Sudan University of Science and Technology
College of Engineering
Electronics Engineering Department

National Electrical Load Dispatch Centre "SCADA" System Performance Evaluation

A Research Submitted In Partial fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronics Engineering

Prepared By:

1- Fatima Kamal Hassan Musa

2- Sharifa Magzob Mohammed Ahmed khalifa

3- Smahir Sir AlkhatemAlhussien Mohammed

4- Yousif Mohammed Yousif Ali

Supervisor:-

D.Yassir Obeid Mohammed

October 2017

الاستهلال

قال تعالي : (وقل اعملوا فسيري الله عملكم ورسوله والمؤمنون)

التوبة (الآية : 105)

الإهداء

الى من كلله الله بالهيبة والوقار الى من علمني العطاء بدون انتظار

الى من احمل اسمه بكل افتخار ستبقى كلماتك نجوما اهتدي بها

والدي العزيز

الى ملاكي في الحياة

الى معنى الحب والى معنى الحنان والتفاني

الى بسمة الحياة وسر الوجود

أمي الحبيبة

الى من بها اكبر وعليها اعتمد

الى شمعة متقدة تنير ظلمة حياتي

الى من عرفت معها معنى الحياة

أختي

إلي أخي ورفيق دربي

في نهاية مشواري أريد إن أشكرك

على مواقفك النبيلة

الشكر والعرفان

أولا نشكر الله سبحانه وتعالى ونحمده أن وفقنا لإكمال هذا البحث، وأجزل الشكر للدكتور ياسر عبيد محمد على مجهوداته المقدرة ودعمه لنا والذي لولاه من بعد الله لما اهتدينا إلي هذا العمل ونشكر مهندسي مركز التحكم الآلي الذين لم يبخلوا علينا بشي كما نود أيضا أن نشكر المهندسين علي عباس ومهند عادل الذين كانوا لنا عونا وسندا في مسيرة هذا البحث الطويلة وكل من ساعدنا من الأصدقاء لاكمال هذا العمل.

Abstract

SCADA is a supervisory control and data acquisition system. This work aims to study and evaluate the performance of the National Load Dispatch Centre SCADA system for enhancement. The analysis is based on the visit of several stations to gather sufficient data to help in analysis based on specific parameters such as communication system, security and so on. A general evaluation of the system is achieved and the strengths and weakness points in the system are determined. An electrical distribution process in NLDC SCADA system is simulated and the result is been presented.

المستخلص

الاسكادا هي نظام مراقبة التحكم و الحصول علي البيانات. هذا العمل يهدف إلي دراسة وتقييم أداء نظام الاسكادا التابع لمركز التوزيع القومي للتحسين. وكان التحليل مبني علي زيارة عدة محطات لجمع بيانات كافية منها لتساعد في التحليل بناء علي عوامل محددة مثل نظام الاتصال والأمن وغيرها وبذلك نصل إلي نتائج تحقق تقييم عام للنظام وتم تحديد نقاط القوة والضعف في النظام.

Table of Contents

Chapter Four :SCADA System analysis and Evaluation

Chapter Five: Conclusion and Recommendation

LIST OF FIGURE

LIST OF ABBREVIATIONS

SCADA	Supervisory Control and Data Acquisition
RTU	Remote Terminal Unit
I/O	Input/output
PLC	Programmable logic controller
HMI	Human-machine interface
ATM	Automated Teller Machine
IEC	International Electro technical Commission
DNP	Distributed Network Protocol
NLDC	National Load Dispatch Centre
DCS	Distributed Control System
WAN	Wide Area Network
LAN	Local Area Network
EFMs	Electronic Flow Meters
SNMP	Simple Network Management Protocol
IP	Internet Protocols
GUI	Graphical User Interface
SDH	Synchronous Digital Hierarchy
MTU	Master Terminal Unit
CPU	Central Processing Unit
OPC	OLE for Process Control

SQL	Structured Query Language
ISO	International Standards Organization
OSI	Open Systems Interconnection
ASCII	American Stander Code for Information Interchange
DNP	Distributed Network Protocol
TCI	Tele Control Interface
RTC	Real Time Communicator
IM	Information Management
UI	User Interface
PDM	Protection Data Management
EMS 1	Energy Management Server
EMS 2	Energy Management Server
NA	Network Application
DMA	Distribution Management Appl
DTS	Dispatcher Training Simulator
HFD	Historical and Future Data
CB	Circuit Breaker
SPM	Switching Procedure Management
EDFA	Erbium Doped Fiber Amplifier
TDM	Time-Division Multiplexing
CWDM	Coarse Wave-Division Multiplexing
EMP	Electromagnetic Pulse
OPGW	Optical Fiber Grounded Wire

TCP	Transmission Control Protocol
EN	Enterprise Network
PCN	Process Control Network
NAT	Network Address Translation
PC	personal computer
PDU	protocol data units
EIA	Electronics Industries Association
UDP	User Datagram Protocol
SAS	Substation Automation System
BCU	Bay Control Unit
AVR	Automatic Voltage Regulator
SW	SWITCH
SP	Single Point
DP	Double Point
BCD	Binary Code Decimal

Chapter One
Introduction

1.1 Preview:

Supervisory Control and Data Acquisition (SCADA) system means a system consisting of a number of remote terminal units (or RTUs) collecting field data connected back to a master station via a communications system.

SCADA systems collect sensor measurements, operational data from the field process and display this information. Also they relay control commands to local or remote equipment [1].

1.2 Problem Statement:

Several manufacturing area use SCADA systems which may have some problems in design or implementation. National electrical load dispatch center SCADA system is to be considered as a case study.

1.3 Proposed Solution:

Analysis and evaluation of national electrical load dispatch center SCADA system for enhancements.

1.4 Approach:

First intensive study of SCADA systems is to be performed that include learning about hardware and software then a number of visits to establishments that use SCADA is to done. Finally an agreed upon system (SNLDC) is to be examined and evaluated.

1.5 Thesis outlines:

This thesis is composed of five chapters organized as follow:-

Chapter one: provides an overview, states research problem and proposed solution and outline work approach and organization.

Chapter two: presents the literature review of different fields of SCADA system.

Chapter three: covers in details SCADA hardware and software.

Chapter four: system analysis and results presentation.

Chapter five: gives research conclusion and future work recommendations.

Chapter Two
Literature Review

2.1 SCADA system performance evaluation parameters

2.1.1 Levels versus Components

SCADA levels:

- Level 0 contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.
- Level 1 contains the industrialized input/output (I/O) modules, and their associated distributed electronic processors.
- Level 2 contains the supervisory computers, which collect information from processor nodes on the system, and provide the operator control screens.
- Level 3 is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.
- Level 4 is the production scheduling level [3].

SCADA Components:

- Supervisory computers.
- Remote terminal units.
- Programmable logic controllers.
- Communication infrastructure.
- Human-machine interface [2].

2.1.2 SCADA Communications

2.1.2.1 Communication architectures:

1. Point-to-point (two stations):

   This is the simplest configuration where data is exchanged between two stations.

2. Multipoint (or multiple stations):

In this configuration, there is generally one master and multiple slaves. Generally data points are efficiently passed between the master and each of the slaves.

3. Relay Stations:

   There are two possibilities here: store and forward relay or talk through repeaters.

- Store and forward relay operation: there one station retransmits messages onto another station out of the range of the master station.
- Talk through repeaters: this retransmits a radio signal received simultaneously on another frequency. This is generally the preferred way to increase the radio system range [2].

2.1.2.2 Communications types

It is basically classified to wired and wireless communications.

2.1.2.2.1 Wired communications

It is uses physical media to exchange data between devices , it has many types illustrated here:

Coaxial Cable: Very mature technology. Better data bandwidth than a telephone line.

Fiber Optics: Similar to the traditional copper telephone lines, but differs by utilizing optical fibers made of glass or plastic and uses light

to transmit the data, with is faster and has less losses as compared to copper wires.

Telephone Line**:** A system that utilizes electrical signals in order to transmit data over a distance using a single pair of copper (traditionally) wires [5].

2.1.2.2.2 Wireless communications:

Does not use physical media to exchange data between devices, and it may has many types that can be outlined as:

Radio: is considered to be a reliable form of communication.

Microwave: Potentially very good option for linking sites with good elevation, such as water towers.

Cellular: Quickly gaining in popularity, especially as pricing continues to decline and for areas that may not have strong radio signals or line-of-sight conditions. The area for coverage should have good, consistent cellular coverage.

Satellite: Good application where there is no, or unreliable cell coverage, such as extreme terrains, very remote locations [5].

2.1.3 Security types used in SCADA

2.1.3.1 Cryptography

It is the conversion of information from a human readable state to apparent nonsense one. The originator of an encrypted message (Alice) shared the decoding technique needed to recover the original information only with intended recipients (Bob), thereby precluding unwanted persons (Eve) from doing the same. The cryptography literature often uses Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve (" eavesdropper ") for the adversary. Applications of cryptography include military communications, electronic commerce, ATM cards, and computer passwords [4].

2.1.3.2 Firewall

A firewall is a mechanism used to control and monitor traffic to and from a network for the purpose of protecting devices on the network. It compares the traffic passing through it to a predefined security criteria or policy, discarding messages that do not meet the policy's requirements. In effect, it is a filter blocking unwanted network traffic and placing limitations on the amount and type of communication that occurs between a protected network and other networks (such as the Internet, or another portion of a site's network)[4].

2.1.3.3 Physical security

Describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm; Such as:

1. Physical barriers.
2. Natural surveillance.
3. Security lighting.
4. Alarm systems and sensor.
5. Video surveillance [5].

2.1.4 SCADA protocols

A communications protocol is a standard rule for data representation and data transfer over a communication channel.

Following protocols are commonly used for SCADA applications:

• IEC-60870-104.

• IEC-61850-GOOSE.

• DNP3[6].

2.2 Literature review

2.2.1 National Load Dispatch Centre (NLDC)

For the control of the national HV power transmission network a new control system will be installed at the National Load Dispatch Centre providing the same functionality (SCADA/EMS and Network Applications (NA)) as the existing control system. The system currently in operation was commissioned in 2006. They uses software from both Siemens and nary companies, and their data is stored in server and backed up in another server to retrieve it in case of main station failure. In order to keep secure operation against any probable failure there are four types of redundancy Server redundancy, Hardware redundancy, Line redundancy, Power supply redundancy. Their redundant systems ensure that the system work well when failure occur and prevent any probable catastrophe because of that uses hot standby mode. In this system the communication media is optical fiber. Security is increased by using firewall system and to ensure authentication access for servers they use a unique password and user name.

2.2.2 Bahri water station

It is a water treatment station which has three steps, dragging water from the Nile, intrusion it and the last step is store it for distribution to substation.

Uses an incomplete SCADA system that consists of three parts A, B and C to control and monitor the process. Both parts B and C are operating, but A is not operating because of development works. The station uses SCADA system from Siemens Company and PLCs from Schneider company and Siemens. Radio is the communication means and they use soft starter to operate motors of air blower and pump.

Their SCADA system was installed by MENA WATER in 2005, operated for two years and stopped for lack of equipment and problems in the quality of the actuators used. Now there is only readings of the pumps and is used to read the deposition by sensors at controller levels. Control programs for the system PLCs is written by Schneider Company. There is no system security protection mechanism adopted and no system backup process.

2.2.3 Conclusion

After stations visits and data analysis, NLDC was chosen because it implements a fully operating SCADA system while others are DCS systems. Also, their SCADA system covers most of our evaluation parameters which would enable as to conduct extensive analysis and complete a perfect project that helps institutes that need to design SCADA system by offering a useful catalog.

Chapter Three

Hardware & software of SCADA System

3.1 Introduction

Supervisory control and data acquisition (SCADA) systems are vital components of most nations' critical infrastructures. Most popular SCADA system applications are found in water treatments, chimerical plants, and power networks. SCADA Systems became popular in the 1960's and arose to more efficiently monitor and control of the state of remote equipments.

SCADA provides management and monitoring with real-time data on production operations, implement more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. However, these benefits are acquired at the price of increased vulnerability to attacks or erroneous actions from a variety of external and internal sources[6].

There are different types of SCADA systems that can be considered as SCADA architectures of four different generations First Generation Monolithic or Early SCADA systems, Second Generation Distributed SCADA systems, Third Generation Networked SCADA systems and Fourth Generation Internet of things technology SCADA systems[8].

3.1.1 Monolithic or Early SCADA Systems

The first architecture concept of SCADA was based on the mainframe systems, in which networks are basically not existent. Therefore, first control systems were not able to interconnect with any other, so they were standalone systems. Figure 3-1 represents an example of this generation of SCADA systems

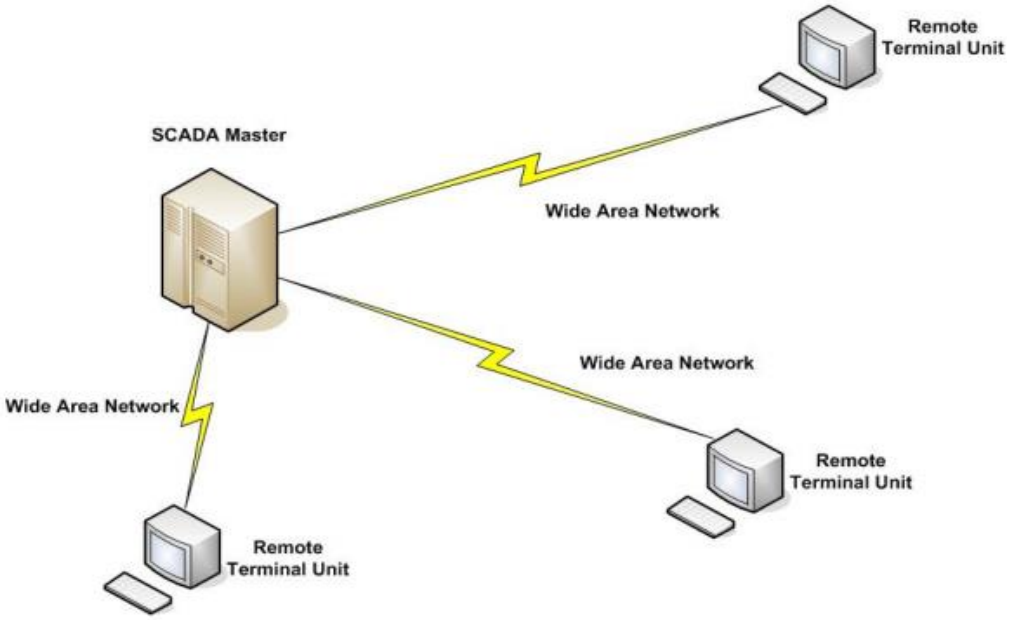


Figure 3-1: Monolithic or Early SCADA Systems [8]

Even if the term of Wide Area Network (WAN) was used, the only purpose of this "network" was to connect to different Remote Terminal Units (RTU) and interchange data with the master computer. Also, at that time, the protocols that we use today for WAN were not available. However, the communication protocols available were developed by various RTU vendors and they were usable only with proprietary master computers from the same vendor. Even so, the protocols were only able to permit scanning, control and data interchange between the master computer and the remote terminal's field sensors or actuators.

The interconnectivity between different RTUs to a master computer was practically impossible, but the need of the industries forced the vendors to improve this disadvantage of SCADA systems. This is how these systems evolved to the second generation [8].

3.1.2 Distributed SCADA Systems

It is the second generation; the process is distributed across multiple stations that are connected through a Local Area Network (LAN), sharing information in real time. Each station is responsible for a particular task thus making the size and cost of each station less than one used in a Monolithic system. Network protocols were still mostly proprietary. These types of systems like the one shown in Figure 3-2 continued to require multiple RTUs and EFMs onsite, but utilized one host system to communicate to each controller [12].

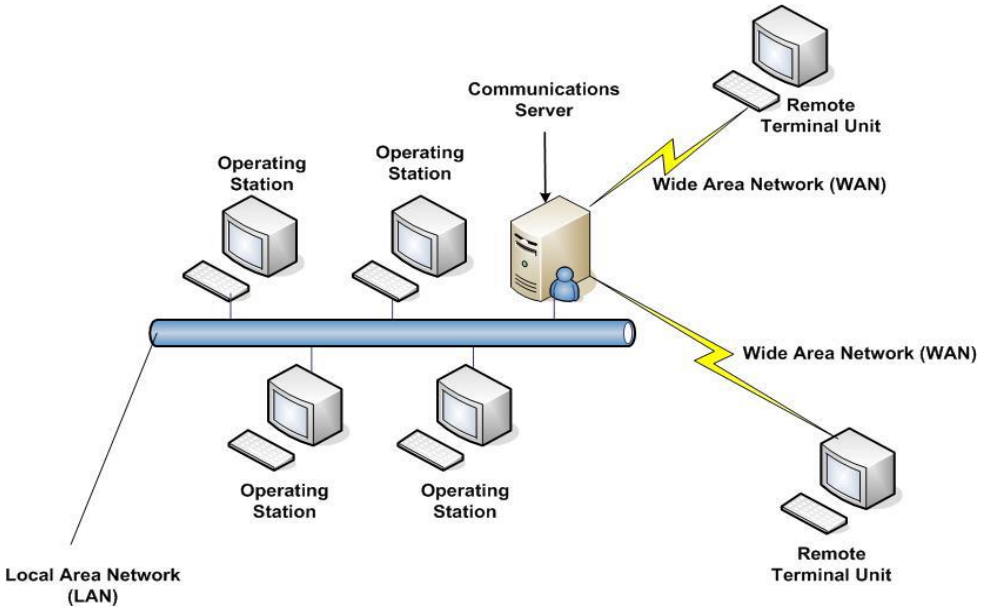


Figure 3-2: Second Generation SCADA Architecture [9]

3.1.3 Networked SCADA Systems

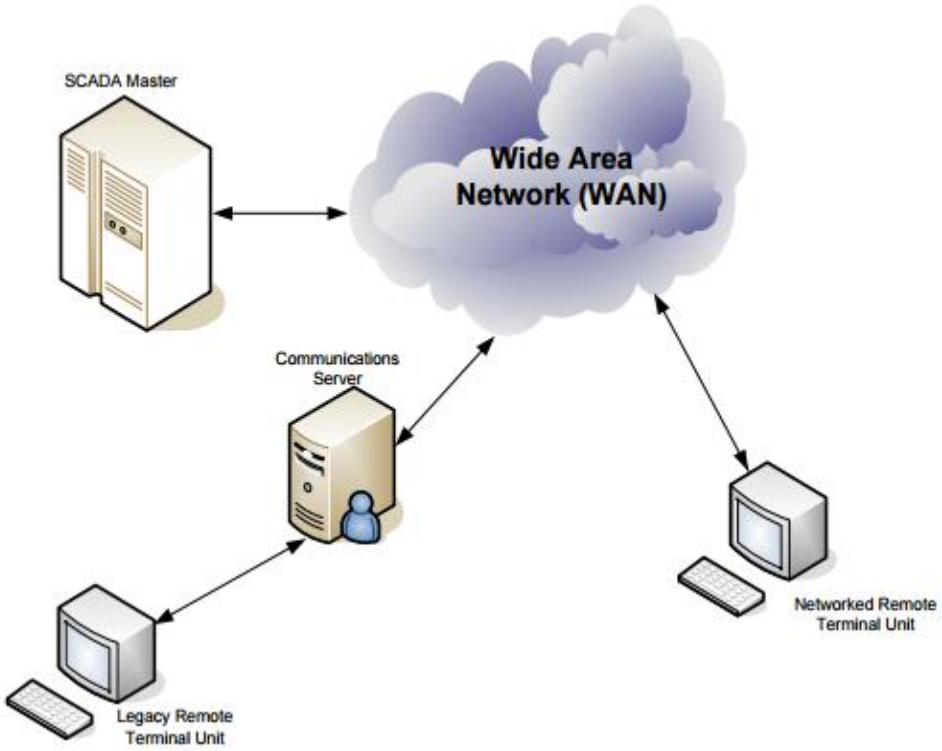


Figure 3.3: Example of Networked SCADA [8]

Figure 3-3 gives an example of this generation of SCADA architecture. Networked systems are the current generation of SCADA and EFM Measurement Systems, using open architecture rather than a vendor-controlled proprietary environment. The SCADA system utilizes open standards and protocols, thus distributing functionality across a WAN rather than a LAN. It is easier to connect third-party peripheral systems such as Wireless Communication, Infrastructure-Monitoring Systems and Network Monitoring Systems (SNMP), due to the use of open architecture. WAN protocols such as Internet Protocols (IP) are used for communications between the master station and communications equipment [14].

3.1.4 Internet of things technology SCADA systems

In fourth generation which is show in Figure 3-4, the infrastructure cost of the SCADA systems is reduced by adopting the internet of things technology with the commercially available cloud computing. The maintenance and integration is also very easy for the fourth generation compared to the earlier SCADA systems [17].

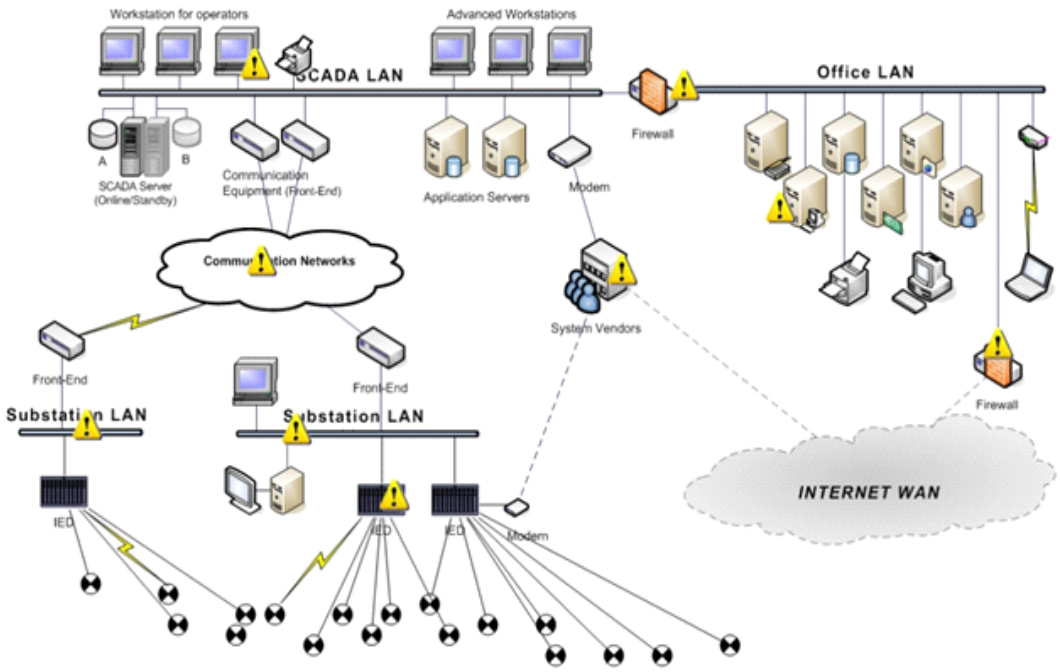


Figure 3-4: Internet of Things [17]

These SCADA systems are able to report state in real time by using the horizontal scale from the cloud computing facility; thus, more complex control algorithms can be implemented which are practically sufficient to implement on traditional PLCs.

3.2 SCADA hardware

A SCADA system consists of a number of remote terminal units (RTUs) collecting field data and sending that data back to a master station, via a communication system. The master station displays the acquired data and allows the operator to perform remote control tasks. The accurate and timely data allows for optimization of the plant operation and process. Other benefits include more efficient, reliable and most importantly, safer operations. These results in a lower cost of operation compared to earlier non-automated systems [2].

On a more complex SCADA system there are essentially five levels or hierarchies:

- Field level instrumentation and control devices.
- Marshaling terminals and RTUs.
- Communications system.
- The master station.
- The commercial data processing department computer system [2].

These levels are shown in Figure 3-5.

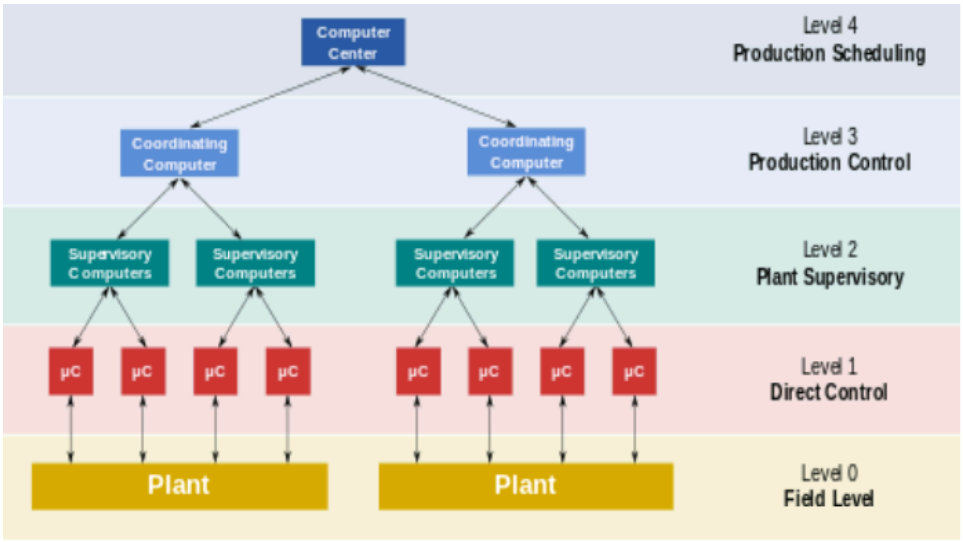


Figure 3-5: SCADA levels [17]

3.2.1 Filed level

It contains sensor which read the physical quantity (temperature, humidity, pressure and status of filed devices etc) and converts it to electrical mount and sends it to the master station across the communication system. At this level actuators may be used to perform some control commands to control other devices like motors, relays, circuit breakers etc [18].

3.2.2 Remote terminal units

An RTU (sometimes referred to as a remote telemetry unit) as the title implies, is a standalone data acquisition and control unit, generally microprocessor based, which monitors and controls equipment at some remote location from the central station. Its primary task is to control and acquire data from process equipment at the remote location and to transfer this data back to a central station. It generally also has the facility for having its configuration and control programs dynamically downloaded from some central station. There is also a facility to be configured locally by some RTU programming unit.

Although traditionally an RTU communicates back to some central station, it is also possible to communicate on a peer-to-peer basis with other RTUs. The RTU can also act as a relay station (sometimes referred to as a store and forward station) to another RTU, which may not be accessible from the central station [2].

3.2.2.1 Typical RTU hardware modules (Architecture of RTU)

Smaller RTUs are built with fixed architecture and generally around an 8-bit microprocessor or microcontroller. Larger RTUs are designed with modular architecture and around a 16-bit microprocessor or microcontroller. Programmable logic controllers (PLCs) are very

often configured and programmed as RTUs [2].

The modular architecture of a typical large RTU is shown in Figure 3-6. As shown, the system bus is used to interconnect the CPU and various modules, which are mentioned here:

- Control processor and associated memory.
- Analog inputs.
- Analog outputs.
- Counter inputs.
- Digital inputs.
- Digital outputs.
- Communication interface(s).
- Power supply.
- RTU rack and enclosure.

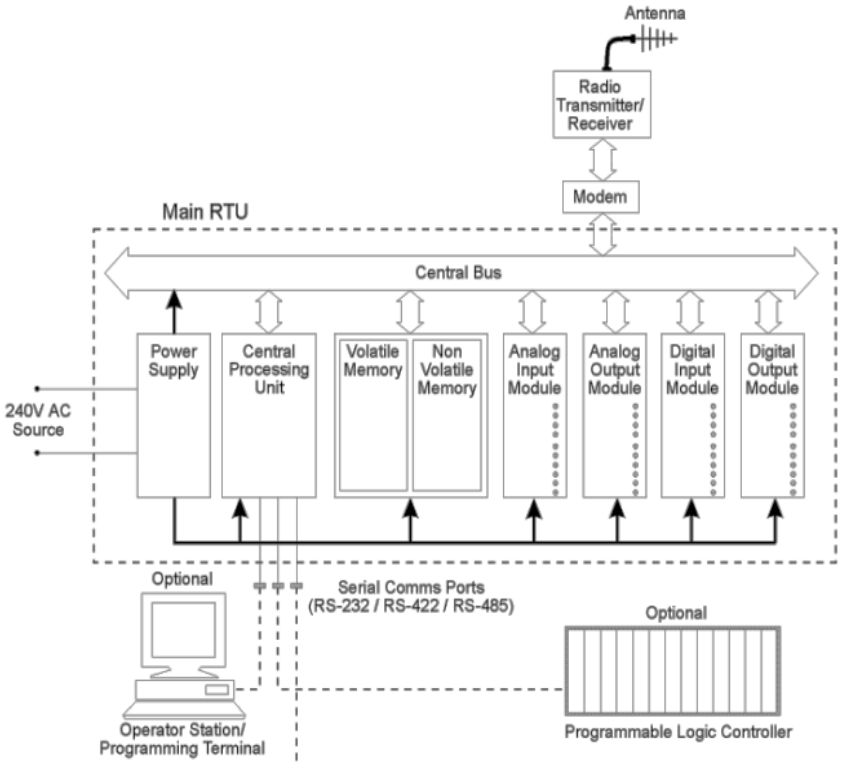


Figure 3-6: Typical RTU Hardware Structure [2]

3.2.3 Programmable Logic Controller PLC

A PLC is another SCADA device similar to an RTU. “A Programmable Logic Controller is a small computer running a program. The program reads the inputs of the logic controller, calculates a custom logic function, and then produces the outputs” They are typically programmed using a language called ladder logic and are used in industrial automation. [10].

PLCs similar to an RTU except that outputs are logic functions of the inputs. Both devices collect data and send it back to a central master. While their primary purpose might be the same, there are differences with respect to their design, installation, and operation which are detailed in the following points:

3.2.3.1 Capacity

A PLC has relatively small input/output capabilities; a couple of digital/analog inputs, a similar number of open-collector/relay outputs and sometimes a single interface shared for configuration. A RTU has more capacity with 30+ inputs, several outputs and a lot of communication interfaces [11].

3.2.3.2 Ease of Use

It is not uncommon for a PLC to require external programming or script writing in order to perform its monitoring role. While this can often be done with an included GUI application, the point is it must still be done, more than likely by someone with a lot of programming knowledge. RTUs, on the other hand, come pre-set for deployment into a SCADA system. A RTU often includes an embedded configuration web application that requires nothing more than a standard browser connection for setup. A RTU can also be accessed for configuration even while it is actively monitoring [11].

3.2.3.3 Space Requirements

Just because an RTU has a lot of capability compared with a PLC, that doesn't mean you will need acres of space to install one [11].

3.2.4 Communications system

Generally the combination of radio and direct wired connections is used for SCADA systems, but in case of large systems like power stations and railways SONET/SDH are frequently used.

3.2.5 Master Terminal Unit (MTU)

It is located in a central place, called control room, from where the complete process is supervised. It is built around one or more computer, which works as server and workstation. Its major function is to monitor and control (supervise) the controlled process through a number of RTUs distributed throughout the process [2].

3.2.5.1 Schematic of MTU

A simplified schematic of MTU, depicting its basic components and their interconnections, is shown in Figure 3-7. At the heart of the MTU is a computer or computers, comprising both hardware and software. On one side, it is interfaced with operators through human-machine interface (HMI) and, on the other side, to the RTUs through a digital communication network (data network) and a communication port [13].

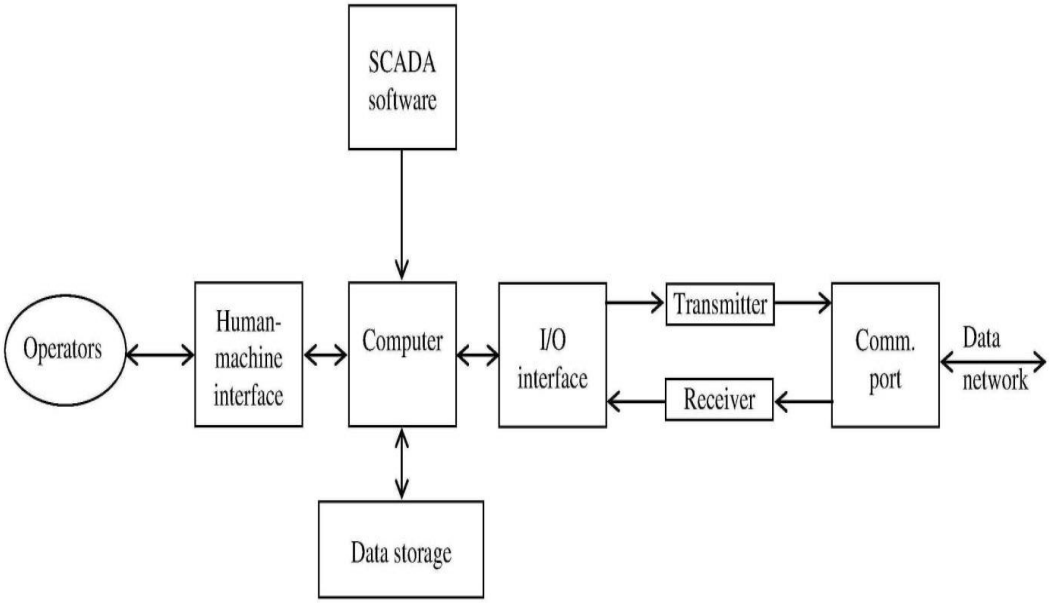


Figure 3-7: Simplified Schematic of MTU [13]

3.2.5.2 The number of computers in MTU may be:

(a) Single Computer: Used exceptionally, because failure of the computer would lead to the failure of the complete SCADA system and thus the controlled process may have to be shut down.

(b) Dual Computer: Used as a rule to avoid shutting down of controlled process. In the event of failure of one computer (which is active), the other (standby) computer takes over immediately [13].

3.2.5.3 The number of processors in the computer may be

(a) Single Processor: Rarely used.

(b) Multi-Processor: Almost always used. This gives the very important benefit that apart from a fast CPU, other processors are optimally designed to perform specific support functions. Thus, in addition to the CPU, the computer may typically have Math processor, HMI processor and Communication processor [13].

3.3 SCADA Software

SCADA software can be divided into two types, proprietary or open. Companies develop proprietary software to communicate to their hardware. These systems are sold as ‘turnkey’ solutions. The main problem with this system is the overwhelming reliance on the supplier of the system. Open software systems have gained popularity because of the interoperability they bring to the system. Interoperability is the ability to mix different manufacturers’ equipment on the same system [2].

SCADA software is one of the main parts of the SCADA system. There are several software packages used for designing HMI and SCADA. WINCC from SIEMENS, Complicity HMI from General Electric, and Lookout from National Instruments are well known examples for efficient commercial SCADA packages. However, professional computer programmers are biased to standard programming languages and tools in building SCADA applications. This lower level programming approach offers them more freedom to configure their projects with highly reduced restrictions which are associated to these higher level packages. Moreover, while using standard programming languages allows SCADA developer to put their own character in the final product, the cost of extra programming efforts is fairly compensated by savings in software packages expenditure [14].

The main feature of SCADA system is the software application program, including: Graphical User Interface (GUI), multiple screen navigation, animations, trends, alarms handling, archiving.

3.3.1 Human Machine Interface (HMI)

SCADA system includes a user interface, usually called Human machine Interface (HMI). The HMI of a SCADA system is where data is

processed and presented to be viewed and monitored by human operator. This interface usually includes controls where the individual can interface with the SCADA system [14].

HMI‘s are an easy way to standardize the facilitation of monitoring multiple RTUs or PLCs. RTUs or PLCs run a pre programmed process, and spread out over the system so monitoring each of them individually may be difficult. Also, RTUs and PLCs have no standardized method to display or present data to the operator, the SCADA system communicate with the PLCs through the system network and processes information that is easily disseminated by the HMI. HMI‘s can also be linked to database, which can use data gathered from PLC‘s or RTU‘s to provide graphs of trends, logistic information, schematics for specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

3.3.2 Database Server

SCADA Database servers are one of most important software‘s used by SCADA system. Any of the database servers used to store and implement data as SQL server, SQL Server Desktop, Access and Oracle. The traditional database server used in SCADA systems is SQL server from Microsoft Company. OPC servers deal with database servers in managing SCADA system data which includes Data Logging archiving, paging, alarm and authentication. All system data is stored in the database server. Then it is managed by the SCADA system designer to display the data to the operator simply and quickly using different ways of data management as alarms, SMS messages and reports [14].

3.3.3 Graphical User Interface(GUI)

The main function of SCADA is to provide clear monitoring for each process, hence screen interfaces should be designed to be user friendly and covering all the process aspects.

3.3.4 Trends

System of SCADA can provide the user with capability of recording and plotting the parameters of the system at real time so user can recall and show the system at any past time needed and parameters of system can be shown at graphical chart for whole system or separate charts which enables zooming, panning and scrolling.

3.3.5 Alarms

To keep system controlled by SCADA in save area SCADA screen must be provide with an alarm to be annunciated on predefined condition such as malfunction operation and fault signal, alarm handling could be seen directly at screen as indicating message or saved within the date at server. An alarm can be created based on the importance of danger (low, medium, high and critical) where each alarm can be activated by different color code, alarm data also can be used for archiving, analyzing, reporting and printing [19].

3.3.6 Data logging and archiving

Logging and archiving of data are used to describe same facility, but logging mean medium-term storage while archiving mean long-term storage of data on the disk.

3.3.7 Report generation

SCADA system can generate daily, weekly and monthly report of separated process or whole system and report can be configured for automatic printing, fixing and e-mailing.

3.3.8 Access control

Software of SCADA enable software to be allocated to different groups, which there is different read-write access privileges to the process parameter, so the user can be connected physically to any part of the system using communication buses [19].

3.4 Protocols

The RTUs are pre-programmed to communicate with the central station SCADA and other networked systems in protocols that are designed to deliver reports on the status of all the input and output devices in the field.

Protocols are similar to languages, which allow the RTU/SCADA units to communicate with each other. All network architectures are loosely based on ISO (International Standards Organization) standard seven layer OSI (Open Systems Interconnection) model as below:

- Layer 7 – Application.
- Layer 6 – Presentation.
- Layer 5 – Session.
- Layer 4 – Transport.
- Layer 3 – Network.
- Layer 2 – Data Link.
- Layer 1 – Physical [15].

The objective of the OSI model is to establish a framework that allows any system or network to connect and exchange signals, messages packets and addresses. The model makes it possible for communications to become independent of the devised system and shield the user from the need to understand the complexity of the network. In general, the bottom four layers cover the physical wiring, network and

communication protocols of the local and wide area networks such as Ethernet and Frame Relay. The presentation and session layers usually deal with establishing and then terminating the session between the two hosts. The Application (Layer 7) and above is where a typical PLC/RTU Protocol (such as Modbus) provide the data at a typical SCADA workstation/ server in a user format from the field RTUs and local PLC systems [15].

3.5 SCADA/RTU Protocols

A large part of any complex SCADA system design is involved in matching the protocol and communication parameters between connecting devices. These include proprietary and non- proprietary protocols, proprietary protocol like Allen Bradley DF1, DH and DH+, GE Fanuc, Siemens Sinaut, Mitsubishi, Modbus RTU/ASCII and Other Vendor Protocols.

The industry is now moving away from many of the old and proprietary protocols. The following RTU/ PLC protocols are emerging as virtual standards in modern SCADA systems [15].

3.5.1 Distributed Network Protocol (DNP)

Byte oriented protocols such as DNP3 are used for supervisory and control communications in the electrical power grid domain. It is designed as an open, interoperable and simple protocol specifically for SCADA controls systems. It is a protocol for transmission of data from point A to point B using serial communications. It uses the master/slave polling method to send and receive information, but also employs sub-masters within the same system. The physical layer is generally designed around RS-232 (V.24), but it also supports other physical standards such as RS-422, RS-485 and even fiber optic [2, 9, and 16].

It provides the rules for remotely located computers and master station computers to communicate data and control commands. It provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data [16].

3.5.2 MODBUS

The point-to-point Modbus protocol has become a virtual standard for RTU and PLC communications. During communication on a Modbus network, the protocol determines how each controller knows device address, recognizes a message addressed to it determines the action to be taken and extract any information/data attached to it [15].

Chapter Four

SCADA System analysis and Evaluation

4.1 NLDC Data

4.1.1 System servers

The national load dispatch center SCADA system includes servers listed here and defined in following sections:

- Tele Control Interface Server (TCI).
- Real Time Communicator Server (RTC).
- Information Management Server (IM).
- User Interface Server (UI).

4.1.1.1 TCI

It is a universal process interface for coupling RTUs of different manufacturers' standard IEC Protocol to SINAUT Spectrum distributed control system.

There are five functions performed by TCI which are:

- RTU startup management.
- Data Acquisition.
- Data Conversion from RTU format to Spectrum format.
- Data Preprocessing.
- Data Distribution to all requesting servers.

4.1.1.2 RTC

Performs data Processing on what is received from TCI server, Manages supervisory control and contains the process data of the SINAUT Spectrum database.

4.1.1.3 IM server

Processing features:

1. Source Data Management (SDM): provides the ability to define access and modify the source database.

2. Historical and Future Data Management (HFD): stores, retrieves, archives and schedules historical data.

4.1.2 Data Processing:

Its functions can be summarized the following points.

- Status data processing: used to handle the status of devices such as alarms, normal switching state, and sequence of events.
- Analog data processing: analog data as limit check, threshold adaption, maximum/minimum/average values.
- Dynamic network coloring: uses specific color to distinguish between things such as network topology, network groups and operational status.
- Counter value processing: checks completeness of processes, counts operating hours and describes numbers of operations.

4.1.3 Supervisory control

Focus on the following two main functions:

1. Management of requests from the operator to control power system devices, the control may be single control like circuit breaker (CB) on/off and tap changer raise/lower and predefined control sequences like bus bar change.
2. Impose conditions that affect the operations of power system devices such as tagging for control inhibit, work permit or remove from operation and defining interlocking conditions.

4.1.4 Redundancy Management

In order to keep secure operation against any probable failure there are four types of redundancy:

4.1.4.1 Server Redundancy

Depending on the required availability of a server different types of redundancy are provided:

- **Hot Standby Redundancy**

  Two servers of the same type are combined in a redundancy block and supervise each other which shown in figure 4-1. If the active one fails during the operating phase a switch over is carried out within the shortest possible time, the update of the spare one is performed spontaneously. This is implemented in TCI and RTC servers.

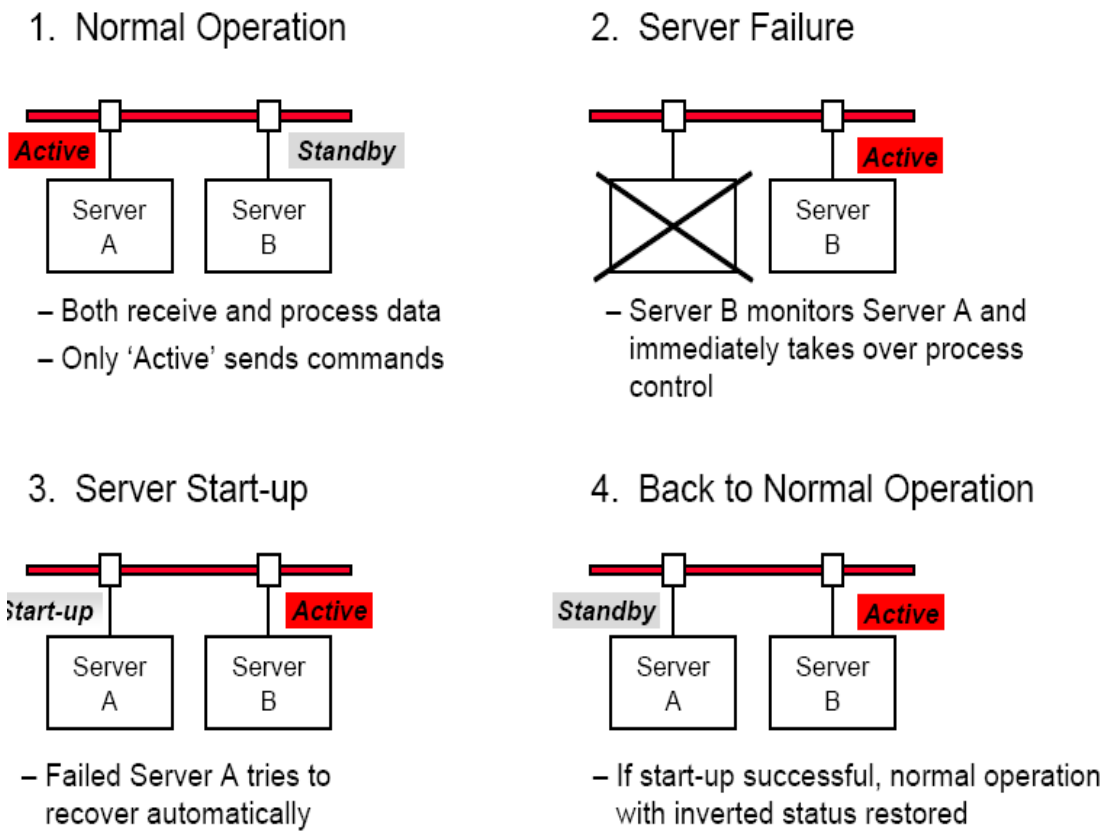


Figure 4-1: Hot Standby Failover

- **Spare Redundancy**

The spare server functions as redundant to the active one however another software or function package may run on it. It updates periodically not spontaneously.

In case the active server fails the spare completes what was running on it and takes over the active's processes. This is adopted in IM server.

- **Hardware Redundancy**

This is the simplest type of redundancy; it provides only another server of the same kind as the one operating in the active status. If for instance an operator's workstation fails the operation will be carried out at a different work station .User interface servers are of this type.

4.1.4.2 Line Redundancy

Every RTU has two links to TCI servers; each link has a different priority (1 or 2). The link with priority 1 becomes active as far as it is available, while the other link is in the standby mode.

4.1.4.3 Power Supply Redundancy

Power supply redundancy which is illustrated in figure 4-2 is very important to prevent problems of system shutdown. They have two power supply units; each of them is capable of powering the system and only one run at time. If the active one fails the other power supply starts running to keep the system on.

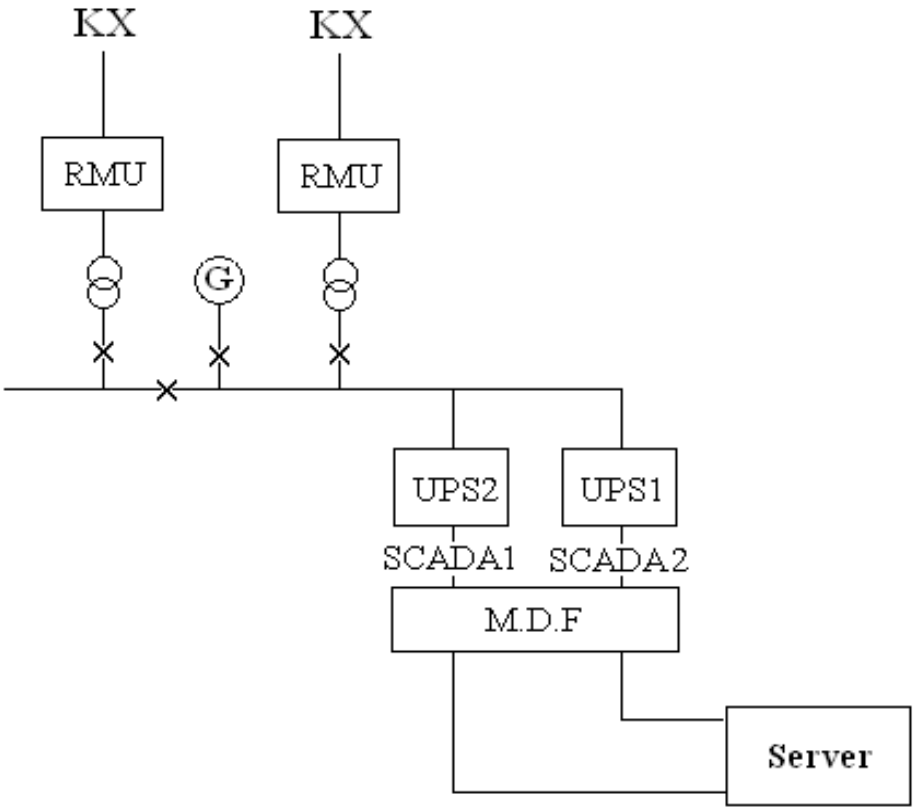


Figure 4-2: Power Supply Redundancy

4.2 NLDC Data Analysis

This section provides analysis of specific parameters which are mentioned in chapter two that are used in NLDC SCADA system dependingon information that we have collected from them.

4.2.1 System communications

4.2.1.1 Fiber optic

Within the power system network, consistent domestic communications are essential to ensure safety, security and control of the power system equipments. Such communications customarily have been provided by methods such as power line carrier and microwave radio systems but are more recently being supplemented or replaced by Fiber optics [20]. An Fiber optic is an optical tube cable that is designed to transport data threw glass over an optical light.

Advantages of Fiber-Optic Communications

In addition to Fiber optics technical advantages, the cost of materials for Fiber optics is becoming more attractive because the cost of copper wire has risen substantially in recent years.

- **Longer Distances**

  A significant benefit of fiber-optic transmission is the capability to transport signals for long distances. Most modern Fiber-optic systems transport information digitally. A digital fiber-optic system can be repeated or regenerated virtually indefinitely [21].

- **Multiple Signals**

  Theoretically, hundreds, even thousands, of video and audio signals can be transported over a single fiber [21].

- **Size**

  Fiber-optic cable is very small in diameter and size when compared to copper.

- **Weight**

  A fiber-optic cable is substantially lighter in weight than copper cable [20].

- **Noise Immunity**

  A fiber-optic signal does not radiate any interference or noise. A signal traveling as photons in an optical fiber is immune to such interference.

- **Ease of Installation**

  A disadvantage of Fiber is that it is difficult to install and maintain. This may have been true in the early days, but now it is as simple to terminate an optical fiber with a connector [21].

- **Low transmission loss**

  The development of Optical Fibers over the last twenty years has resulted in production of Optical Fiber cables which exhibit very low attenuation or transmission loss in comparison with the best copper conductors.

- **Large bandwidth**

  The optical carrier frequency yields a far greater potential transmission bandwidth than metallic cable systems. By comparison the losses in wideband coaxial cable systems restrict the transmission distance to only a few kilometers at bandwidths over one hundred megahertz.

- **Low cost**

  Optical Fibers offer potential for low cost line communication compared to those with copper conductors. Overall system cost when utilizing Optical Fiber communication on long-haul links is substantially less than those for equivalent electrical line systems.

Types of Failures Associated With Fiber Network

The failure classes that are associated with fiber optic networks are classified as patch panel failures, installation failures, and construction failures.

- **Patch panel failures**

  These are failures that create malfunctions in the system by high attenuation. Poor connection points can cause some of these malfunctions when the fiber is not terminated with the appropriate connectors. When the fiber is spliced together poorly the signal inside the fiber optic cable can have large dB losses. If the connections are not inserted in the connectors correctly or the fiber cable has fractured parts in the glass, there can be very high

attenuation to no signal propagation into other parts of the communication network. This is going to possibly show communication outages within the system.

- **Installation failures**

They are associated with failures that are caused when installing the fiber optic network. If a fiber optic cable is bent past the specification bending radius of the cable then the cable can fail instantly or could possible fail over time. This mainly happens when the installer is not aware of the specification of the cable and not paying attention to what he or she is doing. Failures in fiber optics can also be caused by improper dressing. This kind of installation failure is sort of an overlap from a patch panel failure. Terminating fiber optic cable can be a very hard skill to master.

- **Construction failure**

It is the failure that is related to the construction of the fiber optics networks. These cables are always going to be strung from pole to pole, similar to the high or medium voltage lines that form the electric grid.

Optical Fiber Grounded Wire (OPGW)

The OPGW is a combination of fiber and overhead ground line, it is an important development direction of special optical cables, and is widely used with the development of power system's optical fiber communication network.

As the medium of transmitting light signal, the OPGW cable can be used to transmit audio data, video data, control signal, etc. The data speed can reach 50 Mb/s [20].

Generally there is a connector box every two kilometers on the OPGW cable, cooperating with the technology of wireless and multi-hop

transfer, the number of connector points can be reduced, the influence for the existing fiber communication is farthest reduced.

NLDCuses optical grounded wire (OPGW) with a length of 500km that starts from Rosaries up to KILO 10 substation in Khartoum city. It connects all 220 and 110kv substation, this OPGW contains 24 fibers .

Underground optical fiber cable which links the NLDC building with KILO X substation and head quarter via substation Morgan contains 48 fibers.

Keeping in mind comparison between wire and wireless communication techniques, we believe that NLDC took the right decision by choosing fiber optic as a type of wire communications.

Being a control center it is necessary to meet two essential requirements:

First: it needs accurate data according to enable it to take a correct or right decision, therefore wireless communications is not suitable because, the transmitted signal may is susceptible to interference with an information signal that carries the same frequency.

Second: should not permissible their data to unauthorized peoples, to avoid any required effect on the control process. Wireless solutions in particular needs to pay attention to the possibility of a nearby devices eavesdropping on it otherwise it would provide secure conversation. Although wireless is less expensive, but it is not highly suitable solution in this system.

We realize that NLDC SCADA system that connects power stations which may contain vitalism areas need high speed communication; therefore fiber optic is right decision. Also Because of use huge amount of data due to the large number of stations; fiber optic is suitable solution too. The optical fiber here is grounded, system is grounded to ensure personal safety and to protect component from damage [21].

4.2.2 Firewall

In recent years, Supervisory Controls and Data Acquisition (SCADA), process control and industrial manufacturing systems have increasingly relied on commercial information technologies such as Ethernet, TCP/IP and Windows for both critical and non-critical communications. The use of these common protocols and operating systems has made the interfacing of industrial control equipment much easier, but there is now significantly less isolation from the outside world. Network security problems from the enterprise network (EN) and the world at large can be passed onto the SCADA and process control network (PCN), putting industrial production and human safety at risk.

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliance running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of protected hosts.

Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and

therefore cost of obtaining enough public addresses for every computer in an organization. Although NAT on its own is not considered a security feature, hiding the addresses of protected devices has become an often used defense against network reconnaissance.

Figure 4-3shows a simple firewall protecting a personal computer (PC) and programmable logic controller (PLC) from unwanted traffic from the Internet, while allowing requests coming into the corporate web server.

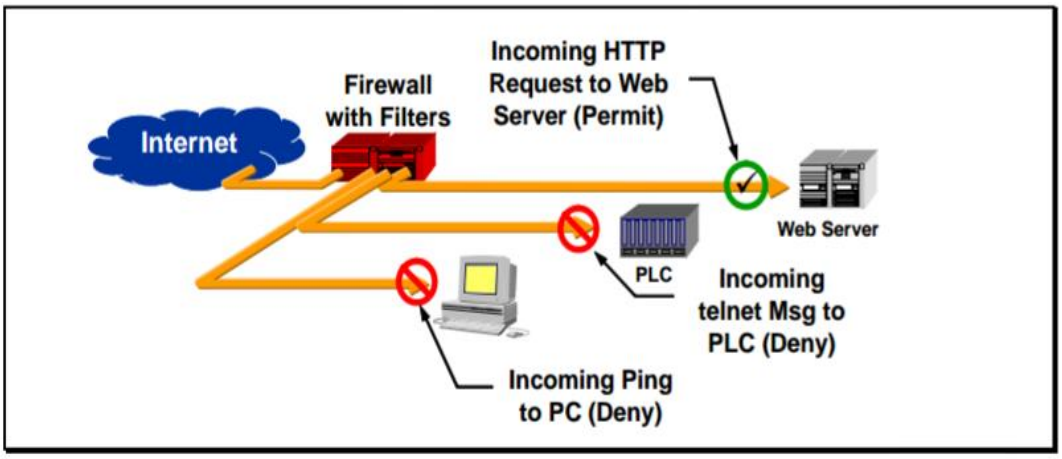


Figure 4-3: A Simplified Example of an Internet-Facing Firewall [4].

In NLDC SCADA system they are using software firewall which is less expensive than hardware firewall, because hardware firewalls require purchase and installation for each network node. It is easier to deploy, but require terminal recourses.

Based on advantages and disadvantages of the two types of firewall that mentioned, NLDC uses software firewall, where they benefit from its advantages, like ease adaptability and updatability, and they though it provides acceptable level of security, and does not allow any hackers.

NLDC is very important system, because it controls all Sudan electricity, so if blackout occurred in system, it may result in putting in

dark the whole country which may leads to propagation of crime, stoppage of vital foundations and systems. On/off to the system from unauthorized people, can cause damage of very expensive machine (reaches thousands of dollars) like transformers, and may cause death to the operator in field. Unauthorized people can delete important data or change alarms states. So the security of this system is very much important.

In our opinion it is better to make hybrid system between software and hardware firewall, and use hardware firewall in fixed parts to make flexible, cost effective, fast and more consistent system.

4.2.3 SCADA protocols TCP/IP

TCP/IP refers to the Transmission Control Protocol and Internet Protocol suit, which provides the transmission medium for Modbus TCP/IP messaging. Modbus TCP/IP is simply the Modbus RTU protocol with a TCP interface that runs on Ethernet. The Modbus messaging structure is the application protocol that defines the rules for organizing and interpreting the data independent of the data transmission medium. Simply stated, TCP/IP allows blocks of binary data to be exchanged between computers. It is also a world-wide standard that serves as the foundation for the World Wide Web. The primary function of TCP is to ensure that all packets of data are received correctly, while IP makes sure that messages are correctly addressed and routed. Note that the TCP/IP combination is merely a transport protocol, and does not define what the data means or how the data is to be interpreted (this is the job of the application protocol, Modbus in this case). So in summary, Modbus TCP/IP uses TCP/IP and Ethernet to carry the data of the Modbus message structure between compatible devices. That is, Modbus TCP/IP combines a physical network (Ethernet), with a networking standard

(TCP/IP), and a standard method of representing data (Modbus as the application protocol). Essentially, the Modbus TCP/IP message is simply a Modbus communication encapsulated in an Ethernet TCP/IP wrapper [25].

Modbus is an application-layer messaging protocol which is situated at level 7 of the Open Systems Interconnection (OSI) model. Modbus is a request/reply protocol and offers services specified by function codes. Function codes are elements of Modbus request/reply protocol data units (PDUs). Besides the standard Modbus protocol, there is another Modbus protocol, called Modbus Plus. Modbus Plus allows for communication between many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer. It provides a client/server communication between devices connected on different types of buses or networks. Figure 4-4 shows protocol structure for both serial and TCP/IP communication [26].

Modbus is accessed on the master/slave principle, the protocol providing for one master and up to 247 slaves. Only the master initiates a transaction. SCADA users have the freedom to choose what standard interfaces to use in their system especially in sending binary data signals among devices. Existing standard interfaces to be used are Electronics Industries Association (EIA)-232, EIA-422, EIA-485 or 20mA current loop. However, most Modbus devices communicate over a serial EIA-485 physical layer. Modbus communication interface is built around messages. For serial connections, Modbus RTU and Modbus ASCII are used with different representations of numerical data and slightly different protocol details.

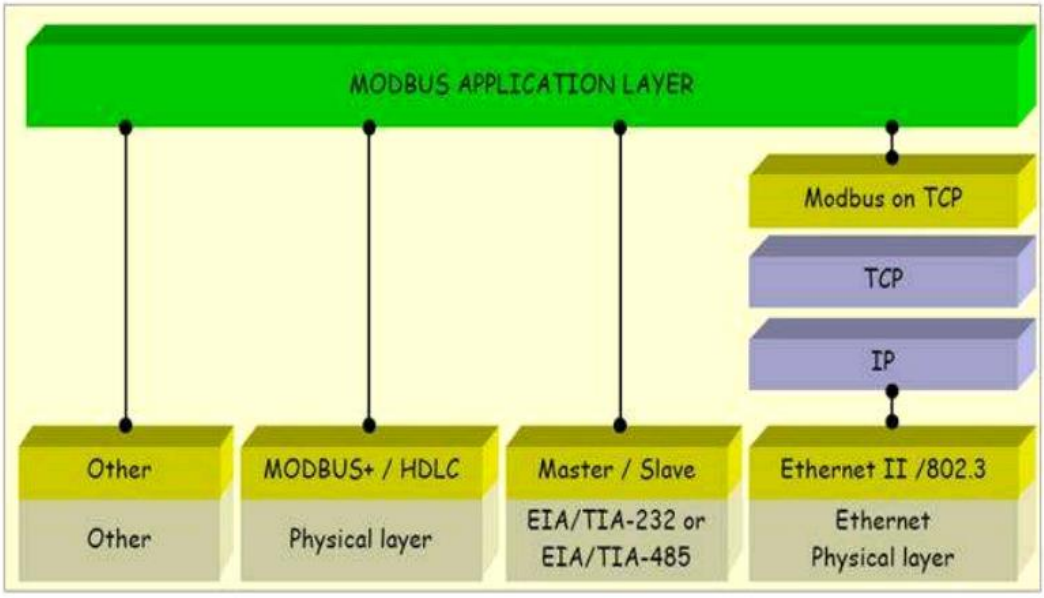


Figure 4-4: MODBUS Communication Stack [26]

Advantage of TCP/IP

1-Its everywhere

2-It is global – the whole world uses this protocol in its internet

In NLDC SCADA system Data they use TCP/IP Protocol and Based on what is mentioned earlier about the TCP/IP protocol, we see that NLDC choice of this protocol is appropriate for the advantages found in it, the users have a great experience in it and it is not expensive in addition to that it also licensed by RSP-TCP [29].

4.2.4 SCADA Backup

4.2.4.1 Traditional SCADA Backup Strategies

- **Manual offline (cold) backups**

  This process is common for smaller SCADA systems. First, someone basically shuts down the system. Then, they save the whole application (or just the historical and configuration data) to a secure location like a tape device, hard drive, or network folder.

When this is complete, they restart the application. Although relatively simple, this is a time-consuming process that usually takes place outside of regular business hours. For this reason, backups can be irregular or dropped entirely [28].

- **Time-based offline (cold) backups**

  At regularly scheduled times, usually in the middle of the night, the SCADA application shuts down automatically and its data is exported to an SQL-based database format. This data is then recorded and archived as outlined above. Backing up offline ensures that files will not be corrupted if they are read while being updated by the running system. However, depending on the size and age of the application, this process can take anywhere from a couple of minutes to a couple of hours. All the while, operators cannot see their process displays. Alarms cannot be viewed, disseminated, or acknowledged. Thin client remote access is unavailable. Worst of all, process interviews collected during this period will be permanently lost. The system fail and need to be restored, all process data and configuration changes since the last backup will also be lost [28].

- **Time-based online (hot) backups**

  Online backups are useful for mission-critical systems where downtime is not an option. In this scenario, the monitoring and control process remains active while the application is being saved. This ensures that alerts are managed and operators are not left in the dark. However, this runs the risk of reading files while they are being written which can affect performance and corrupt the backup database. As with cold backups, restored databases will not include process or configuration data recorded since the last backup [28].

- **Change-based online (hot) backups**

  Rather than updating the whole running application at once, the system backs up each change as it occurs. This eliminates the risk of losing data between backups but, like time-based hot backups, there is a risk of impeded performance and corruption as the backup process effectively "steps on the toes" of the running SCADA system [28].

4.2.4.2 Other Issues with Traditional Backups

- **Long-term compatibility of backup utilities**

  Although some SCADA software platforms include built-in tools for backing up historical and configuration data, others require third-party utilities. As these components are individually upgraded over time, they can determine to function together, which results in dropped backups or lost data [27].

- **Specialized technical knowledge**

  Most backup methodologies require an SQL-based database format. SQL (structured query language) requires specialized knowledge to configure, backup, and restore. This means an investment of time and money for the system integrator or the internal IT department at each point of the process [27].

In NLDC they are using two types of backup ,server backup every three months and database backup every 15 days, and also be on two levels level system backup for each server function and a copy of the information is made and Hard and replay in the case of failure and the second level data base backup. And the backup strategy used is hot and is suitable because the system is critical, depending on what was said in the top ,we find that the hot backup is most appropriate.

4.2.5 Redundancy Analysis

In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe, and to improve actual system performance. Redundancy applies to both hardware and software and implies minimal loss of continuity during the transfer of control between primary and redundant component [23].

Critical system components include

- Power supply.
- Processors.
- I/O modules.
- Sensors and actuators.
- PCs/HMI.
- Networks.
- Servers.
- Databases.

They are two types of redundancy:

Cold Standby Redundancy

A secondary node acts as backup for another identical primary system. It will normally be installed and configured only when the primary node breaks down for the first time. In case of failure in the primary the secondary node is powered on and the data restored before finally starting the failed component. Data for primary system can be backed up on a storage system and restored on secondary system when required. This generally provides a recovery time of a few hours.

Cold redundancy is used where response time is minimal concern and may require operator intervention. However, when time is more critical hot redundancy is the best approach [22].

In NLDC They adopt redundancy in hardware beside spare redundancy. It is good in hardware (used in user interface server) because it ensures that there is another component from the same type and database of the operated ones.

The time after failure occurs does not cause problem or loss of data, help prevent situation where an error on one server result in the overall system becoming inoperative and take a lot time to replace it. It is also good since spare redundancy is used in IM because it may effectively replace the operating component when failure occurs, the time after fault occurs is not important, they need copy of database and historical data because they need it in the operation and forecasting of the future uses, improve stability and make the system more effectible.

Hot Redundancy

Hot standby is a redundant method in which one system runs simultaneously with an identical primary system. Upon failure of the primary system, the hot standby system immediately takes over, replacing the primary system. However, data is still mirrored in real time. Thus, both systems have identical data. Software components are installed and available on both primary and secondary nodes. The software component on the secondary system is up but will not process data or requests [23].

Hot redundancy is used when the process must not go down for even a brief moment under any circumstance, its combines the highest redundancy technology and the best performance. In hot standby the redundant system runs together with the default system, take several millisecond to convert from fail component to another and there is no lost of data. In cold standby the standby system is only powered up when

the default system becomes inoperative, it takes several minutes to switch the standby system and there is large amount of lost data.

In NLDC they are using it in server, power supply and network redundancy. It is suitable for server redundancy (used in TCI and RTC server) because it fully automatic matches process variables, automatic failover upon detecting internal errors, automatic system matching, automatic application synchronization and Millisecond-precise synchronization, since the TCT and RTC have important and critical function and processing (like alarm, status, sequential event, single command, and monitoring the data , etc.) those can be made in real time when the fault or disconnect may cause loss of data. When a failure occurs the time of detecting and correcting it must be too short (by millisecond), which provides high availability of the servers and it have they have critical response time [24].

It is good to be used in network (line redundancy) because it ensures minimal downtime and ensures continuity of network services, provide addition of alternate network paths, it serves a backup mechanism for quickly swapping network operation onto redundant infrastructure in the event of unplanned network outages by providing addition alternates to network paths.

It is suitable in power supply redundancy because it increases uptime, Improve the reliability, Track power quality, monitors power supply system hardware status and can easily integrate into (automation, plant asset management, and other systems). It also prevents the problem of power failure when they use one power supply when it is lost this supply make the entire service unavailable, it makes the system stable. When there is a fault in the electrical supply in all the country it is allocated to the engineers to realizes the problem and keeps the servers from that problem which during power on and power off or when there is

unstable electric supply and it increases system reliability and availability [23].

4.2.6 NLDC RTU

The RTU is one of the most important components of the Substation Automation System (SAS). It collects the signals of key positions, isolators and protection signals in addition to the various measurements and sends them to the national control center. It also receives the operating commands sent from the control center and sends signals to the terminal RTU that shown in figure 4-5. This is done in one of the following two methods:

1. Hardware connection where signals are connected directly from different components of the terminal.
2. Indirectly via the BCU, this requires a communication protocol with the terminal.

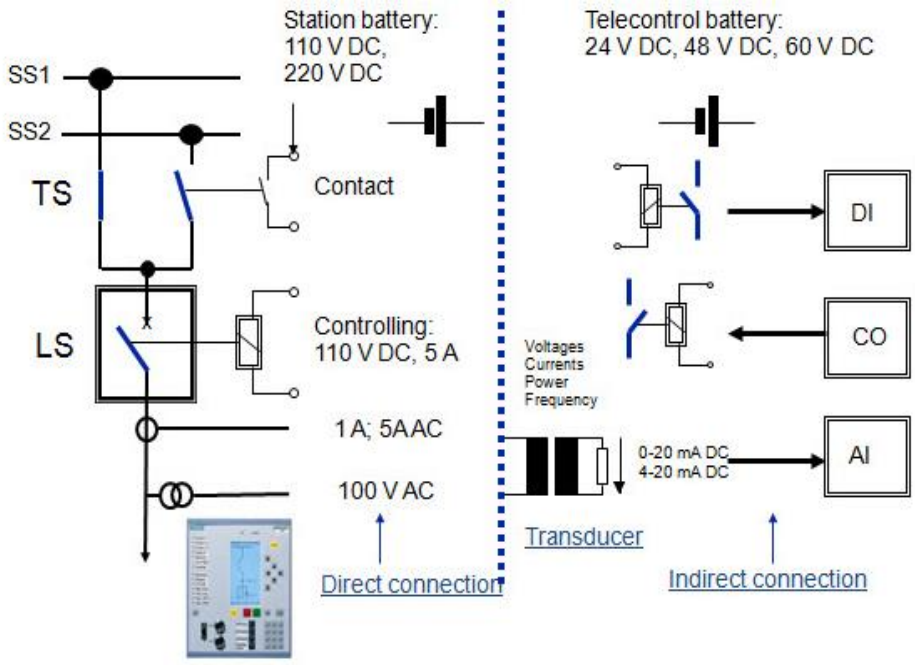


Figure 4-5: Field Connection - Direct Or Indirect

The uses of indirect connection between field devices and RTU is suitable because it decrease the processing operation in RTU.

4.2.5.1 Control Devices in RTU Substation

Following are the control devices in RTU substations of NLDC SCADA system:

- Relays which are protection devices.
- Bay control unit (BCU) which is a device that reads states of switches; values of current and voltage then transmits them and receive the control command.
- Meters.
- Automatic voltage regulator (AVR) which is a device that controls the tap changer of transformer.

All these devices are connected to the RTU by software and standard protocol like IEC101, IEC103 and IEC104 in the format shown in figure 4-6. IEC103 is used for connection between RTU and BCU which is serial protocol suitable for short distance while IEC104 is used for connection between RTU and master station since Ethernet protocol is suitable for use in long distances.

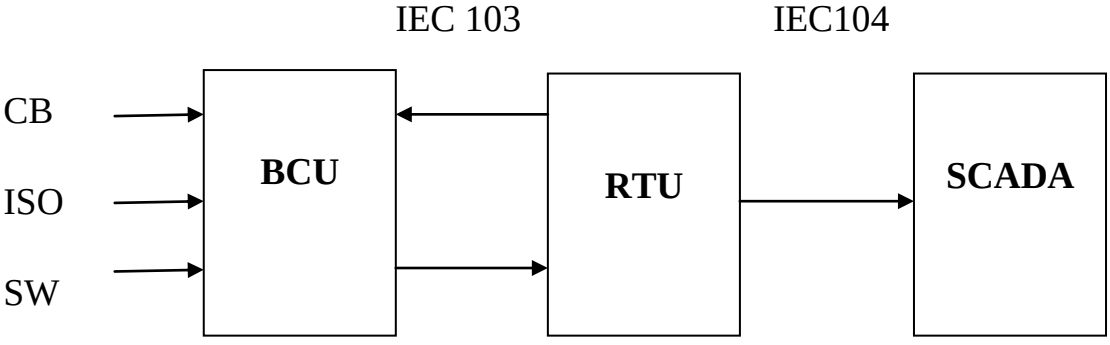


Figure 4-6: RTU Substation

4.2.6.2 Bay Control Unit (BCU)

The operating system, protection and measurement systems are included in one device (Bay control unit), which is engaged in functions of controlling opening and locking of keys, the protection of lines and transformers and measurements of voltage, current, power and energy. This helps ease of operation and reduce the areas of devices.

It is connected to the RTU terminal with a connection protocol until the remote lock and key are controlled from the national control center. The bay engineer's task allows the SCADA engineer to control the keys and gives commands to unlock and lock the keys depending on the current readings and send to SCADA the keys mode and the SCADA send commands.

4.2.6.3 RTU Functions

1- **Command direction**

The RTU receives commands from MTU through communication depending on the status that is displayed in HMI as illustrated in figure 4-7.

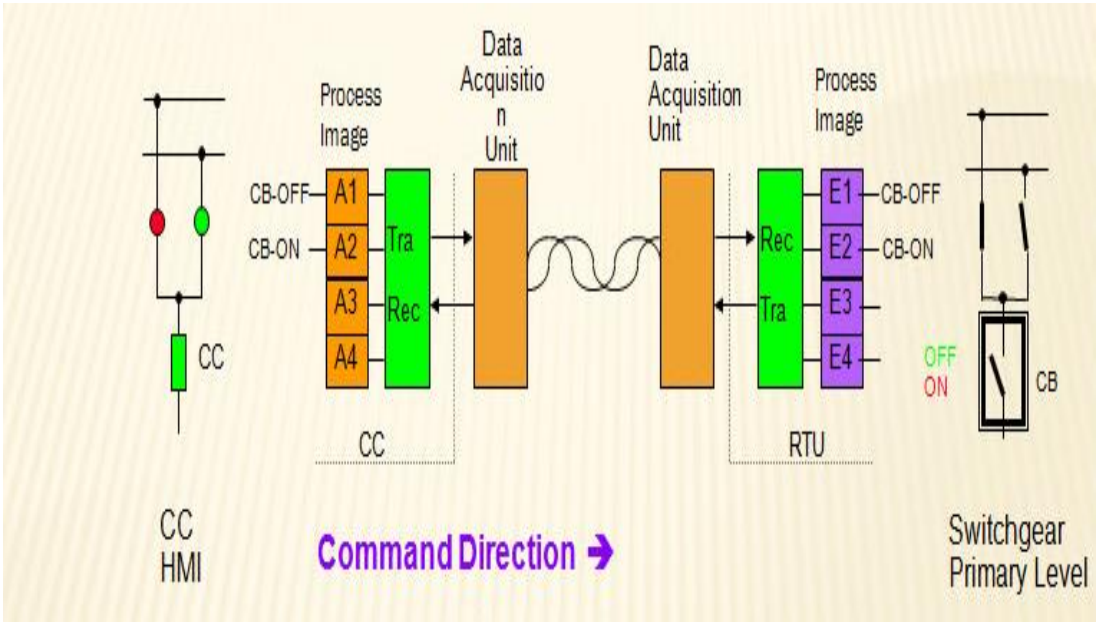


Figure 4-7: Command Direction

2-Monitoring Direction

RTU sends the status of the field devices to the master station through communication media to be displayed in HMI as can be seen in figure 4-8.

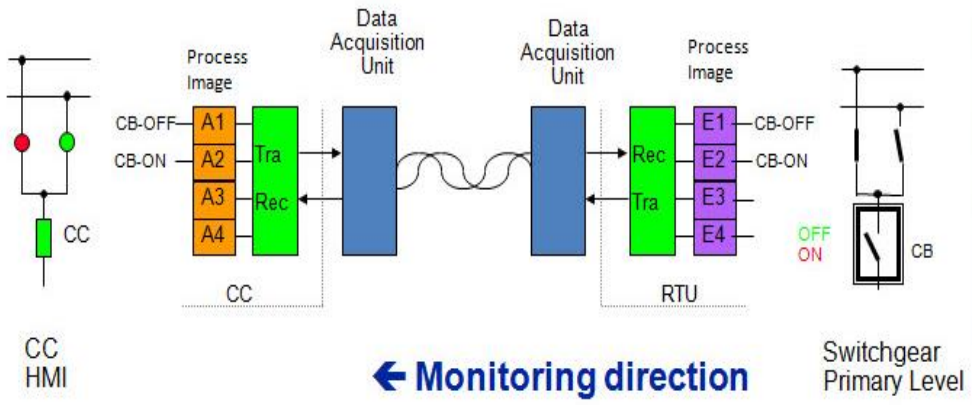


Figure 4-8: Monitoring Direction

4.2.6.4 RTU Field Interfacing

Digital input: This reads switch status, transformer steps and counter values by:

- Single Point (SP): which represents the ON/OFF status by using single bit, it used for alarm protection, trip and etc..
- Double Point (DP):This represents the ON, OFF, Intermediate and Error status by using two bits. Normally used for switching objects like Circuit breakers and Disconnectors status inputs.
- Counter value: used impulses to calculate energy inputs, with or without freezing. .
- Transformer steps: expressed by BCD, analog.

Analogue Inputs: This read analogue inputs like current, temperature and other transducers.

Digital output: It sends three types of commands, double commands, single commandsregulating commands by digital set point has 1 to 4 byte pattern command.

Analogue outputs: to set points to the current and voltage.

4.3 Simulation

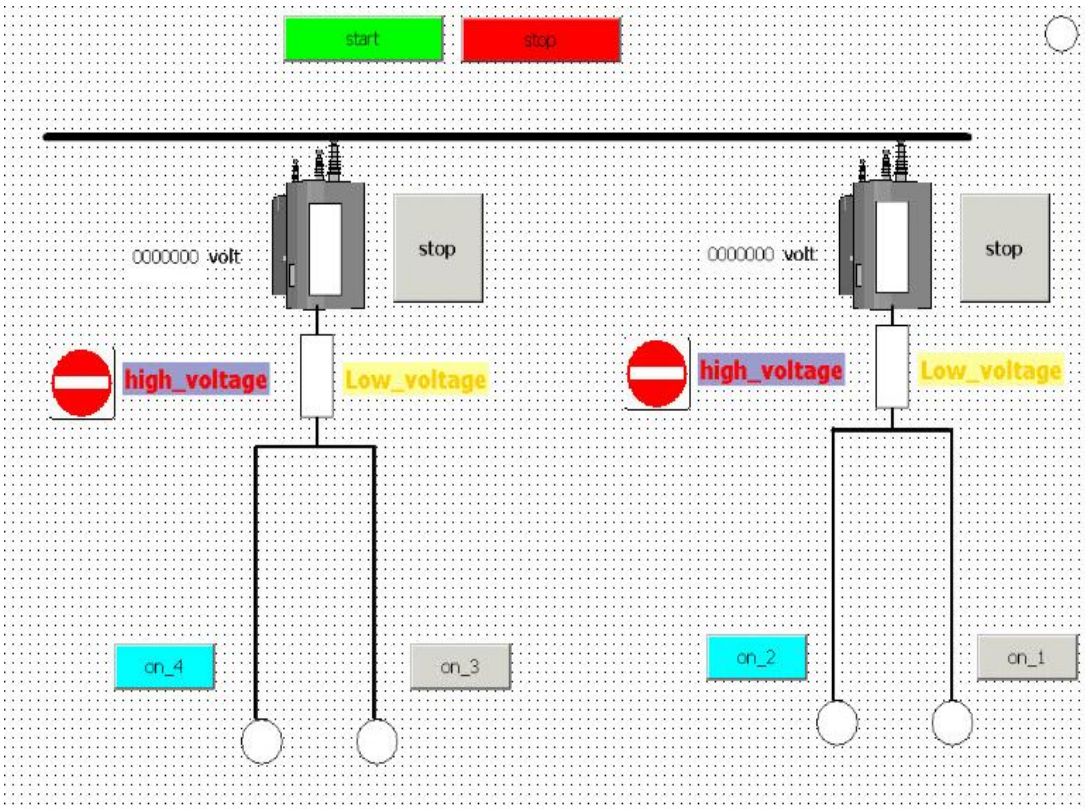


Figure 4-9: Simulation Screen to Control two Transformer Lines

Figure 4-9 shows a number of stations monitored by SCADA system, by displaying the level of voltage which is transferred throw a transformer and then control the states(on, off) by using switch in touch screen.

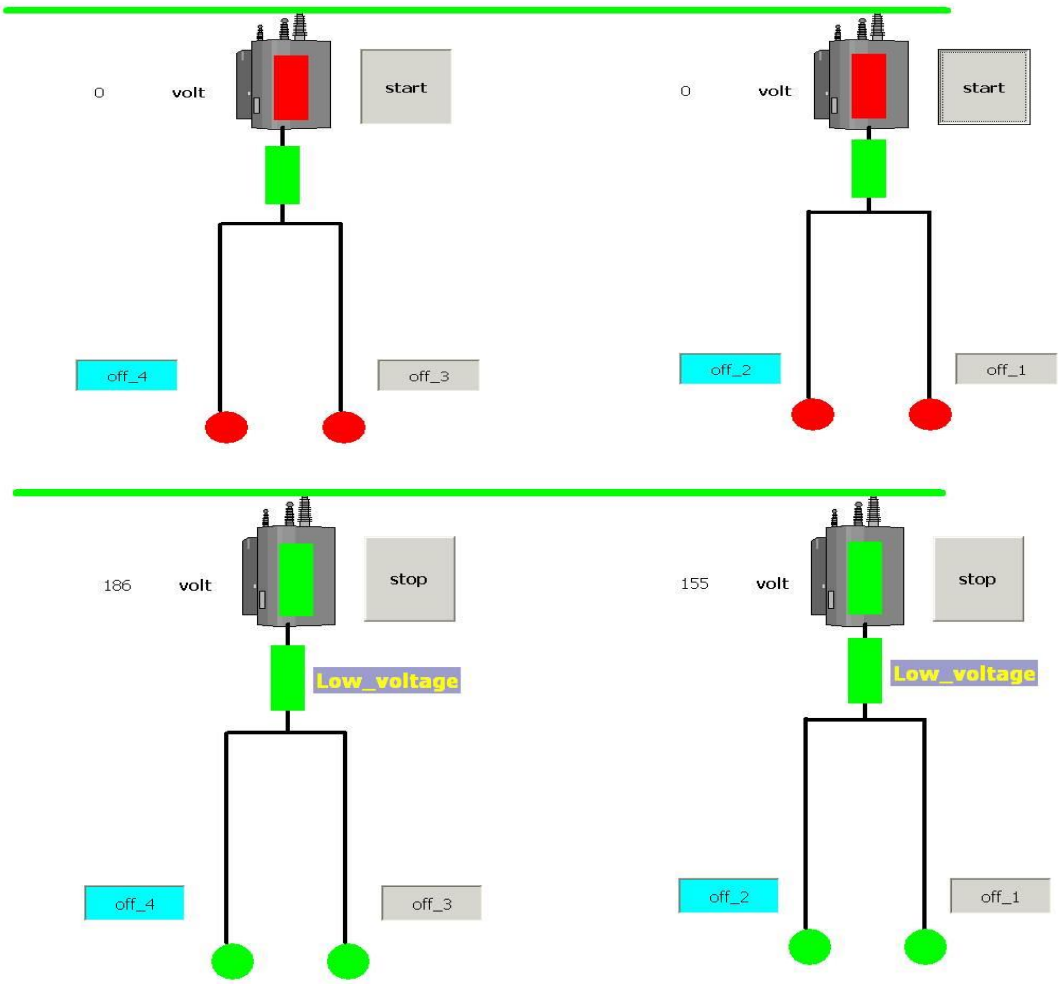


Figure 4-10: Low Voltage Indicator

The level of voltage is represented by an alarm function which displays it using two texts in the touch screen, ”low voltage” that shown in figure 4-10 define the uncritical state which means that the level of voltage is less than that is required by station devices.

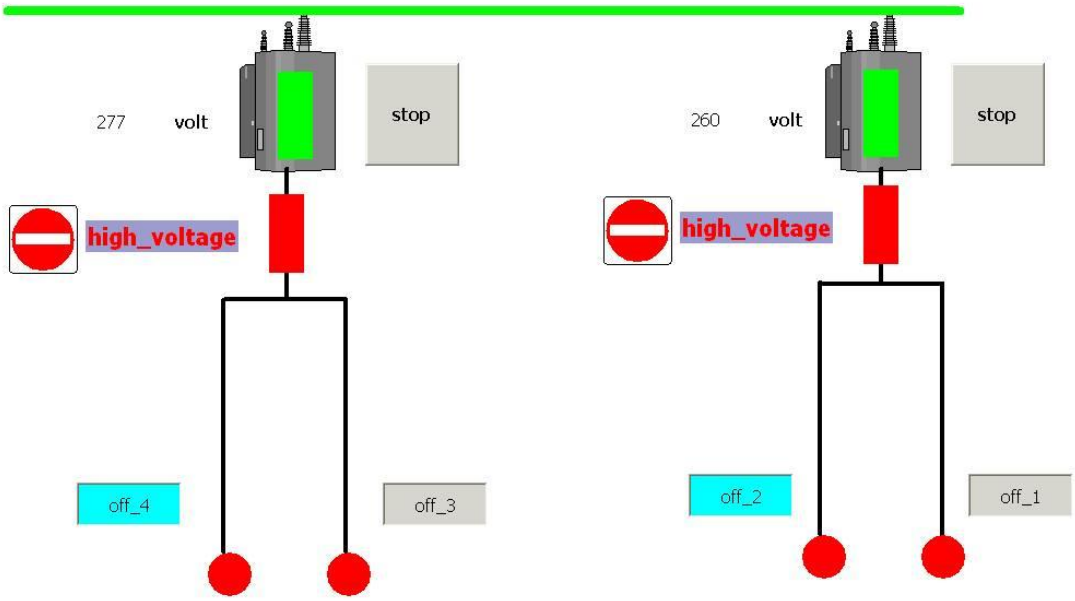


Figure 4-11: High Voltage Indicator

”high voltage” viewed in figure 4-11 indicate that the voltage level is above than the normal level, in this case the station will be disconnect.

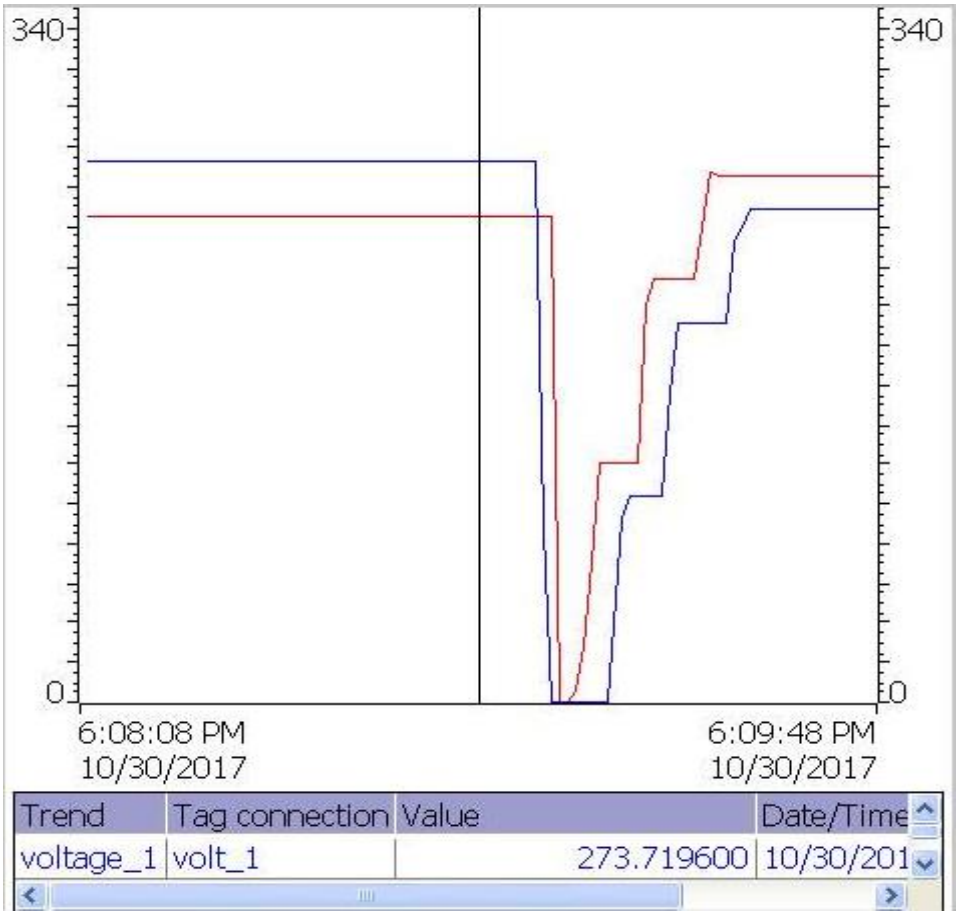


Figure 4-12: Level of Voltage Using Trend

The level of voltage is displayed by two methods: first method, represent all voltage values by using trends in trend view screen which are seen in figure 4-12.

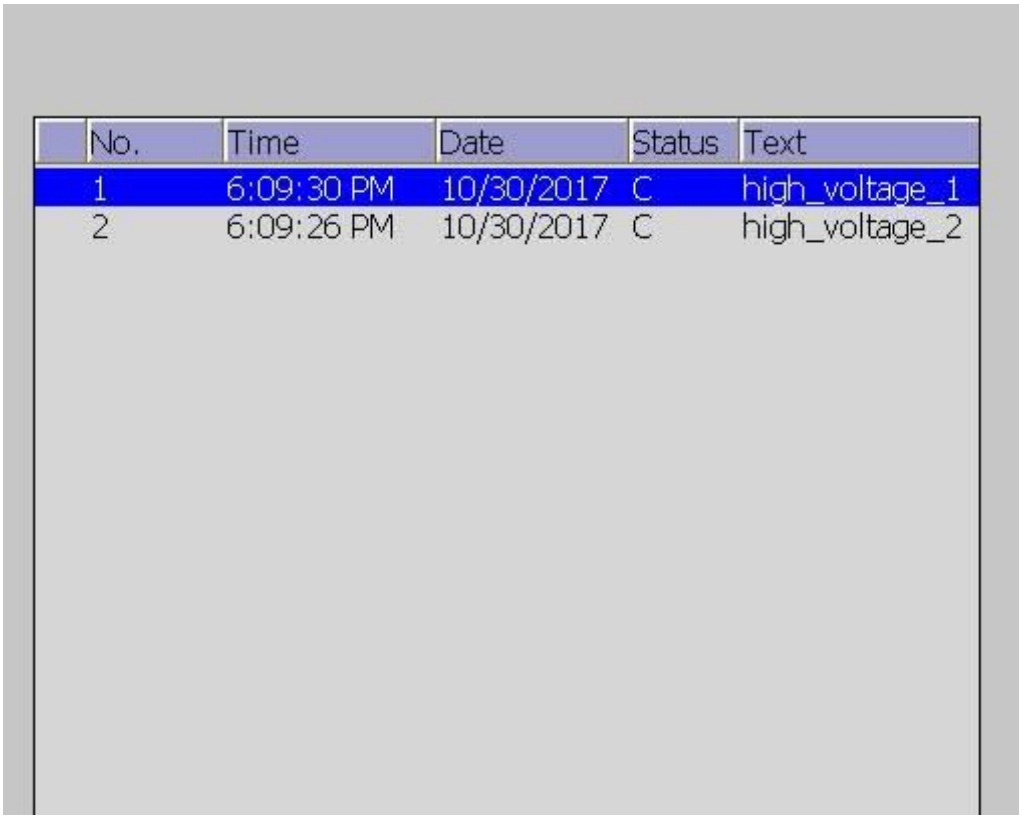


Figure 4-13: System Alarms

Figure 4-13 represented the second method that only displays the alarms (low and high level) in real time with date and time of occurrence.

4-4 Results and Enhancement

Final results according to our evaluation can be summarized in the following points:

- In communication the fiber optic is suitable choice.
- In firewall it is better to upgrade their firewall by making hybrid system between software and hardware firewall.
- Communication protocols that are used are suitable choice.
- Using hardware, software, and information redundancy in all parts of the system in order to make the system more reliable is acceptable but including time redundancy makes the system more appropriate.

The NLDC SCADA system can be improved to more advance by:

- Use smart sensor instead of analog sensor because the smart sensor has the preprocessing of data capability.
- Use PLC or/and RTU with large number of inputs and outputs module to make the system more scalable.
- Use networking SCADA system that is capable of dealing with the problems and challenges of the Industrial Internet of Thing (IIOT).

Chapter Five

Conclusion and Recommendation

5.1 Conclusion:

In this research analysis of a SCADA system to control energy management system using Programmable logic control (PLC) and Remote terminal unit (RTU) to monitor and control any process viewed by alarm function has been done successfully. An analytical study of National Load Dispatch Centre in all its parts for any level in both the hardware and software has been done as well. The energy management system has been represented by using SIMATIC Manager, SIMATIC WinCC flexible, and STEP7 (S7-PCT port Configuration Tool) and then the system has been simulated. the system is accurate in communication and redundancy and needs enhancement in terms of sensors and firewalling.

5.2 Recommendation

- Cover more evaluation parameters.
- Simulate all system parts.

Reference:

1. Rajesh Singla and Arun Khosla,Intelligent Security System for HMI in SCADA Applications. *4*, August2012.
2. Bailey, D. and E. Wright, *Practical SCADA for industry*. 2003: Newnes.
3. https://en.m.wikipedia.org/wiki/scada (10-8-2017).
4. (BCIT), C.B.C.I.o.T., *FIREWALL DEPLOYMENT FOR SCADA AND PROCESS CONTROL NETWORKS.* 2005.
5. Administrator, *COMMUNICATION NETWORK.* 2011.
6. https//en.m.wikipedia.org/wiki/SCADA (8-9-2017).
7. AbuMeteir, H.A., *A Proposed SCADA System to improve the conditions of the Electricity sector in Gaza Strip*. 2012, The Islamic University Of Gaza.
8. Ujvarosi, A., *EVOLUTION OF SCADA SYSTEMS.* Bulletin of the Transilvania University of Brasov. Engineering Sciences. Series I, 2016. 9(1): p. 63.
9. Communication Technologies, I., *Supervisory Control and Data Acquisition (SCADA) Systems.* 2004.
10. McHugh, D., *Implementing TCP/IP in SCADA systems.* 2003.
11. http://dpstele.com/rtu/scada/monitor-network.php,20.october.2017.
12. Rutherford, b.D., *Ethernet for SCADA Systems.* 2012.
13. VERMA, D.H.K., *HARDWARE OF SUPERVISORY CONTROL & DATA ACQUISITION SYSTEM.* 2014.
14. Alihussein, A.M., *A Supervisory Control And Data Acquisition (SCADA) for Water Distribution System of Gaza City*. 2010.
15. Kalapatapu, R., *Scada protocols and communication trends.* ISA2004, 2004
16. uddin, M.S., *SCADA Protocols and Security.* 2006.

17. http://www.eedgefxkits.com/blog/scada-systeem-architecture-types-application/(21-8-2017).

18. https//en.m.wikipedia.org/wiki/SCADA. (5-9-2017).

19. Ashour,P.H.A., Advance automated and smart system 2016.

20. Zhaia, S., et al., *Research of communication technology on IoT for high-voltagen transmission line.* International Journal of Smart Grid and Clean Energy (IJSCCE), 2012.

21. Ezeh, G. and O.G. Ibe, *Efficiency of optical fiber communication for dissemination of information within the power system network.* IOSR-JCE, 2013.

22.https://www. ibm.com / developeworks/ community/blogs/RohitShetty/entry/high-availability-cold-warm-hot?lang=en.(12-10-2017)

23. https://en.m.wikipidea.org/wiki/redundancy-(engineering) (13-10-2017)

24. Dorran Bekker Application versus network redundanccy.june 2012.

25. Acromag, *INTRODUCTION TO MODBUS TCP/IP*. 2005.

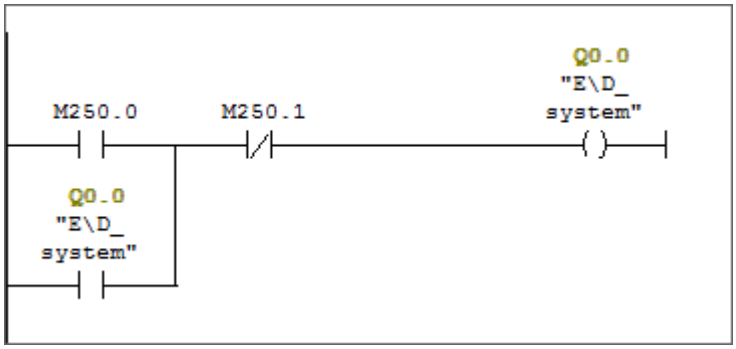
26. A., G., et al., *SCADA* Network Insecurity: *Securing Critical Infrastructures through SCADA Security Exploitation.* 2009.

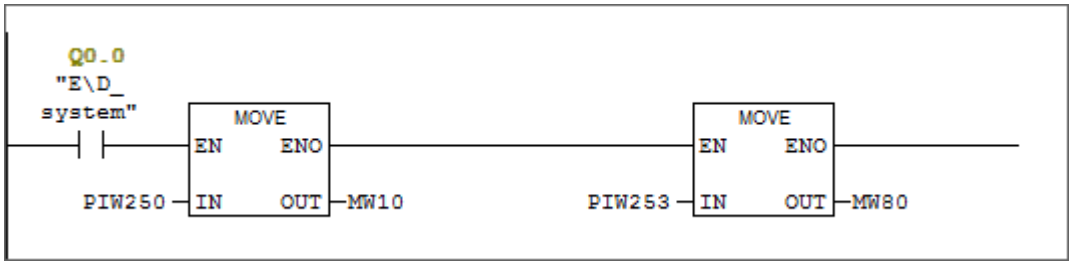
27. https://www.wateronline.com/doc/a-better-way-to-back-up-scada-0001 (11-10-2017).

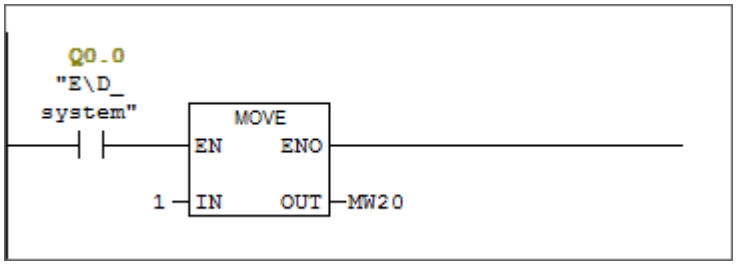
28. http://www.science/article/pii/s1474667017464573 (29-9-2017).

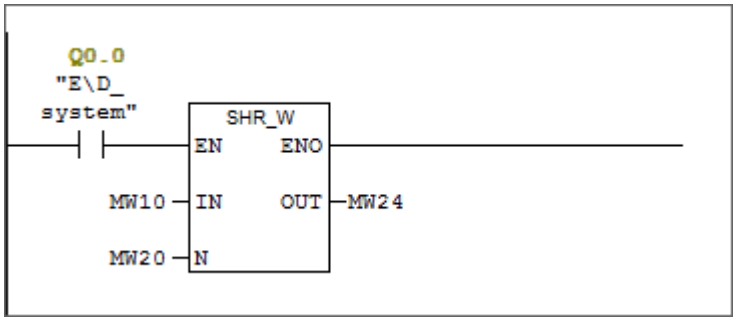
Appendix :

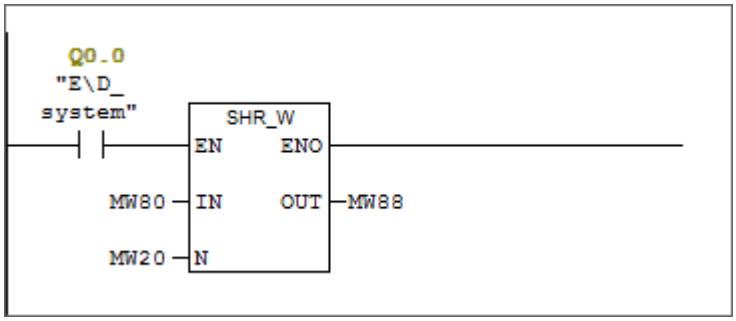
A.1 Code

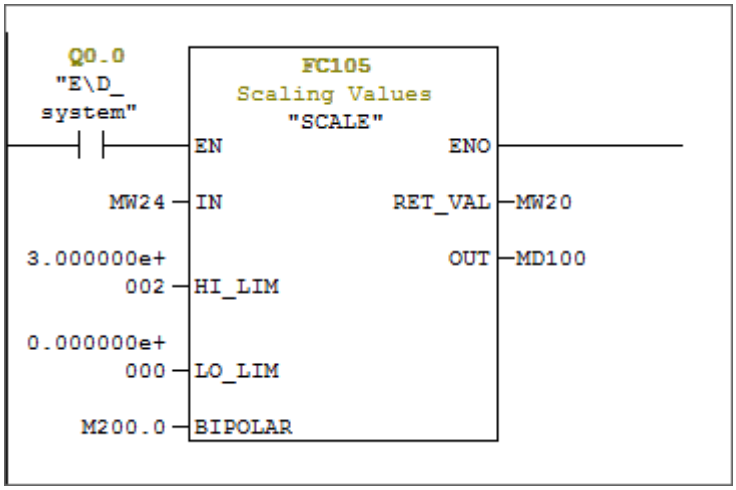


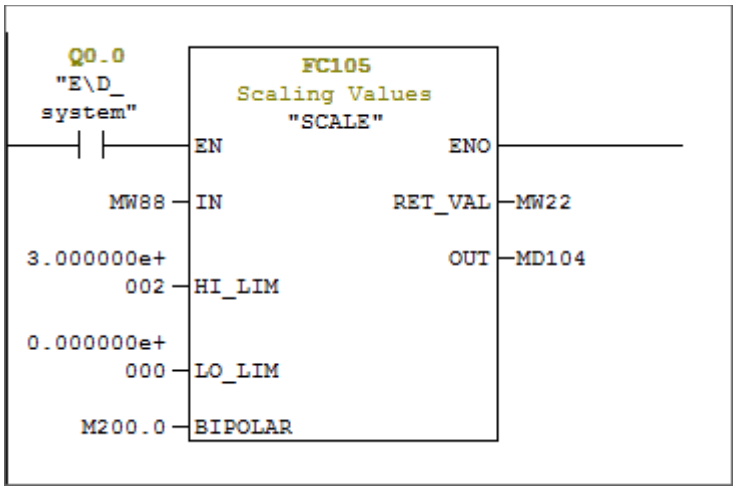


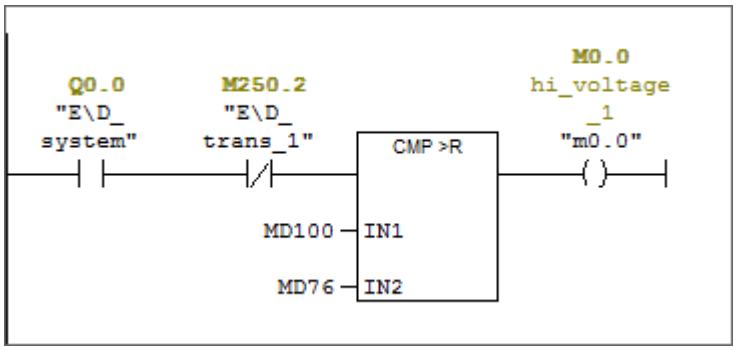


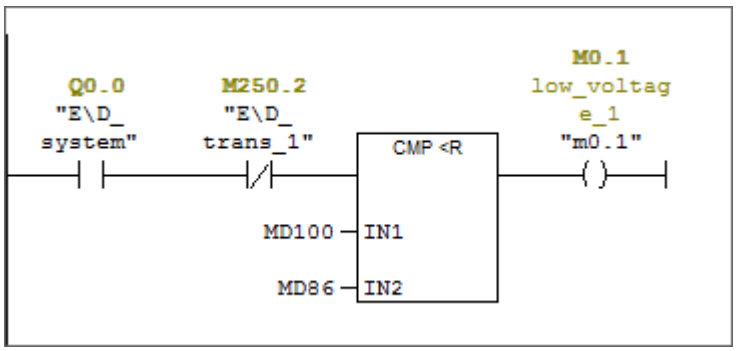


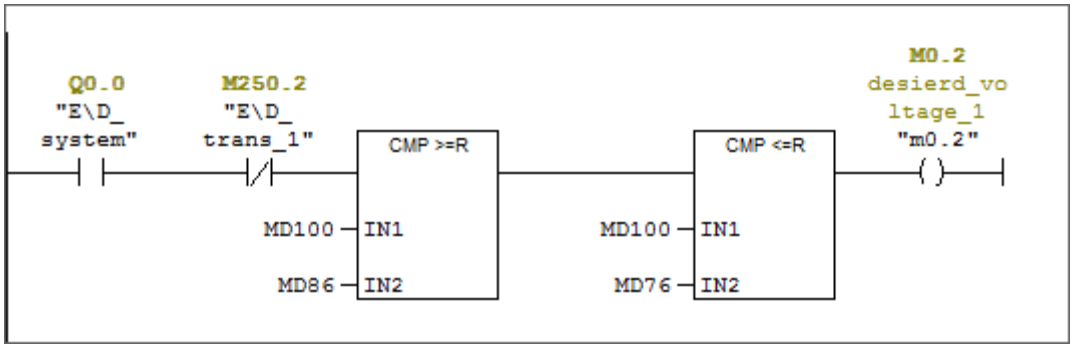


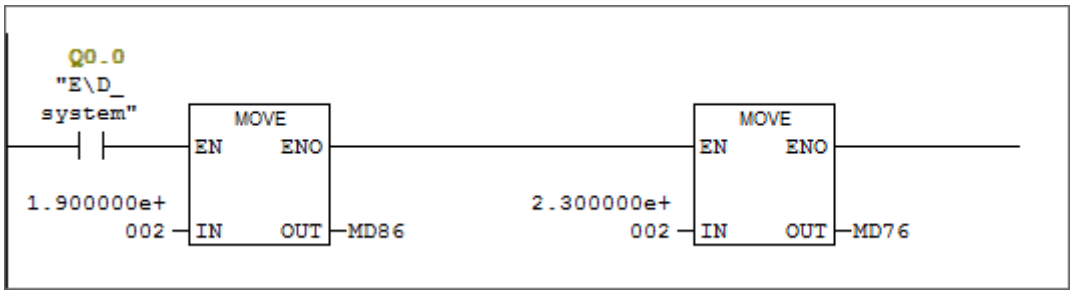

Q0.0
"E\D_
system"
FC105
Scaling Values
"SCALE"
EN
ENO
MW24
IN
RET_VAL
MW20
3.000000e+
002
HI_LIM
OUT
MD100
0.000000e+
000
LO_LIM
M200.0
BIPOLAR

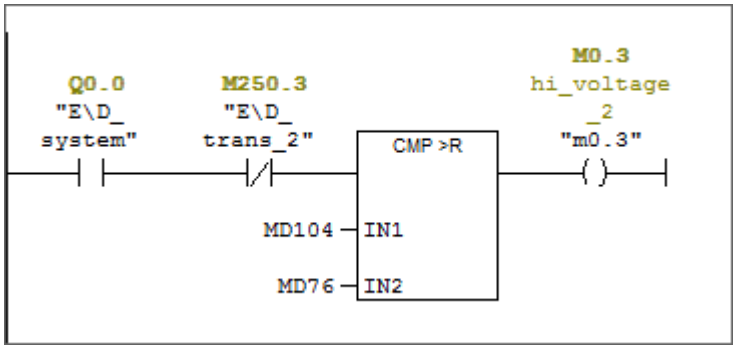

Q0.0
"E\D_
system"
FC105
Scaling Values
"SCALE"
EN
ENO
MW88
IN
RET_VAL
MW22
3.000000e+
002
HI_LIM
OUT
MD104
0.000000e+
000
LO_LIM
M200.0
BIPOLAR

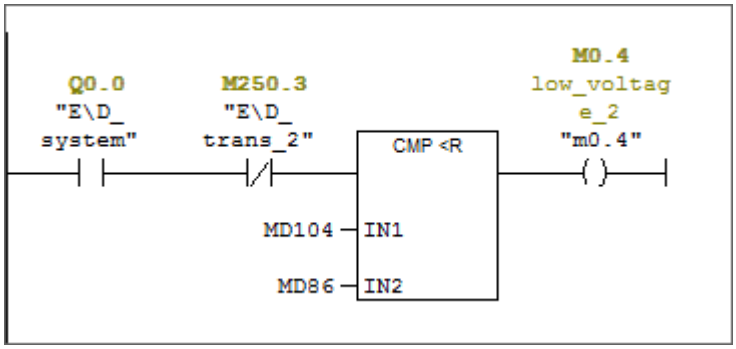

Q0.0
"E\D_
system"
M250.2
"E\D_
trans_1"
CMP >R
M0.0
hi_voltage
_1
"m0.0"
MD100
IN1
MD76
IN2

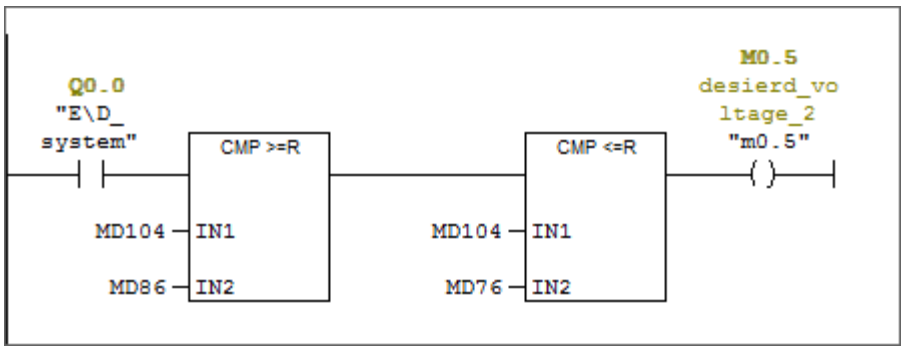

Q0.0
"E\D_
system"
M250.2
"E\D_
trans_1"
CMP <R
M0.1
low_voltag
e_1
"m0.1"
MD100
IN1
MD86
IN2

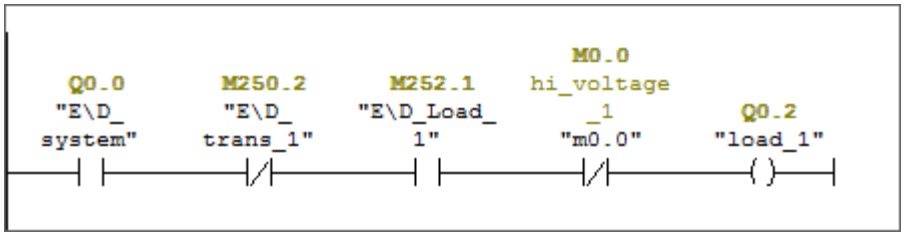

Q0.0
"E\D_
system"
M250.2
"E\D_
trans_1"
CMP >=R
MD100
IN1
MD86
IN2
CMP <=R
MD100
IN1
MD76
IN2
M0.2
desierd_vo
ltage_1
"m0.2"

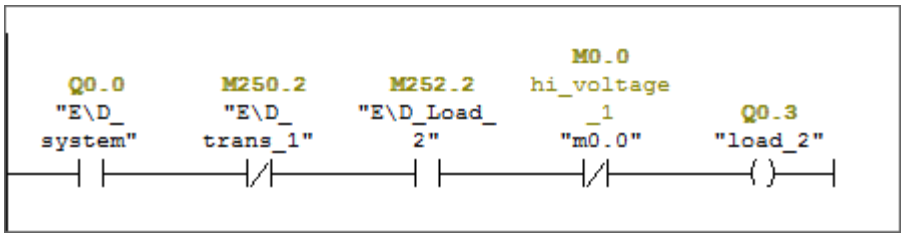

Q0.0
"E\D_
system"
MOVE
EN
ENO
1.900000e+
002
IN
OUT
MD86
MOVE
EN
ENO
2.300000e+
002
IN
OUT
MD76

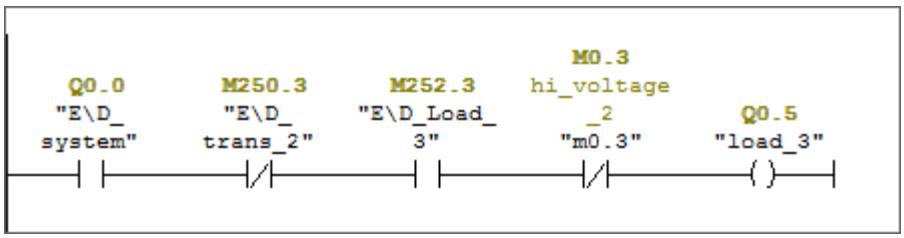

Q0.0
"E\D_
system"
M250.3
"E\D_
trans_2"
CMP >R
MD104
IN1
MD76
IN2
M0.3
hi_voltage
_2
"m0.3"

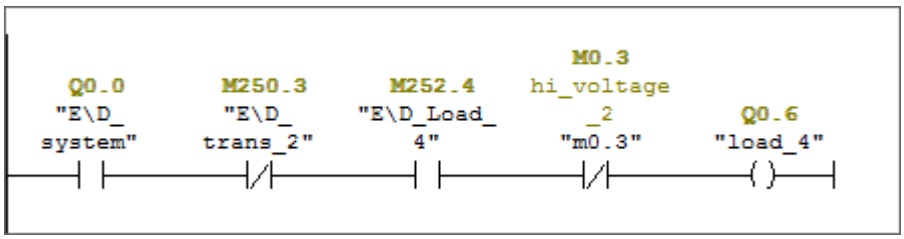

Q0.0
"E\D_
system"
M250.3
"E\D_
trans_2"
CMP <R
MD104
IN1
MD86
IN2
M0.4
low_voltag
e_2
"m0.4"


Q0.0
"E\D_
system"
CMP >=R
MD104
IN1
MD86
IN2
CMP <=R
MD104
IN1
MD76
IN2
M0.5
desierd_vo
ltage_2
"m0.5"


Q0.0
"E\D_
system"
M250.2
"E\D_
trans_1"
M252.1
"E\D_Load_
1"
M0.0
hi_voltage
_1
"m0.0"
Q0.2
"load_1"


Q0.0
"E\D_
system"
M250.2
"E\D_
trans_1"
M252.2
"E\D_Load_
2"
M0.0
hi_voltage
_1
"m0.0"
Q0.3
"load_2"


Q0.0
"E\D_
system"
M250.3
"E\D_
trans_2"
M252.3
"E\D_Load_
3"
M0.3
hi_voltage
_2
"m0.3"
Q0.5
"load_3"


Q0.0
"E\D_
system"
M250.3
"E\D_
trans_2"
M252.4
"E\D_Load_
4"
M0.3
hi_voltage
_2
"m0.3"
Q0.6
"load_4"