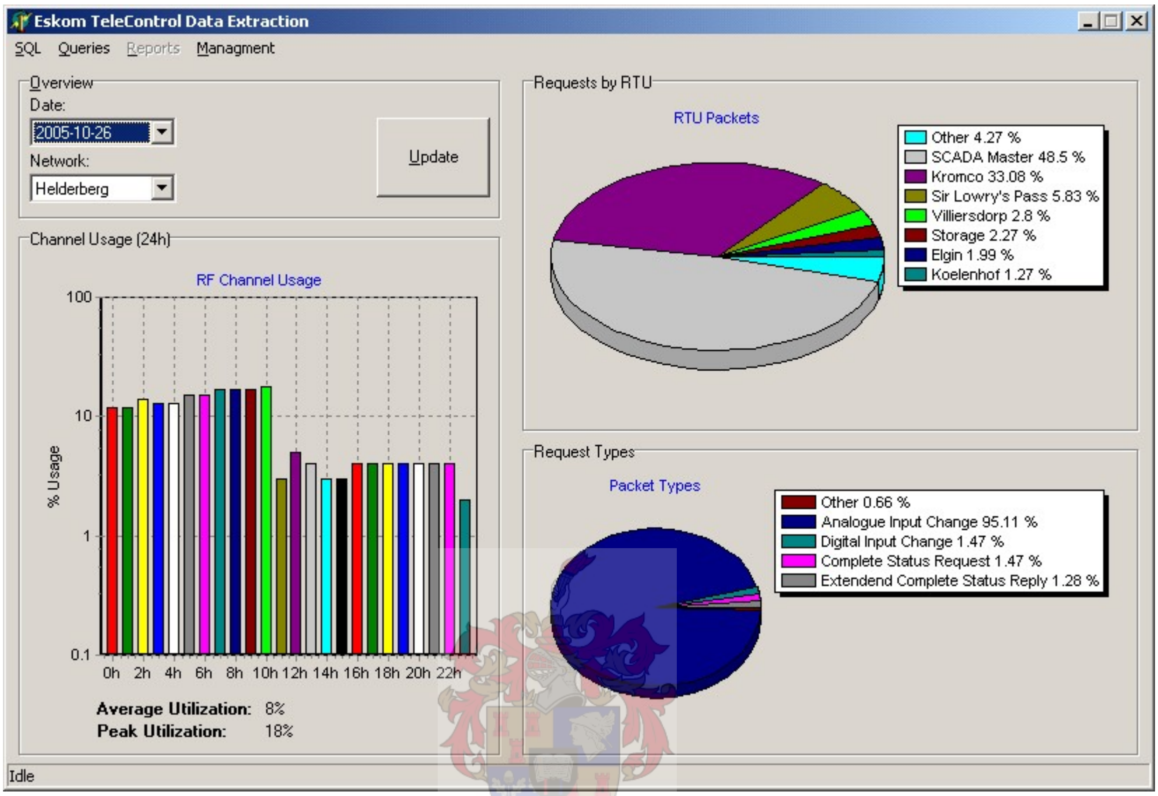


Figure 6.9. Kromco network activity for 25 October 2005.

The jitter factor in the RTU configuration file was changed to the standard of 80 counts and the new RTU configuration file for Kromco was created and downloaded to the RTU. The RTU was initialised with the new data at 11h00 and the network data was analyse to establish the impact of the new configuration on the network utilisation. The Helderberg telecommunication network utilisation data for 26th October is shown in Figure 6.10.

The network utilisation came down from 18 % peak before 11h00 to 4 % peak after 11h00. The *analogue input changes* request type decreased from 97.39 % to 95.11 % average for the day.



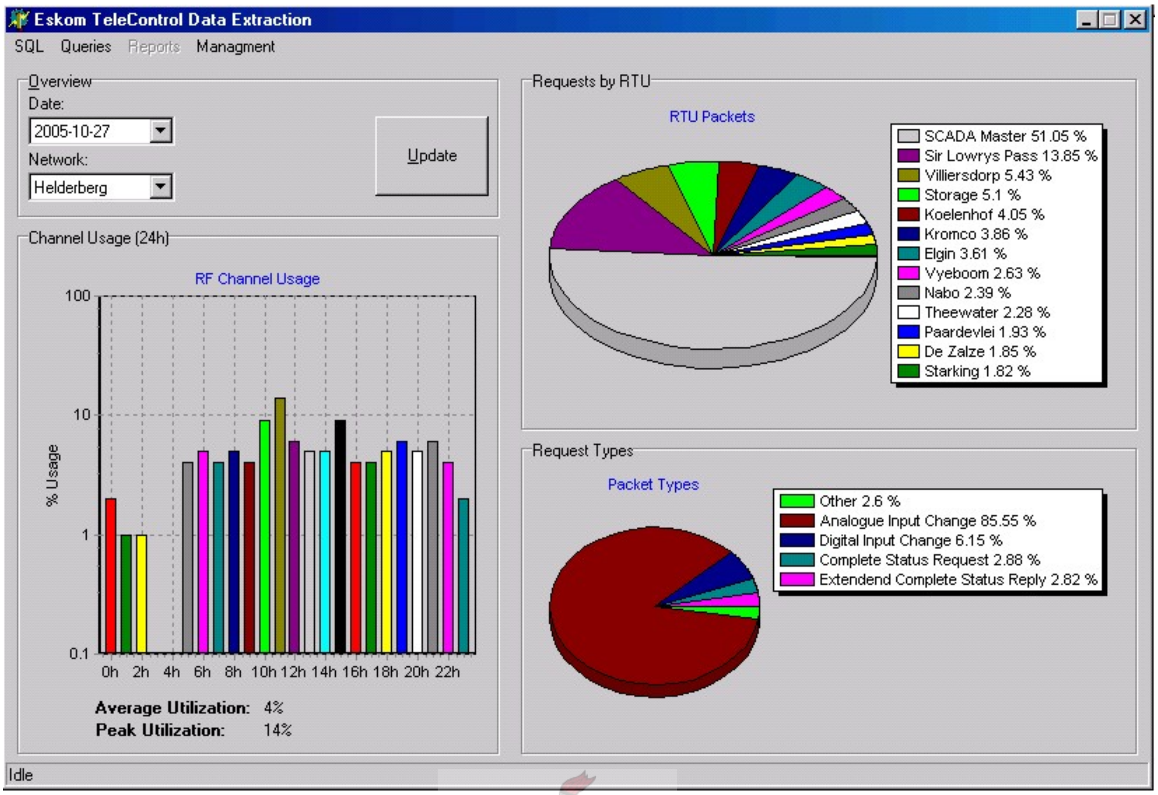
Date: 2005-10-26
Network: Helderberg

Average Utilization: 8%
Peak Utilization: 18%

Figure 6.10. Helderberg utilisation for 26 October 2005.

The Helderberg network data for 27th October 2005 was captured and analysed and is displayed in Figure 6.11. It was found that the Helderberg network average utilisation decreased from 15 % on the 25th October to 4 % on 27th October 2005. The *analogue input changes request* type decreased from 97.39 % on the 25th October to 85.55 % on 27th October 2005. The network utilisation of Kromco substation decreased from an average utilisation of 49.17 % to 3.86 % after the site was reconfigured.

The effect that one incorrectly programmed RTU has on a network can clearly be seen with the Helderberg network study. This emphasise the importance of accurate commissioning processes and the need for maintenance in the form of site audits and functional tests from the RTU to the SCADA master.



Date: 2005-10-27

Network: Helderberg

Average Utilization: 4%

Peak Utilization: 14%

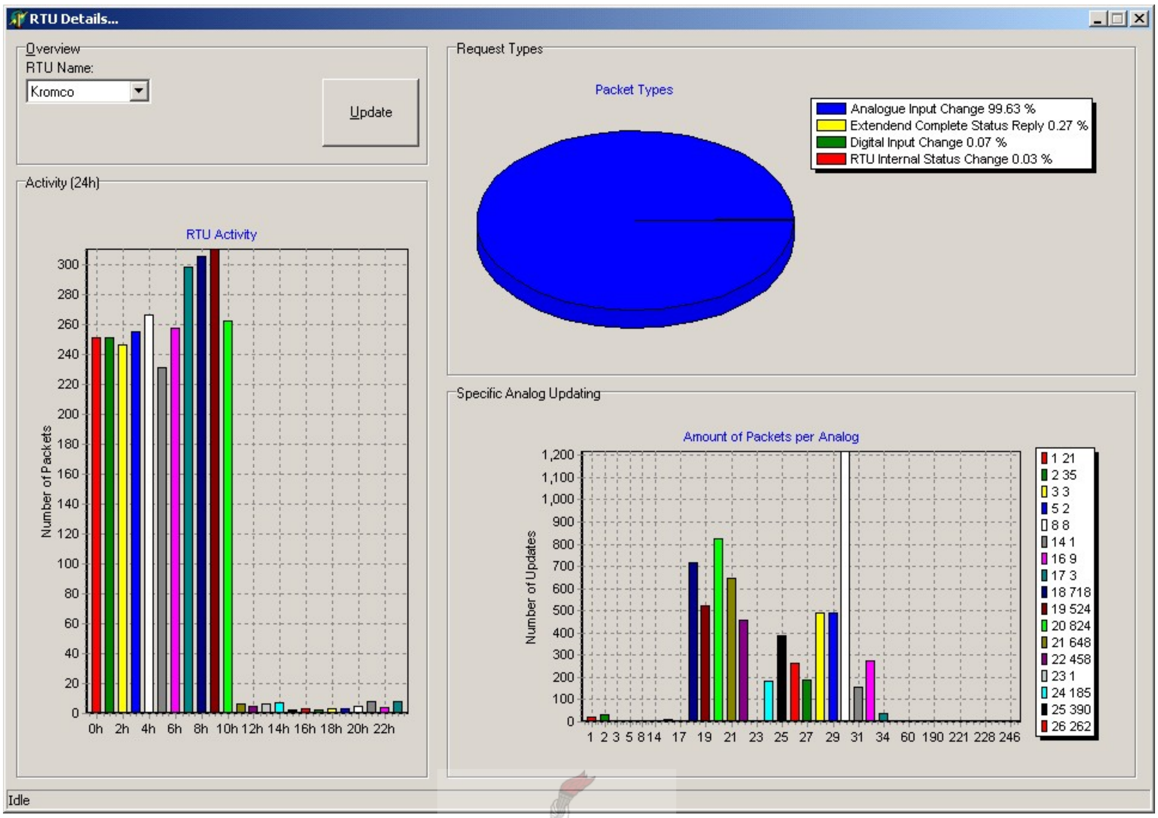
SCADA Master 51.05 %
Sir Lowrys Pass 13.85 %
Villiersdorp 5.43 %
Storage 5.1 %
Koelenhof 4.05 %
Kromco 3.86 %
Elgin 3.61 %
Vyeboom 2.63 %
Nabo 2.39 %
Theewater 2.28 %
Paardevlei 1.93 %
De Zalze 1.85 %
Starking 1.82 %

Other 2.6 %
Analogue Input Change 85.55 %
Digital Input Change 6.15 %
Complete Status Request 2.88 %
Extendend Complete Status Reply 2.82 %

Figure 6.11. Helderberg utilisation for 27 October 2005.

The data for Kromco substation was captured an analysed to establish the impact of the RTU configuration at the site itself. The data between 25th October 2005 and 27th October 2005 was compared to establish the changes in number of packets per hour and request types. It was found that the RTU activity at Kromco changed from 320 packets per hour peak decreasing to 8 packets per hour after the new configuration at the site was initiated. This is shown on the graph in Figure 6.12.

The average of analogue updates was still at a high of 99.63 %, but this was due to the very high analogue activity of up to 11h00. A more accurate value can be seen on the date of 27th October 2005. This is displayed in Figure 6.13. Here the analogue updates decreased from 99.8 % on the 25th October 2005 to 89.63 % on the 27th October 2005.

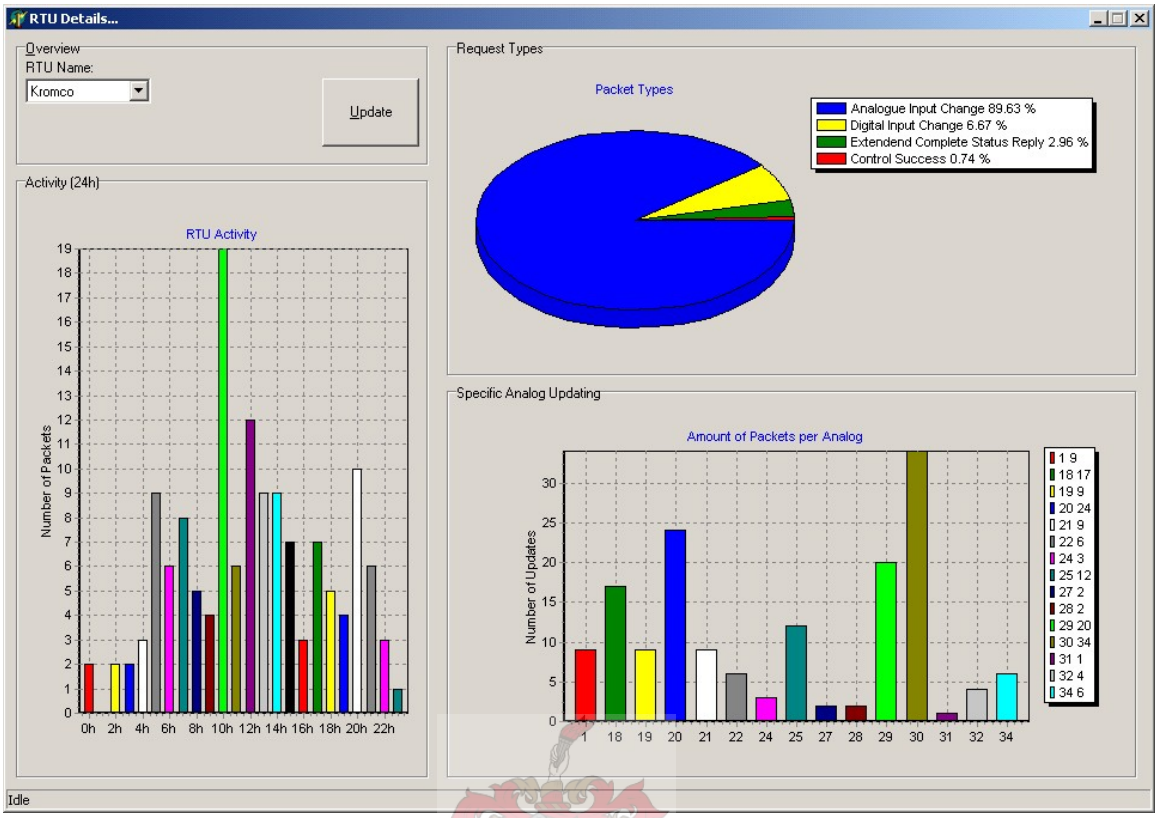


RTU Name: Kromco

Figure 6.12. Kromco activity for 26 October 2005.

To realise the full impact of the new configuration the data for Kromco substation was captured an analysed for 27th October 2005. It was measured that the RTU activity at Kromco was fluctuating between 19 packets per hour peak and 1 packet per hour for the day. This is shown on the graph in Figure 6.13. The average of analogue updates decreased to 89.63 % from 99.8 % on 25th October 2005. The activity at Kromco substation was further captured and analysed for another two weeks, but stayed constant during that time period.

It is remarkable that the SCADA master did not flag this high network and site activity. With further investigation it was realised that the SCADA master does not have the ability to measure high network utilisation and the operators were also not aware of the abnormal conditions on the telecommunication network. This emphasise the need for an active fulltime network analysis system that can monitor all telecommunication networks in real-time. This system should be setup to flag personnel automatically whenever a network or site is performing below a defined parameter.



RTU Name: Kromco

Figure 6.13. Kromco activity for 27 October 2005.

7 SCADA system design and maintenance standards

The following was published by Microwave Data Systems (MDS) and must be taken in consideration with the design and maintenance of radio based RTU installations. [16]

7.1. Evaluating communication path quality

Except for short-range paths that can be visually evaluated, a path study is generally recommended for new installations. A path study predicts the signal strength, reliability and fade margin of a proposed radio link. While terrain, elevation and distance are the major factors in this process, a path study must also consider antenna gain, coaxial cable loss, transmitter power, and receiver sensitivity to arrive at a final prediction.

Path studies are normally performed by a communications consultant or a system integrator who uses topographic maps or a software program to evaluate the feasibility of a proposed path. Computer-assisted studies have become very popular in recent years and greatly simplify the process of path planning. The current software tool used by ESKOM Distribution is called *Pathloss* and proved in practice to be a valuable tool. It was proven in practice that path studies provide valuable assistance in system planning, but they are not infallible. It is difficult, for example, to consider the effects of man-made obstructions or foliage growth without performing an actual on-the-air test. Such a test can be done using temporarily installed radio equipment. It is found quite often that the performance of a specific network degrades with time due to forestry activities in the Cape Peninsula area.

Ideally, a radio site will provide enough natural elevation to clear surrounding terrain without the need for a tall antenna tower. In these cases, the station antenna can often be mounted to a short mast and affixed to the equipment building or to an existing utility pole. If site elevation is not sufficient, a tower or other support structure must be used to raise the antenna above surrounding obstructions.

7.2. Antennas and coaxial cables

The single most important item affecting radio performance is the antenna system. Careful attention must be given to this part of an installation, or the performance of the entire system will be compromised. High quality, gain antennas as discussed in the literature study should be used at all master and remote stations. The antennas should be specifically designed for use at the intended frequency of operation.

SCADA communication antennas are made by a number of manufacturers and fall into two general categories, omni-directional, and directional. An omni-directional antenna provides equal radiation and response in all directions and is therefore appropriate for use at repeater stations, which must communicate with an array of remote stations scattered in various directions.

Directional antennas confine the transmission and reception of signals to a relatively narrow lobe, allowing greater communication range, and reducing the chances of interference to and from other users outside the pattern. It is necessary to aim these antennas in the desired direction of communication, i.e. at the repeater station.

The end of the antenna (furthest from the support mast) should face the associated station. Final alignment of the antenna heading can be accomplished by orienting it for maximum received signal strength. Measurements should be done with calibrated measuring equipment.

7.2.1. Direction of transmission and reception

Directional antennas are normally used at remote sites and require alignment with the repeater station for maximum effectiveness. In windy areas there antennas are prone to movement and there may be a need for regular maintenance to check the alignment of the direction.

7.2.2. Antenna mounting considerations

The antenna manufacturer's installation instructions must be strictly followed for proper operation of a directional or omni-directional antenna. Using the proper mounting hardware and bracket ensures a secure mounting arrangement with no pattern distortion or de-tuning of the antenna. The following recommendations apply to all antenna installations:

- Mount the antenna in the clear, as far away as possible from obstructions such as buildings, metal objects, dense foliage, etc. Choose a location that provides a clear path in the direction of the associated station.
- Polarization of the antenna is important. Most systems use a vertically polarized omni-directional antenna at the repeater station. Therefore, the remote antennas must also be vertically polarized (elements perpendicular to the horizon). Cross-polarization between stations can cause a signal loss of 20 dB or more.

7.2.3. Coaxial antenna cable

The importance of using a low-loss antenna coaxial cable is often neglected during radio installation. Using the wrong cable can cause huge reductions in efficiency and these losses cannot be recovered with any amount of antenna gain or transmitter power. For every 3 dB of coaxial cable loss, half the transmitter power will be lost before reaching the antenna. To illustrate the importance of this loss, consider the following: At 950 MHz, a 30.5m length of RG-8A/U coaxial cable (commonly used at VHF and lower frequencies) introduces a loss of about 8.5 dB. A 5 W transmitter operating into such a coaxial cable would produce only 700 mw at the antenna and a similar loss in receive sensitivity would occur.

On the other hand, a 30.5 m length of 22 mm semi-rigid coaxial cable operating under the same conditions will introduce only 1.28 dB of insertion loss, and will deliver 80 % of the transmitter's power to the antenna. For every 3 dB of coaxial cable loss, half the transmitter power will be lost before reaching the antenna. The choice of which coaxial cable to use depends on:

- the length of cable required to reach the antenna,
- the amount of signal loss that can be tolerated, and
- cost considerations. For long-range transmission paths, where signals are likely to be weaker, a low-loss cable type is recommended, especially if the length of the cable must exceed 15m. For a short-range system, or one that requires only a short antenna coaxial cable, a less efficient cable may be acceptable, and will cost far less than large diameter semi-rigid cable.

7.3. Maintaining system performance

Over time, any communications system requires a degree of preventive maintenance to ensure peak operating efficiency. Periodic checks of master and remote sites should be made to identify and correct problems before they become threats to system operation. The following areas should be given special attention:

7.3.1. Antennas and coaxial cables

Visually inspect the antenna and coaxial cable for physical damage, and make sure that the coaxial connections are tight and properly sealed against the weather. Directional antennas must be checked to see that the antenna direction has not shifted since installation especially in windy areas. This should also be visible with a signal strength measurement at the RTU.

The forward and reverse transmitting power at the antenna system should be checked from time to time using a through-line Wattmeter. Defects in the antenna system will frequently show up as reflected power on the meter. It is good practice to accept only a maximum reflected power of about 5%; this corresponds to an SWR of approximately 1.5:1. For any condition exceeding this value, search for and correct the cause-damaged antenna, defective or improperly installed connectors, water in the coaxial cable, etc.

7.3.2. Cable connections

All power, data, and ground connections should be secure and free of corrosion or oxidation. All outside cable connectors should be sealed to inhibit water entry and corrosion.

7.3.3. Power supply

The voltage of the station power supply should be measured to verify that it is within the operating specifications for the RTU and radio. Batteries, if used, should be checked for charge level and signs of leakage or corrosion. If possible, the radio should be keyed during this test while the charger is disconnected from the battery to ensure maximum current draw from the battery.

7.3.4. Function test with SCADA master

All input and output functions between the RTU and SCADA master should be proven on periodic cycles. All alarms and indications should be initiated from the RTU and checked at the SCADA master for accuracy. Analogue values should be compared on site with the values at the SCADA master. If necessary a current injection test should be done at the RTU and validated at the Master. These tests should validate the following:

- Master database integrity.
- RTU setup.
- RTU hardware.
- RTU cabling.
- Communication medium.

7.3.5. Safety

All work must be done to prescribed safety standards. This will reduce the risk of injuries, loss of life, damage to equipment and potential revenue loss. Adhere to the official company safety procedures and wear appropriate safety equipment at all times. This is especially important when working on antenna masts and other antenna fixtures.

7.4. Maintenance policies

There are basically four different maintenance policies to choose from, namely

- Design out maintenance (DOM).
- Run to failure (RTF).
- Preventative maintenance (PM).
- Condition based maintenance (CBM).

The different policies are described in more detail as below:

7.4.1 Design out maintenance (DOM)

The focus of DOM is to improve the design of the equipment or system to prevent it from failing or to minimize maintenance cycles. The feasibility of DOM will depend on financial impact of the new design. This option will be feasible if the financial impact is low or if the risk of failure is high. From an engineering point this is probable the best solution, but not always from a financial view.

7.4.2 Run to failure (RTF)

RTF is also known as failure based maintenance is carried out only after the equipment or system has failed. This maintenance type can only be done when the risk is not high or there should be a backup system in place to take over with failure of the primary equipment or system. The cost implications may be high with expensive equipment. For example it may be technically feasible to use RTF on certain equipment, but it may be economically better to maintain the equipment before failure.

With most electronic and microprocessor controlled equipment this is the only viable solution as it is basically impossible to predict failure on there systems.

7.4.3. Preventative maintenance (PM)

Preventative maintenance is done to prevent failures. This may be done as Time Based Maintenance (TBM), which is done at cyclic time or as Used Based Maintenance (UBM) where the maintenance is done after a certain amount of usage or operations.

This is normally done with high-risk systems, very expensive equipment and where failures will result in high loss of income due to plant failures.

7.4.4. Condition based maintenance (CBM)

Condition based maintenance is carried out each time the value of a given parameter exceeds a predetermined value. This method is gaining popularity due to the fact that conditions can be remotely monitored via SCADA systems and alarms can be set to notify maintenance personnel in advance of failures.

CBM can save money and time if implemented correctly. With electronic systems this may be the alternative to RTF as regular inspections is possible. For example temperature measurements, battery checks, voltage and current measurements may be the only way to predict failures. The functional tests of all input and output functions between the RTU and Master are in fact CBM as well as the measurement of receive signal strength and transmit power of the RTU radio.

The current ESKOM Distribution approved telecoms maintenance philosophy document [12] describes minor and major maintenance for RTUs in detail. This document was published and implemented in June 2002 and is currently in process of being reviewed. The findings of this project will positively influence the revision of the current philosophy. RTF will be used for all electronic modules within the RTU, while CBM will be used to do functional tests and measuring voltages and radio levels.

7.5. Work management system

7.51. Introduction

A work management system is used to log all work requests, schedule the work, create work orders and capture actual information with regards to the specific work order. This information includes travel time, travel distance, equipment worked on, hours worked and detail of the work done. A work management system is an essential tool for work planners and schedulers to assist with work planning and to optimize personnel utilization. All types of work must be logged on the system to capture all work done by field teams for example faults, investigations, maintenance, inspections, installations and commissioning work. The information gathered would supply vital information with respect to performance that will assist planning personnel with maintenance planning.

7.5.2 Work types.

Work types should be defined which will assist with personnel performance, budget purposes and future trending. A list of possible work categories and subcategories is shown in Table 7.1. Information derived from this detail for example will show the percentage of time spent on maintenance, faults, investigations, etc.

Table 7.1. Task type and sub type example.

Task Types	Task Sub Types
Commissioning	Outage
	Workshop test and setup
	On site pre
	On site activation
Construction	Labels
	LPU
	Panels
Data related requests	Records
	Update Database
Decommissioning	
Fault	Hi Priority
	Negotiated
Installation	
Investigation	Audit
	Data
Maintenance	Major
	Minor
	Verification
	Impedance Test
	Nicad Overhaul
	Settings Change
	Firmware Upgrade
WorkshopTest and Setup	

7.5.3. Actions and causes

It is a good idea to define actions and causes related to use with breakdown incidents. These categories will assist with queries related to performance investigations as well as future planning and refurbishment. The usage of fixed categories rather than free text is more to ensure that the data is purified and not contaminated with spelling mistakes, spaces and the inconsistent usage of capital and small letters. Table 7.2 shows examples of causes that may be used and Table 7.3. shows examples of possible actions types. The usage of *no fault found* and *cause unknown* should be discouraged and be restricted as much as possible as it does not assist the investigator with any relevant information.

Table 7.2. Example of fault causes.

Category	Cause	Category	Cause
Man Made	Accidental Damage	Wiring and cables	DC Supply
	Malicious Damage		Mains Supply
	Damaged in Transit		Voltage Surge
	Operator Error		Connector Fault
	Theft		Dry Joint
	Working Party		Incorrect Wiring
	Records		Open Circuit
Environmental	Corrosion		Short Circuit
	Foreign Matter		Earthing
	Humidity	Other	Frequency Interference
	Lightning		Instability (Drift, etc.)
	Static		Low Insulation
	Storm		Fading
	Temperature		No comms
	Vermin		Poor comms
	Clouds		Ageing/Wear
Data and software	Data Entry		Cause Unknown
	ESKOM Software		Decommissioned
	Supplier Software		No fault found
	Manufacturer Fault		
	System Lock-up		

Table 7.3. Example of action types.

Action	Action
No Action	Power Restored
Equipment Replaced	Re-Calibrate
Module Replaced	Re-programmed/Settings Change
Component Replaced	Reset
Re-cabled	Outage required
Re-wired	Further investigation required
Repaired	Boost Charge
Sent in for repair	Cleared while Localising
Equipment removed	Handed over
No Fault Found	

7.5.4. Plant information

All the relevant plant data pertaining to the sites and equipment at the sites that is to be maintained must be populated into the work management system database. This data includes site names, plant slots, equipment types, model, manufacturer and asset detail. This information is used to establish trends on failures and for maintenance planning.

7.6.5. Actual information of work done.

All actual information pertaining to a work order must be captured onto the work management system. This includes the time departed to site, the time of arrival at site, the time that the breakdown is cleared, the total hours worked, the equipment worked on, detail of work done and travel information. From this data essential performance indicators can be calculated, for example the customer down time, repair time and typical equipment failures.

8. Conclusions and Recommendations

8.1. Introduction

It was found that there are many international standards organizations which focus on Supervisory Control and Data Acquisition (SCADA) systems, but only two define Remote Terminal Unit (RTU) protocol specifications, namely the IEC and the DNP3 users group. The two published standards are not compatible, although both standards are open standard protocols. There is a need for one international standard for all RTU protocols, which will ensure better interfacing between SCADA masters and different RTU makes and models.

While SCADA protocols are more open today, there is no clear consensus of which protocol is best. The IEC 60870-5 series and DNP3 have many similarities but are not 100% compatible. Only manufacturer proprietary protocols were implemented in the past by ESKOM due to the lack of international standards on RTU protocols. ESKOM is starting to follow international trends by adopting the DNP3 protocol. It must be said however that DNP3 is not really designed to work at its optimum over an UHF radio network. It should however work well on the wideband optical fiber and microwave networks. Current manufacturer specific and ESKOM specific protocols are being phased out.

8.2. Research objectives

As defined in Chapter 3 the research for this thesis focused on the following:

- Communication system configurations for SCADA systems used by Eskom Distribution.
- SCADA Key Performance Indicator (KPI) research.
- RTU availability analysis.
- Control success rate analysis.
- Communication channel utilisation research on area radio communication systems.
- RTU maintenance standards.
- RTU telecommunication design standards.

Two basic telecommunication configurations were being used by ESKOM distribution, namely solicited and unsolicited systems. The unsolicited or Report by Exception (RBE) communication systems were the worst performing systems and were used on UHF area radio based communication systems. The other focus areas are discussed in detail below.

8.2.1. Key performance indicators

Key Performance Indicators (KPIs) were defined and implemented to establish the performance of the SCADA system. Two KPIs were used, namely RTU availability and Control Success Rate (CSR). RTU availability measures the communication system, while CSR measure the complete SCADA system including the operating personnel and the plant at the substation. Specifications for a data-mining tool were compiled and the software was developed. The chosen database was MS SQL and the user interface was developed in Access 97. The software was developed to import data from the SCADA master and to provide reports and graphs to assist with the performance measurement of the defined KPIs. Data for three years was analyzed for both KPIs and were trended over the period from January 2002 to December 2004.

8.2.2. RTU availability

It was established that the worst performing RTU protocols were the area radio based protocols, namely DNP3, Estel Variant (EV) and the Motorola Intrac protocol.

Two measures were implemented to improve the performance of the SCADA system, namely changing the radios, antennas and coaxial cable at the worst performing sites and also to redesign the area radio telecommunication systems. The main objective with the redesign of the systems was to restrict multiple RTU protocols on the same network and to reduce the network utilisation per network. Standards for the usage of antennas, radios and coaxial cables were established, published and implemented. The installation of new digital radios together with low loss coaxial cable and the usage of specific antennas improved the RTU availability from 96.87 % for the year 2002 to 99.17 % for the year 2004, which realised an increase of 2.83 % for 432 installed and operational RTUs. This measure however did not influence the control success rate at all. It was also found that the output power of the radios at some sites were too high, which in turn could influence the performance of other sites. The telecontrol antenna and radio output power guideline is currently being reviewed and should be published for implementation during 2006.

The low RTU availability performance of the Distributed Network Protocol version 3 (DNP3) still needs to be investigated, as limited time was available during the study. An audit should be done for each DNP3 RTU installation and research needs to be done to establish the cause of the low performance. The DNP3 protocol in itself may be setup incorrectly as there are more than one variation to the protocol. The impact of DNP3 performance will only be realised after a trend can be established in comparison with the other traditional protocols. This study will take at least one year.

8.2.3. Control success rate

The implementation of the newly designed communication systems was done during May 2004 had a quite an influence on the control success rate of the SCADA system. The control success rate increased from 77.65 % for the year 2002 to 78.76 % for the year 2003 and to 80.88 % for the year 2004. A drastic increase in performance was observed after the restriction of multiple RTU protocols on the same network during May 2004, where the value for twelve months prior to September 2005 was measured at 84.38 %. From this we can conclude that it is important to design an area radio system in such a way to restrict the usage of multiple RTU protocols on the same network. It was found that the main cause for control failures were due to plant failures, which averages 47.7 % per year. The plant failures were investigate further and it was found that the biggest contributor to this was Sensitive Earth Faults (SEFs), which were at 35 % out of a total of 28 defined causes. It was not possible to investigate this further due to a lack of information for each specific incident. This should be investigated further due to the fact that SEFs is such a big contributor to control failures. More investigations need to be done on sites with low control success rate to establish the real cause behind the control fails due to communication failures. There is also a need to compare the control success rate between the different protocols, as this was not done due to time constraints. Data is available from start January 2004 on up to October 2005 to assist with this investigation.

8.2.4. Network utilisation

The network utilisation study was done on two of the thirteen area radio communication networks, namely Tygerberg and Helderberg network. Tygerberg network comprised of three repeaters and 84 RTUs and an average network utilisation of 17 % and a peak network utilisation of 25 % was measured. Helderberg network had an installed base of 4 repeaters and 15 RTUs and an average network utilisation of 3 % and a peak utilisation of 8 % was measured. Only RTUs using the Estel Variant (EV) protocol were monitored on both communication networks as there was not enough time available to develop a DNP3 protocol analyser.

On the Tygerberg communication network one site was singled out as a site with above average utilisation, namely Bower that were measured at an average of 9.95 %. It was found that this was due to excessive analogue updates from the site. The RTU configuration at the site was investigated and it was found that the site was configured to the specified standard parameters. It is recommended to reconfigure standard jitter factor of the RTU at Bower from the 80 counts standard to 100 counts to minimise the analogue updates to the SACDA master. This value can be adjusted up or down if the utilisation does not change significantly after implementation.

During the study of the Helderberg communication network it was found that Kromco substation was averaging at a measured utilisation of 49.17%. This was further investigated and it was found that the RTU at the site was configured incorrectly. It was established that the analogue update jitter factor was programmed incorrectly, namely at 8 counts instead of the 80 counts standard configuration. A new configuration file was created and downloaded to the RTU. The utilisation at the site decreased from 49.17 % to 3.83 % after the configuration was corrected. The utilisation of the Helderberg network itself decreased from an average utilisation of 15 % to an average utilisation of 4 % after the reconfiguration. This highlights the impact of one incorrectly configured RTU on a communication network. This may have a catastrophic impact on a communication network in adverse weather conditions when a SCADA system is relied on to supervise and control the electrical network to an optimum. Care should be taken with installations, commissioning and maintenance to minimise problems like this.

The utilisation of both communication networks was within specification of the recommended value of 40 % specified by the IEEE standard 999-1992 (Recommended channel utilisation for a SCADA communication network) [20]. It is also well within the Ethernet specified capacity of 30 % and well within the recommended value of 35 % by the ESKOM user requirement document DSP0009 [18]. It is recommended that all networks should be monitored on a permanent basis to establish a baseline from which the effect of future expansion on the networks can be calculated. Incorrectly configured sites will also be identified as well as faulty equipment. The network monitoring tool should be upgraded that would enable it to analyse the DNP3 protocol as well. The network monitoring tool should be integrated with the RTU monitor software system as this will enable the user to analyse RTU availability, control success rate and network utilisation with the same software.

The impact of abnormal electricity network conditions and adverse weather conditions on the utilisation of the communication networks was not established during the period of time that the networks were monitored. This will be the real test to establish if the networks will be able to handle excessive data over a short period of time. This will only be realised when such a condition occurs during the time of network monitoring. It should be ensured that the network monitoring equipment is connected to an Uninterruptible Power Supply (UPS) to ensure reliable data during a power outage.

8.2.5. Maintenance standards

It was found that a maintenance standard was published and in place for RTUs in ESKOM distribution. This was compared with international trends and it was established that the same generic maintenance practices were used. The Eskom distribution RTU maintenance document is currently being reviewed and it is recommended that Run to Failure (RTF) maintenance should be used for all electronic modules within the RTU, while Condition Based Maintenance (CBM) should be used to do functional tests, measuring voltages and radio levels. Visual inspections should be done regularly to establish the condition of antennas, coaxial cables and connectors. It is essential to record all work on a work management system. All work requests must be recorded and work orders created. These work orders must be scheduled and assigned to the relevant personnel. All the actual data pertaining to the specific work order must be captured into the work management system after the work is completed. Care must be taken to provide accurate and comprehensive information as this will assist with further investigations as well as future planning.

8.2.6. Telecommunication design standards

It was found that current ESKOM telecommunication designs for RTU systems are not based on scientific studies, but rather on assumptions. Detail studies should be done on the current telecommunication system at the planning phase of any new RTU. This should include current network utilization and the impact of the expansion on the network and system. The telecommunication network should be redesigned if the study shows the network utilization will go beyond 40 %. It was found that in some cases the maximum Effective Radiated Power (ERP) of 20 W as dictated by ICASA are not adhered to. When a radio is configured to transmit at 5 W and a corner reflector or 12 element YAGI antennas are used, the ERP will be at 23 W for the corner reflector and 56 W for the 12 element YAGI. The antenna and radio output power standard is currently being reviewed to get all radios within ICASA specifications. Audits will have to be carried out at all sites to establish if the communication equipment conforms to published specifications.

It is recommended that work management software be used to create all work requests and work orders for the field technicians. The system must be populated with all the relevant plant locations and data and all the actual work done by the field technicians must be logged onto the system. A work management system is an essential tool for work planners and schedulers to assist with work planning and to optimize personnel utilization. All types of work must be logged on the system to capture all work done by field teams for example faults, investigations, maintenance, inspections, installations and commissioning work. The information gathered would supply vital information with respect to performance that will assist planning personnel with maintenance planning.

Acknowledgements

The author would like to thank the following persons and institutions:

- The University of Stellenbosch for using their laboratory facilities to setup the telecommunication network monitor equipment.

- ESKOM for the usage of a personal computer to monitor the telecommunication network.

- ESKOM for financial assistance.

- Christiaan Brand for the development of the telecommunication network monitor and analysis software.

- ESKOM for the usage of digital radios and corner reflector antennas.

- My supervisor Dr. H.J. Vermeulen for assistance during the project.

Bibliography

[1] DNP Users Group,DNP3 Specification, Volume 1 DNP3 Introduction, 2002.

[2] IEC 60870-5-101 (2003-02) Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic Telecontrol tasks, IEC, 2003.

[3] IDC Technologies, Practical Distributed Network Protocol 3 & Modern SCADA Communications for Engineers and Technicians, IDC Technologies, V1.2.

[4] T Gosai,The ESTEL Variant Telecontrol Protocol Specification ,EDNS - Technology Eskom Distribution - Central Region, June 2004.

[5] LM van Wyk, *ESTEL Variant : PMRTU Multiple Access version 1.2-5.*. Measurement and Control Department, National PTM&C, Eskom Transmission Group, April 1996.

[6] SA Dumakude, *ESTEL Variant : Multiple Access version 1.4-3.*. Measurement and Control Department, National PTM&C, Eskom Transmission Group, January 1994.

[7] West A, SCADA and Substation Control Communications, The Southern African SCADA and MES Conference, Johannesburg, South Africa, 11 & 12 May 2005, p 1 – 21.

[8] University of Seville, Using Protol Engineering Techniques to improve Telecontrol Protocol Performance, Department of Electronic Technology.

[9] Gütschow D, Operational Key Performance Indicators for SCAD, Distribution Technology, ESKOM Distribution, SCSASACE2, April 2004.

[10] Tebekana K.E, Definitions and terminology used in the evaluation of transmission control performance, PM&C Operational Support, ESKOM Transmission, Draft, May 2001.

[11] Escudo JJ, Gonzalo F, Luque J, Quality Of Service In The NOMOS TMN System, International Conference on Power Sector Telecommunication System for the 21st Century, Nueva Delhi India), January 1997.

[12] Gütschow D, Pierre Delport, Telecontrol Maintenance Philosophy, Distribution Technology, ESKOM Distribution, SCSASACL4, April 2004.

[13] Trulong Le, SCADA SYSTEM PERIODIC MAINTENANCE, UTSI International Corporation, ENTELEC 2002, 2001.

[14] The American Public Transport Association, Standard for SCADA System Inspection, Testing and Maintenance, , Volume 6 – Signals & Communications, APTA RT-S-SC-034-03, 26 July 2004.

[15] Jean Tourrilhes, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.modem.htm, July 2005.

[16] Microwave Data Systems, http://www.microwavedata.com/products/whitepapers/planning.asp, July 2005.

[17] Westwood R, Telecommunication Guideline : Antenna Selection for Telecontrol RTU Applications, Distribution Technology, ESKOM Distribution, DISAGABD2, REV 0, November 2003.

[18] Gütschow D, Telecommunications: High-Level User Requirements for Telemetry Communications in Distribution, Distribution Technology, ESKOM Distribution, DDSP0009, REV 0, September 2005.

[19] 3-COM, http://support.3com.com/infodeli/tools/netmgt/tncsunix/product/091500/c8bandut.htm#17277, October 2005.

[20] IEEE Standards Association, IEEE Std 999-1992 - IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications –Description, 7 March 2005.

[21] Dale Barr, Technical Information Bulletin 04-1, Supervisory Control and Data Acquisition (SCADA) Systems, October 2004.

[22] Gütschow D, Technical Bulletin 04TB-037: Telecontrol antenna guideline for SABRE, Revision 0, 22 October 2004.

[23] IEEE Standards Association, IEEE Technical Report 1550 – Utility Communication Architecture, USA, 1999.

[24] IEEE Transactions on Power Delivery, Volume 17, No. 3, ESTELLE: A Method to Analyze Automatically the Performance of Telecontrol Protocols in SCADA Systems, July 2002.

[25] IEEE Transactions on Power Systems, Volume 9, No. 1, A Framework for the Specification of ACADA Data Links, February 1994.