

UNIVERSITY OF NAIROBI



SCHOOL OF COMPUTING AND INFORMATICS

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM LIVE
MEMORY ACQUISITION FOR THE MODBUS PROTOCOL FORENSICS. A CASE OF
THE PETROLEUM DEPOTS IN KENYA

BY:

JOHN ONYIEGO

P53/86208/2016

SUPERVISOR:

DR. ELISHA ABADE

PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE AWARD OF MASTER OF SCIENCE DEGREE IN DISTRIBUTED COMPUTING
TECHNOLOGY.

DECLARATION

I, Onyiego John, do hereby declare that this research project is entirely my own work and where there is work or contributions of other individuals, it has been duly referenced as acknowledgement.

To the best of my knowledge, similar research has not been carried out before or previously presented to any other university.

Sign: ----- Date: -----

Name:

Reg. No:

School of Computing and Informatics

University of Nairobi

This project has been submitted in partial fulfilment of the requirements for the Master of Science degree in Distributed Computing Technology of the University of Nairobi with my approval as the university supervisor.

Sign: ----- Date: -----

Name: Dr Elisha O. Abade

School of Computing and Informatics

University of Nairobi.

Abstract

Supervisory Control and Data Acquisition (SCADA) has been at the core of Operational Technology (OT) used in industries and process plants to monitor and control critical processes, especially in the energy sector. In petroleum sub-sector, it has been used in monitoring transportation, storage and loading of petroleum products. It is linked to instruments that collect and monitor parameters such as temperature, pressure and product densities. It gives commands to actuators by the use of the application programs installed on the programmable logic controllers (PLCs). Earlier SCADA systems were isolated from the internet, hence protected by an airgap from attacks taking place on interconnected systems. The recent trend is that SCADA systems are becoming more integrated with other business systems using Internet technologies such as Ethernet and TCP/IP. However, TCP/IP and web technologies which are predominantly used by IT systems have become increasingly vulnerable to cyberattacks that are experienced by IT systems such as malwares and other attacks. It is important to conduct vulnerability assessment of SCADA systems with a view to thwarting attacks that can exploit such vulnerabilities. Where the vulnerabilities have been exploited, forensic analysis is required so as to know what really happened. This paper reviews SCADA systems configuration, vulnerabilities, and attacks scenarios, then presents a prototype SCADA system and forensic tool that can be used on SCADA. The tool reads into the PLC memory and Wireshark has been used to capture network communication between the SCADA system and the PLC.

CONTENTS

Abstract	i
LIST OF ABBREVIATIONS.....	iii
DEFINITION OF IMPORTANT TERMS	iii
LIST OF FIGURES	iii
LIST OF TABLES.....	iv
CHAPTER 1: INTRODUCTION	1
1.1.1 Background to the study	1
1.1.2 Problem statement.....	1
1.2. OBJECTIVES	2
1.2.1 Main objective	2
1.2.2 Specific objectives	2
1.3.0 Research questions.....	2
1.4 Justification of the problem.....	2
1.5 Scope of the study	3
1.6 Significance of the study.....	3
1.7 Organisation of the Study	3
CHAPTER 2: LITERATURE REVIEW	4
2.1.0 Introduction to Operational Technology (OT) systems	4
2.1.1 Supervisory Control and Data acquisition main components	6
2.1.2 SCADA Protocols.....	8
2.1.3 SCADA Network overview	9
2.1.4 Vulnerabilities in SCADA Systems and threats.....	10
2.1.5 Attacks on a SCADA system.....	11
2.2.0 Related work	12
2.2.1 Conceptual Architecture	14
2.2.2 SCADA forensics.....	16
2.3 Analysis of MODBUS TCP/IP	18
CHAPTER 3: RESEARCH METHODOLOGY	20
3.1 Introduction.....	20
3.2 Research design	20
3.3 Tools used in data collections	22
3.4 Sources of data.....	22
3.5 Data analysis methods.....	22
CHAPTER 4: TESTBED SETUP AND DATACOLLECTION	23
CHAPTER 5: EVALUATION	30

CHAPTER 6: DISCUSSION	31
CHAPTER 7: CONCLUSION AND FUTURE WORK.....	31
REFERENCES.....	32

LIST OF ABBREVIATIONS

SCADA system:	Supervisory control and data acquisition system
RTU:	Remote terminal units
MSU:	Master Station Unit
IDS:	Intrusion detection system
HMI:	Human Machine interface
DCS	Distributed control system
IED:	Intelligent electronic device
PLC:	Programmable Logic Unit
OT	Operational Technology
IT	Information Technology
ICS	Industrial Control systems

DEFINITION OF IMPORTANT TERMS

- **Critical infrastructure:** - are those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon where by the loss or compromise would lead to severe economic or social consequences or to loss of life
- **Modbus:-** Modbus is a serial communication protocol developed by Modicon
- **SCADA:** it’s a software application that is used in the process automation
- **OT:-** this is a combination of both hardware and software that is used to automate industrial operational process

LIST OF FIGURES

Figure 1 Simple SCADA display (Rockwell foundation, 2016).....	4
Figure 2 Basic topology of SCADA network	7
Figure 3DPN3 Master/ Slave architecture (Guillemp A. et al 2016).....	9
Figure 4: Modbus Client/Server communication model.....	9
Figure 5: SCADA System network arrangement block diagram.....	10
Figure 6: Modbus Attack tree for a SCADA system	12

Figure7: Honeywell oil depot SCADA system.....	14
Figure 8: Architectural framework	18
Figure 10: Experimental SetUP for the tests.....	24
Figure 11: Ladder Logic program code in Ecostruxure control expert Software	26
Figure 12: Ladder logic program code in Ecostruxure control Expert Software	26
Figure 13: SCADA Implementation of the Prototype.....	27
Figure 14: Test bed circuit fabrication.....	27
Figure 15: CAPMod tool to read into PLC Registers	28
Figure 16: Analysed data from the engineering workstation	29
Figure 17: Captured packet . Master to PLC	30
Figure 18: PLC to Master packet analysis	30
Figure 19; query response and acknowledgement	31

LIST OF TABLES

Table 1: Modbus functions.....	19
---------------------------------------	-----------

CHAPTER 1: INTRODUCTION

1.1.1 Background to the study

Most modern Energy utilities infrastructure such as Electrical, and the Oil and gas rely heavily on computerised systems, networked control systems, and embedded devices to provide safe real time and reliable operations. In these systems both data acquisition and control are very critical.

SCADA systems defined as the Supervisory Control and Data acquisition forms part of operational Control (OT), which are used in manufacturing processes, chemical plant and refinery operations and even for building automation. In a typical SCADA system, sensors acquire data pertaining to process behaviour, process it as per the control algorithms implemented in the SCADA systems [1].

SCADA systems are used to automate processes, such as Electrical power generation, transmission and distribution, gas and oil depots and pipelines, water and waste management. Their main design requirement is efficiency and safety, which essentially requires real-time response to any change in the monitored processes. Due to this interconnection and automation the systems are now prone to cyber-attacks which were not considered during the initial design of the plant. Early SCADA systems were deployed in isolated 'air-gap' networks, which were not interconnected to the corporate networks. Thus, they were protected from remote attacks by virtue of not being accessible over the network.

SCADA systems allow the monitoring and control of remote operations and processes using some communication protocols such as Modbus, Profibus and TCP/IP. These systems are required to operate in harsh industrial set up

1.1.2 Problem statement

Current digital forensic tools are used in IT forensics to identify, acquire, store, analyse and present artefacts from computers running either Windows or Linux. This makes them incompatible with embedded devices found on OT systems such as Programmable Logic Controls or RTU, that have their own customised operating system

The interconnection of the SCADA system to the internet led to increased attacks on these systems, for safety critical installations such as the SCADA systems these attacks can lead to dire consequences such as loss of life, property and loss of critical data.

Due to safety, costs and time requirements of this critical installations, even after an incident occurs, live forensic is required and its vital that it takes as soon as possible after the incident to avoid loss of critical information , PLCs have limited memory and short data retention which prevents the use of IT forensic tools

1.2. OBJECTIVES

1.2.1 Main objective

The main objective of this research project is to enhance Live SCADA forensics by acquiring PLC memory.

1.2.2 Specific objectives

1. To investigate constraints in a SCADA security system
2. Research on current cyber security threats experienced in operational technologies in the energy sector
3. To create a prototype SCADA system
4. Design a prototype PLC memory capture tool
5. Carry out forensic capture of digital artefacts on a SCADA system
6. Evaluate the performance of the forensic tool on the prototype SCADA system

1.3.0 Research questions

The research will try and answer the following questions,

1. What are the vulnerabilities and threats to a SCADA system?
2. What are the main security challenges in a SCADA system?
3. How can we acquire memory in a Live SCADA system?
4. What are the effects of a live memory acquisition tool to the overall performance of a SCADA system?

1.4 Justification of the problem

If a SCADA system is attacked the environmental effects, safety and economic ramifications from the results can be detrimental. SCADA system has a requirement of availability where it's required to run seven days a week 24 hours a day. SCADA systems logs are designed based on any disturbance that may be generated by the system and not an indicator of a security breach.

1.5 Scope of the study

The study will entail design and development of a Live memory acquisition tool in a SCADA system to aid in digital forensics of the Modbus protocol

1.6 Significance of the study

The study is expected to provide a tool which can be used to acquire the live memory of a SCADA system and thus enhance the SCADA forensics.

The study also aims to reduce downtimes and consequences that may be caused by bringing a SCADA system offline in oil and gas depots and pipeline facilities and the subsequent environmental effects it may cause.

1.7 Organisation of the Study

This research study is organised as follows:

1. INTRODUCTION

The introduction chapter defines the problem and the objectives of the study.

2. LITERATURE REVIEW

This chapter discusses the problem in deeper context, reviewing the relevant literature and also looking at previous solutions to the problem

3. RESEARCH METHODOLOGY

This chapter concentrates on the methods used to carry out the research the type of research carried out and justification for the type of research design selected, also looks at data analysis methods and their justification.

4. CONTROL TRAFFIC VIA MODBUS

This chapter describe systems communication via Modbus , and also a live PLC memory capture forensic tool design

5. TEST BED SETUP AND DATA COLLECTION

This chapter will outline the development of a prototype SCADA tool, experiments that will analyse the forensic tool, investigate the system and document the outcomes

6. EVALUATION AND DATA ANALYSIS

This chapter will include analysis of the collected artefacts, implications, consequences and limitations of the investigation.

7. DISCUSSION

This chapter summarises the achievements of the study

8. CONCLUSION AND FUTURE WORK

9. REFERENCES

CHAPTER 2: LITERATURE REVIEW

2.1.0 Introduction to Operational Technology (OT) systems

OT is a technology that is used in the industrial control, monitoring and management of industrial operations with a focus on the physical devices and processes they use and its based on both software and hardware. OT is about control and safety systems and industrial process assets, OT includes both SCADA and Distributed Control Systems (DCS)

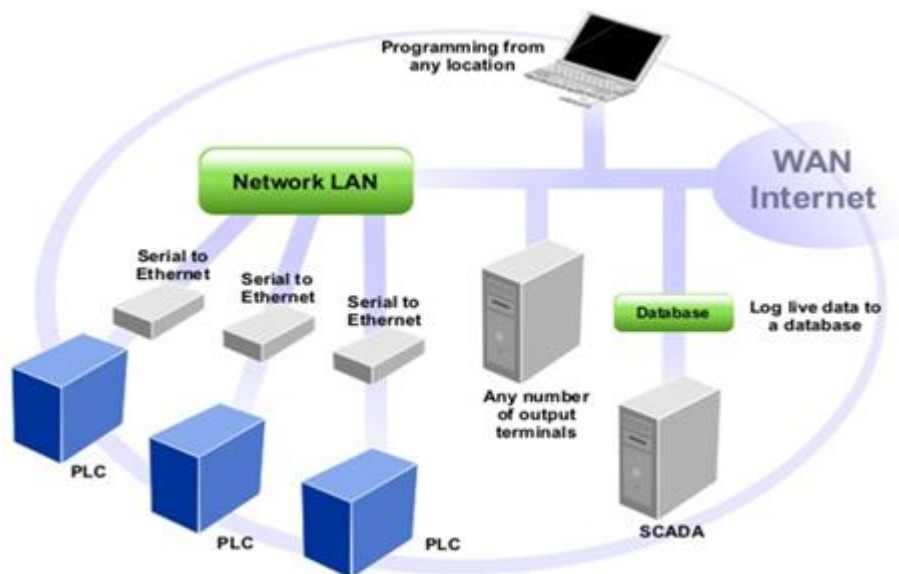


Figure 1 Simple SCADA display (Rockwell foundation, 2016)

According to [3] SCADA systems refers to an application that that collects data from field or remotes instruments and once it acquires this data it processes it based on a set algorithm and displays it graphically. It also can be used a s a master by an operator to control key processes that are required in operations of a facility [3].

The SCADA station refers to servers which interacts with devices on the field through the RTU or PLCs. The PLCs are connected to the data servers either directly or via a network. The SCADA system utilizes a networks, that consists of communication protocols that is used to convey a particular message between the master station and devices. The PLCs/RTUs convert the sensor signals to digital data and sends it to the master. According to the master feedback received by the PLC it applies the control algorithm or philosophy and applies the electrical signal to relays. Most of the monitoring and control operations are performed by PLCs as shown in the figure 1 above

The SCADA servers are used for data gathering and handling. The systems application software program is responsible for provision of trending, diagnostics, and information management such as scheduled maintenance processes, detailed schematics for a particular instruments or equipment. It also presents the operator with a schematic representation of the plant being controlled.

SCADA systems may cover large geographical areas, where they typically WAN. The communication channel may be satellite, radio, power line based or a combination. These systems are designed to provide real time instrument data 24 hours a day for all days in a week

A SCADA system can perform below functions that are carried out by the Sensors, PLCs and the communication network, where the communication is from Master to a slave and a response from the slave to the master. In addition to the hardware, the software components of the SCADA architecture are important. These functions are, Data Acquisitions, processing, Communication, data presentation, Monitoring and Control

According to the status of the system, the operator can issue commands to other system components as per the set schedule of operation, this is done via the communication network.

Data Acquisitions:

OT systems are Real time systems and consists of thousands of components and sensors and it's important to know the status of a particular components and sensors at any one time, this is done by checking and acquiring the instruments status. For example, some instruments measure the petroleum products flow-rate from the storage tanks to a transporting truck and some sensors measure the pressure of the pipeline as the petroleum product is release from the tanks.

Data Communication:

The SCADA system can use wired or wireless network to communicate between Master and the slave devices. The SCADA system uses communication protocols so as to communicate with this remote instrument such as Profibus, Modbus, DNP3 and fieldbus actuators and other field instruments are not able to communicate with the network protocols so PLCs communicates with them via a wired network and it communicates with the Master SCADA system via this communication network

Information/Data presentation:

The SCADA system uses the HMI to display the data gathered from the field instruments, it also displays the alarms raised by field instruments or when there is a communication breakdown. From the display the control schematics can also be accessed

Human machine interface(HMI):

The SCADA system uses a HMI which displays the monitored information, from the HMI the operator can monitor and control the entire plant, the HMI has also the alarm monitoring and action system which gets activated as per the set application and predefined values the HMI can have the geographical representation of the entire system. For example, it provides the graphical picture of the loading pump connected to the storage tanks several parameters can be viewed from here such as product levels, tank pressures and flow rates

2.1.1 Supervisory Control and Data acquisition main components

SCADA systems consists of both hardware and software components, one or more control centres depending on the size of the plant and geographical distribution. It also consists of field devices such as PLCs that links up field devices such as actuators, meters, tank gauging systems, pressure transmitters, transmission line monitors. PLCs receives data from the field instruments and converts it to digital data which it sends to the master terminal unit. PLCs takes decision based on the user installed application programs. [4] the MTU issues commands to the PLCs and gathers data from it

Communication on a SCADA system network is key to a good performance. Messages are exchanged between master devices Programmable Logic Controllers (PLCs), which control operation of other devices and slave devices such as actuators, pressure transmitters, thermoprobes and other measuring sensors ,which send messages to master devices and perform actions at their command, and also between field devices using a peer-to-Peer communication model [5] PLCs are connected to the control room by means of some links such as fiber cable or ethernet cables. Commands are sent from the PLCs back via the communication channels to the field instruments such as actuators. Some systems also have local control loops, which operate autonomously. The data collected from field instruments is stored in a SCADA server, from where it can also be processed and displayed on the HMI, which the operator uses to get a complete overview of the system.

The field instruments are connected to a respective PLC, the Controls this actuators as per the set control philosophy and saved application, the plcs are connected to the control centre via a network , the control centre has the MTU , historians and the HMI

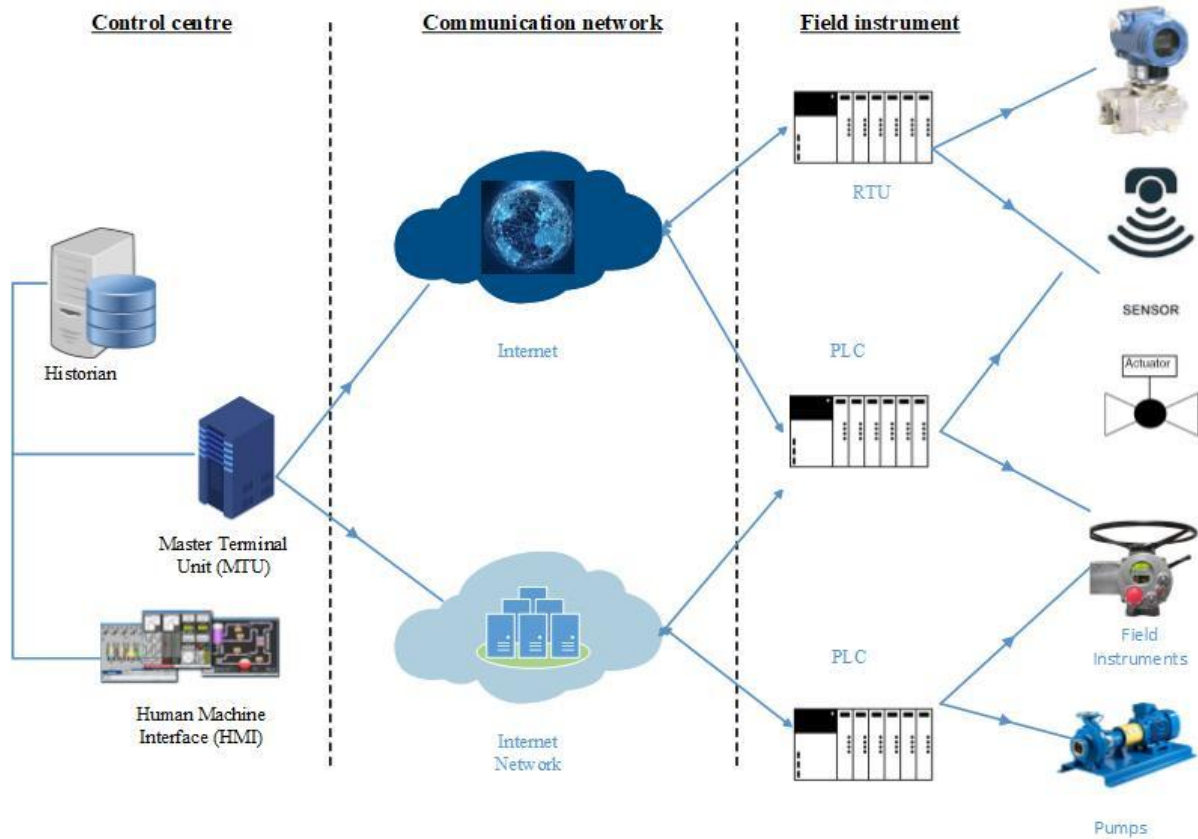


Figure 2 Basic topology of SCADA network

The control systems have unique characteristics such as being real time, safety critical and can survive on harsh industrial setup. Any interference or disruption of the services due to a cyber-attack poses a significant risk to the environment, properties and human life [6], SCADA systems can monitor and control hundreds and thousands of I/O points, including HMIs, PLCs and Historians.

A PLC is a microcomputer that monitors sensors and takes decisions based upon a user created application to control valves, pumps and other actuators. A control centre includes an MTU, which issues commands to and gathers data from RTUs, it also stores and processes data to

display information to process operators to support decision making. The operator monitor and control the system from a control centre via Human–Machine Interface (HMI) displays [4]

According to, [7] , OT systems relied on the custom embedded devices and clear text communication protocols that were not discrete and it relied on lack of external connectivity that is an air gap for security. Air-gapped systems are progressively uncommon approach as there is increasingly connectivity between SCADA and IT infrastructure. And have expanded SCADA to external threats.

Due to their geographically dispersed characteristics, the SCADA systems become more and more susceptible to cyber-physical attacks, not only on the physical infrastructures but also on the communication network and the control centre [8]

2.1.2 SCADA Protocols

For the SCADA system to communicate with the slave devices or field devices it depends on a communication protocol. Communication on a SCADA network is critical as this is what enables field instruments to communicate with the Master. Messages are shared , between master devices like MTU and the PLCs which in turns controls its slave devices such as sensors and actuators, using a peer-to-peer communication model [9] These protocols are; Ethernet/IP, ControlNet, Modbus RTU , Modbus TP/IP, DeviceNet, Fieldbus, MODBUS TCP/IP and DNP3 [10]. This use of standard communication protocols has enabled integration of a SCADA system with a corporate ICT systems and connection to the internet

i. PROFIBUS (Process Field Bus)

This a field bus communication that was developed by the German department of education and research and its mostly used in Siemens PLCs. PROFIBUS network make use of three separate layers of the OSI Network model and communicates via RS485, The PROFIBUS uses the bus topology whereby a central line is wired throughout the system

ii. Distributed Network Protocol Version 3(DPN3)

it is a master/slave control system protocol that is usually configured with one master and multiple slave devices [11]

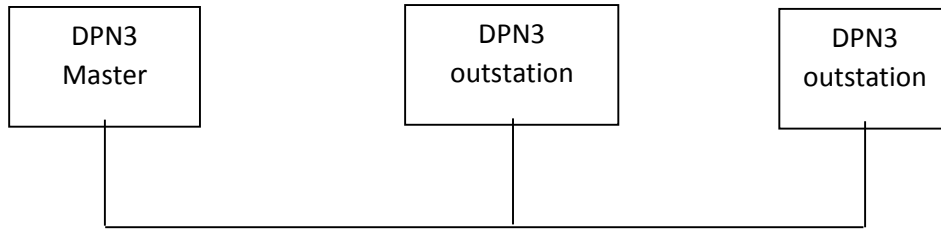


Figure 3 DPN3 Master/ Slave architecture (Guillemp A. et al 2016)

iii. PROFINET

Is a protocol based on PROFIBUS and adopts Ethernet as its physical interfaced for connections rather than RS485, it has a repetition-based system based on passing on tokens and offers a complete TCP/IP functionality for data transmission, which allows for wireless applications and high-speed transfers (incibe 2017)

iv. Modbus

This Modbus is an open source serial communication protocol developed by Modicon. It is a universal open and easy to use protocol, which is based on master-slave communication between a MTU and a PLC in a SCADA system. The Modbus protocol provides four message types used in client/server communication, which are; request, confirmation, indication and response.

All PLC and field instruments can use MODBUS protocol [12].

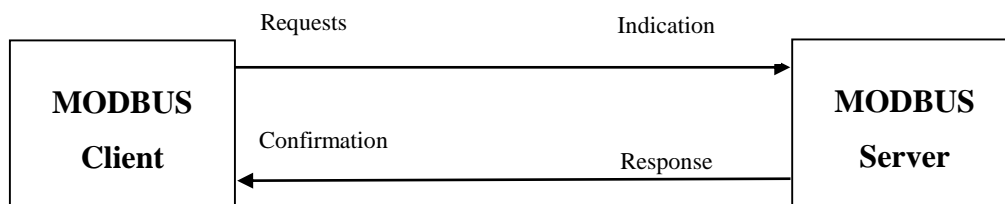


Figure 4: Modbus Client/Server communication model

2.1.3 SCADA Network overview

In the SCADA networks, data acquisition systems, data transmission systems and HMI applications are integrated for providing the centralized processing of outputs and inputs for process control and monitoring.

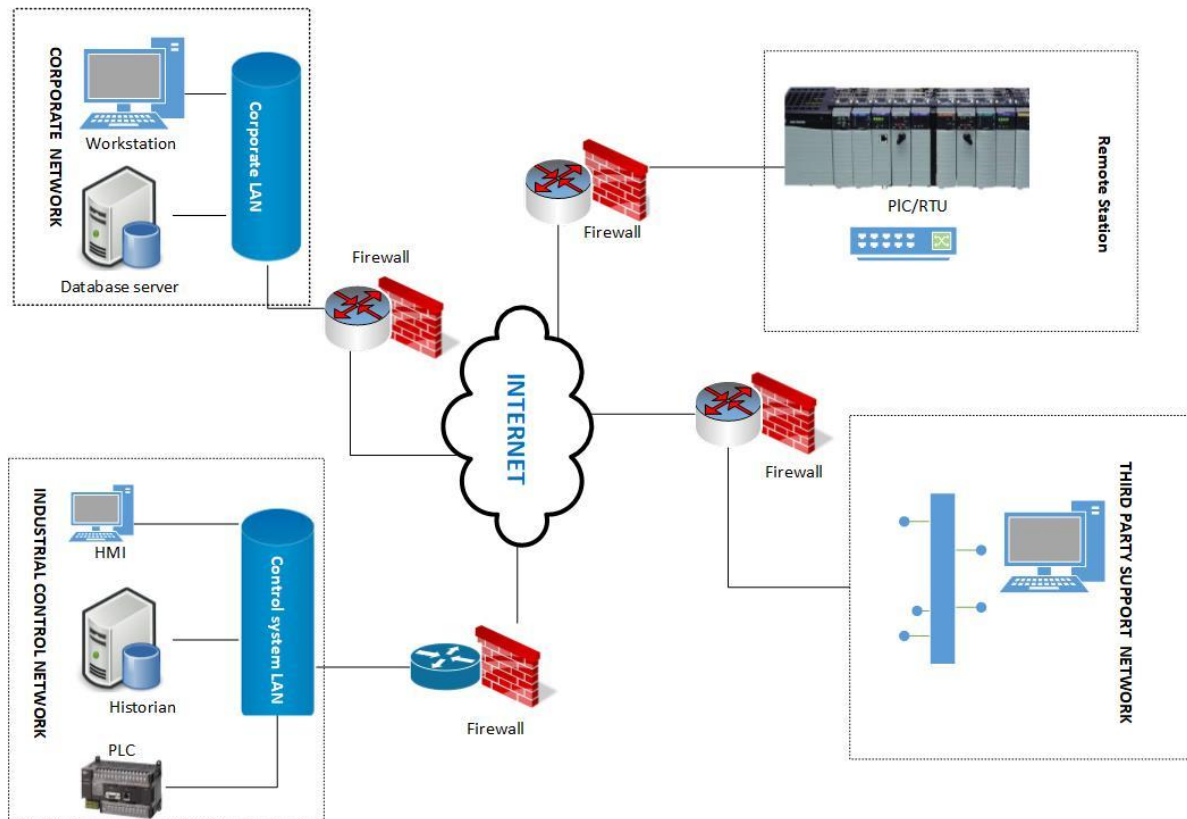


Figure 5: SCADA System network arrangement block diagram

SCADA networks collect field instruments information, transferring it to a central server, and displaying the information graphically to the operator, hence allowing the operator to have real-time monitoring and control of an entire plant from a remote control room.

A SCADA network has two main parts, the main control centre and the plant being controlled. The control center is the hub and it contains the engineering workstations, HMIs, and Plant data historians. The SCADA server functions as the sole interface between the control center and the remote sites. The SCADA architecture consists of both software and hardware. The hardware includes; MTU, which is placed at a control centre and sub-MTUS and a remote field sites consisting of PLCs which monitor and control sensors, actuators, communication media and equipment [14]

Communication on a SCADA network is key. Messages are exchanged between the MTU and field devices like PLCs and slave devices such as sensors, actuators, tank gauging and meters, which send messages to master devices and perform actions at their command, [10]

2.1.4 Vulnerabilities in SCADA Systems and threats

Modern SCADA systems have moved from the isolated case with airgap, to more

interconnections with open standards for cost efficiency and easy integration into corporate IT systems. Communication is now common over Ethernet TCP-IP including more standardized control protocols and applications, making the SCADA systems more susceptible to external attacks and other IT based vulnerabilities [3]

SCADA control systems major attack vectors are through backdoors and holes in the network perimeter which may arise from configuration of “Air Gaps” or links to other IT infrastructure, PLCS Operating system known as a firmware lacks critical security features such as certificates cryptography and intrusion detection such as those found in normal IT operating systems, [15]. If the OS is compromised by an attacker, all devices controlled by PLCs, can be completely taken over; leaving them vulnerable to varieties of malicious attacks.

Another line of vulnerabilities is the HMI, which may be an application software or a user interface terminal this include the DTU which is used by the operator to control and monitor the system and the HTU which logs the devices, Like any other IT equipment’s they are vulnerable to any threats within the network and inherit all the vulnerabilities of the OS that are built on.

Modern HMIs have become generic or of-shelf s products that are built on and share common computer architectures and operating systems like Windows OS [16]. Attacking the HMI, together with its database, can lead to severe consequences on software such as manipulating application program , change alarm set points or database records as well as on hardware. Attacks on the SCADA systems typically take advantages of unsecured networks or infected devices to create software manipulation or to steal confidential information [17]

2.1.5 Attacks on a SCADA system

Attacks on a SCADA control system can be lumped into three

General categories:

- I. Attacks through the configuration workstation or the communication network,
Here attacks can occur on the network layer, they can also occur on the transport layer such as a SYN flood attack overcrowding resources. Most protocols used in SCADA have little security considerations on the application layer.
- II. Attacks through the Ethernet network,

Occurs when unauthorised remote access is gained into the device, and equipment set points are changed or reconfigured leading to a SCADA system crash. This can also take place via an malware installed in the engineering workstation

III. Non-Ethernet attacks.

These attacks are mostly caused by internal disgruntled employees who have direct access to the system. Social engineering also falls in this category where the SCADA system administrator leaves all the access controls open or forgets to apply the correct authentication system and allows an authorised access to the system. An employee may also plug in an infected storage media into the engineering workstation therefore introducing a malware.

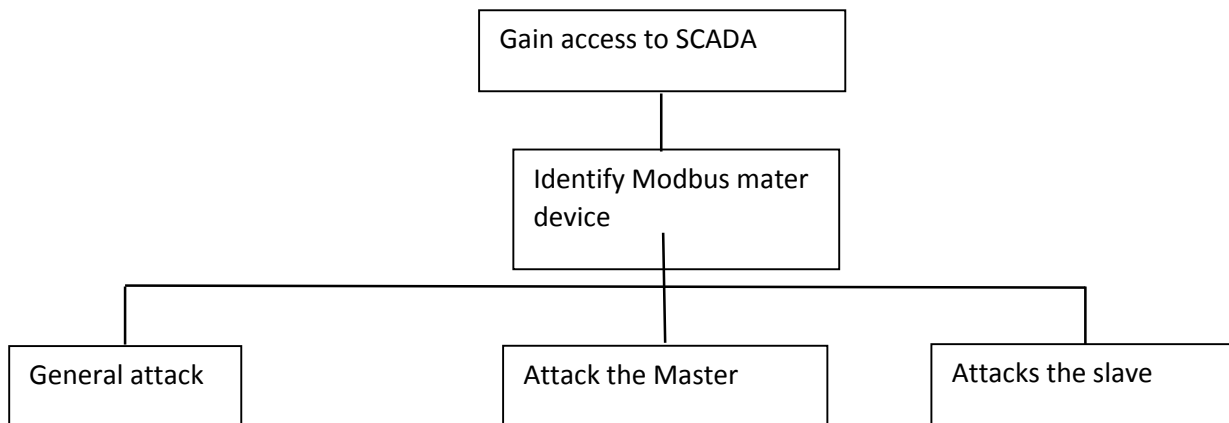


Figure 6: Modbus Attack tree for a SCADA system

2.2.0 Related work

In this section various SCADA forensics research and implementations are evaluated and their limitations outlined

[18]demonstrated attacks on a Siemens PLC TIA portal, PLCs are the essential components of the OT systems. The security flaws of these devices expose the OT system to security flaws and attacks. Interruptions to the OT systems may lead to serious environmental hazards, loss of both property and life. The authors developed a prototype testbed with a siemens plc and a compromised machine using tools such as like Windbg and Scapy, it was found out that an operator can go online to a PLC, steal a session , introduce a phantom PLC, and even introduce a DOS attack on the system.. A virus running on the PLC will cause manipulation on the output or it does change the output signals to field devices connected to that PLC.

SCADA risk assessment methods were reviewed by [19], this was due to the increased cyber threats on SCADA systems.

[3], proposed a structured SCADA forensics process model to be used to carry out a forensic investigation. Many SCADA system do run on windows XP as the systems were created with this operating system in mind, which does lack patches and has auto run features enabled making it an easy target. His tool was based on the siemens Simatic S7 PLC, his proposed architecture enabled the recording of any modification on the PLC program which could be used to detect any attack and modifications. This was lacking as it could not be used to capture program changes on other PLC models and also could not capture the changes if the whole architecture had been compromised as the tool had to be installed in the engineering work station. It also could not record logs and modifications resulting from the HMI.

[21] demonstrated and reviewed a SCADA digital forensic process which has the following steps

- a) Examination. To Identify the likely sources of digital evidence.
- b) Identification of the systems type to be investigated
- c) Collection of evidence from the SCADA systems and its devices
- d) Documentation of evidence to ensure collect and accurate chain of custody.

This model lacked a detailed method of capturing all the artefacts from a SCADA system

[3] proposed a SCADA digital forensic process, this model combined the incidence response and cyber forensics investigative model. The model was based on seven digital forensic investigation steps which are; Identification and Preparation, Identifying evidence sources, Preservation of evidence ,examination, analysis, reporting and Presentation and final reviewing of results

The major huddle was to capture and record digital artefacts from embedded devices like PLCs.

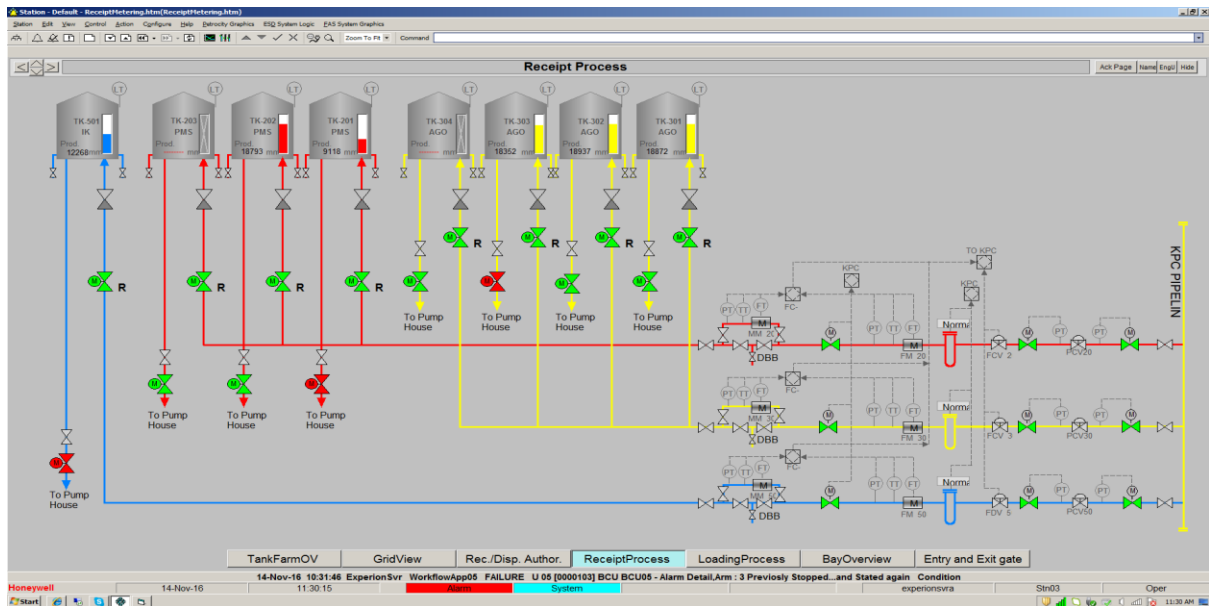


Figure7: Honeywell oil depot SCADA system

Cyber security vulnerabilities in the Kenyan oil terminals OT Systems

- i. Lack of system patches
- ii. Access of the system by third parties via the internet is done securing the system using Firewalls
- iii. Intrusion detection systems are not implemented on the SCADA systems connected via the network
- iv. No regular patches carried out in the systems
- v. Data recovery sites are not implemented for the OT systems

2.2.1 Conceptual Architecture

The Architecture is categorized into three elements

1. Programmable logic control (PLC)
2. Field instruments
3. Engineering work stations and HMI
4. Power supply unit (PSU)
5. Pipeline and Tank system
6. Communication network
7. Forensic tools

Programmable Logic Control(PLC)

The PLC is the main controller and it collects the data from field instruments and sensors and makes a decision based on the user stored program. The data from the field may be Product temperature captured by the resistor temperature device, pipeline pressure which is captured by the pressure transmitters and pressure switches, Flow rate being capture by the flow meter, product density being captured by the densitometers, based on this information the PLC issues control commands to pumps and actuator operated valves

Field Instruments

The field instruments collect data from the field such as temperature, product pressure, product level in the tanks, product density, water presence and levels, liquid leakages through gas detectors and liquid detectors, and pump temperatures. This data is then collected by the PLC and is interpreted to control or manipulate the motorized valves being controlled by the actuator sand pumps which do pump product from the selected tank into the waiting trucks

Engineering work stations and HMI

the Engineering work station contains the PLC programming application which is used to create a PLC code and upload it to the PLC and download programs from the PLC. It is also used to program and design the SCADA software and at the same time monitor alarms from the SCADA system. For actions like repairs and failures. The Operators monitor the system from a control PLC via the HMI

Communication network

This is used to transmit information between the PLC field devices and the servers using peer to peer communication model

Power supply unit (PSU)

The Power supply unit provides the power source to power the PLC, which requires clean power. This is mostly obtained from the uninterruptible power supply, Motor s which are powered direct from the power line with non-clean power and also to power the field instruments using the clean power.

The Pipeline system and Tanks

the tanks are used to store the petroleum products which are to be loaded to trucks. The loading gantry is connected via pipes which are controlled by motorized valves placed at strategic points on the line depending on the HAZOP and HAZIP studies done on the depots

2.2.2 SCADA forensics

SCADA systems reliability is dependent on both security and safety. Recent attacks on SCADA systems such as STUXNET, Flame, BlackEnergy and crash override demands [22], demands forensic investigations to determine the cause of intrusion and also to improve cyber security. The systems needs to be protected from both internal and external threats. A forensic investigation on the system can help in analyzing underlying SCADA IT systems vulnerabilities.

A SCADA system can be categorized in into three different forensic layers as illustrated in figure 8 based on connectivity of various components. Due to the criticality of systems, [9] in utilities forensic investigations need to be carried out on a live system. This should be carried out early on after an incident to capture traces left behind by an attacker. However, the live forensic have an effect of altering the live acquisitions by the system.

There are several challenges experienced by a forensic investigator on a SCADA system, this includes the deterministic network traffic, this is due to the fact that the system component communication is in a predefined way as compared IT systems whose communication is non deterministic. The SCADA systems operating system is customized and hence difficulty to patch for new updates, PLCs memory is low hence provide limited capabilities for data acquisitions in forensics hence a need for light weight forensic tools. the logging systems in SCADA systems is in adequate since they are geared towards discovery and diagnosing process disturbances [23]

Control center equipment's are based on the traditional IT operating systems such as windows and Linux. data can be retrieved using forensic tools such as volatility, recall, Encase and redline and Wireshark. According to [24] opensource tools provide network analysis for SCADA control center systems such as engineering workstation SCADA Main HMI system and data historian this was based on both Modbus and DNP3 protocols. this involved a methodology relying on robust IDS System. [24] carried out a study of the SRTP protocol used by the GE Fanuc series of PLCS. He carried out reverse engineering on the protocol to be able to change logic of the program and read and write into the PLC memory registers.

[20] developed a model for SCADA systems to gather and analyze data from SCADA systems which involved gathering, preserving and documenting the digital evidence based on Siemens PLC which showed any changes in memory addresses. [3], suggested using semi supervised machine learning to detect anomalous behavior of the PLCs so as to accurately determine abnormal behavior.

Forensic Artefacts from a SCADA systems

An artefact is a piece of data that may be relevant to the investigation. This artefact can be obtained from various levels of a SCADA system as depicted on figure 8 Below, these artefacts may include

- a. PLC application program and settings
- b. Network traffic
- c. Engineering workstation memory and program
- d. Field devices such as process logs, date and time
- e. HMI Logs and settings

Modification of a PLC Memory can be recorded as a digital forensic artefact, which can be used to reconstruct a timeline of events. [25]. Encase scripts have been used to carry out network acquisition to test the effects of a forensic tool on a SCADA system. The result showed that the test on network acquisition have minimal effects on the normal operation of a SCADA system. Memory addresses in a PLC are rarely modified. If a change happens then this can be recorded as a change in the programming code or logic.

A capture of a PLC memory addresses would form a useful forensic artefact, that will assist to capture volatile data for digital forensic on a SCADA system.

Forensic tools

Forensic tool is used to capture the live PLC memory status, which will be evaluated. The Network packets will also be captured for analysis, the ports will be mapped using port mapping tools and the communication between individual SCADA systems will also be monitored and analysed

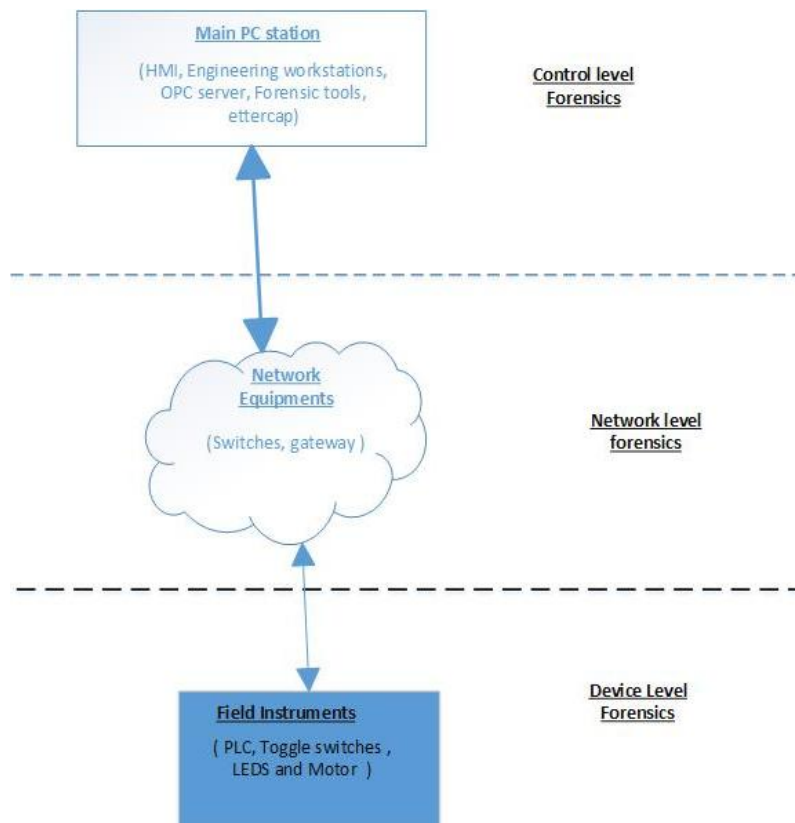


Figure 8: Architectural framework

2.3 Analysis of MODBUS TCP/IP

Modbus devices communicates using a master/slave model in which only one device initiates transactions. The slaves respond to the master by giving the requested data or by initiating the action requested in the query. A slave can be any peripheral device or the Input and output devices such as valve, network drive, pressure transmitter or field instrument which processes information and sends its response to the

In a SCADA system the HMI is the master while the field devces such as input devices and transducers act as the slave. The MODBUS Application header (MBAP) has four field covering seven bytes. The header is added to the beginning of the message. the MBAP has the fields below [26]

- a. Transactional identifier- has 2 bytes
- b. Protocol identifier – has 2 bytes its used for intra-system multiplexing.
- c. Length – has 2 bytes
- d. Unit identifier 1 byte

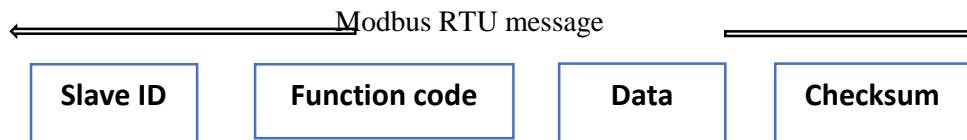


Figure 4.1 Modbus RTU Message (www.modbus.org)

MODBUS messaging services are used for real time messages exchange between the SCADA and the PLC.

Table 1: Modbus functions

Primary tables	Reference	Description
Discrete Input	1XXXX	Read Discrete Inputs.
Coils	0XXXX	Read/Write Discrete Outputs or Coils
Input Registers	3XXX	Read Input Registers.
Holding Registers	4XXX	Read/Write Output or Holding Registers..

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter concentrates on the methods used to carry out the research the type of research carried out and justification for the type of research design selected. It also looks on the study population, sources and methods of data collection.

In this chapter we also look at the data analysis methods and their justification, limitations of the methods and assumptions made

3.2 Research design

Research design is the plan according to which the research's participants have been identified and to collect information from them. This will be an experimental study where the evaluation seeks to determine whether the created prototype forensic tool had the intended causal effect on the program participants. In this research we study the effects of the forensic tools on the performance of the SCADA system.

The results of the experimental research are not known in advance and the study results in the collection of data. This is done by manipulating the conditions of the experiment and checking the effects of the manipulation.

The experiment will be based on a prototype SCADA system. The system will be that of a petroleum depot, the depot operations can be summarised into

- a) Pipeline receipt operation: this starts from the receiving tank manual valve being opened manually and the take receipt authorised in the system. The delivery pipeline is aligned to receive the product into the main storage tanks the product information in the mainline must be known and its conditions will be collected and recorded. This includes, product temperature density, pressure and flow rate. This will be collected by the PLC and the flow computer. Based on this data, the PLC will control the pressure, emergency shutdown (ESD) and the Flow valves. If the density is out of range for the respective product, the ESD valve shall be triggered and the receipt pipeline shut off. If the product density and pressure is okay the opening of the control valves and the flow, and pressure valves shall be operated based on the control algorithm for the receipt line. When all is okayed the product shall flow into the tank.

- b) Tank line up and dispatch operation. The tank has installed instruments such as the tank gauging system, the tank temperature probes, pressure transmitters to record and transmit the tank pressure to the PLC, tank discharge motorized valves and transfer pumps which transfer the products to the trucks waiting from the loading gantry. The pumps have pressure switches across them. This records any pressure differences on the pump and shuts off the pumps in case the tanks discharge valve is crossed. This prevents any damage to the pump and avoids running the pumps dry. For the dispatch operation to take place, the pump will require authorisation from the terminal manager, and based on the control algorithm and the conditions from the tanks instrument, the valves can open and shut
- c) Loading pump and loading operations
Based on the product to be loaded into the trucks, the pipeline conditions must be collected, this includes the product temperature which is recorded by the RTD, pipeline pressure transmitted to the PLC by the pressure transmitters, the loading is now start with the pumps activated to start by a command from the PLC based on the volumes to be loaded as fed into the system per compartment

The product receipt and discharge should not be done at the same time. This is to allow the product to settle in to the tank, allow its temperatures to lower. This also to ensure that product from the main line is not siphoned out without a proper stock management system, also product being received into the tanks should have a release order from the revenue authority.

No product should be dispatched from the tanks without the revenue authority order number, bank payment details from the terminal accountant to ensure only product paid for leaves the terminal. To ensure safe receipt of the products no tank should receive the product with its field instruments that are collecting the tank levels switch off. This is to avoid any spillage occurring into the environment and also to obtain tank levels at real time basis.

Attack scenarios to be employed in the experiment

1. If a malware is installed into the system, the malware may switch off alarms from being received from the system. This may make the plant operator and the control logic in the PLC to miss critical alarms from the field instruments like high level alarms, gas detectors recording spillages

2. Bypass of critical controls like the authorisation from the terminal manager, revenue authority and the accountant. If the PLC program is manipulated to bypass this critical controls, product might leave the depot without being account for. This cyber-attack may occur from an internal employee or an external attacker
3. Denial of service attack. This may occur when an attacker may intrude the system and initiate a DOS attack this may stop the depot operations like receipt, dispatch and also safety control and operations

3.3 Tools used in data collections

The tools below will be used in data collections

- i. Wireshark software
This will be used for the network packets capture
- ii. Ecostructure Control expert software to be used in the PLC programming and downloading of the program from the PLC
- iii. Developed tool: to capture live PLC memory status
- iv. Ethereal is an open source tool that will used to analyse and monitor communication between individual SCADA system components
- v. Autopsy to be used in carrying investigation on the Engineers workstation and the SCADA server.
- vi. FDK tool for mapping of the Engineers workstation

3.4 Sources of data

The network traffic data capture using wire shark and, PLC program capture using MS logic to monitor any modification to the PLC program and any malicious code which has been injected to the PLC, also data was generated using the developed memory capture tool, any malware originating from the engineer's work station shall be captured and analysed using the autopsy tool. For the secondary data this will be obtained from published material on SCADA security.

3.5 Data analysis methods

This will entail finding relationships between the captured artefacts and that received from the evidential data. This focus on how to organize data in a way that provides answers to research questions and ensures research objectives are met. This involved

1. Data cleaning
2. Data sorting
3. Tabulation of results
4. Analysis of digital data obtained

CHAPTER 4: TESTBED SETUP AND DATA COLLECTION

A test bed was set up to collect digital artifacts from a scada system. This was a prototype pipeline transporting petroleum product from one pump station to the next depot.

For this project Modicon M340 plc was used. It consists of a CPU, I/O modules, power supply module and a communication module on a rack. the set up in figure 4.3 below was used, it consists of a Modicon M340 PLC, Ecostruxure control program programming software, BMX DDI 1602 input modules connected to toggle switches and push buttons representing field instruments, BMXDDO1602 discrete output module connected to six LEDS and a Motor connected to the output port. The PLC and the physical computer are connected via an ethernet cable, the HMI and the engineering workstation running Ecostruxure control,

The PC station also known as the Engineering work station runs the Ecostructure control expert the Modicon PLC programming software and the Citec HMI software , the Engineering software can read and write into the PLC and also change the SCADA settings and parameters set.

The Master workstation has the following software's

- i. Windows 10 professional operating system
- ii. Ecostructure Control expert software
- iii. Citec Vijeo Scada Software
- iv. Ettercap
- v. Autopsy
- vi. Wireshark
- vii. Unity Differencial software
- viii. Developed Tool

Connecting the above mention parts leads to the prototype shown in figure 5.1 below

Modicon M340 PLC consists of several registers which can be programmed and can be accessed using a HMI software. the memory register information was obtained from Schneider reference manual (System Bits and Words Reference Manual), the (%) Percentage sign is attached before the register type to assign it

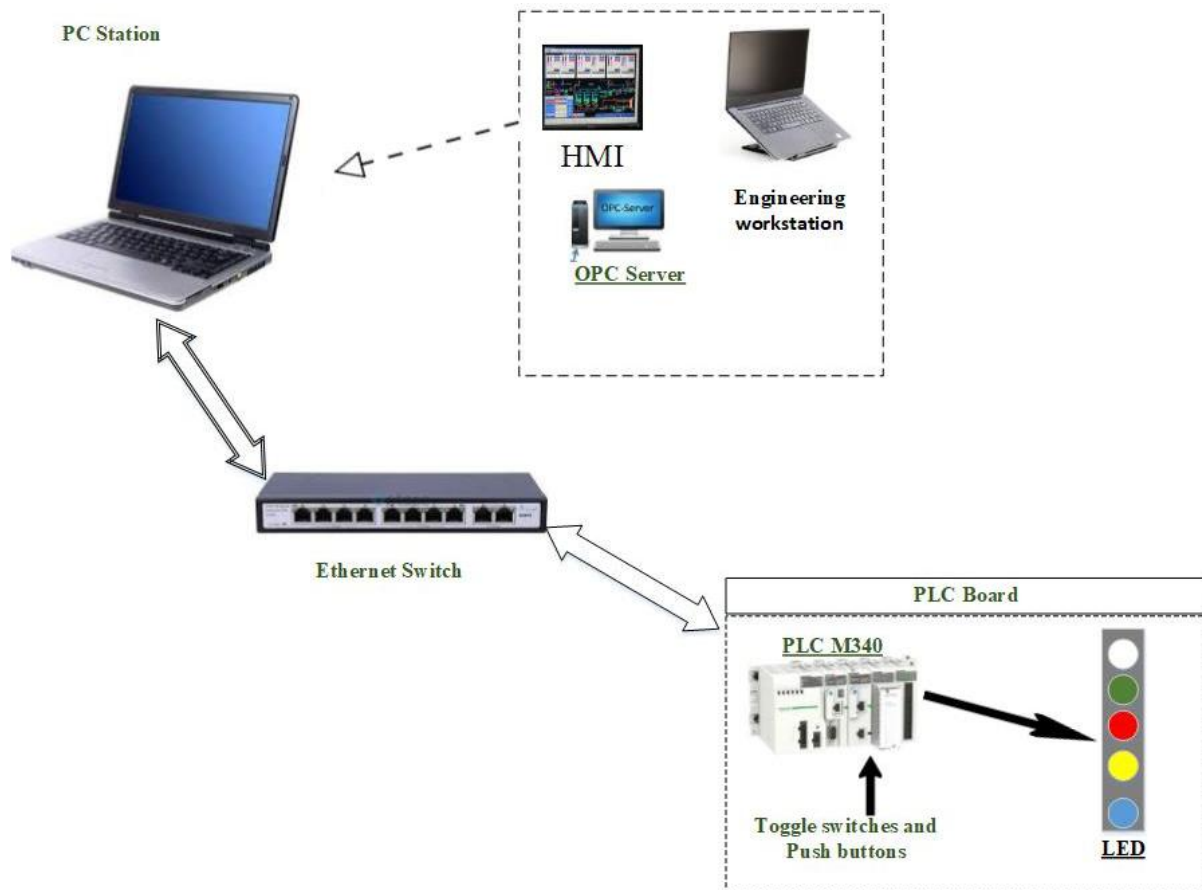


Figure 9: Experimental SetUP for the tests

Modicon M340 PLC can be accessed using a HMI Software.. The PLC has a Firmware installed, this is an embedded operating system (OS), alternatively called firmware, for this project the PLC runs on BMXP342020_SV320 Firmware

The PC runs the engineering workstation which has the Unity pro programming software installed and Wireshark and the test tool, wire shark captures all network traffic. the LED displays the output from the PLC while the toggle switches acts a digital input to the Modicon M340 PLC

The power required by the PLC and indicator switches is supplied by a 24v DV power supply

supplied by a 240 V Ac supply. The PLC was programmed to control a typical pipeline using ladder logic as per IEC 61131-3 using the Ecostruxure control expert, the petroleum product runs from one terminal to the next to be stored in a tank, the product is pumped by a booster pump, the pipeline is monitored with flow, density and temperature sensors to ensure the correct product at the correct safety levels are transferred. Alarms shown on the HMI are PLC communication failures, control power lost, and valve opening delay. A communication alarm is raised when connection is lost between PLC and the HMI. HMI acts as the Master and communicates with the PLC requesting for the information as per the commands issued

To program a PLC we can use several languages, this language are as follows;

- a. Ladder diagrams (LD)
- b. Sequential function charts (SFC)
- c. Structured texts (ST)
- d. Instruction list (IL)
- e. Function blocks diagram (FBD)

Wireshark was used to capture the communication between the PLC and the HMI, the results are as indicated in appendix 1, this was done prior to launch of attack and when the PLC is obtaining commands from the PLC. The HMI sent a command to the PLC initiating a valve open,

For this project ladder logic was adopted as depicted on figure 5.3 a and b below was used, this was created using ecostruxure control expert and downloaded to a PLC via Ethernet port

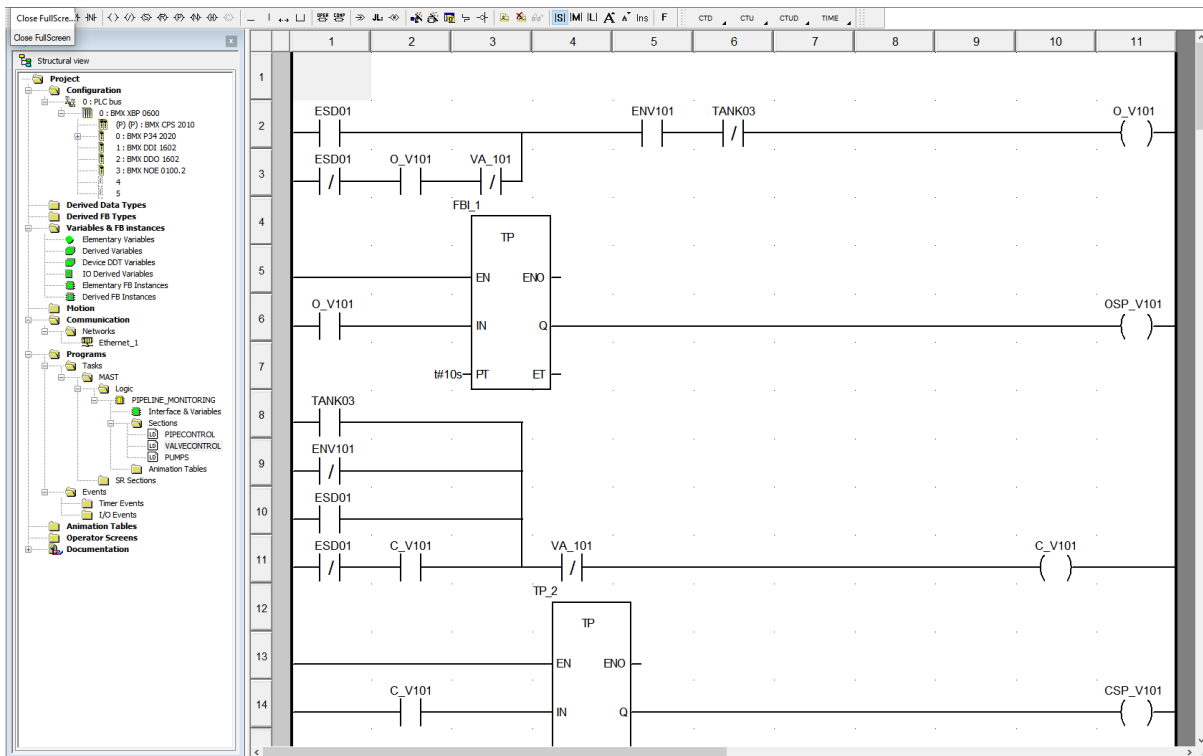


Figure 10: Ladder Logic program code in Ecostruxure control expert Software

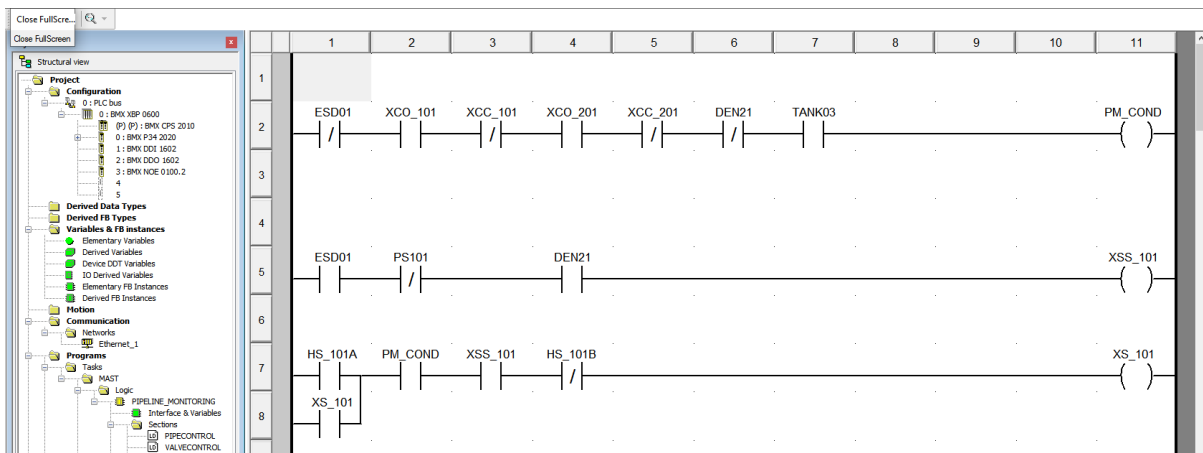


Figure 11: Ladder logic program code in Ecostruxure control Expert Software

A HMI project was written on Citec SCADA and ran on the master workstation to control the PLC. using the HMI and tool communication we captured communication and analyzed it forensically. Using the tools

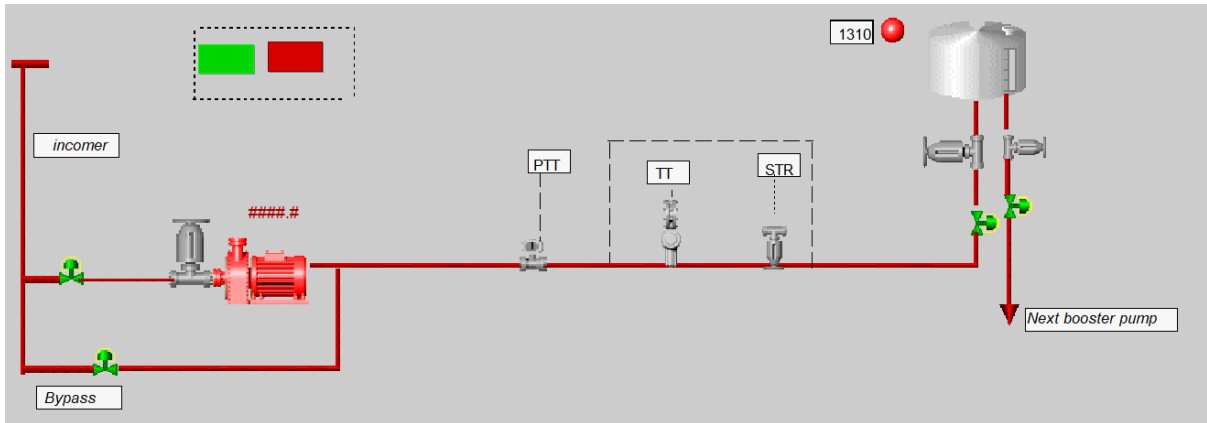


Figure 12: SCADA Implementation of the Prototype

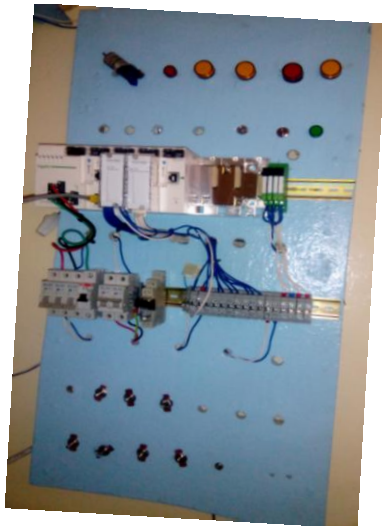


Figure 13: Test bed circuit fabrication

Unity diff software from Schneider electric was used to compare two application programs files, this will be used to compare. ZEF, STU, and XEF. programs and detect anything added, deleted and modified, if an authorised access has taken place and program parameters edited, this program will be able to tell the difference in the two projects, this data was captured and analyzed using Hex tool kit to read into the hex data. We started by sending commands to the PLC from the HMI like open valve close valve and read register values

Prototype tool to read and write into the PLC

We built a tool to read the current memory addresses of the PLC to extract some artifacts from the PLC using the Modbus TCP/IP. Modbus TCP/IP communicates via port 502. setting a PLC communication using the Easymodbus library, we can read into the plc and capture current

settings. To tool consist of 3 functional modules. Read, write and display current register setting. The application was created using c#. once installed the IP address of the PLC must be keyed in to access the PLC.

Application capability

The tool has a capability of reading the PLC on specific registers and record current register status. To test the tool the application above was written and SCADA system run, we sued the tool to read into the PLC and get current plc settings. in hexadecimals

the tool will require the target Slaves IP address and the port. Modbus TCP/IP uses port 502 . with this detail we can read into the Modbus TCP/IP configured PLC and obtain the configured registers

Modbus TCP/IP communicates via port 502. The tool is to reads the PLC memory and capture the memory status The created tool looks as per figure below

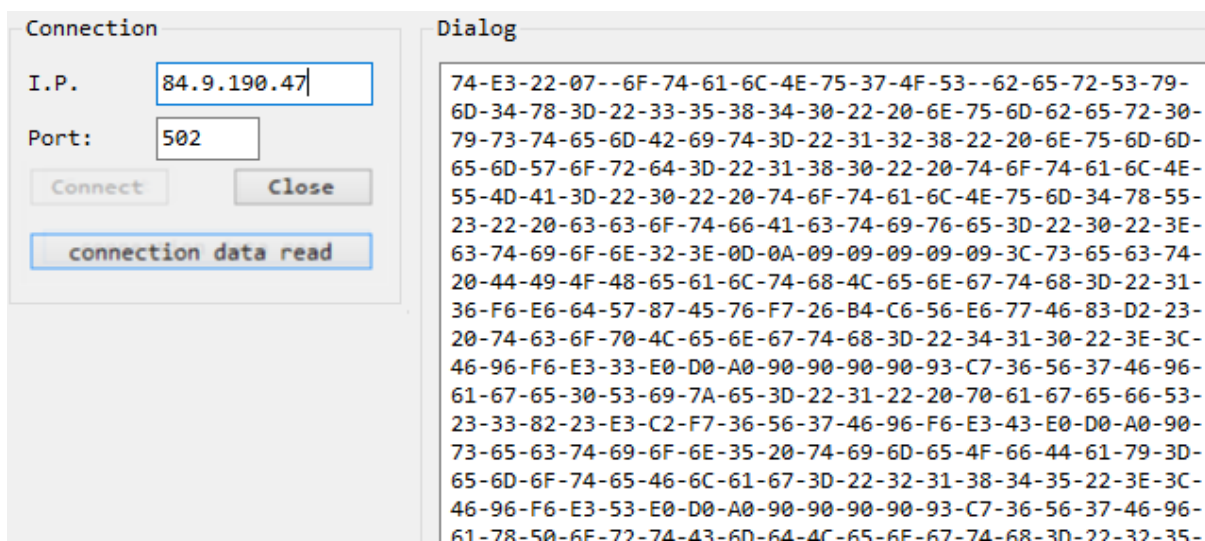


Figure 14: CAPMod tool to read into PLC Registers

Ettercap was used to generate MITM attacks on both the Master and slave, this attack depicted man in the middle attacks on the PLC and on the HMI, this combines with themodified command to change the signal sent to the Modbus slave

Data collection

To analyse Modbus TCP protocol traffic We carried out several steps to capture the artifacts

1. Wrote acontrol logic to control a simple petroleum pipeline process

2. Built a HMI project with Citec Vijeo
3. Read and wrote into various memory register using the HMI software
4. Analysed the captured section

In this research we aim at collecting forensic artefacts from a SCADA system to be used for the forensic analysis. This analysis includes:

- i. Analysis of the network traffic using wireshark system
- ii. Capture the ladder logic and control program using the ecostruxure control program
- iii. Capture and analyse data from the engineering workstation and SCADA server by use of Encase
- iv. PLC memory reading with he created tool

Wireshark was used to capture communication between the PLC and the HMI, the results are as indicated in appendix 1, this was done prior to launch of attack and when the PLC is obtaining commands from the PLC. The HMI sent a command to the PLC initiating a valve open,

From the engineering workstation, it was possible to obtain and analyse using a hexfile reader the projects. STU or STA program, code. For this case WINHEX was used to read into a STU program that is generated when a programme is created in the control expert program, data below was captured

```

000001B0 61 3D 22 54 43 50 49 50 22 20 6E 62 54 72 69 65 a="TCPIP" nbTrie
000001C0 73 3D 22 33 22 20 74 69 6D 65 6F 75 74 3D 22 33 s="3" timeout="3
000001D0 30 30 30 22 20 68 69 67 68 53 70 65 65 64 3D 22 000" highSpeed="
000001E0 30 22 3E 3C 2F 50 4C 43 41 64 64 72 65 73 73 3E 0"></PLCAddress>
000001F0 0D 0A 09 09 3C 73 69 6D 75 6C 61 74 6F 72 41 64 <simulatorAd
00000200 64 72 65 73 73 20 61 64 64 72 65 73 73 3D 22 31 dress address="1
00000210 32 37 2E 30 2E 30 2E 31 22 20 6D 65 64 69 61 3D 27.0.0.1" media=
00000220 22 54 43 50 49 50 22 20 6E 62 54 72 69 65 73 3D "TCPIP" nbTries=
00000230 22 33 22 20 74 69 6D 65 6F 75 74 3D 22 33 30 30 "3" timeout="300
00000240 30 22 3E 3C 2F 73 69 6D 75 6C 61 74 6F 72 41 64 0"></simulatorAd
00000250 64 72 65 73 73 3E 0D 0A 09 09 3C 62 61 6E 64 77 dress> <bandw
00000260 69 74 68 20 61 6E 69 6D 61 74 69 6F 6E 3D 22 37 ith animation="7
00000270 30 22 20 50 4C 43 4D 6F 6E 69 74 6F 72 3D 22 31 0" PLCMonitor="1
00000280 30 22 20 50 4C 43 4D 6F 6E 69 74 6F 72 3D 22 31 0" PLCMonitor="1

```

Figure 15: Analysed data from the engineering workstation

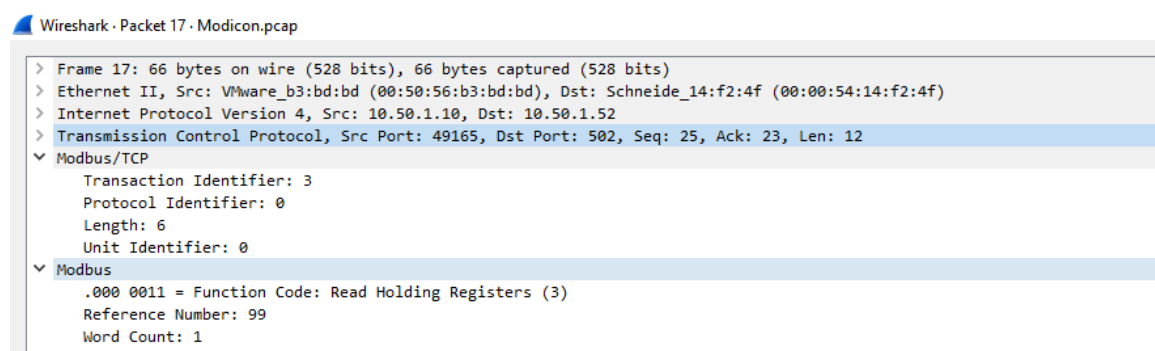
CHAPTER 5: EVALUATION

From the captured program from the engineering workstation, were able to capture the ladder logic running on the PLC and the configurations thereof sample of the ladder logic and register settings is as per appendix 2

From the engineering workstation its possible to obtain, the program currently running on the PLCS or the RTUs and the settings thereof. This can be compared to the program already saved in the redundant controller to identify the file types FC03 and 0x83

A packet analysis of the with the wire shark tool confirmed the frames received the components of the Modbus TCP with the MBAP, the PC as the Master station sends a packet to the slave that is the PLC to turn on a coil.

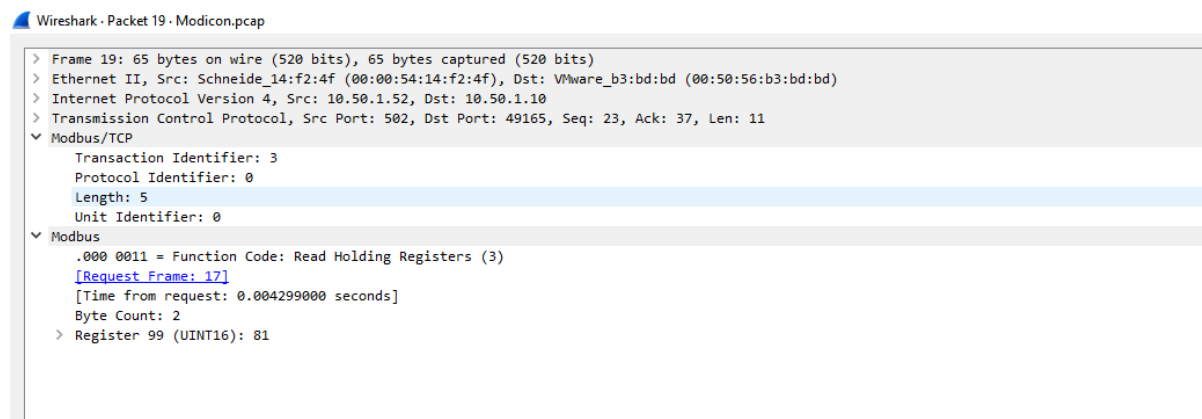
Wireshark software was used to evaluate the network communication between the master and the slave, from the PCap capture below confirms that frame 17 had a unit id of 0, function code to read a register and a word count of 1



```
Wireshark - Packet 17 - Modicon.pcap
> Frame 17: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: VMware_b3:bd:bd (00:50:56:b3:bd:bd), Dst: Schneide_14:f2:4f (00:00:54:14:f2:4f)
> Internet Protocol Version 4, Src: 10.50.1.10, Dst: 10.50.1.52
> Transmission Control Protocol, Src Port: 49165, Dst Port: 502, Seq: 25, Ack: 23, Len: 12
  Modbus/TCP
    Transaction Identifier: 3
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 0
  Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    Reference Number: 99
    Word Count: 1
```

Figure 16: Captured packet . Master to PLC

The PLC gives a response back in frame 19 to the master to confirm register number 99 within its Modbus TCP packet as shown in figure 18



```
Wireshark - Packet 19 - Modicon.pcap
> Frame 19: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
> Ethernet II, Src: Schneide_14:f2:4f (00:00:54:14:f2:4f), Dst: VMware_b3:bd:bd (00:50:56:b3:bd:bd)
> Internet Protocol Version 4, Src: 10.50.1.52, Dst: 10.50.1.10
> Transmission Control Protocol, Src Port: 502, Dst Port: 49165, Seq: 23, Ack: 37, Len: 11
  Modbus/TCP
    Transaction Identifier: 3
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 0
  Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 17]
    [Time from request: 0.004299000 seconds]
    Byte Count: 2
    > Register 99 (UINT16): 81
```

Figure 17: PLC to Master packet analysis

Finally, in frame 20 an acknowledgement from the master workstation to the PLC was sent to indicate that the communication was complete. The entire communication of query response and acknowledgement is as in the figure 19 below.

17	2.030215	10.50.1.10	10.50.1.52	Modbus...	66	Query: Trans: 3; Unit: 0, Func: 3: Read Holding Re...
18	2.031032	10.50.1.52	10.50.1.10	TCP	64	502 → 49165 [ACK] Seq=23 Ack=37 Win=4091 Len=0
19	2.034514	10.50.1.52	10.50.1.10	Modbus...	65	Response: Trans: 3; Unit: 0, Func: 3: Read Holding Re...
20	2.241151	10.50.1.10	10.50.1.52	TCP	60	49165 → 502 [ACK] Seq=37 Ack=34 Win=252 Len=0
21	2.454153	10.200.1.06	10.50.1.52	TCP	78	56809 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=5...
22	2.454686	10.200.1.06	10.50.1.52	TCP	78	56898 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=5...

Figure 18; query response and acknowledgement

The created forensic tool has a capability of reading a program task currently running on a PLC and the values of the all registers on the PLC. The tool is written in C# and is designed in three parts one is the GUI part the other offers communication to the PLC to avoid a delay or affecting the PLC cycle time, with the tool we were able to acquire the program from the PLC in binary. This code can be analyzed using a hex tool. this digital artefact can be used to analyze the program on the PLC to check for any change on the application

CHAPTER 6: DISCUSSION

Currently attackers are not only concentrating on on IT equipments but also on any connected devices and equipment's. The research concentrated on threats mostly relating on the oil and gas sectors and on Modbus protocol. Another limitation with industrial control systems is the time allowed for the system to be offline for analysis based on the control requirement of the critical instruments

Performance Evaluation of the tool

In this we do discuss the time it takes the tool to capture the hex file from the PLC. The time is calculated from the time the connect button is hit until the time the data is captured by the tool. the tool takes around 8 seconds to get the data from a plc

CHAPTER 7: CONCLUSION AND FUTURE WORK

Modern day attackers are not only focusing on IT but also on Operational technology that includes SCADA systems and DCS systems, due to the interconnection of the SCAD systems into the internet , their interconnected systems such as the PLC also forms part of the targeted system as it holds the application that collects and controls field instruments,. PLC and industrial control protocols don't have security as part of their configuration. From our research once an attacker gains access to the SCADA network they can manipulate start and stop the PLC and change the programs therein. In this research we were able to capture a control program from a plc that may be analysed using a hex program, to connect the plc from the tool

we did use the PLC IP address the Modbus TCP/IP ethernet port 502. We were also able to capture communication between the PLC and the SCADA system and analyze it. This captured digital artefacts can be used to retrace the attack trail on this critical system

In addition to collect digital artefacts using Modbus TCP/IP the tool was tested using Modicon M340 PLC. Further research is needed to test the tool with other PLCs that support Modbus TCP/IP and with other industrial control protocols,

Limitations

The tool can only capture live data from a Modicon PLC and PLCs operating on Modbus TCP/IP only

REFERENCES

- [1] Tim Kilpatrick, Rodrigo Chandia, Mauricio Papa, Jesus González, "An architecture for SCADA network forensics," vol. 222, pp. 273-285, 2015.
- [2] Irfan Ahmed, Sebastian Obermeier, Martin Naedele, Golden G. Richard III, "SCADA Systems: Challenges for Forensic Investigators," in *Computer*, vol. 12, pp. 44-51, 2012.
- [3] J. Stirland, K Jones, H. Janicke, Tina Wu, "Developing Cyber Forensics for SCADA Industrial Control Systems," Kuala Terengganu, Malaysia, 2014.
- [4] Yulia Cherdantseva, Pete Burnap, A. Blyth, P. Eden, "A Review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1-27, 2016.
- [5] Ralston, Patricia AS, James H. Graham, and Jefferey L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, vol. 6, pp. 583-594, 2007.
- [6] Betts, M. C. ., Joseph Stirland, Funminiyi Olajide, Kevin Jones and Helge Janicke. , "Developing a State of the Art Methodology & Toolkit for ICS SCADA Forensics.," *International Journal of Industrial Control Systems Security (IJICSS)*, , vol. 1, no. 2, 2017.
- [7] M. Horkan, "Challenges for IDS/IPS Deployment in Industrial Control systems," *SANS*, 2015.
- [8] Van Long, L. Fillatre, I. Nikiforov, "Sequential monitoring of SCADA systems against cyber/physical attacks," *IFAC*, vol. 48, pp. 746-753, 2015.
- [9] Stouffer, Keith, Joe Falco, and Karen Scarfone, "Guide to industrial control systems (ICS) security," *NIST special publication*, vol. 800, pp. 16-16., 2011.
- [10] Ijure V, Laughter S, Williams R., " Security issues in SCADA networks. *Computers and Security, Information Security Forum (ISF)*., vol. 25, p. 498-506. , 2006.

- [11] Guillermo A. Francia III, Xavier P. Francia, and Anthony M. Pruit, "Towards an Indepth Understanding of Deep Packet Inspection Using a Suite of Industrial Control Systems Protocol Packets," *Journal of Cybersecurity Education, Research and Practice*, 2016.
- [12] D. H. a. N. K. EricJ. Byres, "A study of Security Vulnerabilities in Control protocols,," 2016.
- [13] Abdalhossein Rezai, Parviz Keshavarzi, Zahra, "Key management issue in SCADA networks: A review",," 2017.
- [14] Abdalhossein Rezai , Parviz Keshavarzi, Zahra Moravej, "Advance hybrid key management architecture for SCADA network security," *Security and Communication Networks*, vol. 9, no. 17, pp. Pages 4358-4368, 2016.
- [15] Z. Zhang, W. Susilo and R. Raad, "Mobile ad-hoc network key management with certificateless cryptography,," Gold Coast, 2008.
- [16] Abraham Serhane, Mohamad Raad, Willy Susilo,, "Programmable logic controllers-based systems (PLC-BS): vulnerabilities and threats,," *SN Applied Science*, 2019.
- [17] S. Krishnan and M. Wei, , "SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics,," Barcelos, Portugal, 2019,, 2019.
- [18] K. M. Henry Hui, "Investigating Current PLC Security Issues Regarding Siemens S7 Communications and TIA Portal," in *Industrial Control Systems Cyber Security Research*, 2018.
- [19] Mira Stojanovic,Jasna Markovic-Petrovic, "An Improved Risk Assessment Method for SCADA Information Security," *Elektronika ir Elektrotehnika*, vol. 20, pp. 69-72, 2014.
- [20] George Denton, Filip Karpisek, Frank Breitingner, and Ibrahim Baggili, "Leveraging the SRTP protocol," *Digital investigations* , vol. 22:, pp. S26-S38, 2017.
- [21] Umit Karabiyik,Faruk Yildiz,James Holekamp,Khaled Rabieh, "Forensic Analysis of SCADA/ICS System with Security and Vulnerability Assessment," in *ASEE Annual conference and exposition* , Salt Lake City , 2018.
- [22] B. Zhu, A. Joseph and S. Sastry,, "A Taxonomy of Cyber Attacks on SCADA Systems,," Dalian, 2011.
- [23] S. O. M. N. a. G. G. R. I. I. Ahmed, "SCADA Systems: Challenges for Forensic Investigators,," in *Computer*, vol. 45, no. 12, pp. 44-51, 2012.
- [24] C. Valli, "Snort IDS for SCADA Networks. 618-621," Las Vegas, 2009.
- [25] Qasim S.A., Lopez J., Ahmed I., "Automated Reconstruction of Control Logic for Programmable Logic Controller Forensics," 2019.
- [26] Modbus.org, MODBUS Messaging on TCP/IP Implementation Guide V1.0b, http://www.modbus.org/docs/modbus_messaging_implementation_guide_v1_0b.pdf, 2006.
- [27] Schneider Electric, , Modicon M340, User manual, Schneider Electric, 2018.

