YAŞAR UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

MASTER THESIS

A SECURITY ANALYSIS AND SECURE MANAGEMENT MODEL FOR SCADA SYSTEMS

CAGRI DOGU

THESIS ADVISOR: ASSOC. PROF. AHMET TUNCAY ERCAN

DEPARTMENT OF COMPUTER ENGINEERING

PRESENTATION DATE: 08.08.2019

BORNOVA / İZMİR
AUGUST 2019

We certify that, as the jury, we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Jury Members:	**Signature:**
Assoc. Prof. Ahmet Tuncay ERCAN Yasar University	....
Assoc. Prof. Mehmet Hilal ÖZCANHAN Dokuz Eylul University	....
Prof. Mehmet ÜNLÜTÜRK Yasar University	....

Prof. Cüneyt GÜZELİŞ

Director of the Graduate School

ABSTRACT

A SECURITY ANALYSIS AND SECURE MANAGEMENT MODEL FOR SCADA SYSTEMS

DOGU, Cagri
M.Sc., COMPUTER ENGINEERING
Advisor: Assoc. Prof. Ahmet Tuncay ERCAN
August 2019

Supervisory control and data acquisition (SCADA) frameworks assume a significant job for the board and controlling mechanical plants. Out of sight, these frameworks utilize a modern system among PLCs and electromechanical gadgets for robotization and continuous administrations. Setting up a protected correspondence between these field gadgets and the control room is essential from the security perspective. Since the most powerless piece of SCADA frameworks is their communication protocols, this work centers around the shortcomings of SCADA frameworks against the interior digital assaults, for example, Denial of Service (DoS), Man-in-the-Middle (MITM) and Replay. For this point, an example SCADA testbed condition has been planned at first and after that the assaults referenced above are tried on it. Test results demonstrate that although SCADA frameworks achieve some mission basic errands, the conventions utilized in their correspondence frameworks still need essential safety efforts. Along these lines, some prompt safeguards to alleviate the vulnerabilities are proposed toward in the end of study.

Key Words: SCADA, PLC Security, Cyber-attack, Countermeasures, Internal attacks

ÖZ

SCADA SİSTEMLERİ İÇİN GÜVENLİK ANALİZİ VE GÜVENLİ YÖNETİM MODELİ

DOĞU, Çağrı
Yüksek Lisans, Bilgisayar Mühendisliği
Danışman: Doç. Dr. Ahmet Tuncay ERCAN
Ağustos 2019

Merkezi Denetleme Kontrol ve Veri Toplama Sistemi (SCADA) veri paketleri, endüstriyel tesislerin kontrol edilmesi için önemli bir görev üstlenmiştir. Bu veri paketleri, robotların yoğun kullanıldığı sürekli uygulamalar için PLC'ler ve elektromekanik araçlar arasındaki haberleşmede kullanılmaktadır. PLC'ler ile kontrol odası arasında korumalı bir haberleşme kurmak güvenlik açısından çok önemlidir. SCADA veri paketlerinin en zayıf parçası, haberleşme protokolleri olduğu için, bu çalışmada SCADA veri paketlerinin iç ağ saldırıları (Hizmeti engelleme saldırısı (DoS), Ortadaki adam (MITM) ve yeniden gönderme saldırısı gibi) incelenmiştir. Bu noktada, ilk önce SCADA test ortamı yaratılmış ve daha sonra bu saldırılar denenmiştir. Test sonuçları, SCADA veri paketlerinin bazı temel görevler almasına rağmen, haberleşmede kullanılan protokollerin hala önemli güvenlik önlemlerine ihtiyaç duyduğunu göstermektedir. Bu çalışmada ayrıca SCADA sistem risklerini önleyebilmek için alınabilecek bazı tedbirler önerilmiştir.

Anahtar Kelimeler: SCADA, PLC Güvenliği, Siber saldırı, Karşı önlemler, İç saldırılar

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof. Ahmet Tuncay ERCAN for his guidance and patience during this study.

I would like to express my enduring love to my parents, who are always supportive, loving and caring to me in every possible way in my life.

Cagri DOGU
İzmir, 2019

TEXT OF OATH

I declare and honestly confirm that my study, titled “A SECURITY ANALYSIS AND SECURE MANAGEMENT MODEL FOR SCADA SYSTEMS” and presented as a Master’s Thesis, has been written without applying to any assistance inconsistent with scientific ethics and traditions. I declare, to the best of my knowledge and belief, that all content and ideas drawn directly or indirectly from external sources are indicated in the text and listed in the list of references.

Cagri DOGU

Signature

……………………………………

September 4, 2019

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SYMBOLS AND ABBREVIATIONS

ABBREVIATIONS:

EU	European union
USA	United States of America
AGE	American Gas Association
API	American Petroleum Institute
ARP	Address Resolution Protocol
CIP	Critical Infrastructure Protection
NIPC	National Infrastructure Protection Center
DDOS	Distributed Denial of service
NSA	The National Security Agency
DNP3	Distributed Network Protocol 3
ICS	Industrial Control System
GRI	Gas Research Institute
HMI	Human-Machine Interface
IED	Intelligent Electronic Devices
IGT	Institute of Gas Technology
ISO	The International Standards Organization
MITM	Man in The Middle Attack
MTU	Master Terminal Unit
NERC	North American Electrical Safety Organization
NIST	American National Institute of Standards and Technology
NSTB	National SCADA Test Bed

OSI	Open Systems Interconnection
PLC	Programmable Logical Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition System
SQL	Structured Query Language
IDS	Intrusion Detection System
TCAE	Tehama Colusa Canal Authority
VECS	Virtual Environment Control System
VPST	Virtual Power System Test

CHAPTER 1
INTRODUCTION

Throughout history society when examining the social and economic development process it is observed that humanity passes through three main phases. First; it is the people's land and agrarian societies settle. Secondly, the 18th century towards the end of mass production, consumption and industrial society in which education is important, and the third one is the production of today that we live in the era of information technology and usage. The information technology and usage are gradually increased, accessed and instant information, transmitted and can be produced. Almost in every field such as the education, communication, health and energy, these information technology and usage can be used by the information society.

Nowadays, the knowledge is becoming the only factor of production through the improvement of information technology. Technologies of information and communication in the market statistics are seen that produced to use examination by the year 2016 constitutes more than 97% of the world market (Information Technology Agreement, 2018). Because of many countries are in the information age, they need to produce more knowledge in order to remain strong and ensure the security of the information, which is produced. The communities are considering to produce their own information systems within their information policies about economic, socio-cultural and technological accumulation of their countries.

The knowledge and life of people, who need rapid developments in communication technologies facilitate the services, offered in both sector services of public and private and ensuring the quality and presentation of the digital media which raises the very top level. Especially in Turkey, the establishment of an Information and Information Technologies Group in the Turkish Grand National Assembly (TBMM) with the aim of using information and communication technologies in the public and private sector since from 1998, and to be became a party to the eEurope+ initiative prepared for EU candidate countries through EU harmonization packages, the transition to information society has gained speed early of 2000 (Yılmaz, Ulus, & Gönen, 2015).

Radical changes and innovations in information technology during the last 20 years; individuals, communities, organizations and institutions and the state of social due to facilitate the life and governance, health, economy, energy, administrative, communication, education, every sector and field use, such as finance and industry has become widespread and has created an infrastructure, which is based on information systems. Community order and national security can be influenced in the event of a malfunction or the occurrence of each of these areas, which mention to every aspect of human life. In short, societies and states become addiction to information and communication technologies and reveal the notion of cyber dependence.

In figure 1.1, at the bottom, we defined the modern ICS trends. IEDs are usually connected to sensors and controllers by automation networks such as HART, Fieldbus, Profibus, or increasingly by Ethernet. Although one process control vendor already offering IPV6 wireless on battery-powered sensors next level of network consists of ICS master and systems used for operating and managing the ICS next level of network provides advanced applications, such as optimization and gateways to the enterprise network.

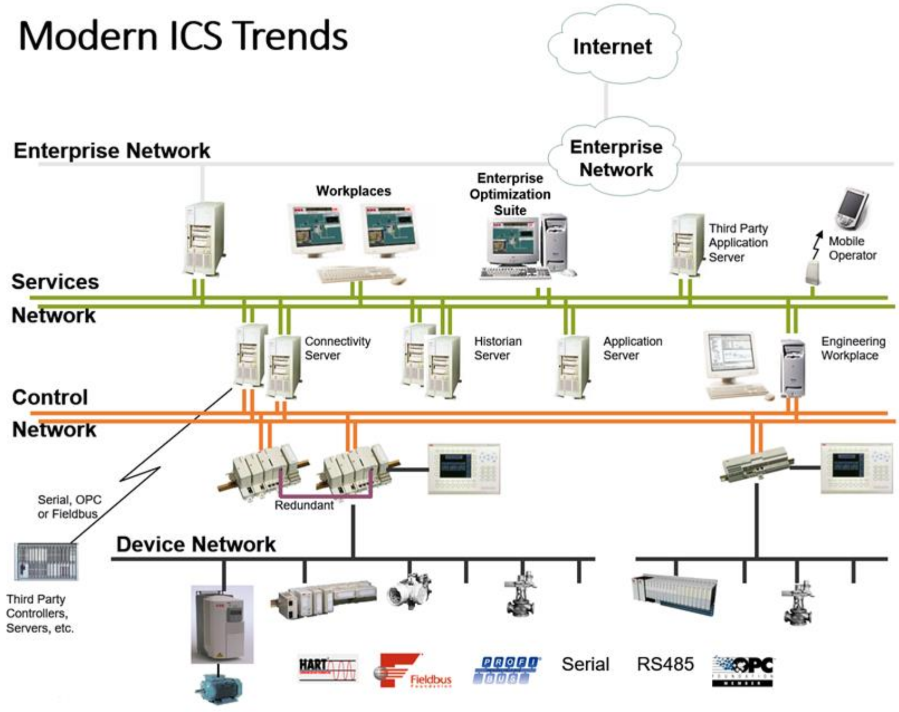


Figure 1.1. Modern ICS network

In today's world where cyber addiction increase, the development of internet technology has eliminated the boundaries between countries and has become an important global information network. Especially, increasing use of technologies such as internet of things, big data, cloud computing which quite improves in recent years, work as integrated with internet technologies, has caused to be considered that it will cause to life and life style of society being difficult to predict.

As mentioned, the use of information technologies leads to ease life through reasons such as speed, convenience, transparency and cost effectiveness. However, besides the advantages of this technology, there are some risks and disadvantages. The security of these systems, which brings with them weaknesses and risks, is important for the welfare of societies and public order.

Knowledge of the function, operation of critical infrastructure and land use also influence almost every field of communications technology and bring radical changes occur. The use of information and communication technologies in almost every field affects the functioning and operation of the critical infrastructures of countries and creates fundamental changes. Especially the information systems and infrastructures, which if damaged or affected, will disrupt or damage community life and national security, are defined as critical infrastructures (Unver & Canbay, 2010). In this regard, each country develops security measures and information security policies by considering its own critical information systems and infrastructures, their technological knowledge and capacity for external or internal threats.

“Critical infrastructure” is a concept that has been discussed in almost every part of the world in recent years and has not yet been defined concurringly by countries. However, mainly US and EU countries have defined the water, banking, energy, nuclear / chemical facilities, health, transportation and communication infrastructures as critical sectors and they have defined infrastructure of these sectors as critical infrastructures. The definitions of critical Infrastructure are mentioned in dated 2004 communiqué of EU Commission, which is titled "Protection of Critical Infrastructures within the Scope of Anti-Terrorism" (UNITED NATIONS OFFICE OF COUNTER-TERRORISM, 2019), and legislation of USA. It is defined as the assets, systems or related parts that are necessary for the maintenance of vital social functions, health, safety, security, economic and social well-being of people and whose disruption or destruction is insufficient to sustain these functions in a member state.

Nowadays, electricity, gas, water, sewer, transportation, pharmaceutical and chemical industries, pulp and paper industry, control and monitoring of the food and beverage sector and industrial production are partly provided with control systems. Obtaining unauthorized access can be performed with physical and cyber-attacks on this system and the functioning of these systems function with different intervention and can be modified and be deteriorated.

SCADA control systems referred to in the literature as a system designed in the first period in which Internet technology, wired and wireless access technologies cannot be compared with today's technology was level (Sanz & Årzén, 2003). SCADA systems were schemed to be insulated from other information technology infrastructure (Chandia, Gonzalez, Kilpatrick, & Papa, 2007). Also, the operating system's security running on the system and application vulnerabilities are considered by the thought of being isolated and there was no system in mind. But today, with the improvement of internet technology, operators managing SCADA systems monitor and control these systems by using internet technology. Also, SCADA system components still use internet technology to communicate among themselves.

In Turkey in 11.06.2012 "2013 - 2014 National Cyber Security Strategy and Action Plan" was prepared and put into effect as the first strategy and action plan prepared for the security of critical infrastructures monitored and controlled by SCADA systems with the contribution of Information Security Association (REPUBLIC OF TURKEY Ministry of Transport, Maritime Affairs and Communications, 2014). Also, recently, "National Cyber Security Strategy 2016-2019" has been prepared and will enter into force. These strategies include the information systems of critical infrastructure. Primarily, including information systems of critical infrastructure, institutional studies to ensure cyber security taken the decision to be made, information systems of critical infrastructure, criticality levels, it was decided that the determination of and responsible relationship with each other.

Many national and international institutions and organizations have prepared policies, strategies, action plans or reports on the security of critical infrastructures in the world. In particular, the policies and strategies published by some internationally recognized organizations provide significant guidance on the protection of critical infrastructures. Especially internationally recognized policies issued by some organizations and strategies, constitute a significant guideline on the protection of critical infrastructure. American Gas Association (AGA), the AGA to develop SCADA security to protect against cyber-attacks of communication system, the result of the efforts of the various organizations concerned with the number of gas have been developed. These are: The Institute of Gas Technology (IGT), the Gas Research Institute (GRI), the Gas Technology Institute (GTI) and the American Gas Association (AGA). AGE 12 field devices with the control center focuses on the security of the communication link between the control servers. Recommended applications are designed to allow communication to SCADA secret and original. AGE 12 prepared based on the standard which is a voluntary and in no way that did not make it mandatory as proposed in the standard installation of encryption technology. AGE 12 are grouped under four main titles. These titles are: (i) the background, policies and testing plan, (ii) enhanced link encryption for serial asynchronous communication, (iii) the protection of the network system, and (iv) the protection of the embedded SCADA component (Carlson, Dagle, Shamsuddin, & Evans, 2015). AGE 12 Standard; Cyber security, social engineering, physical security, and provides best practices for developing security policies and procedures.

Center for the Protection of National Infrastructure (CPNI) by the UK Government in 2007 to determine the UK's critical infrastructure is established for the protection and service. There is too many information in the literature because it is based on privacy organization. Britain's critical infrastructure; health care, emergency services, food, energy, communications, public services, transportation, and water were determined. It is tried to ensure security of critical infrastructures in the study titled "Cyber Security and the United Kingdom's Critical National Infrastructures" (Centre for the Protection of National Infrastructure, 2014).

The purpose of the NIST 800-82 the study titled “Industrial Control Systems Safety Guide" that it is prepared by American National Institute of Standards and Technology (NIST) is to provide a guideline for securing SCADA systems, industrial control systems and other systems that provide control function (NIST, 2014). The NIST 800-82 does not provide a direct safety checklist. It offers security requirements and solutions for risk assessment studies. In addition to this, it examines hardware or software components used in the infrastructure of industrial control systems and makes recommendations for more secure network-application services and provides examples. Therefore, it is among the sources that can be consulted for practical reviews and corrections.

This standard provides guidance SCADA security for gas and oil operators to manage the integrity and security of the system. API 1164 safety standard for reach control, security of communication (including encryption), classification of information distribution, operating systems, physical problems (business persistence and including disaster recovery), business and the exchange of data between management systems, customers, configuration of area devices and tackles local reach (American Petroleum Institute, 2009).

The ISO / IEC 27002 standard includes recommendations for information security management for the use of organizations that initiate, implement and maintain information security. ISO/IEC 27002 ISO / IEC 27002 Code of practice for Information Security Management is a guide which is prepared for organizations to set up, implement, maintain and improve their information security management system. Unlike the previous version, it also includes information security audits and related practices for the management of Information Security Violations, which enable the establishment of the necessary management mechanism to take lessons from problems, failures and accidents and to take necessary measures to prevent them from happening again (Schaffner, 2007).

The study titled "Control Systems Security Catalog: Recommendations for Standard Developers" which is prepared by DHS – Department of Homeland Security that was established after 11 September 2002, is designed for to provide the necessary framework to various industrial sectors to develop robust safety standards, guidelines and best practices. It includes a list of recommended controls for many sources. The aim of the document, which is divided into 18 separate sections, is to provide the opportunity to balance security while working with limited resources. The document mentions security policy, configuration management, security awareness, training and access control (Nordlander, 2009).

Some of the topics of the US Department of Energy's study titled "21 Steps to Improve Cyber Security of SCADA Networks", which briefly but informatively describe the security of SCADA systems in 21 steps; (i) identification of all connections of SCADA connections, (ii) manufacturer-specific protocol insecurity to protect the system, (iii) establishment of a network prevention strategy situated on defensive profundity principle, (iv) establishment of system backup and disaster recovery plans (Office of Energy Assurance U.S. Department of Energy, 2018).

Public Responsibility Office is an independent and impartial institution working for the US Congress "for the Protection of Critical Infrastructure Cyber Security" titled work; (i) necessaries of cyber security in every sector of the critical infrastructure protection, (ii) which can be applied to critical infrastructure protection cyber security technology, existing cyber security research, (iii) privacy and including policy issues such as information sharing on cyber security technology used to protect critical infrastructure practice focuses on relevant issues such as determining the problem (Wilshusen, 2015).

SCADA systems, such as information and communication technology of integrated study results indicated above, the weaknesses and the resulting improvements in this technology affects directly the SCADA system. Parallel to these developments, the United States and throughout the world, especially the EU strategy for the security of these systems and policies are developed. Turkey is also being studied for the protection of their critical information systems within the scope of international studies. In this study under the axis of the communication protocols to be the most common deficiencies and removed hosting component usage statistics of the web open SCADA communications protocols, methods and approaches available in the literature for the cyber security of the axis of the second part of the particular SCADA systems was studied in detail. As a result of the screening, a solution has been developed for the security of Modbus TCP protocol which is the most used 50% worldwide.

In the second part of the study, the methods and approaches in the literature related to cyber security of EMSs in SCADA systems are examined in detail. This investigation was conducted within the scope of test setup environments, attack vectors, defense methods and risk assessments for the security of SCADA systems.

In the third part of the study, the working logic, components and functions of SCADA systems which are evaluated as critical infrastructure are examined in general. In addition, statistics of the most commonly used communication protocols in EKSs were obtained by using the Shodan search engine and the usage rates were determined on the basis of countries. Based on the Modbus protocol, the structure and detailed examination of the EKS communication protocols were carried out.

In the fourth part of the study, the relationship between SCADA systems and cyber security was examined and the most common vulnerabilities and cyber-attacks against

SCADA systems are analyzed. In addition to this, weaknesses in the axis most often used communication protocols previously established communication protocol that the SCADA system is based on the Modbus protocol and can be realized for these system cyber-attacks were discussed in detail. In the last part of this section, the tools used in the security tests of SCADA systems are examined and the results are analyzed by using them in a test setup environment at Gazi University Smart Grids Laboratory.

Finally, in the fifth part of the study, the Modbus TCP protocol was examined using Wireshark tool in a local network using Modbus Poll simulation environment and it was determined that this protocol did not check the source IP address during data transfer and did not use any encryption. The exploit of detected weakness was realized and attack packages were analyzed and a security architecture was proposed as a solution to prevent these attacks and a Modbus Sandbox, which is designed as the control middle layer within this architecture, provides control of Modbus TCP packets and runs on Python code. Thus, it is aimed to write the maximum threshold value by providing control over the threshold values specified in the registers of the devices working in the enterprise or in the field by an attacker.

In this study, the axis has been shown most commonly used Modbus detected by the TCP protocol source IP address by exploiting the control of weakness can be blocked performed cyber-attacks and unauthorized values in the registers of the devices in the field cannot be entered. Furthermore, this study is considered that will provide for security of critical infrastructure to the country's contribution to the studies.

1.1. Related Works

This literature research includes cyber-attacks against these systems in test environments developed for the physical and cyber security of critical infrastructures and different security solutions. Sayegh et al. (2013) have demonstrated that cyber-attacks against SCADA communication protocols used in an experimental network designed to bypass security measures very easily. The experimental setup in denial of service (DoS) replayed (redirect) and showed the weakness of performing cryptographic attacks SCADA components and protocols (Sayegh, Chehab, Elhajj, & Kayssi, 2013). A real network using a traffic simulation environment in cyber-physical PLC performed cyber-attacks Intrusion Detection Systems (IDS) used the security rules. The simulation environment of subsystems on the network is prepared by using designed simulation Matlab / Simulink environment. As a result of the attacks, traffic on the STS was analyzed (Koutsandria, et al., 2015).

In this environment, cyber security studies related to industrial control systems, different engineering and computer science courses are given. Efforts are underway to exploit cyber security vulnerabilities discovered in the experimental setup environment and the effects of these attacks are examined under the title of risk analysis (Morris, et al., 2011). The layered approach of the control system, layered control, communication and power system was applied with simulation and emulation techniques of industrial control systems. At the same time, different cyber-attacks were analyzed with STS, which was used to detect cyber-attacks against electrical grid systems (Hahn A. , 2013). Intelligent network that is considered critical infrastructure in another study conducted for providing cyber security, in control group and cyber-communications ability to provide a physical environment and have prepared the experimental setup environment of the physical system components (Hahn, Ashok, Sridhar, & Govindarasu, 2013). Two different cutter DoS attacks and its results to be harmful to the internal and external network prepared experimental embodiment are discussed.

The National SCADA Test Scheme (NSTB) is a large-scale project that includes network generation and distribution components to provide a common national laboratory environment. As a result of this study, very serious cyber vulnerabilities related to critical infrastructures were identified and security assessment methods were produced for SCADA systems. Since the physical setup of the experiment will be economically costly, it requires considerable effort in practice (Kuipers, 2008). In order to provide a reconfigurable platform and more cost-effective, the Sandia National Laboratory has created a Virtual Control System Environment (VCSE), which allows it to work with simulation, emulation and physical systems. VCSE utilizes the OPNET loop system to ensure the integrated operation of simulated network and physical network devices. This enabled the communication between emulated and physical PLC devices and the PowerWorld simulator of power system. VCSE also used Umbra, the central simulation managing device, to ensure control over many elements. VCSE is planned to assist business teaching, vulnerability definition, attacks reduction, and computational activities (Mcdonald, Conrad, Service,

& Cassidy, 2008). Another similar project that combines simulation and physical elements is the Virtual Power System Testbed (VPST) designed by the University of Illinois. The University of Illinois is like VCSE in the use of the PowerWorld power system simulation tool, which will work in integration with the Real-Time Immersive Network Simulation Environment project (Bergman, Jin, Nicol, & Yardley, 2009).

European crucial project scope in order to observe the effects of different cyber-attack scenario two experimental setup has been developed. Priority control center as in the first experiment were also considered apparatus and communication infrastructure between the simulated subsystems. DoS attacks against specific communication infrastructure of these systems have been analyzed. Intelligent Electronic Devices emulated in another test device (IED-Intelligent Electronic Device) physical network infrastructure controlled by micro was used. Where IEDs over a local network using MATLAB/Simulink communicates using. In this environment of Distributed Energy Resources (DER-Distributed Energy Resource) is used for the detection of potential security vulnerabilities in applications (Dondossola, et al., 2009) (Dondossola, Deconinck, Garrone, & Beitollahi, 2009). Anomaly-based Test System for Security Analysis of SCADA Control System for IDS survey (TASSCS-The Testbed for Analyzing Security of SCADA Control Systems) has been improved at the University of Arizona. VCS project at Sandia similar OPNET loop system emulation and simulation used the electricity network in order to provide PowerWorld software. Simulation-based control solutions are represented using Modbus communicates with PowerWorld simulator software (Mallouhi, Al-Nashif, Cox, Chadaga, & Hariri, 2011).

At the University of Dublin, an experimental setup was prepared using the DIgSILENT power system simulator to detect both attacks and calculate their physical effects (Wu, et al., 2011). The SCADASim experimental setup was designed by the Royal Melbourne Institute of Technology for analyzing performance of network under cyber-attack. In the SCADASim experimental setup where is utilized from SCADA communication protocols that is used commonly, is focused on the emulated communication infrastructure using interconnected physical devices (Queiroz, Mahmood, & Tari, 2011). This experimental setup can be used to analyze the system communication infrastructure requirements of cyber-attacks.

Modbus Poll SCADA systems, which is a suitable software platform for testing and simulating the most widely used Modbus protocol among SCADA communication protocols, have been used in cyber security studies. Yanfei et al. used Modbus Poll as a software testing tool when developing Modbus-based ZigBee wireless sensor technology (Yanfei, Cheng, Chengbo, & Xiaojun, 2009). Beresford (2011), in the study which belongs to him, is able to capture password summaries and important information from the TCP breakdown by exploiting the fact that the ISO-TSAP and Profinet protocols used for communication of Siemens PLCs do not use encryption. Thus, replay and MITM attacks can be performed with this information. With these attacks, the PLC can be reprogrammed, the CPU can be turned on and off, authentication can be bypassed, authentication passwords can be changed or completely erased and memory can be read and written.

DDoS (Service Blocking) attacks against SCADA systems, which are considered critical infrastructure, can also be carried out. In the literature study for these types of attack, chemical plant that generates the simulated environment (Chabukswar, et al., 2010) have performed the DDoS attack and the target system have been engaged in intensive request packet and the system became unable to carry the normal traffic or slowed down much traffic.

Indicate that for political purposes and used only hacktivism used DDoS attacks are now making more systematic and complex structure, gives heavy damage to many systems (Elkin, 2016). It is difficult to mention that there is sufficient awareness on this issue, including those that manage many critical infrastructures. As mentioned in the study, as a result of the survey, many employees and managers do not think that this situation will not happen on their own, do not strive for the development of existing security systems by creating a test environment and do not know what to do if such an attack. Another result is that the responsible persons in particular complain about the lack of trained personnel, lack of technology and insufficient budget. On the other hand, the number of cyber attackers and cyber threat tools is increasing, improving themselves and being more effective.

Linux-based systems are more secure against DDoS attacks. The reason for this is that after receiving the first SYN package in the Linux operating system, the SYN cookies are used instead of allocating resources for the connection, and the resource is allocated only when it receives the ACK command. Therefore, it is argued that the use of Linux operating system in SCADA systems will be more accurate. Of course, there are modern exploiters for these operating systems; however, Linux still requires more effort to compromise systems than other systems (Kakanakov & Spasov, 2011). Therefore, it would be more correct to use the Linux operating system in the SCADA system is advocated. Additionally, this is a modern exploitative for operating systems; but still it requires more effort than other systems to overcome the security of Linux systems. The many security issues have made the assessment of the SCADA system architectures (Petrovic & Stojanovic, 2013). Especially in the last decade, many industrial control centers around the world have been attacked and vulnerability in SCADA systems have been reported. The reason for this; not to try to eliminate known gaps using standard technologies, to have control systems connected to other networks, to limit existing security technologies and applications, unsafe remote connection, and to have access to technical information about control systems by everyone. Due to these vulnerabilities, some computers have become slaves (zombies) and the systems can be damaged. It is emphasized that it would cause irreplaceable damages in the economy.

When examining security solutions for MITM attacks; giving priority to existing users to avoid the so MITM attacks from ARP poisoning, when a new node or user network, and sends the request to print its own MAC address in the MAC table, looking at the ethernet existing node table, the other nodes adjacent to the new node sends the query message. By checking the responses received, it is determined whether this node or user is a malicious node or user or a new component that is actually added to the network (Nam, Djuraev, & Park, 2013). This technique for wired networks can be successful since the nodes are stable. However, in wireless and mobile networks, the success rate remains very low due to the nodes are constantly moving. They take advantage of the encryption methods in order to prevent ARP poisoning. Ticket-Based ARP (Ticked-based ARP (TARP)) is the most widely known encryption-based approach. Secure ARP (S-ARP) and the Local Ticket Distributor (Local Ticket Agent-LTE) as the central server can be used for reliable key distribution solution for the problems at specific points (Lootah, Enck, & McDaniel, 2007). But this solution still is not enough for wireless communication.

To protect against MITM attacks identified a method for setting up DHCP servers that are used as the MAC-IP database center. In this method, a new DHCP is proposed for the transmission of MAC addresses between each user (Pansa & Chomsiri, 2008). However, DHCP, which is widely utilized in application, is difficult to set up, thus it is not easily applicable in real life. The biggest reason for ARP fraud is not to authenticate when changing MAC addresses between nodes. Therefore, all of ARP packets may be attacked by malicious users. In the model, when the client transmits the request to the MAC dispenser, the MAC dispenser distributes the open RSA key. In contrast, the client generates the AES key and encrypts it with the public key. It also transmits its own key to the MAC distributor. After the AES exchange is ensured, ARP table information can be received and transmitted securely using the AES key. The main purpose of the model is to send and to receive ARP table information in encrypted form. By blocking the ARP requests and response packets by the drivers, it is aimed to neutralize the ARP poisoning attack (Hong, Oh, & Lee, 2013). In this protection method, although the client side is protected, the gateway part is not fully protected and remains vulnerable to ARP poisoning attacks. Therefore, when this sort of attack is made, the gateway forwards a message to each client that their network is under attack.

SSL / TLS protocol on the server that users access the User Authentication Code (UAC-User Authentication Code) have proposed using as a model for making authentication. The purpose of the model; server is dropping by allowing users to fake (Oppliger, Hauser, & Basin, 2006). The system used in the UAC user must be protected from malicious software. Otherwise, the user's PIN can be intercepted with malicious software such as Trojan horses and system may become vulnerable to attack. In a study (Ciancamerla, Fresilli, Minichino, Patriarca, & Iassinovski, 2014); SCADA devices, and network-based attacker hybrid communicate on a local network intrusion detection system comprising MITM attack is conducted in a test device medium. Attacks on ARP protocol's encryption feature has been entered into between the PLC and SCADA control servers and taking advantage of the lack of ARP poisoning took place. In this way, the attacker has captured packets flowing between two devices and can make changes to these packages. Using the DNP3 protocol ETTERCAP tool for intervening in the work carried out by ARP poisoning attacks that they used the Wireshark tool for the analysis of packets captured and then realized (Lee, Kim, Kim, & Yoo, 2014). ETTERCAP using the DNP3 protocol for intervention tool in the study carried out by ARP poisoning attacks that they used the Wireshark tool for the analysis of packets captured and then realized (Ettercap, 2015). DNP3 packets analyzed user wants to send packets with libpcap vehicle has been modified.

SCADA control system attacks as exploration, response, measurement and command injection and DoS are examined in four classes and explained in detail. Depending on the complexity of the attack, the command injection is subdivided. Each attack described in the study was conducted in laboratory conditions for industrial inspection system (Morris, et al., 2011). Drawing attention to the dynamics of the Stuxnet malware code injection for the S7-300 PLC device showed how much can be realized in an easy way. Snap7 using the library to perform the attack has developed a program in C language code and dynamic security measures have been suggested for injection (Aloui, 2016). Attacks on hardware, software and communication components of SCADA systems are explained; gaining remote unauthorized access and changes to the threshold values at which the device generates alarms or controls, are explained under titled of hardware attacks; Attacks on the embedded operating system, such as authorization upgrade, memory overflow, and SQL injection are explained under titled of software attacks; Attacks by exploiting vulnerabilities such as SCADA communication protocols not encryption and TCP / IP based, are explained under titled of attacks on communication components (Zhu, Joseph, & Sastry, 2011). SCADA has been carried malicious script injection attacks in developed test environment in the Security Laboratory and the control system for the detection of attacks used in the description of the physical characteristics of artificial neural network (ANN) have observed false positive rates as a result of attacks using based STS with experimental results. The obtained results were considered ANN based on the hope that there is a security mechanism IDS transmitter (Gao, Morris, Reaves, & Richey, 2010).

To prevent replay attacks has proposed the single sign-on system. In the model proposed in the study, many databases have been added to protect authentication and authorization (Yang J. , 2010). In this approach, the authentication server that contains information such as the username and the TGT lifetime users (Ticket Granting Ticked) sends. TGS (Ticket Granting Service) user and sends the Ticket Granting Service application server. TGS has its own database and application server and store the ticket in their database. When an attacker attacks a replay against the TGT or SGT, it will be readily understood whether it is an attack or not.

Unlike the single sign-on system logon protocol it has been proposed based on dynamic dual password. In this protocol; user registration and log files are used two passwords that need during the use of the concept (Jian, 2009). The log file containing details of the visit to the authentication server, such as a user's TGT or application server. The application server creates log file thus it sends it to the authentication server. The authentication server redirects the user to the log file. Therefore, you can evaluate the security of the password during the audit log file, and the user can change. In the approach-based Kerberos authentication protocol, the server captures the P (Y) codes of all users on the network and sends the TGT to the user as the encrypted session key (for communication between the TGS and the user). After the user receives a message using the GPS P (Y) code and accepts the message is decrypted. If captured the attacker cannot decrypt the messages of the message. Because the P (Y) code, the size is gigabit size. Fail due to time synchronization problems. Which help to decide where the user's physical location of the message provider in addition to a message has been added to the Kerberos protocol. The server sends a hash of the user's physical location TGT session key is encrypted with valuable (Abdelmajid, Hossain, Shepherd, & Mahmoud, 2010). So, if you receive a message session tickets now considered offensive and is even harder to break the security phase two, including the duration of the ticket in this process.

Work on comprehensive cybersecurity of critical infrastructure, others have suggested that the SCADA security inspection in 4 main categories. These; anomaly detection, analysis and mitigation, real-time monitoring, are arranged in the attack. At the same time, he developed the method of attack for impact analysis. Power system developed for the attack tree model; system, and node level vulnerabilities scenario is calculated by determining threats to the system. Node-level vulnerabilities including password guessing attacks such as port and listening are the most common attack methods in this (Ten, Manimaran, & Liu, 2010). SCADA Yang and others used in the power grid in their work associated to the system's cyber security, the test environment they develop highly qualified IDS proposed to mitigate cyber-attacks. IDS reliable, highly qualified and acceptable behavior includes a concept-based address. SCADA security solution is proposed by ensuring data integrity without compromising normal data to improve the cyber security (Yang, et al., 2014).

In their study (Shang, Li, Wan, & Zeng, 2014) examined IDS for malicious software and Modbus encountered in industrial checking systems have been deeply analyzed in the packet size for TCP protocol from the application layer threats. IDS Modbus TCP communication-based model as a defense for "White list" rule has been proposed. In their study (Chen, Pattanaik, Goulart, Butler-Purry, & Kundur, 2015) have established the intelligent network environment by running an experiment which integrates real-time power system simulator and the telecommunication system simulator for cyber security. RTDS for power system simulation (Real-Time Digital Simulator) power is the network simulator used, Opnet's SITL for communication system simulation (System-in-the-Loop) simulator and open source Linux devices and servers are used. Modbus TCP protocol designed for two types of cyber-attacks and have made recommendations for the prevention and detection of this attack.

Modbus TCP protocol vulnerability analysis for traditional fuzzing (blur) on the outside of the Modbus TCP protocol fuzzing methods has developed a special methodology (Xiong, et al., 2015). According to the results of the simulation environment when applying the technology developed fuzzing compared to conventional processes, it pointed out that satisfactory. Modbus protocol flooding and have mentioned that the host vulnerability to attack command injection comprise the functions of the control system for the reversal of these attacks (Bhatia, Kush, Djamaludin, Akande, & Foo, 2014). In this study, based anomaly detection algorithms for detecting these attacks and signature-based threshold was compared Snort module.

As is obvious from the literature review explained above, the cyber security of SCADA systems are widely available studies is extremely important in this regard. Hence the weakness of the SCADA system has been put forward in this thesis are determined threats that can occur for these systems. Also, thesis a security architecture for the scope of work determined by subtracting the statistics from the most broadly utilized protocols in industrial control systems to eliminate one of the Modbus TCP protocol, source IP address control weaknesses have been proposed. With the proposed functions contained in the components of this architecture with the Modbus TCP protocol security solutions for users of field devices aimed to prevent the entry of unauthorized access and being able to control the external device registers value.

CHAPTER 2
SCADA SYSTEM COMPONENTS AND INFRASTRUCTURE

At the present day, the electricity industry is depended on the formation of a more centralized control of the network and producers. A more distributed and consumer-based transformation of this network is called the Smart Grid (US Department of Energy, 2015). The needs of today's smart grid electricity supply are increasing. Consumers will have the authority to manage more efficiently and economically more appropriate way their energy use. Smart grids also provide power reliability as well as how production and power are distributed.

Additionally, smart grids provide to overcome challenges such as increased power demand, wear and tear of the structure, and the greenhouse gas environmental impact during electricity generation. Power with the use of the smart grids may be used more effectively, and the carbon content may be formed around substantially reduced. Therefore, it should be the focus in order to make the network more automatic functions of the above (Clear Energy Pipeline, 2018). Conceptual architecture of the intelligent network is shown in Figure 2.1. Generator, central power plant, all the named components isolated microgrid SCADA (Supervisory Control and Data Acquisition - Supervisory Control and Data Acquisition System) is associated with architecture.

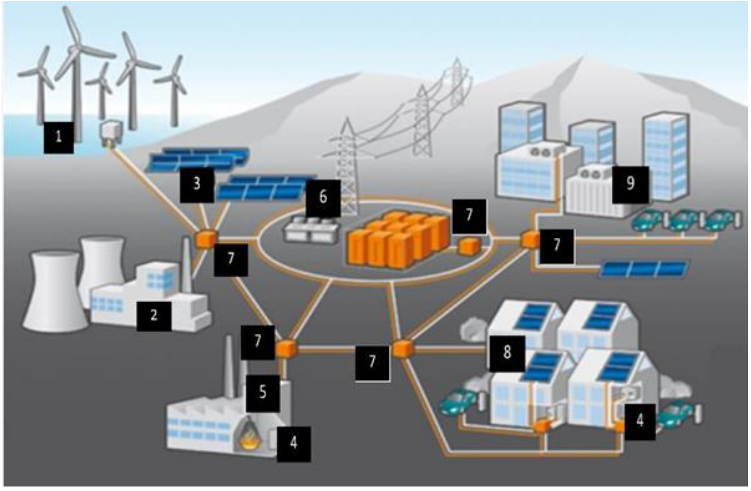


Figure 2.1. Conceptual architecture of the intelligent network

In today's technology, there may be some connections between industrial network and enterprise network. Due to these connection types, it is necessary to separate the two networks from each other by providing firewall positioning in many places, establishing VPN, logging, or providing controlled access. For this purpose, gateways with IDS and sandbox are needed in the software that can recognize industrial packages. In addition, each computer must have its own cloud-based anti-virus software (NIST, 2014). Common safety precautions on ICS systems shown in figure 2.2.

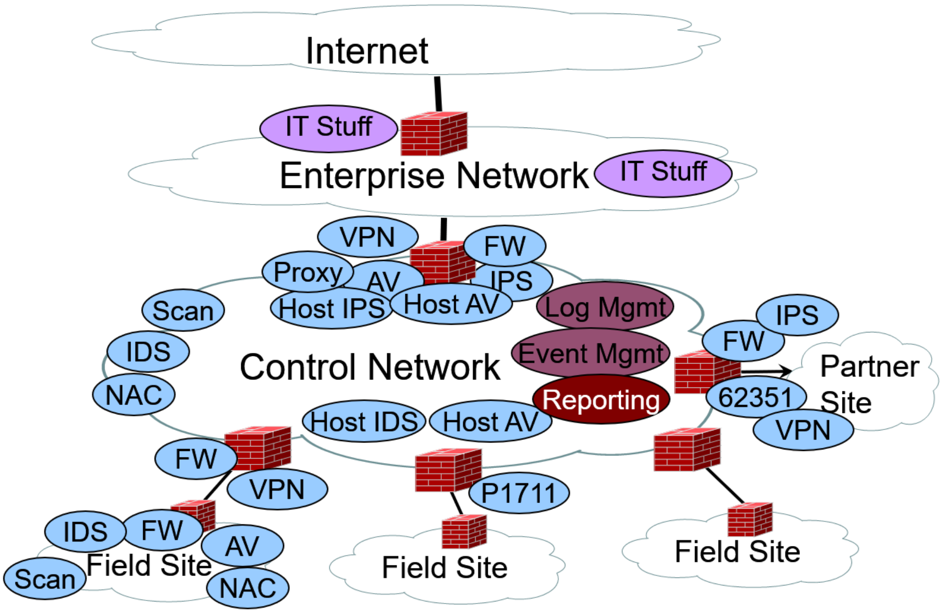


Figure 2.2. General safety precautions on ICS systems

SCADA systems are utilized in critical infrastructures such as energy, banking, communication and production in the use of electrical power systems. SCADA systems are broadly utilized in the industry of critical infrastructure and provide remote checking and controlling. The fundamental function of the SCADA system is to monitor and control the devices responsible for the electricity distribution. Additional functions include fault detection, equipment isolation and restoration, management of load and energy, automatic counter reading and transformer control.

SCADA is a collection of independent systems that measure and report local and geographically distributed transactions in real time. SCADA is a combination of telemetry and data acquisition that allows the user to send and receive commands from remote facilities.

As shown in Figure 2.3, the essential components of MTU (Master Terminal Unit) SCADA control system, RTU (Remote Terminal Unit) and the communications network (Mcdonald J. D., 1993).

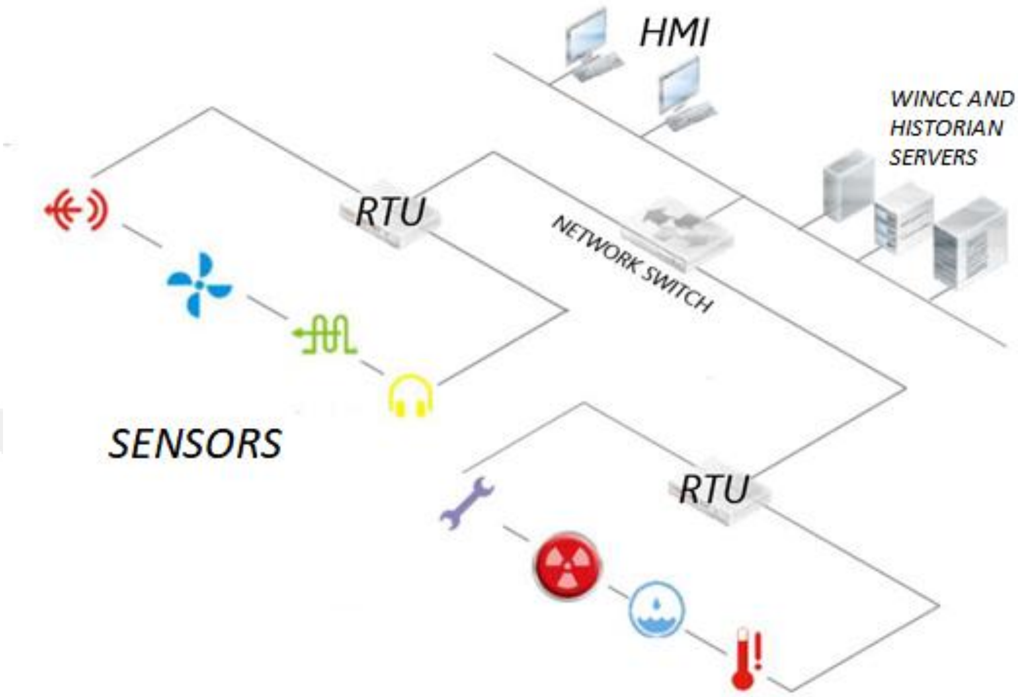


Figure 2.3. SCADA network components

2.1. Master Terminal Units

The MTU, referred to as the central controller or central terminal unit, is the form of connection of a server or a group of computers to a master server through a LAN (local area network) or wide area network (WAN). HMI (Human Machine Interface) software, which will be explained in the heading section, is installed in MTU or control center to add visuality of information coming from field devices. SCADA provides a graphical interface environment that the operator could understand during the communication of its components (Shahzad, Musa, Aborujilah, & Irfan, 2014).

SCADA systems designed years ago had conflicts in software / hardware connectivity or information / data display, but with the development of distributed control systems, today's designed SCADA systems provide a high-resolution interface and high performance compatibility between components (National Commuication System, 2004).

The HMI program runs on the MTU computer and it basically consists of diagrams that simulate the actual system for easier identification of the entire plant. Each entry in the remote system / exit point with the current configuration parameters are presented graphically shown. Configuration parameters, such as stop, and limit values are entered via this interface. This information is transmitted over the network and downloaded to the operating system of the remote location which would update about all these values.

Especially today, office-based personal computers began to have the same network as the SCADA system with the increasing use of personal computers. Thus, software and computer applications used in daily life began to be used in the SCADA server computers that are utilized for the system of management. The last component to be both decision-makers and due to host the MTU records on the system of SCADA is the most important component of the system. Inability to fulfill the functions of these components or exposure to an attack would leave the entire network at risk. In this regard, SCADA poses a risk of unwanted third-party software on computers that are used for the management of the system (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015).

To be made by MTU operations under brief;

- Monitor and control the communication of all SCADA components through the communication environment.

- To view a graphical user interface with data and information relating to the HMI SCADA communication using the software.

- To send commands to field devices and to receive commands from field devices to control the communication link.

2.2. Remote Terminal Unit (RTU)

The units of remote or remote terminal units are known as RTUs behave as slave stations in SCADA architectures. Controlled by the SCADA and consists of monitored equipment or machine is connected to the field devices. These devices contain the stimulant site or actuator to control sensors and systems to monitor the parameters of the modules. RTUs, real-time data from the receivers to send back to MTU station sends and receives information from the base station. RTUs send information to the

MTU, such as disaster, disaster recovery, function codes of the stimulus or sensors, or other critical situations.

RTU sends real-time data to the central station in a distributed manner using LAN / WAN connections, geographically deploying devices in many different locations. It is also responsible for transmitting current status information, such as whether physically deployed devices are correctly configured or functioning correctly (Krutz, 2005).

The most important component of the field device PLC (Programmable Logic Controller) device are defined in the heading subheadings in detail.

2.2.1. The Programmable Logic Controller (PLC) Systems

PLC systems are a special form of microprocessor-based controllers that can use programmable memory to store the instructions entered to implement the operations and control mechanism shown in Figure 3.3 and to implement functions such as sorting, timing and counting. The implementation of logical and switching operations is the primary function of these devices. Another function used by operator is a program with the sequence of instructions entered into the memory of the PLC device. Afterward the controller monitors the outputs and inputs in accordance with this program and applies the audit rules of the program.

PLC devices provides a great advantage due to the use of a broad range of basic controller operations. It may be accomplished with a number of different instructions without the need for rewiring to change the control system and the rules used. As a result, the cost-effectiveness and ease of use that allows many devices compared with the PLC relay system with applications made by the software to get rid of complex hardware problems. Also, it processes more secure and to be robust in terms of running and comprising several complex mechanical components relays is preferable in terms of processing more quickly (Bolton, 2015).

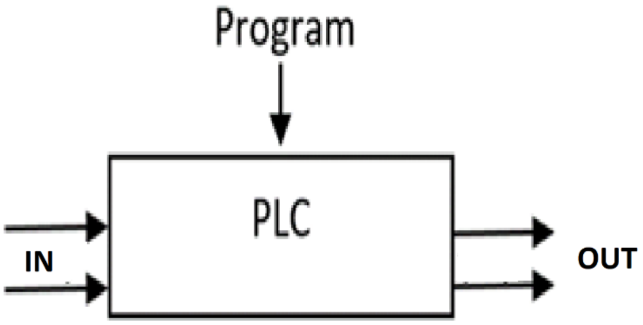


Figure 2.4. The Programmable Logic Controller

Today, first developed PLC in 1969, widespread to use and 20 digital input data received from a plurality of sensors for modular systems in the input/output module would provide increased capacity. Mainly machining, material handling, gas and oil refinery system are utilized by the automation of industrial processes such as the water supply side and transport.

In following sub-headings, architecture, software and hardware features of the PLC device are disclosed.

PLC architecture

In CPU with microprocessor in a characteristic PLC device, memory and input/output circuits are located. Also, in numerous relays in software, counter, timers and data storage units are available.

Input / Output (I / O) unit provides PLC devices with the input and output channels to receive information from the outside world by providing links. Each I / O point's specific address which is utilized by the CPU. This would be considered a home series lined up along the road. For example, 10 numbers being used for input from a sensor may be used for a given number output unit 45 motor (Erickson, 2010).

PLC hardware

A characteristic PLC system consists of basic functional components such as processor unit, input / output interface unit, power support unit, memory, communication interface and programming device. Figure 2.5 gives the components of a fundamental PLC system and details of these components are explained below.

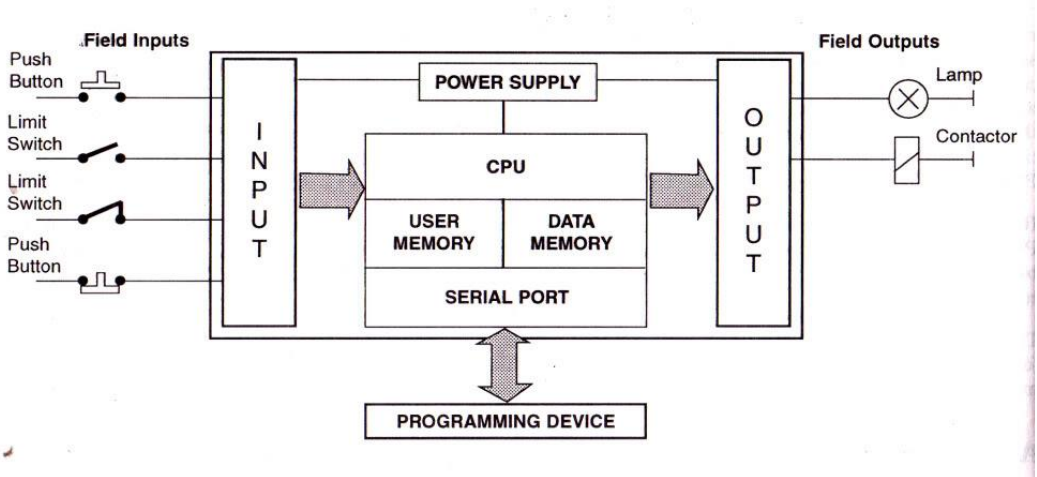


Figure 2.5. PLC System

CPU (The Central Processor Unit) is the unit where the microprocessor is located. This unit interprets the signals of input and performs control action by communicating to determine the action in the output signals in accordance with the program stored in its memory.

Power Support Unit converts AC voltage of the main processor and input-output modules to the necessary interfaces for low DC voltage.

Programming Device is utilized for entering the needed program into the processor's memory. The program is improved in this unit and afterward it is transmitted to the PLC device’s memory unit.

Memory Unit is found that the program units stored in the control action by the microprocessor and stores processing data signals from the output signal from the input (Alphonsus & Abdullah, 2016).

Input and Output Units are the units where the information coming from the external environment is processed and the communication with these external devices takes place. Input unit consists of sensors such as key, photocells, temperature sensor, flow sensor. Output unit, consists of devices such as starter motor and solenoid pump. The devices in the input and output units are classified according to their discrete, digital or analog signals as shown in Figure 2.6.

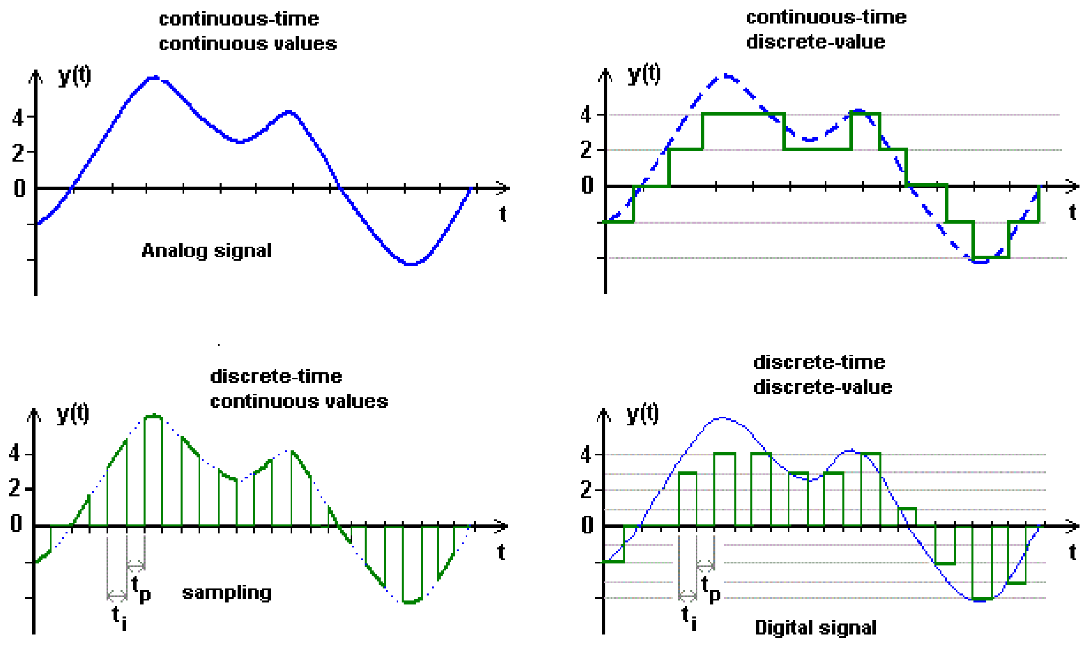


Figure 2.6. Analog to Digital Conversation A Signal

Communication Interface is used to transfer and receive data to communicate with other PLC devices. Device data collection, validation, actions such as synchronization between the user and contact management applications used in these units (NASA, 2015).

PLC software

PLC devices used for programs may be written in several formats. To facilitate the use of programming ladder programming has been developed that does not require too much information. Most PLC manufacturers use this method, but each manufacturer has developed its own version, thus requiring an international standard for ladder programming used for PLC programming. Therefore, in 1993 a standard was developed with the code 1131-3 of the International Electro-technical Commission (IEC). In 2013, the latest version is IEC 61131-3 version. Ladder programming uses graphical elements such as ladder diagrams, sequential function display and function block diagrams (Kiran, Sundeep, Vardhan, & Mathews, 2013).

2.3. SCADA Communication Network

The development of SCADA architecture dates back to the 1900s when telemetry was first used. Telemetry consists of transmission and data acquisition units from real-time sensor applications. The basic SCADA network consists of the receipt of the data collected in the study unit away from the central business units. MT computers allows the company to offer a form readable to the operator and field equipment and control devices, such as automatic meter reading and equipment status information in order to allow the inspection. MTU is the part that initiates almost all communication with all of units operating in the remote terminal (Patel, Bhatt, & Graham, 2009).

It holds the computer's central processing delivers the data to the underlying business operators MTU and decide which function is performed in the next step. Former networks of SCADA are intended to ensure functionality instead of providing credibility. Thus, MTU at 1200 baud (baud rate) sends a command via communication channels and RT function executes the command only detects new data and sends it back again MTU. RT none of the local intelligence unit (measurement data, prior to further processing ability in the same device) does not possess.

With the improvement of present technologies of communications and communication channels' systems are replaced by new technology. Therefore, due to speed up communication channels and make the RTU units smarter, all processing power is realized over SCADA networks. IEDs (Intelligent Electronic Devices) RT with the development, began to have more intelligent processing power. IEDs can run independently of simple logic process that does not require server. Therefore, RT device, system protection, such as data acquisition subsystem of the local processing capacity and allows for performing multiple functional operations. SCADA is given in Figure 2.7 where the communication infrastructure of system components.

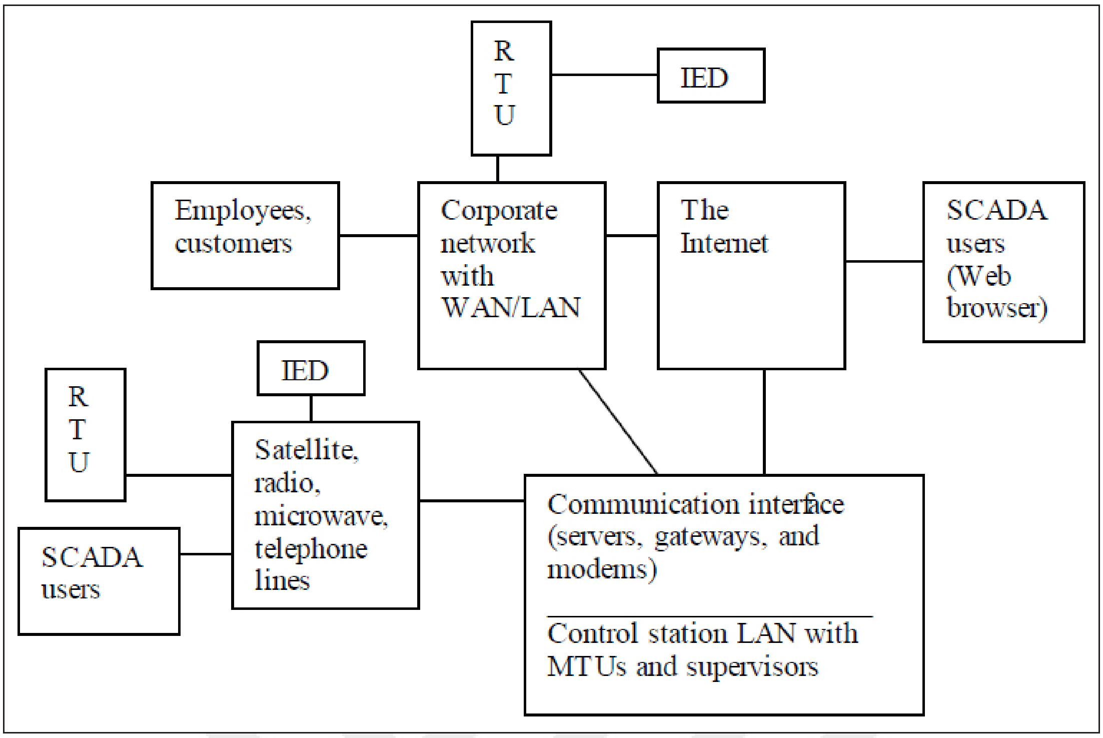

R
T
U
IED
Employees, customers
Corporate network with WAN/LAN
The Internet
SCADA users (Web browser)
IED
R
T
U
Satellite, radio, microwave, telephone lines
SCADA users
Communication interface (servers, gateways, and modems)
Control station LAN with MTUs and supervisors

Figure 2.7. Modern SCADA Communication Architecture (Patel, Bhatt, & Graham, 2009)

2.3.2. SCADA Communication Network

SCADA systems are designed using open or proprietary communication protocols to communicate between the MTU and one or more RTUs. SCADA protocols substation computers, RTUs allows the transmission characteristics for communication with each other IEDs and MTU. Most SCADA communications protocols used are as follows:

- DNP3 (Distributed Network Protocol Version 3.0)
- Modbus
- Profinet

A series of port-based searches have been made within the scope of the thesis with the Shodan search engine, which will be explained in detail in the following sections. Thus, the usage rate of the protocols used in the communication of SCADA systems was made by country and statistical information was obtained by giving the usage rates of these protocols in the world (SHODAN, 2009). This information will not give any real results in order to Shodan identifies the services open to the Internet. But this information will be an important guidance for SCADA statistical information of the protocols used in the system.

In the Shodan search made within the scope of the thesis, the default port numbers of Modbus TCP, EtherNetIP, Profinet and DNP3, which are used in the communication of SCADA systems and used by internet field devices i.e. RTUs, were searched. Obtained results; utilization rates of the protocols, the country shows to what extent it is used in some countries and the countries in which the rate at which our world SCADA communication protocols in use.

According to Figure 2.8, the default port numbers used by SCADA communication protocols in Shodan search engine were scanned and the distribution rates of these ports according to countries were taken. According to this information, the US and China have a significant task in the communication of the industrial dynamo system. In our country, the number 2731 is used at a rate of 1%.

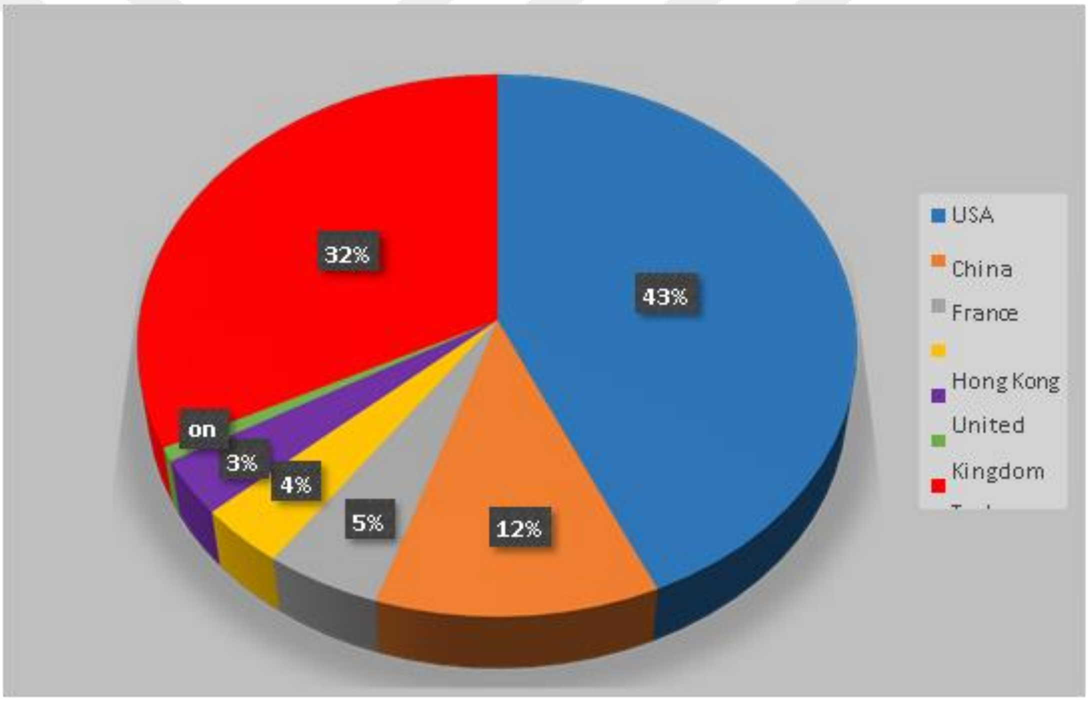


Figure 2.8. Distribution rates for SCADA communication protocols country

The most frequently used protocols rates in industrial control sector according to Figure 2.9 is obtained. This information has been recognized by the Modbus TCP protocol as used in half, with rates of 15% and 5% Profinet and DNP3 protocols are used.

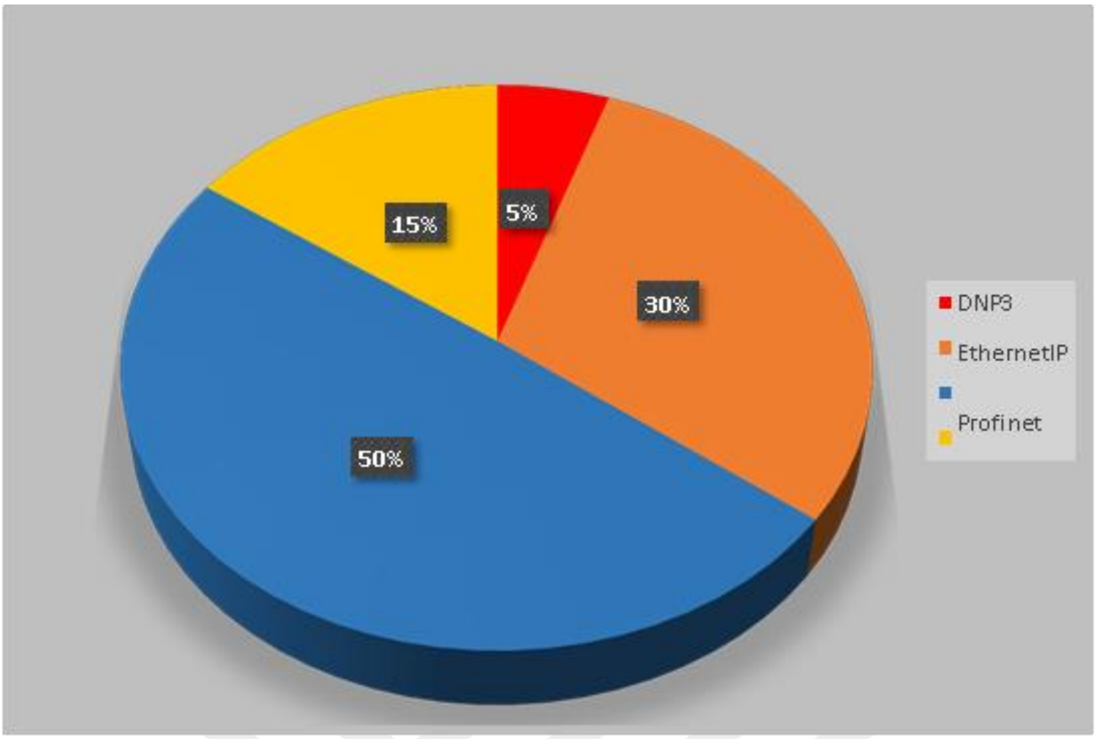


Figure 2.9. Distribution SCADA communications protocols

Figures 2.7 and 2.8 clearly show that there is a half-use rate of the Modbus TCP protocol in the communication of SADA systems in EKS networks. This statistic which was obtained, shows that the impact of cyber-attacks on Modbus TCP protocols will be more widespread in the world and in our country. For this reason, a security proposal which will be developed for the Modbus TCP protocol will make SCADA systems' security used in the worldwide ICS network more effectively.

DNP3 (Distributed Network Protocol Version 3.0)

DNP3 protocol; MTU, RT is a telecommunication standard that defines the communication between IEDs and devices, achieve the interoperability of electricity companies and has been developed by Harris Controls Division for SCADA applications (Clarke, Reynders, & Wright, 2004).

One of the most important features of the DNP3 protocol is not supported by the significant number of open source and producers. The many different manufacturers thanks to open source DNP3 protocol specifications provide many conveniences to users (Bhattacharyya, 2008)

- Open source based.
- Many suppliers provide the joint operation of the device.

- It is supported by many hardware manufacturers.

- IEC has the appropriate tier architecture model architecture for improved performance.

- It was optimized for secure and efficient SCADA communication.

- Comprehensive application is supported by testing standards.

- It submits the capability to choose from multiple suppliers for future system modification and expansion.

DNP3, MT (control center) and other specific devices (RTU, IED) supports 3 basic modes for communication (East, Butts, Papa, & Shenoi, 2009).

1. One-way process; MTU addressing specific device sends the request and returns the response message these devices.
2. Publishing process; MTA sends a general message to all remote terminal device and cannot wait for the return of a response message.
3. Upon request transaction; Fields is a periodic update or warning devices such as information sent by the process.

DNP3 network configuration

DNP3 protocol supports several network most common configurations is shown in Figure 2.9.

1. Literal configuration: a master and a tool divide a single connecting line. This is like a connection between two devices, such as a dial-up connection.
2. The multi-link configuration: one master and used in places where many of the most widely used field device configuration. All field devices receive all incoming requests by the master, but each field device returns only respond to messages addressed to him.
3. Hierarchical Configuration: One device act as a field device in a segment and the other segment of the master and so this is a device bifunctional. This device can also be called sub-master.

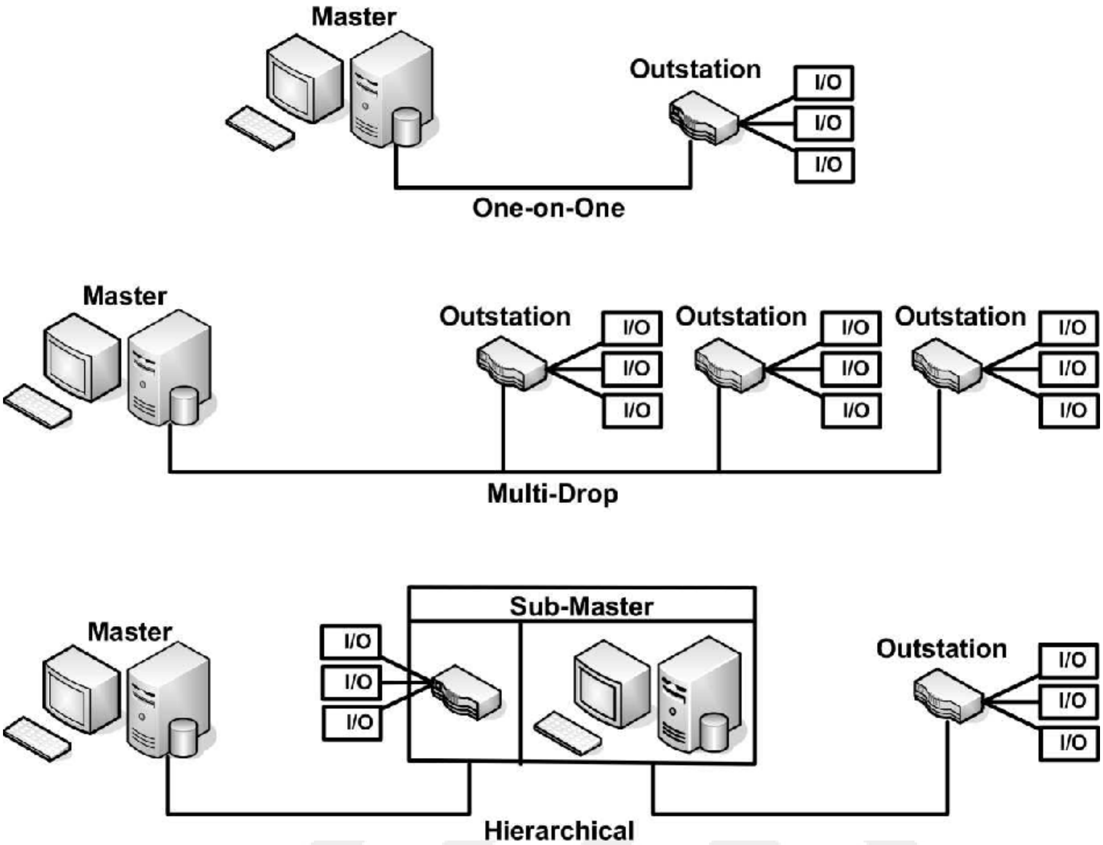


Figure 2.10. DNP3 network configurations (East, Butts, Papa, & Shenoi, 2009)

DNP3 protocol is designed to combine multiple layers. 3-layer "Improved Performance Architecture" (EPA), 7-layer is formed by removal of unnecessary layers in the model. However, in the EPA model, the layer of implementation does not receive large messages from the information link layer, so a new layer called the "pseudo transport layer" has been added to overcome this disadvantage. DNP3 protocol layers shown in Figure 2.10.

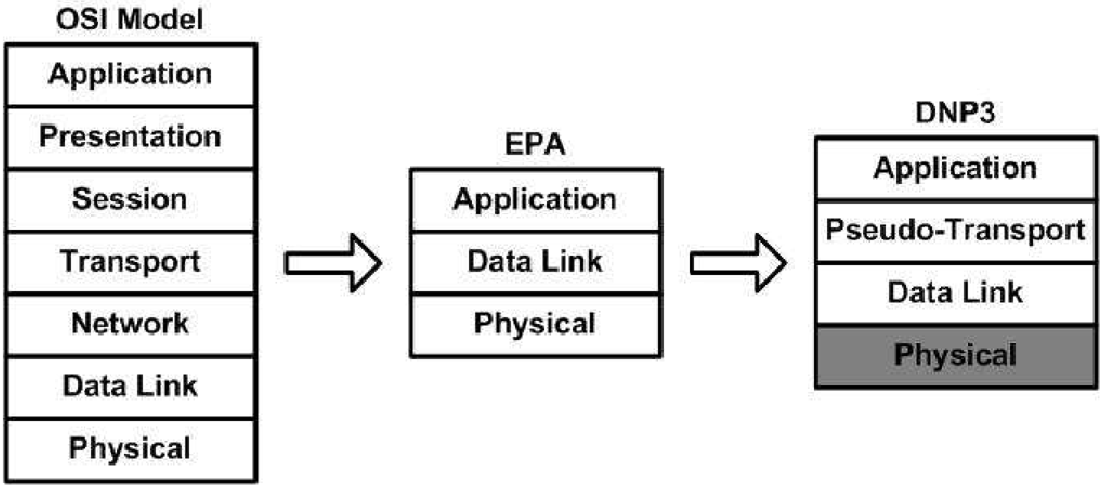


Figure 2.11. DNP3 transition design from OSI (East, Butts, Papa, & Shenoi, 2009)

DNP3 physical layer

DNP3 protocol layers are gathered on a physical layer's top which is in charge of transmitting messages over physical media such as radio, satellite, copper or fiber. Physical layer settings send electrical signals between devices, decides the timing and voltage values. Physical layer; (Send data) (receiving data), (attached), (disconnect), (status update), include 5 service runs.

DNP3 data link layer

The information link layer’s function is to provide a reliable logical connection between the devices in order to transfer the data frame sequentially. The data connection consists of two parts, a fixed header of 10 bytes and a payload of data. Payload top two layers (false transport layer and application layer) framework is activated. Areas length gives the number of bytes remaining. Excluding the CRC data section (data section) maximum length is 250 bytes (16-bit CRC field for every 16 bytes of data - 282 bytes). Therefore, the data link frame is at most 292 bytes.

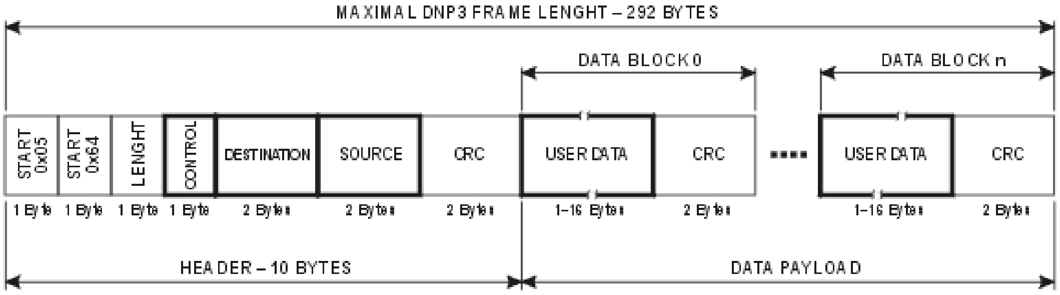


Figure 2.12. DNP3 data link layer frame structure (RACOM, 2014)

The header section consists of the start bit, which is a fixed array for specifying the beginning of the frame. 0x05 and 0x64 consist of 2-byte values. The functions of the link control area help ensure the sequence of the frames, the flow of the control message and the detection of the frame function. The data in the control area assists to determine whether the tool is a main or field tool and ensures a rational connecting between the two devices. The address of 16-bit destination which is located in the information link layer contains the address to be sent and the address of 16-bit source defines the origin. In addition to this, the 16-bit CRC is located in the connection field to confirm the transmission's unity.

DNP3 fake transport layer

The functions of the counterfeit transport layer are fragmentation and reassembly of the packets. This makes it possible to get more frames can carry data link layer of the application layer. Thus, the application layer frame is elaborated in more than one frame. As shown in Figure 2.12 2-byte transport layer in a false "start" and "end" has frames. Each is 1 byte and contains the flags “FIR” and “FIN. These flags indicate the first and last frames of the messages that are broken respectively. A serial number shown for each successive frame (sequence number) of the message for processing by the application layer is used for reassembly (Makhija & Subramanyan, 2003).

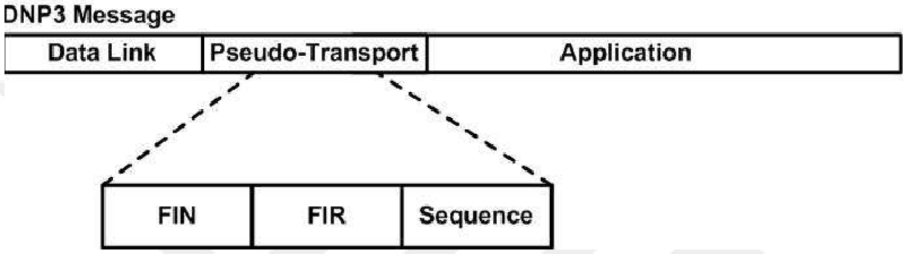


Figure 2.13. DNP3 carrying a fake message field

DNP3 application layer

The application layer’s basic function is to recognize whether the master or slave for each device. DNP3 sends formats for request and response messages. Request message to the master device is sent by the field to bring some calculations or edit tasks such as setting limits. Once this layer fragmentation of messages exceeds the maximum size determined by the receiver's memory size is divided into smaller packets. Normally fragmentation size is between 2048 and 4096 bytes.

Application control of the first and last segments of the transport layer is the same as sending fake messages in the function. Function code area carries the information, what is the purpose of the message. This area is in both the request and response messages, but the use of function codes is different because of their different functionalities. Request for a total of 23 messages defined function code is available. These transfer functions, control functions, freezing function, application control function, the function and configuration can be classified as the time synchronization function. 2-byte internal indicator to determine the function code (internal indicator) are heading. Next item, which transmits the encoded data presentation data objects (data objects). There are many data objects defined, so you can establish interfaces with most systems and binary inputs, binary outputs, can communicate a variety of variables, such as analog input and analog output (Makhija & Subramanyan, 2003). DNP3 protocol use the function codes are given in Table 2.1.

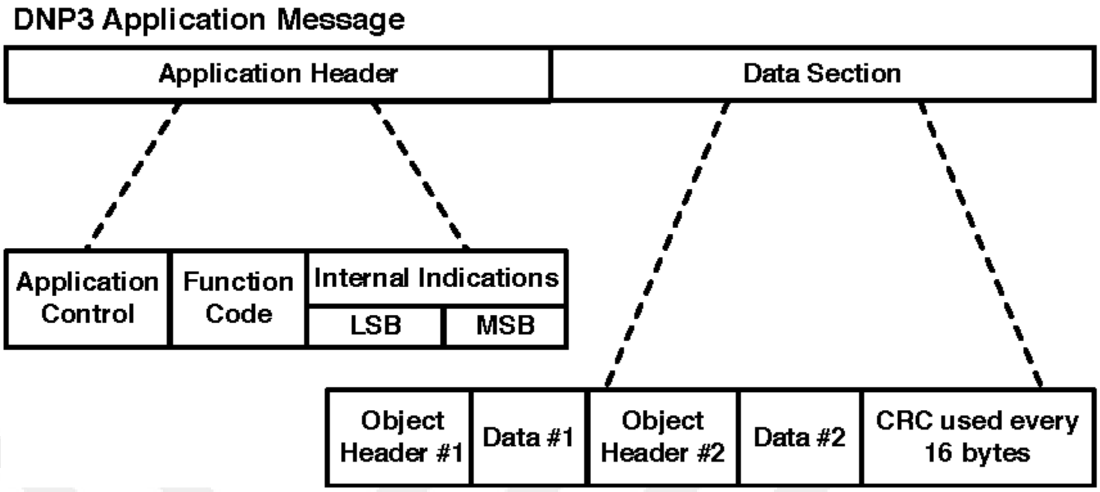


Figure 2.14. DNP3 Application Layer Header

Table 2.1. DNP3 Function Codes

Function Code	Explanation	Function Code	Explanation
0	Credentials	10	Start the application
one	Read	11th	Start the application
2nd	Summer	12	Stop Application
3	select	13	Save configuration
4	operating	14	Enable unwanted
5	Operate with direct confirmation	15	what is not desired activation
6	Operate without direct confirmation	16	assign class
7	Freeze the approval process	17	Time delay

8	Freeze process suddenly without confirmation	18	Save current time
9	Freeze and clear process with confirmation	19	Open file
A	freeze the process and clean without confirmation	1 A	file Close
B	timely freeze	1B	delete file
C	Without timely approval turn	1C	Fetch file information
D	Cold boot	1D	File Configure identity
E	Hot restart	1E	Cancel file
F	Start Data		

Modbus protocol

The protocol of Modbus is a protocol which is developed for specific SCADA and have started to become industrial standards. Many manufacturers use this protocol to develop systems and devices operate production (MODBUS, 2006). Modbus is the application layer messaging protocol for client / server communication between connected devices in different types of networks. Figure 2.14 Modbus communication structure is provided. in the present embodiment is used as follows:

- TCP / IP-based communication via Ethernet,
- through different media (cable: EIA / TIA-232-F, EIA-422, EIA / TIA-485-A, fiber optic, radio, ...) asynchronous serial communication,
- Modbus Plus provides a communication via a rapid token passing network.

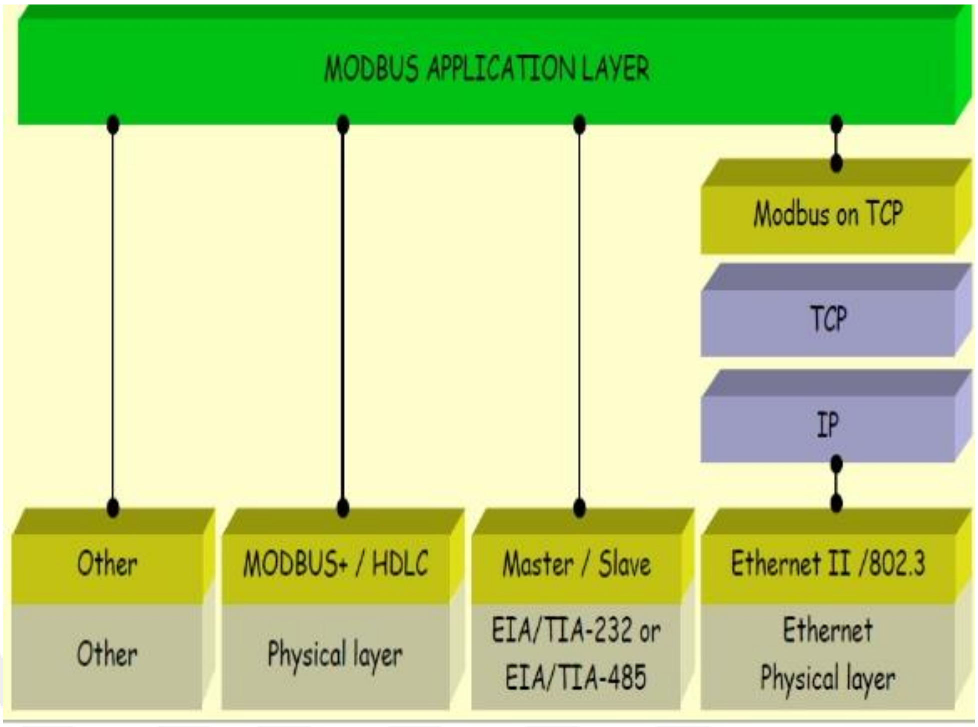


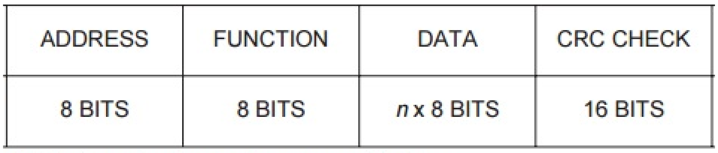
Figure 2.15. Modbus Communication Structure (MODBUS, 2006)

The Modbus protocol works according to the master / slave principle, which sends the request message to the specific RTU and sends it back in response. It does not get any answer if it is broadcast type. Data can be sent and received in two transmission modes - ASCII - readable and RTU - tight and fast. RTU is preferred because of that it has a shorter frame and is parity check, error check, or CRC. ASCII mode slows down the system because of that it has a longer message frame. Modbus protocol, Modbus serial and Modbus TCP has two variables being. IP-connected networks running Modbus TCP, the superior processing feature allows multiple master and RTU allows parallel processing of multiple servers to run. Basic functions of Modbus protocol are as follows:

- control winding or set of windings and a single set of commands for reading
- input control commands to read the input status of input groups
- register control commands to read and set the pending registers
- Error detection and function test report
- The program functions
- Inquiry control functions
- reset

Modbus Specification

The Modbus protocol message structure is shown in Figure 2.15.



ADDRESS	FUNCTION	DATA	CRC CHECK
8 BITS	8 BITS	*n* x 8 BITS	16 BITS

Figure 2.16. MODBUS Message Structure

The message structure's first area is the one-byte field where the address is stored. The request frame includes the destination address's IP address, which is aimed, and the response frame includes the IP address of the master. The Modbus protocol can have up to 248 slave devices, but in practice it is connected to a single master, 2 or 3 slave devices. The second field contains the functions to be implemented on the target device. In the request frame, this byte defines the function of the destination to be applied. If the request is successfully completed on the destination station, the function field is recalled, otherwise the leftmost bit is sent, thus returning the problematic response. The third field is the data section, which is the variable in the function code. The last two bytes are the CRC field for error checking in the frame. The function area where the function codes are located is shown in Table 2.2.

Table 2.2: Function Codes in Modbus Protocol

Code	hex	Function	type	
01	01	Read helices	Single-bit access	
02	02	Read discrete inputs		
05	05	Write wrap Single		
15	0F	Multiple wraps summer		
03	03	Waiting Read registers		
04	04	Read Input registers		
06	06	written by writing Single		

16	10	Multiple writing by summer	16-bit access	Data access
22	16	Masks writing Writing		
23	17	Multiple registers read / write		
24	18	read FIFO query		
20	14	Read the file record	Recording file access	
21	15	File record summer	Fault Detection of	
07	07	Read exceptional case		
08	08	Fault detection		
11th	0B	receive the communication event counters		
12	0C	receive the communication event log		
17	11th	Server ID report		

Modbus TCP protocol

This protocol works with both LAN-based and IP-based networks shown in figure 2.16. The main device via the IP-based networks was shown to be due to several slave devices. Modbus TCP protocol, the slave device slave devices only when the server is designed as a passive process intended as the main instrument for his client. Modbus TCP/IP (also Modbus-TCP) 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. TCP/IP refers to the Transmission Control Protocol and Internet

Protocol, which provides the transmission medium for Modbus TCP/IP messaging. 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.

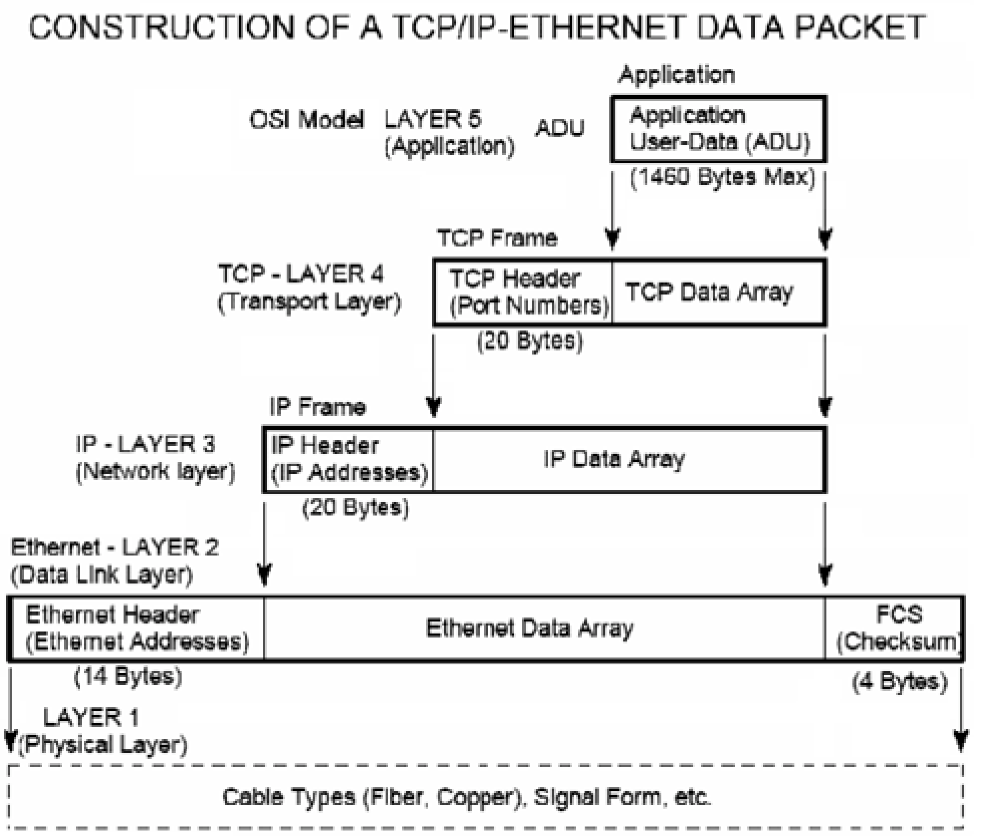


Figure 2.17. Modbus TCP architecture (MODBUS, 2006)

Because of that the Modbus TCP protocol messages that encapsulate TCP packets in a TCP PDU (Protocol Data Unit), Modbus application protocol (MBAP) hosts. The

MBAP header contains four fields: protocol identifier, process identifier, length unit and unit identifier. Request identifier and the protocol identifier of the process which are carried out by matching the response MBAP double header (0 for Modbus) protocol encapsulated by the application shows. Unit identifier shows slave devices related with process and is utilized just for legal systems. The area of length indicates the number of remaining bytes of the data packet.

Profinet protocol

Profinet is an open industrial Ethernet standard developed by the World Profibus Association, Profinet manufacturers and users. Profinet is standardized to IEC 61158 and IEC 61784't. Real-time Profinet requirements cover a great number of applications.

Profinet is the continuation of Profibus, one of the most used field communication standards. Profibus is the serial industrial communication standard used for more than 25 years. Today, the two variations of Profibus are utilized. Some of the most frequently encountered Profibus DP (Decentrilized Peripherals - Decentralized Peripheral); simple, low cost, with high-speed communication capabilities. Other variations Profibus PA (Process Automation - Process Automation); more technology-based applications. Profibus uses technology of master / slave communication in combination with switchgear between master devices (Patel, Bhatt, & Graham, 2009).

All Profinet device is designed as active or inactive compared to the surrounding industrial process. As network devices used in real-time requirements can be used.

Profinet's development began in early 2000 and the first technical feature of the Profinet CBA (component-based automation) unless otherwise published. Profinet CBA over TCP / IP communication from machine to machine and which is object-oriented program. It is also compatible with all network devices. The other Profinet version is Profinet IO with Profinet RT and Profinet IRT.

Profinet versions

Profinet IO and Profinet Profinet including CBE's are designed for communication between these two versions of the controller and the IO devices in real-time requirements of Profinet version shown in Figure 2.17.

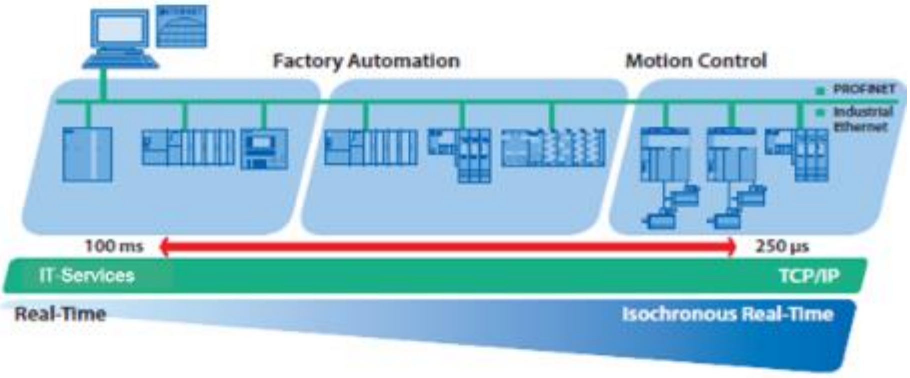


Figure 2.18. Real-Time Requirements of Profinet Version (SIEMENS, 2008)

As shown in Figure 2.17, Profinet CBA is mainly used in non-Real-Time environments, while Profinet RT is used in automation of process and factory and in implementations of motion checking that receive the most demand, such as robots in Profinet IRT assembly lines.

Profinet CBA

Profinet CBA, also known as Profinet Class A, is an object-oriented program designed to communicate from machine to machine over TCP / IP. The basic idea behind the Profinet CBA is the implementation of intelligent and autonomous subsystem that can communicate with each other via the controllers.

Automation is the concept of using symmetric and asymmetric communication with Profinet CBA 10-millisecond response time. Only TCP / IP communication systems support the Profinet CBA response time of 100 milliseconds and above when used (SIEMENS, 2008).

Profinet IO

Ethernet connected directly to the distributed I / O devices that use Profinet IO Profinet systems are called. Manufacturer has sent the data to be processed in consumer producer / consumer model is used. In Figure 2.18, the model that is used by Profinet, is mentioned.

IO controllers are devices that automation program, such as a PLC. The outputs of the IO devices are managed by the IO controllers. distributed by one or more IO controller IO device is connected through IO Profinet I / O operates as a field device.

IO Manager program, such as error messages and engineering tool, is used for parameterization. IO Manager program can be a computer or HMI for commissioning or diagnostics purposes (PHOENIX CONTACT, 2010).

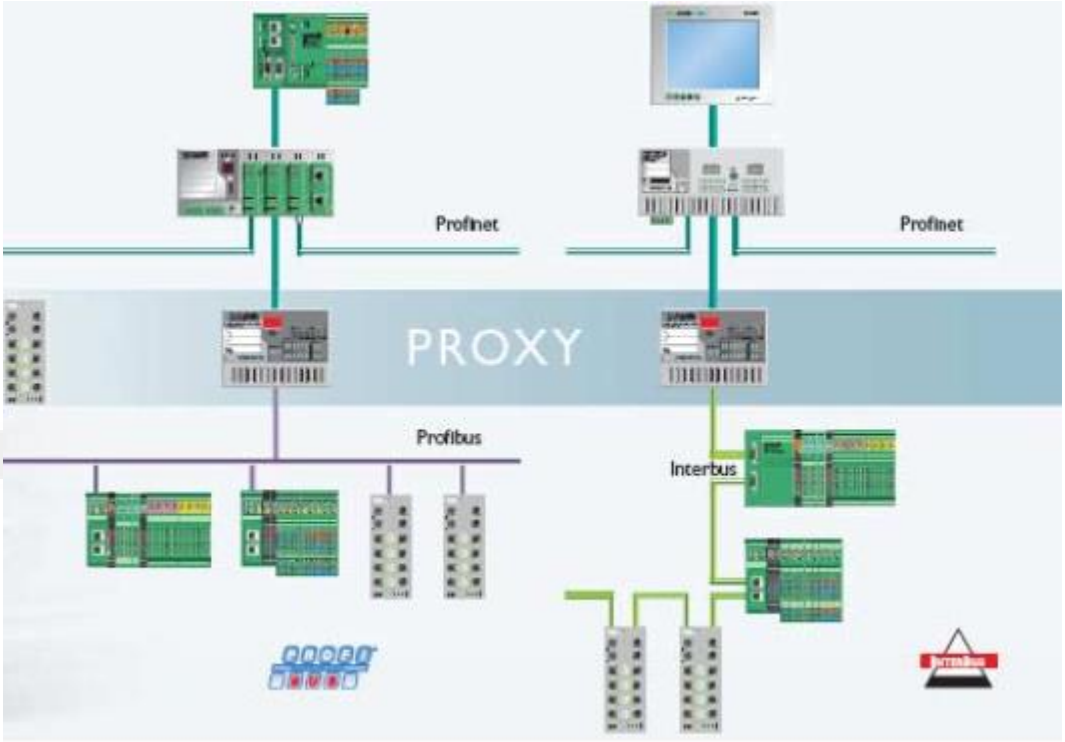


Figure 2.19. Profinet IO communication path (PHOENIX CONTACT, 2010)

In Profinet RT, which is known as Profinet Class B, data communication takes place via OSI layer 3 and layer 4 in parallel to TCP / IP. Each device receives an IP address through TCP / IP, which allows communication over other protocols, such as HTTP. Figure 3.19 shows the Ethernet frame and protocol structure in Profinet RT communication.

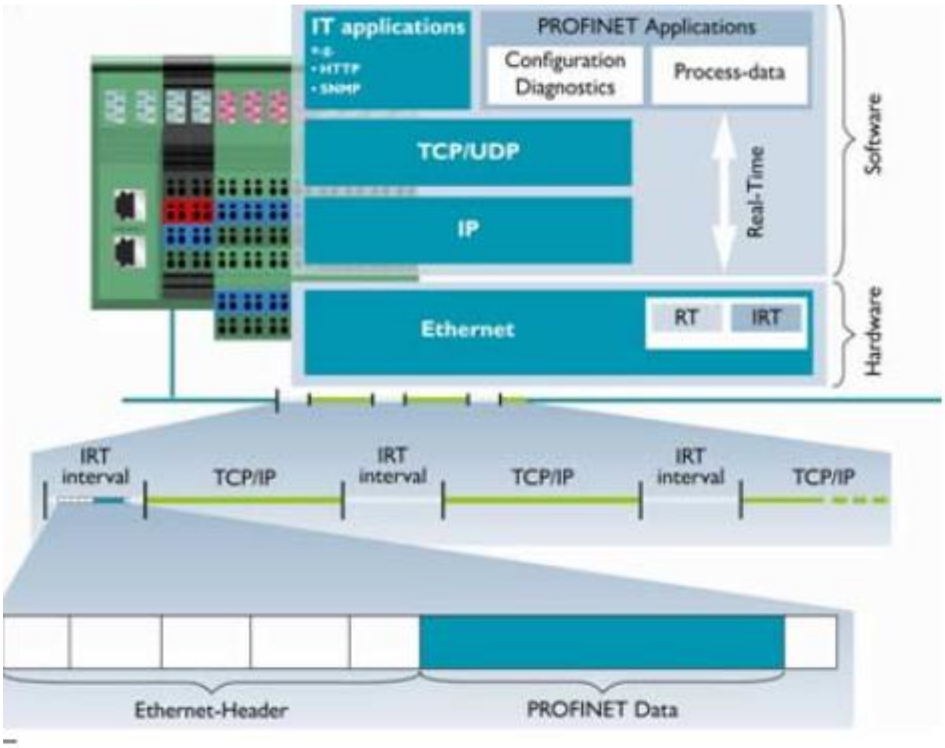


Figure 2.20. Profinet RTU Data Transfer in the Ethernet Frame (PHOENIX CONTACT, 2010)

The Ethernet frame exists of Profinet data parts and an Ethernet header. The roll-out label for Profinet real-time messages is placed in the Ethernet header. The roll-out is applied by appointing VLAN ID 0 and priority sequence 6. It indicates that it communicates with Profinet RT or IRT with Ethernet type 0x8892.

Profinet IRT which is accepted as Class C, is utilized when real-time processing is most required, such as motion checking implementations. The features are the same as Profinet RT, but are enhanced with special hardware for real-time performance. Profinet IRT suffers tools on the Profinet network for synchronizing communications by using technology such as time zones. The time zone technology here specifies a slot for the IRT data and clock signal in each communication cycle.

They used in most need of real-time process when needed PROFINET IRT Profinet class known as motion control applications. Features are the same as Profinet RT real-time has increased, but a special hardware in terms of performance.

Profinet IRT Profinet allows the devices in order to synchronize the communication network using technologies such as time zone. the time frame technology wherein IRT specifies a slot for data and clock signals in each communication cycle. Profinet IRT and RT communication OSI layers 3 and layer 4 protocol uses the structure. Thus, all the TCP / IP protocol structure is circumvented and will not receive an IP address. RT and IRT communication are limited to a single logical subnet.

In this section, the software and hardware architecture of the MTU, RTU, PLC, and DNP3, Modbus and Profinet components which are the most commonly used communication protocols in EKS systems are mentioned. According to the analysis, Modbus is one of the most common protocols in EKS systems and the risks that may arise as a result of threats to SCADA systems using this protocol can affect large areas. In order to reduce this risk, the security of Modbus protocol is discussed in the thesis.

CHAPTER 3
SCADA SYSTEM AND CYBER SECURITY

Although SCADA processing system is designed, it operates as an independent unit in a corporate environment. The most important objective of the control system design is efficiency and safety. SCADA provides to remote access to perform a routine maintenance operation seen in other cases the system. While designing SCADA communication protocols, security features are kept in the background. Such vulnerabilities in critical infrastructures have made critical infrastructures more vulnerable to cyber-attacks. The attackers, attacks exploiting the vulnerabilities performs. The effects and results of these attacks are discussed below (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015):

- Physical effects: the results of the inactivation of SCADA systems are considered in this field. This effect is most important result is that the results would endanger human life. Other results in data loss and harm to the environment.

- Economic impact: Economic effects occur after cyber-attacks. Physical serious economic losses in an effective ripple effect of the plant or company brings. Greater local impact, causing economic losses to the national and even the global economy.

- Social impacts: the physical and economic damage will be the result of damage to public confidence and national security. Social effects may become depressed may lead to public safety or increasing popular extreme.

A common security threats and in a more secure SCADA due to the size of the outcomes of their attacks on various institutions and organizations in order to improve the system to make extensive studies and research against attacks on SCADA systems.

In the literature, the most recent statistics of the vulnerabilities identified in the SCADA system shown in Figure 3.1 is formed in the vulnerability information system is understood to significantly increase. The last 15 years have been identified in open security are perceived to be approximately 12-fold growth. integrated with information technology employees SCADA systems it is also directly affected by this threat.

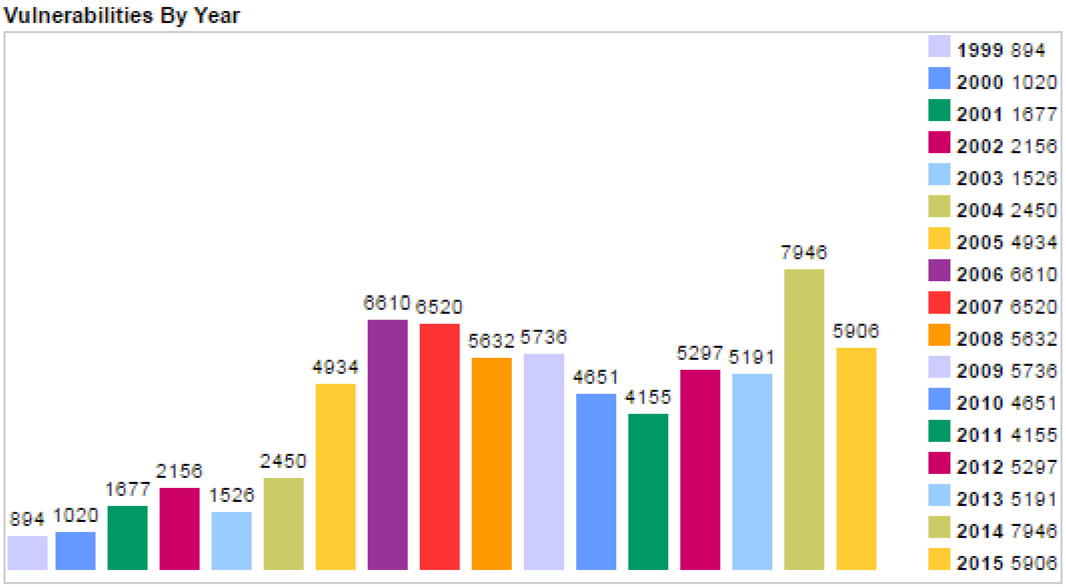


Figure 3.1. In some years, the change in vulnerability (Risk Based Security, 2015)

SCADA systems vendors' SCADA systems are separate and independent from each other physically wrong thinking is a general thought. Many SCADA systems were built before the network components and were designed to be separate from the rest of the network, convincing system administrators that there would be no access to these systems from other corporate networks or access points. Unfortunately, this idea is completely wrong. The real scenario is bridged due to the changes that occur in the SCADA network management information and corporate networks. Who played an important role in this change are described below (Amanullah, Kalam, & Zayegh, 2005):

- The first change is the increasing demand in the enterprise network that allows SCADA engineers to connect to the system for remote monitoring and control of the system from the access point.

- The second main reason is access to information to help a corporate decision. Many public institutions have corporate connectivity permission to SCADA systems, such as providing critical access to critical information and functional status for better management or corporate decision-making.

Another major misconception about the SCADA system is " The connection between SCADA systems and other corporate networks are protected by strong access control". Many links between the corporate network and SCADA systems require system integration with different connection standards. Because network administrators ignore network access keys, access control designed to protect SCADA system from unofficial accession over corporate networks is generally minimal. Firewalls and intrusion detection systems (IDS) is recommended for use with strong password protection.

3.1. SCADA System Vulnerabilities

Idaho National Laboratory (INL) report to the US Department of Energy's Electricity Distribution and Energy Security Department that aims to ensure the safety and flexibility of the national energy infrastructure against cyber-attacks through the National SCADA Test Assembly (NSTB) program (IDAHO NATIONAL LABORATORY, 2011). The main objective of this program is to take precautions against attacks SCADA approach to identify and mitigate the effects of attacks by analyzing the vulnerabilities in the system. The vulnerabilities were exploited in the realization of cyber-attacks against SCADA systems are classified and analyzed in the report. Although the related report was published in 2011, the information and the results obtained were the most comprehensive of the technical studies related to the cyber security of SCADA systems in the literature and this report was used in this thesis. In Figure 3.2, the percentages of the vulnerabilities observed according to the NSTB are given.

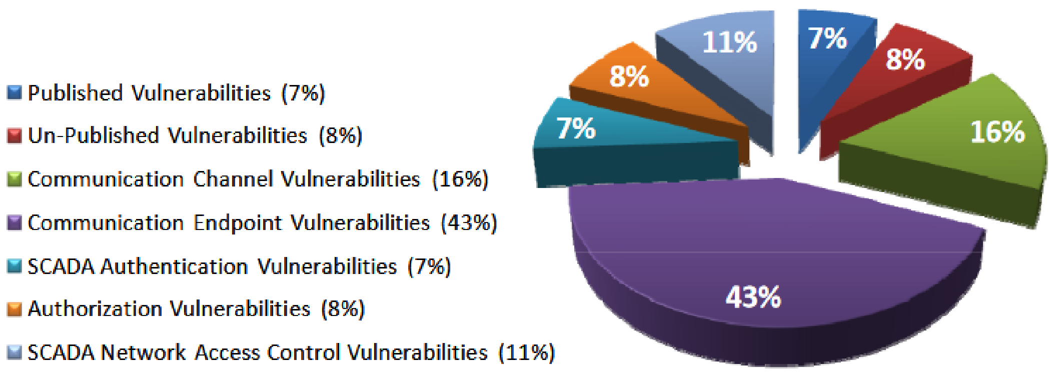


Figure 3.2. NSTB SCADA vulnerability frequency (IDAHO NATIONAL LABORATORY, 2011)

Many of the vulnerabilities shown in Figure 4.2 are buffer overflow. For example, in an illustrated embodiment, 50 out of 50 attack vectors have detected memory overflow, all of which have been calculated as a single vulnerability. A single authentication bypass technique was also calculated as a vulnerability.

A single vulnerability in SCADA system may be much more extensive critical or large compared to other systems. For example, a SCADA system may affect the whole vulnerability of a communication channel in the protocol, which is regarded as a weakness.

Assessment team and SCADA manufacturers of experience with a defined NSTB reviews seize the SCADA system, likelihood and impact of some of the evaluation objectives (which cause serious effects on the control system entry point, processes, protocols, ...) it was given priority. SCADA vulnerability types in Table 3.1 and described evaluation target on basic SCADA functions can access

Table 3.1. Openings and Related Assessment Objectives can access the Basic SCADA Functions (IDAHO NATIONAL LABORATORY, 2011)

Vulnerability Type	Rating Target Category	Source Vulnerability
Known Vulnerabilities	Best Possible Ways to Attack	SCADA products it added the old or unpatched third-party applications
		SCADA Servers Operating Systems running on unpatched
Unpublished Vulnerabilities	0-day or unpatched Potential Vulnerabilities	Unnecessary Services Do not leave out in the open SCADA Servers
		Incorrect SCADA Code
Communication Channel Vulnerabilities	Vulnerabilities in the SCADA communication channel functionality through Unauthorized Access	weakness hosting remote access protocols against spoofing and intrusion attacks
		SCADA communication and data transfer protocols

Communication Endpoint Vulnerabilities	Unauthorized access to the SCADA server or application or DOS	Applications for hosting server weakness
		Database Security deficits

According to the results of the evaluation NSTB SCADA functions to assign risk and capable of preventing or may disrupt communication to SCADA server vulnerabilities have been identified and analyzed capable of providing unauthorized access to applications or data. The vulnerabilities are described as follows.

3.1.1. Source Code Design and Implementation

SCADA vulnerabilities in applications and services is required to minimize the secure coding. Vulnerabilities in the software can be exploited for malignant aims and make the SCADA system vulnerable to attack, thus administrators of system may hesitate to make changes after the initial configuration (Centre for the Protection Of National Infrastructure, 2011).

SCADA software inspection and reverse engineering shows that the work is always done in a secure SCADA software concept. SCADA software deficits monitored in NSTB evaluations were found to be the result of insecure software and insufficient tests. The three most important openings observed were; input certification, authentication and accession checking. Many of the vulnerabilities in NSTB assessments can run remote code that causes dangerous functions.

SCADA software can be large, complex and legacy code-based, and SCADA operations may require high availability and scenarios of update can be complicated. Unlike standards for software models of ready-to-use computer, maintenance, security correction costs and support have traditionally been transferred to SCADA users. Publication of SCADA product vulnerabilities can find code checks and associated code alterations with a new necessity for SCADA security.

The sources of safe code can be reached whole languages and application types. CWE (Common Weakness Enumeration) list (OUCHN, 2015) of many known SCADA programming errors, including information about all of software vulnerabilities are shown in Table 4.2.

Table 3.2. SCADA unsafe code design and known apertures in the application (Alves, 2014)

Openness Classification	Known openings
CWA-19 Data Processing	CWE-228: invalid syntactic structure of incorrect handling of the
	CWE-229: Value of improper handling of
	CWE-20: Incorrect input validation
	CWE-116: Incorrect coding
	CWE-198: Incorrect use of byte order
CWE-119: error in processing memory limit restrictions	CWE-120: Introduction copy size control without memory (memory overflow Classic)
	CWE-121: Stack-based (stack-based) memory overflow
	CWE-129: Array index faulty verification
	CW-190: Integer Overflow or delete
	CWE-680: Integer overflow or memory
CWE-398: bad code quality indicator	CWE-454: Starting from the outside of trusted devices or data
	CWE-456: Missing start
	CWE-400: Uncontrolled resource consumption
	CWE-252: Unchecked return value
	CWE-772: Missing resource to be published
CWE-442: Web Problem	CWE-22: Restricted to a directory path name incorrectly limited lease (Road Crossing)
	CWE-79: Web page error protection area (XSS)
	CWE-89: SQL query structure protection error (SQL injection)

3.1.2. Memory Overflow (Buffer Overflow)

Memory overflow vulnerability stems from the most common SCADA input validation weaknesses in the system. Memory overflows occur when the software writes more data to the memory than the space assigned in the memory. “Extra” information overwrites the adjacent memory and induces the program to run out of regular functions. Writing carefully planned and executed memory causes the program to be executed by the attacker. Using the buffer overflow to send malicious code exploiting command with an interactive session to create the program's authority and abused.

Memory overflow stopped by changing the input value during the data transfer process is performed by applications in network traffic being exploited. As a result, network protocol applications without the verification of input values are vulnerable to memory overflow attack (Zhu, Joseph, & Sastry, 2011). For example, developer, no one can consider whether to create characters as the username longer than 1024 characters. If the developer creates 1024 bytes of memory for the user name and does not verify input, an attacker could try many user names to discover more than 1024 characters. The developer can close the gap by validating the input size so that it does not exceed the size assigned for the memory stored in the field of input.

3.1.3. SQL Injection

The SQL injection vulnerability caused by incorrect or inadequate filtering of user inputs that do not guarantee the unity of the private characters utilized in the SQL query command can affect the SCADA history database. For example, if an attacker to add an escape character is ready to query database information, database offensive random read / write access can provide. The SQL command is utilized to communicate with the database. At the same time, SQL queries can be utilized for safety checks, such as authentication, so attackers can change the logic in these queries to circumvent security (Eden, et al., 2015).

SQL injection vulnerabilities exist on client (typically Web) implementations. SQL injection misuses the database by redirecting SQL commands to the database. It is SQL injection’s purpose if database-supported applications can retrieve information from the server on a safe network. For example, a client application can be secured over an isolated Web server in a DMZ, a physical or logical subnet, which includes services that are open to external networks and expose these services to a larger insecure network (usually the Internet). Even if the firewall blocks whole connections against to the server, an accomplished attack provides the attacker to check the SQL server on the safe network.

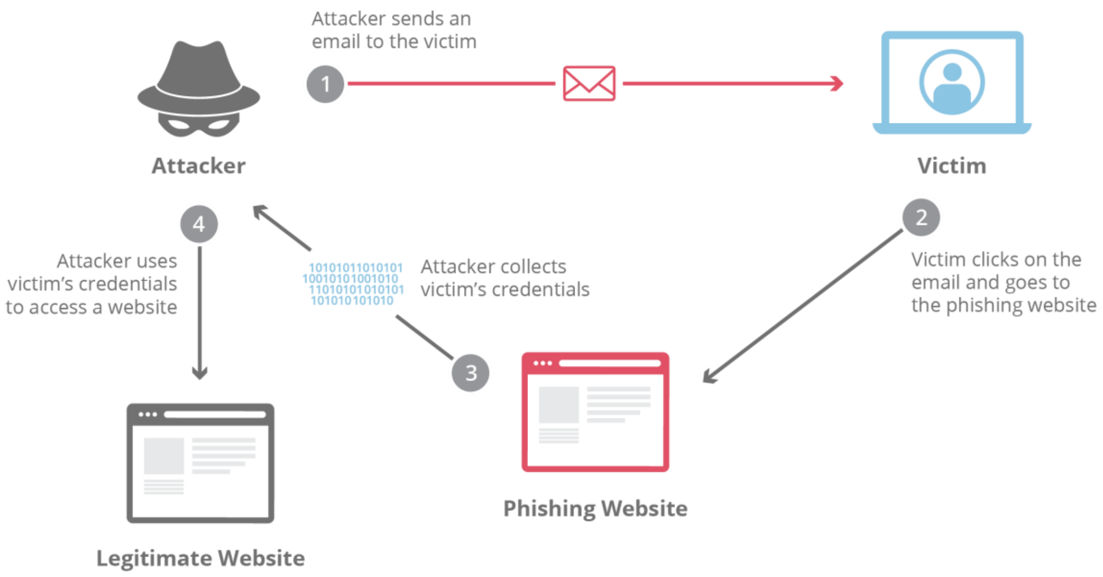

Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

Figure 3.3. SQL injection attacks via Web applications (REPUBLIC OF TURKEY Ministry of Transport, Maritime Affairs and Communications, 2014)

3.1.4. XSS (Cross Site Scripting) Vulnerability

The fundamental cause is due to input validation lack of XSS vulnerabilities as SQL injection. In addition to this, XSS attacks, malicious code in web implementation sends the user. 2010 CWE / SANS 25 Most Dangerous Programming Errors in the report (Martin, Brown, Paller, Kirby, & Christey, 2011) was released as XSS most broadly utilized and serious programming errors. Code to the web page generated by the web application vulnerability the attacker is quite dangerous because it allows placement. The code of attack is operated by the user under the authority of the web server.

3.1.5. Unnecessary Ports and Services

Implementations and services operating on the system may obvious some network ports to communicate with the outside world. An attacker could gain reach to the SCADA system owing to an open port and gather data about the system. All of open port can suffer the attacker to send misuse code and to revoke information. If an attacker initiates a remote link to services that listen on reachable network ports, the attacker can settle itself on the aim network and aim all of services that listen on the local network servers. A vulnerable network implementation can be abused by an attacker and may raise malignant code to send unjustified information (Industrial Defender, 2012).

The more service that runs on SCADA servers, the more potential the SCADA system is exposed to. As a result, the necessary services and applications should be run on the SCADA system as much as possible so that unused ports will be closed.

3.1.6. Effective Patch Management Application

Operating system, services, effective managing of patch for users and third-party software is very important. SCADA product manufacturers in applying the patch so users can mitigate the vulnerability. Mitigation before application of security patches faster identification of clear and minimizes the risk of disclosure of the opening to be done. At the same time test their products on third-party manufacturers and then patches patch SCADA product base.

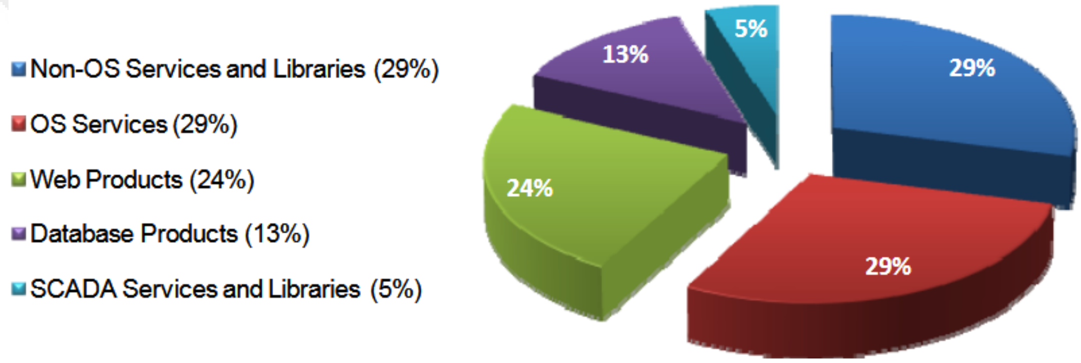


Figure 3.4. Unpatched Percentages of Components in the SCADA System (IDAHO NATIONAL LABORATORY, 2011)

Operating system patches allows attackers to run code on the running system is released to close the vulnerability. 2009 Cyber Security Risks According to the report (Nordlander, 2009), security is much more than the obvious discovered vulnerabilities in running systems for applications in recent years. As a result, the application program recorded in the attempt to attack more. Figure 3.4 shows the NSTB ratings are given in percentage of product present unpatched SCADA software system.

3.1.7. Communication Channels Vulnerabilities

SCADA systems, due to the increase of connection to the internet with the company intranet and external network are more exposed to cyber-attacks. Communication channels are important in this regard because they connect with different security domains will have the same access privileges and SCADA functions can be modified in order to manipulate the system. The following topics were examined for open channels of communication:

- SCADA collect personally identifiable information
- SCADA data and commands deception and manipulation
- DoS risking their communication to SCADA functions

SCADA system; network device management, IT protocols found in normal IT functions such as remote reach or transferring file are used. This protocol also applies to threats to SCADA systems. For example; SSH, FTP, Telnet, rlogin, and protocols such as transferring file and remote reach, can be used SCADA system network. It is important that these protocols are preferred. For example, communications protocols may be tunneled owing to SSH or http sent over SSL (HTTPS) (Graham & Patel, 2004).

3.1.8. Communication Protocols of Openings

From this subtitle DNP3 SCADA communications protocols listed in Section 2 below, is described weaknesses and Modbus TCP and Profinet protocol attacks.

DNP3 openings and attacks

DNP3 protocol attacks; protocol features are performed by exploiting weaknesses in applications or infrastructure manufacturers. Manufacturer of attacks on applications, configuration error takes the form of abuse of the system. Infrastructure attacks carried out by exploiting vulnerabilities in policies and platforms. The attacks perpetrated against the protocol specifications and DNP3 communication architecture is concerned with more structure. Attacks density MTU and RTU communication path is to be held for three goals. Thus, attacks by cutting traffic to the destination as shown in Figure 3.5, capturing, modifying and producing is performed again.

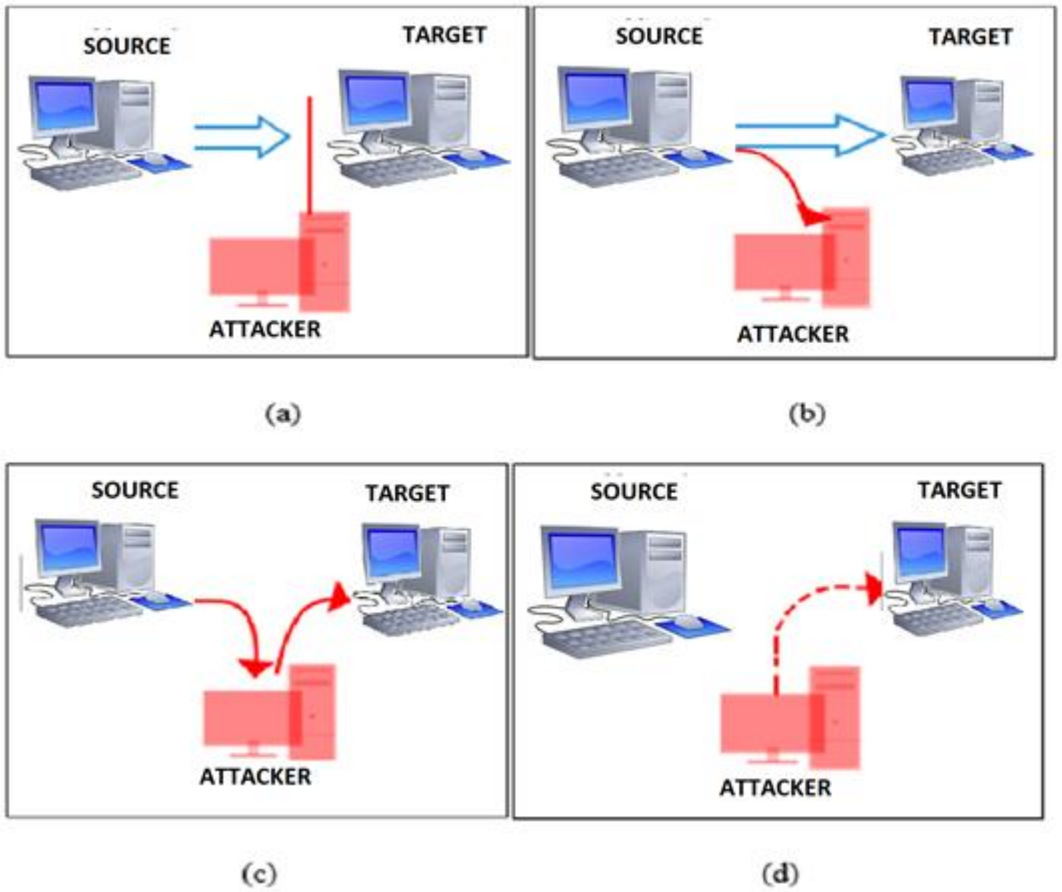


Figure 3.5. DNP3 Attacks (a) log (b) Capture (c) Switching (d) The regeneration

DNP3 authentication messages are sent without applying any prevention parameters, such as certification and encoding. Exploiting these vulnerabilities can completely mask systems running on the remote terminal, and malicious operations can be executed on those systems. 3 attacks that also affected the protocol layers are listed below (Yun, Jeon, Kim, & Kim, 2013).

1. The attacker captures the messages. analyzes network topology and devices and obtains the memory address of the function package. So, evaluated in this kind of threat data capture category. With this attack, main data, remote station data and network topology can be captured.

2. DNP3 is viewed attacker sends malicious traffic patterns and responses to the main terminal operated devices. It can also generate its own messages and send them to the remote terminal device. This type of threat can be considered in the categories of reproduction, modification, and interruption. The other types of attacks are settled between the two devices readable messages with employees

carried out the attack and intrusion changed. This type of attack cut, capture, modify and re-evaluated in producing category.

These attacks are carried out by general attack on all protocol layers. The structure of each layer to the protocol layer that there are special attacks to exploit. These attacks can affect system privacy by obtaining configuration data and network topology information. Attacks that affect the integrity of data are performed by adding incorrect data or reconfiguring external stations. Accessibility attacks cause or prevent the communication to the main terminals to lose the basic functions of the system.

Attacks on the data link layer can be described as follows (Graham & Patel, 2004):

1. Data link layer has a length in the frame structure. This field can be changed, remote terminal message processing deteriorates and can be fooled all the traffic flow. These threats are analyzed in the cutting and replacement category.

2. Under data link layer, which indicates the condition of the door station device is busy and the request should be sent later, the message has a flag. This flag can be changed, and the external station can be shown that suitable device. With the intense desire of the main terminal unit can perform DoS message to the remote terminal unit. If busy is set; MTA accepts the RTU device is busy and does not send any message. Thus, RTU remains pending.

3. The packet's destination address can be changed, so the package can be redirected or may be lost. If the package is a desire to reach another system will be incorrect and returns an incorrect result. If the address broadcast address goes to the entire system as the package is changed and can thus affect the whole system. This type of threat is changing, examined and re-cut produce category.

The attacks on the fake transport layer can be listed as follows (Majdalawieh, Parisi, & Wijesekera, 2006):

1. This layer is only targeted attacks aimed at changing the flag field and the sequence number. change the flag field will be cut to the root of the fragmented message. F indicates the flag is divided into the starting lineup, and if so, the message packet is generated and re-added to the traffic flow as well as all the other FR flag infects and causes the fall of this package. Finnish flag message is reproduced, and the process stops because of incomplete message is added to the end of the message.

2. Transport Package in a row and are marked with the serial number. If a packet sequence number obtained can be read. Due to the increase of the sequence number of the arithmetic produced by the next sequence number and a message may be injected into the traffic flow. This message MTU or RTUs can cause processing errors. This threat group is cut, modify and re-evaluated in producing category.

Performed for the application layer attacks can be listed as follows (Rodofile, Radke, & Foo, 2015):

1. Transport Package in a row and are marked with the serial number. If a packet sequence number obtained can be read. Due to the increase of the sequence number of the arithmetic produced by the next sequence number and a message may be injected into the traffic flow. This message MTU or RTUs can cause processing errors. This threat group is cut, modify and re-evaluated in producing category.

2. A message is sent to clear all data in the process of stopping and starting task in the registers of the destination RTU devices that function code, which is 9 or 10 and RTUs. In this case the loss of critical information can raise the system to crash or run malignant. With 10 functions to detect the message is very difficult because it does not require a notification that the message was received.

3. The time saving task of the function code 18'l data packets sent and thus the functions of the device may quit RT. This situation makes the system unable to respond, thereby blocking services performed.

The above 11 attacks can have serious impact on the system. Attacks can interfere with the service and cause incorrect system integrity by entering incorrect data. The most dangerous of these attacks is the one that deceives the MTU and seizes control of some or all the MTU, thus causing the system to be completely upside down. Data privacy can be lost when the intruder seizes device configuration.

Modbus openings and attacks

Modbus attacks on systems and networks to the features of this protocol is exploited by the applications and infrastructure. DNP3'te threats such as this protocol of cutting, capture, modify, and can be analyzed in four categories, including reproduce. Serial Modbus Protocol for the attack on the main and slave devices and the series was realized for the communication network, Modbus TCP for the attack on the IP network, the master and slave devices is performed (Huitsing, Chandia, Papa, & Shenoi, 2008).

These attacks can be caused to not disclose its confidentiality moved due to be accessible to the message content, denial of service to the cause of that system for accessibility to the effect will and ability to reproduce the information seized together by entering data integrity is affected. Attacks; Modbus serial protocol, Modbus TCP protocol, and both serial and TCP protocols to be examined under three headings.

Modbus serial protocol attacks

Modbus protocol attacks on changing the structure of the function code can crash the last system (MODBUS, 2012).

- When the function and sub-function code 08, code 0 is sent to the target device resets counter and replaces the error register values. This will change the configuration of field devices and error affects the operation. This category is considered a threat to change the field devices in its class
- When the function code 08 01 replaced the last device will restart and power-on test runs. This message causes the change of field device configuration settings. These threats are assessed in the cutting and replacement category.
- Function code 17, status information of field device field returns when they are sent to the device. This information formed the basis of the network can relax and different attacks. This situation will affect the confidentiality of the system.

Modbus serial and TCP attacks

This attack category, by way of blocking all communication services of the Modbus messages can be excluded. There might be more serious attacks can take control of MTU and completely dismantled the functioning of the entire system (MODBUS, 2006).

- Interrupt messages that can be published with the field devices to attack and response messages for broadcast messages that cannot be detected this attack. This attack can download all RTU devices and can be an obstacle to the entire process. These threats are analyzed in the cutting and replacement category.
- Messages flowing between MTU and RTU devices are captured and sent again. end devices by this method may be misled and may damage the flowing process. This threat cutting, modify and re-evaluated in the produce category.

- Status and configuration of field devices intervened to seize the information generated random addresses, messages can be sent to field devices. This information scanning attack causes a violation of privacy. These threats are analyzed in the capture category.
- By delaying the information flowing from the main device to the slave devices may be provided to reduce these messages. cutting message of this attack and cause the system to be changed.

Modbus TCP attacks

The attacks against the Modbus TCP protocol are as follows (Morris T. H., 2009):

- It is intended to affect the structure of the TCP packet frame. Multiple Modbus messages are not found in a single TCP packet. Therefore, the messages are divided into parts by MTU and sent to the RTU. Error messages can be injected in this attack or replacing messages sent to the target system.
- Last bit of a non-legal framework package can cut the TCP connection. Such a package may terminate Modbus messages to be sent and can cause cutting communications.
- In common with the high priority requests to the field device or host device or in other words to make bombardment can cause service interruptions.

The system results in the loss of privacy above-mentioned attacks, distortion effects such as loss of access and data integrity can be seen.

Profinet openings and attacks

ISO-TSAP (Transport Standards Organization Access Point) as the protocols used in industrial system has been formed according to the security concept was developed in the conditions of the period. Control systems and PLC devices that it believed that period was not designed to secure these protocols are completely isolated.

The present situation is considered in the face of increasing cyber threats are becoming impossible not to be thought of the concept of security of these systems. as in the propagation of the worm Stuxnet which will be identified in the heading sections isolated or separated networks, can be overcome via USB and appears to be secure, this network (Yau & Chow, 2015).

Siemens Simatic S7 PLC abuse

Simatic S7 abuse is not intended as a direct Profinet, but Profinet is utilized for connecting to the network will be exploited. Attack, communication of all S7 PLCs manufactured by Siemens and the Siemens engineering software for programming ISO-TSAP.

The attacker's point of view in terms of the S7 PLC device is from 102 ports to communicate with the ISO-TSAP and transmitted packets are sent as unencrypted clear text. Therefore, intervention and redirection attacks are suitable for this system. At the same time between MTU and RTU or PLC devices running all traffic can be captured in an easy way and thus it makes it possible to produce their own package, and to perform reverse engineering for malicious purposes attacker protocol.

Another major vulnerability is that the authentication is weak ISO-TSAP. An authenticated attacker who captures packets, may exceed the authentication mechanism using the same package (AlShemeili, Yeun, & Baek, 2016).

User authentication package is sent to the PLC device, which compares the password in the password or summary package, is configured in the device. If true, this comparison allows the device to the PLC memory access and read / write / give powers to run. This means that the attacker can make the desired changes to the PLC.

Attack vector;

1. Captured with Wireshark and other network monitoring tools traffic flowing between the MTA and the PLC.

2. The client part of the captured packet is extracted and analyzed information flowing between the client and server.

3. New packet is generated based on information obtained from the issuance of the client part.

4. Crafted packets will be redirected to the PLC.

This kind of abuse can be easily prevented by preventing the inclusion of someone with malicious intent into the network, but today, all systems are interconnected. An attacker who unauthorized access to the network can take over the system in this way.

Profinet IO devices of emulation

Profinet IO Profinet standard Ethernet networks for use as components of the systems as shown in Figure 3.6 MITM attack threats standard in Ethernet networks, such as exposure to the same threat. MITM attack is conducted legally intercepts a communication partner communicates the two devices. This situation allows the attacker to communicate between the two devices to capture traffic and allows to inject to reconfigure the device to send packets to an unknown or remote server.

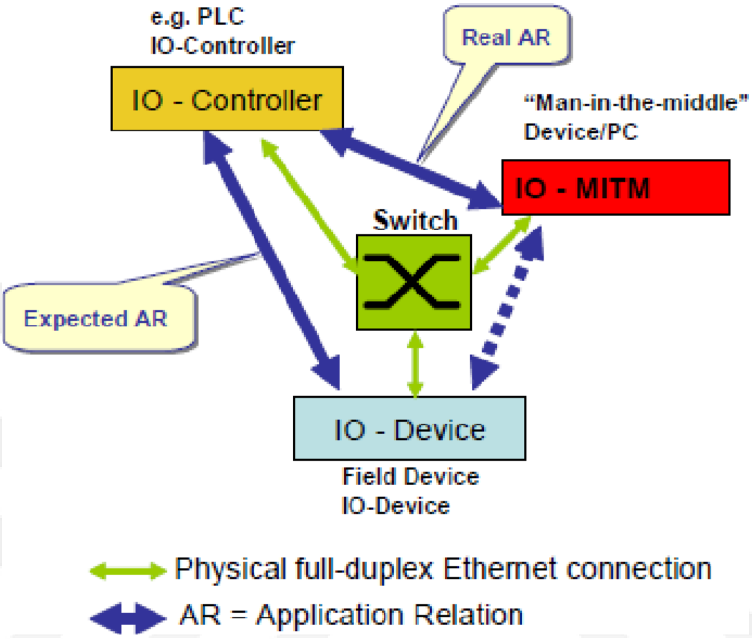


Figure 3.6: MITM attacks for Profinet system (Siven, 2015)

The fundamental form of the Profinet system exists of an IO inspector and one or more IO tools. Two components, which are mentioned, consist of a connection that is called as Application Relation (AR). This is occurred by the IO inspector over UDP / IP with the Distributed Computing Environment / Remote Procedure Call, which is the framework for client / server implementation. The Profinet IO inspector is accountable for allocating IP addresses to IO tools.

Profinet IO tools are not only defined by IP addresses, also defined in Profinet names. Names Profinet IO device is assigned during the engineering process and is saved to permanent memory. These names are then configured the IO controller is responsible for the desired IP address. IO controller, the IO that the device is accessible and sends the first message identifier for the DCP-approved to verify that it has a name. Then the names of the query are made and IP addresses before assigning IO controller, IO device checks the ARP request to check that they have received more than one IP address. If more than one IP address assigned, the IO controller assigns an IP address, AR IO device establishes the connection and TCP / IP sends out configuration.

This style might be inclined to an installation error If the configuration of a careless manner. Most critical errors and possible issuance of more than one IP address and Profinet names. These errors MITM, and ARP poisoning attack can cause the Profinet network. But the attack to take place successfully, certain conditions must be formed. The offending machine, and Profinet device should also be in sync. For example, if 1 ms rpm packages sent MITM machine it should still send their packages of 1 ms speed. MITM machine switch its MAC table fails to do so due to an update every time exposed to all the attacks will fail.

Profuzz

Fuzzing or fuzz testing (Reliability test method), the input of the computer software program to test random, unconfirmed or a black box technique performed by injecting unexpected data. Semi-automatic or carried out in a completely automated manner. The basic logic of fuzzing process, a failure waiting to be discovered by each program (bug) and a systematic approach that can be explored using this bug is located.

Profuzz, developed by Ronald Koch and students at the University of Augsburg is Profinet fuzz program. profuzz uses the framework of a strong package Scapy replacement program. Profuzz supports the following types of Profinet frames (Dale Peterson, 2012):

- AFR (Random alarm Framework)
- AFO (Frame Sequential Alarm)
- PN IO (Periodic Real Time)
- DCP (DCP-Identifier Request)
- PTCP (Transparent Precision Time Protocol)

3.2. Scada Leak Testing Tools

Information and communication technologies in an integrated way employees SCADA determine the vulnerability of the system and determined exploitation of this vulnerability with the infrastructure, the penetration testing tools for systems that use the infrastructure of the normal information technology, or as custom is done using tools designed for SCADA systems. Some of the tools used to infiltrate SCADA system in this part of the study are shown.

3.2.1. Shodan Search Engine

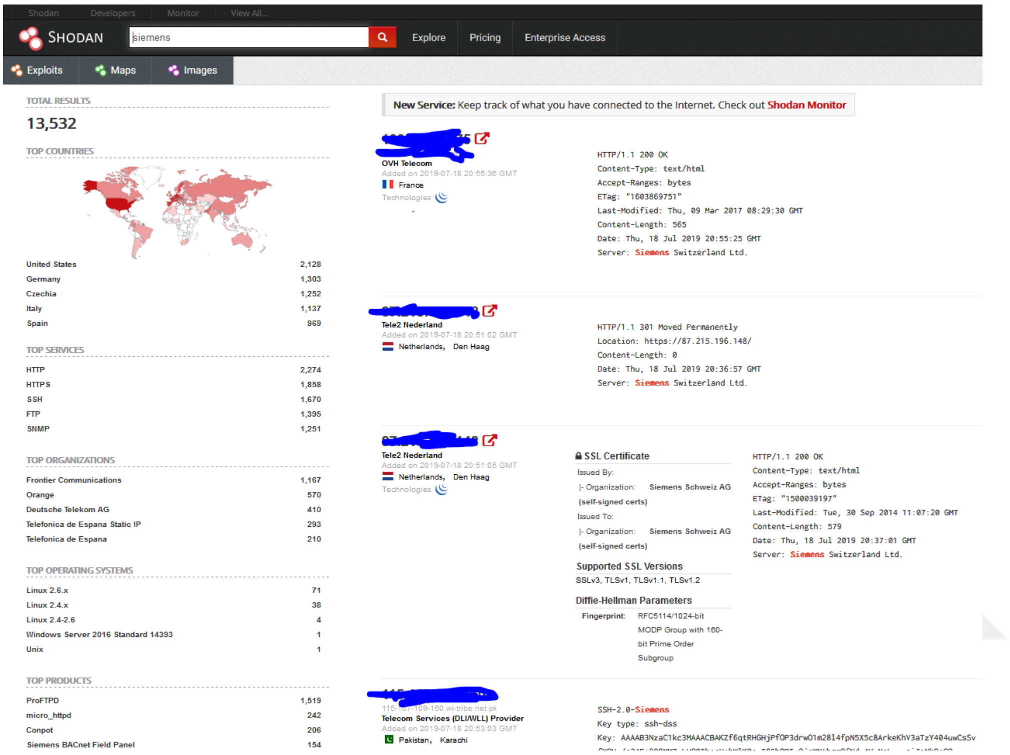
In 2009, a programmer named John Matherly, internet-connected device that can identify and friendly graphical interface, called Shodan has written a search engine (SHODAN, 2009). Especially; computers, printers, define routable IP address devices such as webcams and industrial control devices. Shodan; Scans all web, devices and directories located in the query to the appropriate service. API or Shodan balls out of the IP addresses of the devices in a searchable database that can be accessed on port numbers and employee information service contains the main title. Users; country, server name, specific IP address range, operating system, device brand or port information can be found in the hosting different question.

In October of 2010; ICS-CERT, Shodan control systems of safety interface to be able to determine their ability to open and control system of the device releases a report discussed the importance of being isolated from the internet (Dale Peterson, 2012). As a result of this report, ICS-CERT-10-301-01, the ICS-CERT-301-01, ICS-CERT-11-343-01, ICS-CERT-12-046-01 and ICS-CERT-12-046-01 to 5 units including control systems associated with the Internet has published a report on the importance of device (CISA, 2012).

More than 7500 management system connected to the internet, meters, has used industrial control devices, such as HMI and PLC. Total 29 Shadan query is used for the determination of industrial control devices. As a result of 2 years of assessment 7500 devices detected in 2013 has been found to have increased dramatically and 57.409 pieces (Leverett, 2011).

In 2012, SHINE (Shodan Intelligence Extraction) project is a project carried out by the US Department of Homeland Security (Tofino Security, 2013), this project Shodan API used and throughout the world about the query than 700 different Shodan connected to the Internet 500 000 units have been identified industrial control devices. ICS-CERT conducted over 7200 devices with most devices in the project's continuation has been shown to be very weak security measures (National Cybersecurity And Communications Integration Center , 2013).

Shodan using the web interface SIEMENS branded weakness on the industrial control system and the system was questioning the results obtained from the internet connection was detected. In the investigation of countries and cities where the devices and services running on ports, operating systems, brand name, company name and is working on a range of IP addresses can be searched. Screenshot of interrogations is seen in Figure 3.7.



TOTAL RESULTS

13,532

TOP COUNTRIES	
United States	2,128
Germany	1,303
Czechia	1,252
Italy	1,137
Spain	969

TOP SERVICES	
HTTP	2,274
HTTPS	1,858
SSH	1,670
FTP	1,395
SNMP	1,251

TOP ORGANIZATIONS	
Frontier Communications	1,167
Orange	570
Deutsche Telekom AG	410
Telefonica de Espana Static IP	293
Telefonica de Espana	210

TOP OPERATING SYSTEMS	
Linux 2.6.x	71
Linux 2.4.x	38
Linux 2.4-2.6	4
Windows Server 2016 Standard 14393	1
Unix	1

TOP PRODUCTS	
ProFTPD	1,519
micro_httpd	242
Conpot	206
Siemens BACnet Field Panel	154

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]
OVH Telecom
Added on 2019-07-18 20:55:36 GMT
France
Technologies:

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1603869751"
Last-Modified: Thu, 09 Mar 2017 08:29:30 GMT
Content-Length: 565
Date: Thu, 18 Jul 2019 20:55:25 GMT
Server: Siemens Switzerland Ltd.
```

[redacted]
Tele2 Nederland
Added on 2019-07-18 20:51:02 GMT
Netherlands, Den Haag

```
HTTP/1.1 301 Moved Permanently
Location: https://87.215.196.148/
Content-Length: 0
Date: Thu, 18 Jul 2019 20:36:57 GMT
Server: Siemens Switzerland Ltd.
```

[redacted]
Tele2 Nederland
Added on 2019-07-18 20:51:05 GMT
Netherlands, Den Haag
Technologies:

SSL Certificate

Issued By:
|- Organization: Siemens Schweiz AG
(self-signed certs)
Issued To:
|- Organization: Siemens Schweiz AG
(self-signed certs)

Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC5114/1024-bit MODP Group with 160-bit Prime Order Subgroup

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1500039197"
Last-Modified: Tue, 30 Sep 2014 11:07:20 GMT
Content-Length: 579
Date: Thu, 18 Jul 2019 20:37:01 GMT
Server: Siemens Switzerland Ltd.
```

[redacted]
115-[redacted]-109-160.wi-tribe.net.pk
Telecom Services (DLI/WLL) Provider
Added on 2019-07-18 20:53:03 GMT
Pakistan, Karachi

```
SSH-2.0-Siemens
Key type: ssh-dss
Key: AAAAB3NzaC1kc3MAAACBAKZf6qtRHGHjPfOP3drwO1m2814fpN5X5c8ArkeKhV3aTzY404uwCsSv
```

Figure 3.7: Query Result Shodan

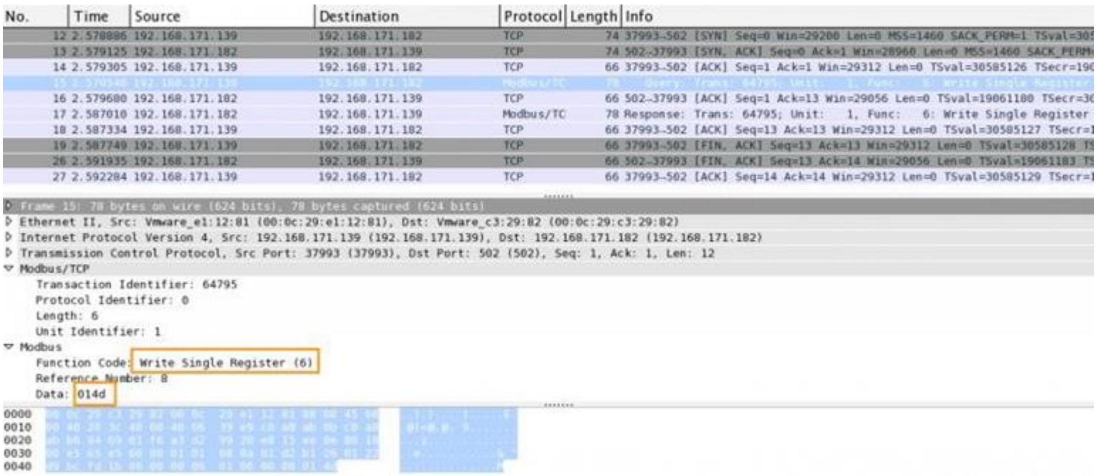
Determined industrial control systems enters the map on the whereabouts of the system, running on service and ports, device, product name, brand, manufacturer, serial number of the device, the device shows the local IP address and the type of device. Many of the queried device has been noticed that this device runs the web service and access to the web interface login screen and input can be done without encryption on access to third-party applications can be made it has been identified. Thus, an attacker listens for traffic, can view the unencrypted data entered by the user.

In order to show the importance of password security, when logging on to an industrial control system that can be accessed via web service, it was checked whether the user information was changed by the system administrator or user and according to the results, it was observed that user information was left by default in many systems. It is found that the default usernames and passwords made on the internet are searched by the type of devices and can be found very easily and the system can be accessed in a simple and unauthorized way.

3.2.2. Wireshark Network Analysis Program

Wireshark packets flowing on the network as needed for imaging are detailed in the open source analysis program is a package (Wireshark, 2013). Captures packets flowing across the network, analyzes examining the package and separate the parts that depending on the protocol analysis "1's and 0's" in the comments. Network use different statistical analysis calculations using the information as accessible parts separated package in Wireshark. In this way, the devices on the network communication, and behavior of complex elements with each other can be virtualized and understandable. At the same time, this program is open source and UNIX, Windows, are widely used because it runs on different operating systems such as MacOS.

Modbus, Profibus, Wireshark is supported by a plurality of protocol used for communication of industrial control system and the behavior of these protocols can be virtualized as DNP3. In figure 3.8 and 3.9 Modbus communication and Profinet Wireshark images are available.

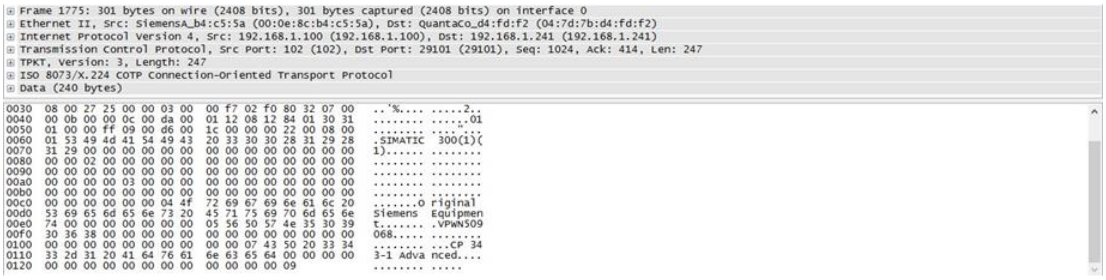


```
No.   Time     Source           Destination      Protocol Length Info
   12 2.578886 192.168.171.139  192.168.171.182  TCP       74 37993→502 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=30
   13 2.579125 192.168.171.182  192.168.171.139  TCP       74 502→37993 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM
   14 2.579305 192.168.171.139  192.168.171.182  TCP       66 37993→502 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=30585126 TSecr=190
   15 2.579540 192.168.171.139  192.168.171.182  Modbus/TC 78    Query: Trans: 64795; Unit:   1, Func:   6: Write Single Register
   16 2.579680 192.168.171.182  192.168.171.139  TCP       66 502→37993 [ACK] Seq=1 Ack=13 Win=29056 Len=0 TSval=19061180 TSecr=30
   17 2.587010 192.168.171.182  192.168.171.139  Modbus/TC 78 Response: Trans: 64795; Unit:   1, Func:   6: Write Single Register
   18 2.587334 192.168.171.139  192.168.171.182  TCP       66 37993→502 [ACK] Seq=13 Ack=13 Win=29312 Len=0 TSval=30585127 TSecr=1
   19 2.587749 192.168.171.139  192.168.171.182  TCP       66 37993→502 [FIN, ACK] Seq=13 Ack=13 Win=29312 Len=0 TSval=30585128 TS
   26 2.591935 192.168.171.182  192.168.171.139  TCP       66 502→37993 [FIN, ACK] Seq=13 Ack=14 Win=29056 Len=0 TSval=19061183 TS
   27 2.592284 192.168.171.139  192.168.171.182  TCP       66 37993→502 [ACK] Seq=14 Ack=14 Win=29312 Len=0 TSval=30585129 TSecr=1

▷ Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Vmware_e1:12:81 (00:0c:29:e1:12:81), Dst: Vmware_c3:29:82 (00:0c:29:c3:29:82)
▷ Internet Protocol Version 4, Src: 192.168.171.139 (192.168.171.139), Dst: 192.168.171.182 (192.168.171.182)
▷ Transmission Control Protocol, Src Port: 37993 (37993), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
▽ Modbus/TCP
    Transaction Identifier: 64795
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 1
▽ Modbus
    Function Code: Write Single Register (6)
    Reference Number: 8
    Data: 014d
0000  [illegible]
0010  [illegible]
0020  [illegible]
0030  [illegible]
0040  [illegible]
```

Figure 3.8: Modbus Wireshark image

Figure 3.8 shows the captured packets for the Modbus protocol in the Wireshark image. The function code of the Modbus protocol and the data sent to the industrial control system with this function code are shown.

Figure 3.9 shows the captured packages of the Siemens Simatic S7-300 device used in the study for Profinet protocol. In the study using S7-300 CPU, CP 343-1 Advanced communication module is used as shown in Figure 3.9.

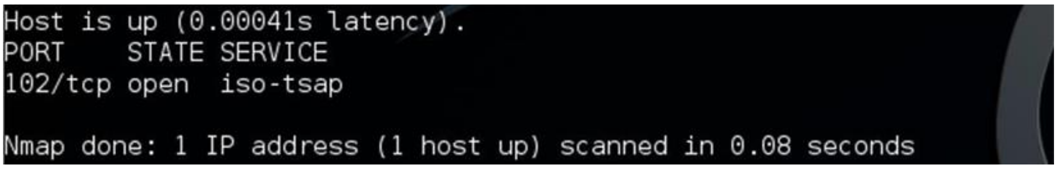


```
⊞ Frame 1775: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits) on interface 0
⊞ Ethernet II, Src: SiemensA_b4:c5:5a (00:0e:8c:b4:c5:5a), Dst: QuantaCo_d4:fd:f2 (04:7d:7b:d4:fd:f2)
⊞ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.241 (192.168.1.241)
⊞ Transmission Control Protocol, Src Port: 102 (102), Dst Port: 29101 (29101), Seq: 1024, Ack: 414, Len: 247
⊞ TPKT, Version: 3, Length: 247
⊞ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
⊞ Data (240 bytes)

0030  08 00 27 25 00 00 03 00  00 f7 02 f0 80 32 07 00   ..'%.... .....2..
0040  00 0b 00 00 0c 00 da 00  01 12 08 12 84 01 30 31   ........ ......01
0050  01 00 00 ff 09 00 d6 00  1c 00 00 00 22 00 08 00   ........ ...."...
0060  01 53 49 4d 41 54 49 43  20 33 30 30 28 31 29 28   .SIMATIC  300(1)(
0070  31 29 00 00 00 00 00 00  00 00 00 00 00 00 00 00   1)...... ........
0080  00 00 02 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 03 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 04 4f  72 69 67 69 6e 61 6c 20   .......O riginal
00d0  53 69 65 6d 65 6e 73 20  45 71 75 69 70 6d 65 6e   Siemens  Equipmen
00e0  74 00 00 00 00 00 00 00  05 56 50 57 4e 35 30 39   t....... .VPWN509
00f0  30 36 38 00 00 00 00 00  00 00 00 00 00 00 00 00   068..... ........
0100  00 00 00 00 00 00 00 00  00 00 07 43 50 20 33 34   ........ ...CP 34
0110  33 2d 31 20 41 64 76 61  6e 63 65 64 00 00 00 00   3-1 Adva nced....
0120  00 00 00 00 00 00 00 00  00 00 00 00 09            ........ .....
```

Figure 3.9: Profinet Wireshark image

3.2.3. Nmap Network Scanning Tool

Nmap TCP / IP-based employee information, open source is used to scan for open ports and services such as potential weaknesses of the system is a versatile scanning tool (NMAP, 2017). It is also used for extracting network topology. Vulnerability assessment and an important part of the information gathering phase is carried out by a port scan. Each machine's list of open ports to infiltrate SCADA constitute a step abusing the weaknesses in the system. Figure 4.10 Siemens S7-1200 PLC device as used in the experimental setup environment list of NMAP scanning results obtained open ports and service are shown. By default, the scan results made 102 runs on port Profinet protocol and it is seen that the ISO-TSAP service.



```
Host is up (0.00041s latency).
PORT    STATE SERVICE
102/tcp open  iso-tsap

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

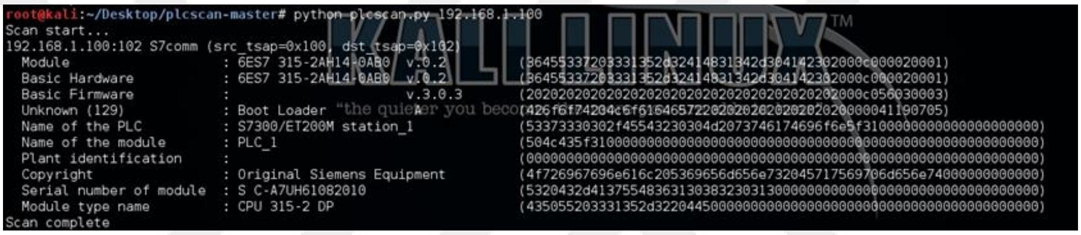
Figure 3.10: Nmap scan

3.2.4. PLCSCAN Tool

PLCscan is a utility released by the ScadaStrangeLove group. It is used for detecting PLC devices and other Modbus devices on the network (Google, 2012).

PLCscan is a Python script for checking the status of TCP / 102 and TCP / 502 ports. If it finds these two ports open, it calls other functions or scripts related to those ports. For example, if it detects that the TCP / 502 port is open, it pulls the MEI type to recognize the device and calls the Modbus functions. The ID of the device will then return, and this information will be displayed on the screen.

PLCscan is a basic tool that receives fast results from PLC. If the information is taken directly from the device and used without similar testing on similar devices, it may cause some problems. It performs some error checks in the code that requires limitation in some subjects. This information collected by PLCscan can be in the form of two outputs with Profinet and Modbus protocols. Outputs from these devices include firmware versions. Figure 3.11 shows the PLCscan scanning results in the experimental setup environment where Siemens S7-300 PLC device is located. According to the results of the scan, module type, serial number, name of the module and plc device used in the project and hardware information were obtained.

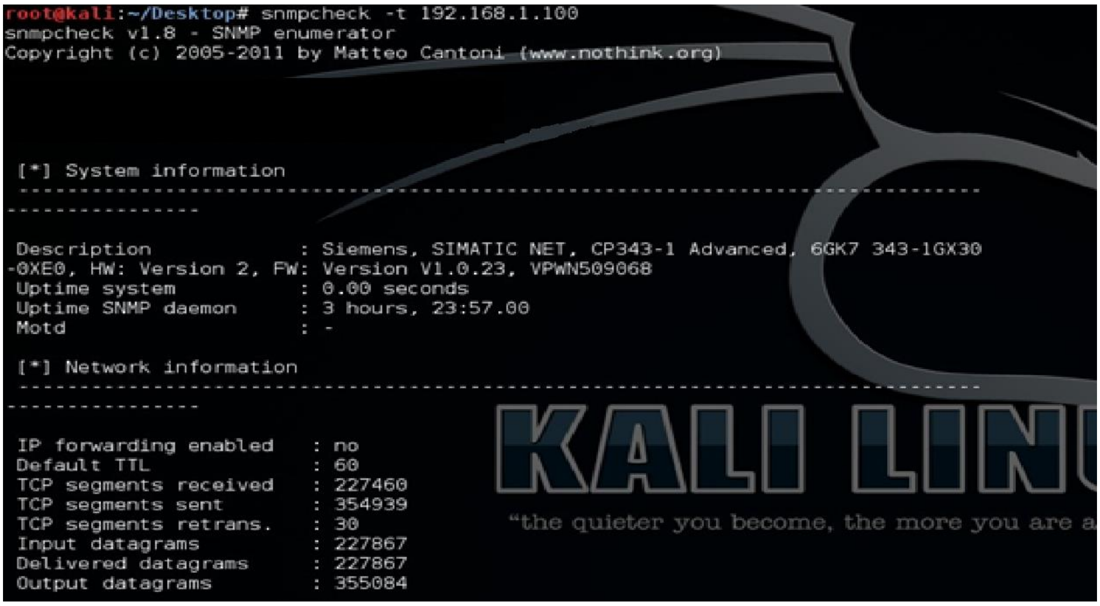


```
root@kali:~/Desktop/plcscan-master# python plcscan.py 192.168.1.100
Scan start...
192.168.1.100:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                   : 6ES7 315-2AH14-0AB0  v.0.2       (36455337203331352d32414831342d304142302000c000020001)
  Basic Hardware           : 6ES7 315-2AH14-0AB0  v.0.2       (36455337203331352d32414831342d304142302000c000020001)
  Basic Firmware           :                      v.3.0.3     (20202020202020202020202020202020202020202000c056030003)
  Unknown (129)            : Boot Loader          A           (426f6f74204c6f616465722020202020202020200000041190705)
  Name of the PLC          : S7300/ET200M station_1           (53373330302f45543230304d2073746174696f6e5f3100000000000000000000)
  Name of the module       : PLC_1                            (504c435f31000000000000000000000000000000000000000000000000000000)
  Plant identification     :                                  (0000000000000000000000000000000000000000000000000000000000000000)
  Copyright                : Original Siemens Equipment       (4f726967696e616c205369656d656e732045717569706d656e74000000000000)
  Serial number of module  : S C-A7UH61082010                 (5320432d41375548363130383230313000000000000000000000000000000000)
  Module type name         : CPU 315-2 DP                     (435055203331352d322044500000000000000000000000000000000000000000)
Scan complete
```

Figure 3.11: PLCscan Scan Results

3.2.5. SNMP Tool

The purpose of the snmpcheck command is to automate the information collection of any device that supports the Snmp protocol, such as Windows, Unix, network devices, printers, and PLC devices. Snmpcheck allows snmp devices to be listed and readable. It is widely used in system monitoring or penetration tests. The information obtained from the S7-300 device used in the operation with the snmpcheck command is shown in Figure 3.11. According to the results obtained, detailed version information of CP 343-1 Advanced communication module and how long the device has been running is seen.



```
root@kali:~/Desktop# snmpcheck -t 192.168.1.100
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)


 [*] System information
 ------------------------------------------------------------------------------------
----------------

 Description              : Siemens, SIMATIC NET, CP343-1 Advanced, 6GK7 343-1GX30
-0XE0, HW: Version 2, FW: Version V1.0.23, VPWN509068
 Uptime system            : 0.00 seconds
 Uptime SNMP daemon       : 3 hours, 23:57.00
 Motd                     : -

 [*] Network information
 ------------------------------------------------------------------------------------
----------------

 IP forwarding enabled     : no
 Default TTL               : 60
 TCP segments received     : 227460
 TCP segments sent         : 354939
 TCP segments retrans.     : 30
 Input datagrams           : 227867
 Delivered datagrams       : 227867
 Output datagrams          : 355084
```

Figure 3.12: Snmpcheck Command Result

3.2.6. Metasploit Framework

The Metasploit Framework is one of the most common and well-known penetration testing tools among information security communities. The first version was published in 2003 by H. D. Moore. In 2007, Moore gave up the perl language in this project and rewrote it from the beginning in ruby code. In 2009 the Rapid7 security firm acquired the entire Metasploit Project. The Metasploit Framework is widely used for exploit code development communities. Security experts and developers use the open source platform to test large infrastructure information systems and write new exploit code for specific target systems. Currently there are more than 1800 exploitation codes for different systems and software. There are 4 basic steps to run the exploit code successfully. First, the type of attack on the target system or software is selected. Specify which code to run on the target machine for the exploit code to run. The procedure for protection from IPS / IDS systems is determined. The attack process is initiated and the communication channel with the target system is opened. Some of the metasploit modules written for the vulnerability of SCADA systems that SCADAhacker has arranged are as shown in Table 3.3.

Table 3.3: Some of the Metasploit module designed for SCADA systems (SCADAhacker, 2015)

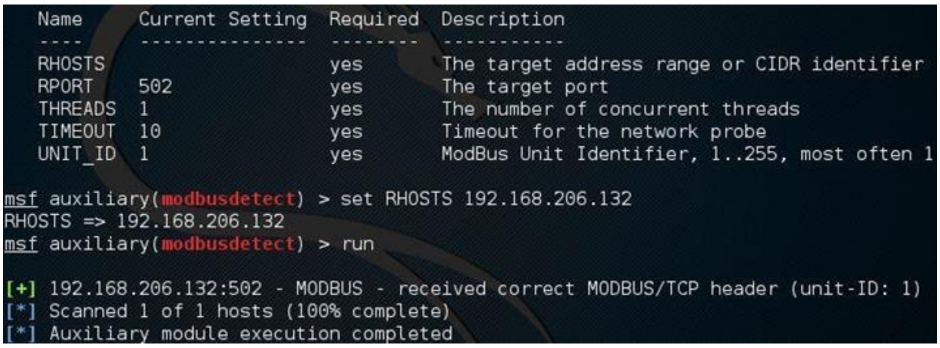
Tools / Code Name Abuse	Developer	System	Metasploit Reference

teechart_pro.rb	BACnet	Operator Workstation	exploit / windows / browser / teechart_pro.rb
simatic_s7_1200_command.rb	Dillon Beresford	Siemens Simatic S7 module	It is downloaded as open source.
simatic_s7_300_command.rb	Dillon Beresford	Siemens Simatic S7 module	It is downloaded as open source.
modbusclient.rb	esmnemo's and Arnaud Soulla	Modbus Client Utility	auxiliary / scanner / SCADA / modbusclient.rb
modbusdetect.rb	the esmnemo	Modbus Client Utility	auxiliary / scanner / SCADA / modbusdetect.rb

Modbusdetect module

This part of the study, the above-mentioned Metasploit Framework modbusdetect and detection using the Modbus protocol module on the target system modbusclient modules and read by the values in registers on the replacement will be made.

In figure 3.13 it aimed to collect information on the destination system using modbusdetect module. Modbusdetect Metasploit module, running on the target system Modbus / TCP in a specific range of IP addresses to scan detects and identifies the protocol Modbus service. This module detects Modbus sending request packets to the destination system port 502 and waits for the response contains the same Transaction ID and protocol ID. Module Modbus / TCP header and returns the Unit ID of the PLC device (Cook, 2017).



```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   RHOSTS                     yes       The target address range or CIDR identifier
   RPORT     502              yes       The target port
   THREADS   1                yes       The number of concurrent threads
   TIMEOUT   10               yes       Timeout for the network probe
   UNIT_ID   1                yes       ModBus Unit Identifier, 1..255, most often 1

msf auxiliary(modbusdetect) > set RHOSTS 192.168.206.132
RHOSTS => 192.168.206.132
msf auxiliary(modbusdetect) > run

[+] 192.168.206.132:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 3.13: Modbusdetect Module

Modbusclient

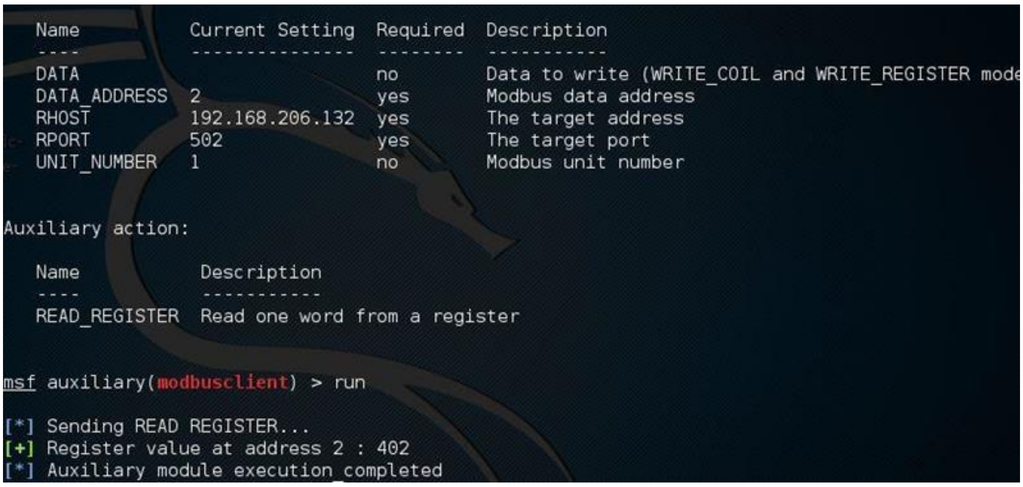
Modbusclient data on the PLC Modbus / TCP protocol for reading or writing using the Metasploit module. Modbusclient by the original protocol was only Function module esmnemo-written code modules using the 0x06 ("Write Single Register"). Arnaud Soulla; 0x01 (Read Coil), 0x03 (Read Holding Register) and 0x05 (Write Single Coil) function has made changes to the code to include code (Cook, 2017)

Function Code 0x01 (Read Coil) modbusclient successfully executed using the module allows to read the status of the neighboring spiral between 1-2000 users in remote PLC devices. DATA_ADDRESS section shown in Figure 13.4, the returned package status (0x0000- 0xFFFF) to indicate the start address of the second byte. representing a status bit for each register is rotating register from the Modbus server response data field (MODBUS, 2006).

Function Code 0x03 (Read Holding Register) successfully operated using modbusclient module allows remote users to read register entries 1-2000 between neighboring devices in the PLC. Section shown in Figure 4.14 DATA_ADDRESS returned status registers (0x0000 - 0xFFFF) to indicate the start address of the second byte. Modbus response returned by the server is a two-byte register value for each register in the response message (MODBUS, 2006).

Function Code 0x05 (Write Single Coil) modbusclient operated successfully using only output to the coil module of the user device to the remote PLC (ON or OFF) allows typing. Figure 4.14 shows the input data value using the DATA field, the value to be ON the output 0xff00 accepts the value 0x0000 to be OFF. All other input values are invalid and will not affect the output (MODBUS, 2006).

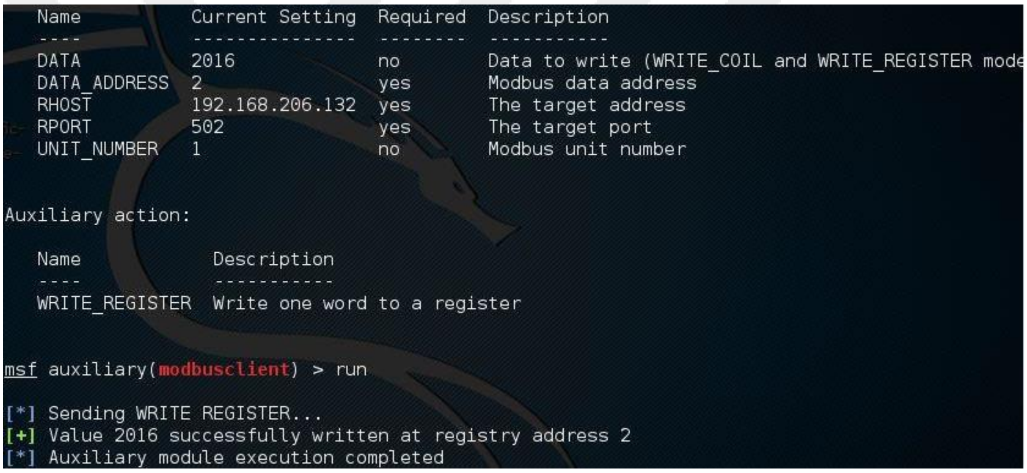
Function Code 0x06 (Write Single Register) modbusclient module successfully operated using single occupancy to register the user to the remote PLC devices (single holding register) allows you to write. As shown in Figure 13.4 DATA_ADDRESS field identifies the address of the register to be written (0x0000 - 0xFFFF). This operation successfully request echoes the value of the defined area DATA (MODBUS, 2006).



```
   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DATA                           no        Data to write (WRITE_COIL and WRITE_REGISTER mode
   DATA_ADDRESS  2                yes       Modbus data address
   RHOST         192.168.206.132  yes       The target address
   RPORT         502              yes       The target port
   UNIT_NUMBER   1                no        Modbus unit number


Auxiliary action:

   Name           Description
   ----           -----------
   READ_REGISTER  Read one word from a register


msf auxiliary(modbusclient) > run

[*] Sending READ REGISTER...
[+] Register value at address 2 : 402
[*] Auxiliary module execution completed
```

Figure 3.14: Modbusclient Action is READ_REGIST

Values above the target system using registers Modbusclient study could read module as shown in Figures 3.14 and 3.15 respectively and could be changed.



```
   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DATA          2016             no        Data to write (WRITE_COIL and WRITE_REGISTER mode
   DATA_ADDRESS  2                yes       Modbus data address
   RHOST         192.168.206.132  yes       The target address
   RPORT         502              yes       The target port
   UNIT_NUMBER   1                no        Modbus unit number


Auxiliary action:

   Name            Description
   ----            -----------
   WRITE_REGISTER  Write one word to a register


msf auxiliary(modbusclient) > run

[*] Sending WRITE REGISTER...
[+] Value 2016 successfully written at registry address 2
[*] Auxiliary module execution completed
```

Figure 3.15: Modbusclient Action is WRITE_REGIST

3.3. Cyber Attacks on Critical Infrastructure in the Literature

With the development of information and communication technology, transportation, critical infrastructure systems such as power and automation have become integrated with this technology works. So that may occur in the information technology can also affect critical infrastructure vulnerabilities system that uses information technology infrastructure directly and may pose a risk. This malware used to infect systems, so information can also be used to damage critical infrastructure systems. The motivation of cyber-attacks made for this system are often political and aims to harm the country's critical infrastructure and projects taken goal.

3.3.1. Siberian Pipeline Explosion

In 1982, an explosion occurred in the middle of Siberia by vaporizing most of the newly built trans-Siberian pipeline. This explosion had a 1/7 impact on the nuclear bomb that was thrown into Japan in World War II, and the pipelines that brought $ 8 billion in oil revenue to the Soviet Union were seriously damaged. However, it has recently been made public by the CIA (Russell, 2004).

The Soviets needed complex control systems to automate the operation of valves, compressors, and storage areas in such an enormous facility. Russian pipeline officials approached the United States for the necessary software but were turned down. The Russians looked undaunted; The KGB attempted to infiltrate the Canadian software supplier to steal the required codes. Vladimir Vetrov (Code Name: Farewell), who has been working bilaterally for American intelligence and Russian intelligence, collaborates with some frustrated Canadians. Pipeline software; to deflect the operation of pumps, bleachers and valves. After a while, it resets pump speeds and valve settings and generates acceptable pressure to the pipeline welds and connections. The result was a huge explosion that could be seen from space. The White House stated that they received some unusual warnings from the infrared satellites in the middle of the Soviets (Weiss, 1996).

3.3.2. The Salt River Project (SRP) hijacking incident

In 1994, Jarrett Lane Davis, Salt River Project (SRP) that allows unauthorized access via dial-up modem to the computer network and access to billing information. Then the system has left the back door to enter. At the same time, the SRP SCADA system in Phoenix to about 210 km of the customer controls the channel used for water distribution. Mr. Davis channels that control over critical system has opened a session for at least 5 hours. Water and power monitoring and distribution, finance, unprotected data, including customer and personal information has been captured. Login and password files, registry files, computer systems and "root" has seized power. Moreover, it has also access to the SRP and the National Weather Service Doppler-radar research project between the National Severe Storms Laboratory. SRP these attacks estimate excluded due to low productivity also lost $ 40,000 (Turk, 2005).

This is linked to the leaking incident of attack on Roosevelt Dam, and has become a legend from constantly on the agenda. In his statement before the US House of

Representatives "it was a kid pirates provide unauthorized access to a network of companies that control the Roosevelt Dam in Arizona's activities" were called. At the same time, this attack on Mr. Davis is 27 years old and said to be a link between SRP and Roosevelt Dam.

3.3.3. Houston Port System Failure

In 2001, a young computer hacker (Aaron Caffrey), has infiltrated the Port of Houston in Texas for computer servers to target a female chat room. The attack, the world's 8th largest drop off service to the computer system used to attack the port arrangement is made. The web service port out of service for critical information including ship's captain remained. That's why the company is responsible for the anchoring and support from the harbor entrance and exit of ships with navigation information have become unable to service status (BBC, 2003).

3.3.4. Slammer Worm

A staff working in a corporate firm in May 2003, was to install software without noticing whether the current version of Microsoft SQL laptops. After a while, the user must connect the computer to the Internet to access the e-mail server through an internet service provider (in violation of company policy). Thus, the SQL slammer worm-infected machines that are connected to the internet. Employees are then brought to the office and the computer connected to the network. So-SQL slammer worm has infected corporate network (Williams, 2003). and no firewall, which controls data collection server system and development control system has been infected. This case has had to be removed from the network server control without further contamination. There has been no significant impact on production, but some historical data is lost in the process of stopping the server, and it has to be manually recreated.

3.3.5. The Channels of California System Hack

An employee of the California Canal System was tried for installing and damaging unauthorized software on a computer used to direct water from the Sacramento River. Michael Keehn, 61-year-old electrical consultant for the Tehama Colusa Channel Authority (TCAA), was sentenced to 10 years in prison for unintentionally damaging a computer that was intentionally protected".

Allegedly; Keehn has installed unauthorized software on the SCADA system in TCAA. Access to this system is on 15 August 2007. As an electrical consultant, he is responsible for computer systems in the TCAA. Together with 16 staff, TCAA controls two channels, California's Tehama Colusa and Corning Canal, for agricultural areas in California. Both systems are under the rule and disposition of the state. Robin Taylor, a US Department of Justice representative; TCAA said that in case of an attack on SCADA systems, the channels will continue to operate even if the system goes offline. Computers are manually operated when not in use. This infiltration caused more than $ 50,000 damage to the TCAA (Weiss, 1996).

3.3.6. Violation of Spying in the US Power Grid

Wall Street Journal wrote in April 2009 that the Russian and Chinese spies hacked into the US electricity grid (Gorman, 2009). Deputies inevitable to combat threats gave the government authority to the electricity sector, including measures have brought proposals to improve cyber security.

In the electricity industry cybersecurity adviser Bob West, NERC’s noted that the industry was encouraging about being proactive.

3.3.7. Nitro Attacks

Nitro attacks primarily working on chemical and advanced materials research, development and production company has targeted. Attackers aim to make industrial espionage, design documents, is to collect intellectual property, such as formulas and manufacturing processes.

The methodology of the attacks, the attackers sent a malicious e-mail plug-in available to employees of the companies they target. E-mail invitations to share content with business partners and to the security update when they come. Company employees creates email content executable files when they open a backdoor and Trojan horse communicates through port 80 in an encrypted form with a C & C server based in China. The attacker then captured password summaries of Windows machines in the domain (Chien & O’Gorman, The Nitro Attacks: Stealing Secrets from the Chemical Industry, 2011).

3.3.8. The Stuxnet Worm

The Stuxnet worm; cyber security community "memorization disrupts" (game-changer) is defined as a malicious software (Leyden, 2010). Because of the complexity of this malware, purpose and implications are different from other malicious software. The Stuxnet worm development and deployment of cyber technology, has shown that a threat may be able to give direction to the world of politics.

Stuxnet worm is spread indiscriminately from one computer to another, such as the vulnerability of other worms. Other thousands of computer worms from the greatest feature of the Natanz matching the characteristics of Iran's nuclear enrichment facility only Industrial Control System (ICS) is entered when it is designed to reveal their load and in 4 Windows abuser operating systems 0 days is no weakness. When this happens, Programmable Logical Controller used for the control of the centrifuges at Natanz (PLC) code tampering. Finally, damaged and thousands of centrifuges Iran nuclear activities have been hampered. Previously it did not physically harm any worms out of the ICS system.

Stuxnet worm, since it contains the function and structure to be evaluated at a different size than the other cyber-attacks performed for critical infrastructure. Therefore, a separate part of the evaluation is made in this section Stuxnet (Knopová & Knopová, 2014), 3 mentions may take place in cyber space of World War II. Conventional weapons and war material and spiritual figures and the cost is very serious cyber war may cost human lives attest to the truth of this thesis. This work has been carried out successfully the target system to infiltrate and damage the party transactions carried out the attack, described Stuxnet worm in and carried out this attack by hiding the source. Thus, normally without causing loss of life and make an attack could be considered an act of war was only damage to the target system. After the alleged attack on Iran as the source of the attack has not started a legal process against the US and Israel. Because the source of the attacks, as mentioned do not indicate the US and Israel.

Found inside Stuxnet worm as described above four 0-day vulnerability and that due to the most complex malware was discovered until the day opened a new area to the malware analyst and made a big impact all over the world. Also, it has enabled an increase of the rising and awareness of the new proposals for the realization of industrial control system providing control of the PLC devices for critical infrastructure protection cyberspace and safety.

3.3.9. Duqu Trojan Horse

In 2011, the Duqu attacks on Word documents were identified with a 0-day vulnerability (CVE-2011-3402). This exploit allows attackers to jump from kernel mode to a Word document. When the Word file is opened, the exploit module is triggered and this exploit contains a kernel-mode shellcode that first checks to see if the computer has been compromised by checking the registry value HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ InternetSettings \ Zones \ 4 \ “CF1D”. If the computer has been compromised, the shellcode is available. If not seized; shellcode decrypts two executable files from a Word document: a driver file and installer DLL. It then passes the work to the extracted installer file, which injects the code into services.exe defined by the installer configuration file. The code then runs the installer DLL. Finally, the shellcode erases itself from memory and replaces it with zeros (Chien, O'Murchu, L., & Falliere, 2011).

3.3.10. The Shamoon Malware

Saudi on August 15, 2012 Arabia's national oil production, sales, crude oil refineries, natural gas and Saudi Arabia, which is the company petroleum products Arabian Oil Firm (Saudi Aramco), based about 30,000 Windows operating system is infected with a computer virus into the computer network. Saudi Aramco, the world has a very large share of the oil market. 10% of the global supply, which holds 13% of the global production and is the world's largest oil producer with annual revenues of $ 200 billion. Shamoon malware infected data on their personal computers at Saudi Aramco employees and computer hard disks were indiscriminately delete. Any oil spill, explosion or failure of this attack despite the absence of a larger company's production and business activities, such as the deletion of the information has been seriously affected production rates. The Shamoon also RasGas Qatar spread to other oil and gas and oil companies such as Exxon Mobil.

Shamoon attacks in the Middle East does not give rise to any physical damage has also been secondary effects on the risk assessment for critical service providers worldwide. This event also raised serious security concerns between the US and Iran. Term US

Defense Secretary Leon Panetta, to the Shamoon "very complex" and "very concerned about the use of this type of vehicle makers" have shaped explanation (Bronk & Ringas, 2013).

3.3.11. Flame malware

Flame virus is highly developed, transmitted based on computers running Microsoft Windows operating system and a software written for the purpose of espionage. At the same time, one of the mechanisms needed to spread within local networks is quite remarkable. Disguising itself as a Windows security update, it spreads over a local network via Windows Update.

According to the Budapest University of technical reports made by the crysys Lab.; Flame, keyboard entries, collects information such as screenshots and possible microphone and camera images. After the initial infection is available in several modules that can be downloaded. Fully configured size is more than 20MB. This is quite a size malware and more. Flame spreads across networks using Windows update and the air gap may exceed also with removable drives. When Flame infect a computer within a network, wpad itself to save as proxy for update.windows.co (Web Proxy Auto-Discovery Protocol) use, and data services fake security update to install itself to other computers on the network (Fillinger, 2013). Flame does not spread quickly, the majority of which are in the Middle East is a very small number of computers affected by this malicious software. First variation of Iran (CERT) was discovered in 2012 by May. According to Kaspersky (REPUBLIC OF TURKEY Ministry of Transport, Maritime Affairs and Communications, 2014); It was active until at least 2010, but CRYSYS Lab, discovered by computer security firm Webroot, which in 2007 and the name of the dynamic link library used in WAVESUP3 Flamini. It has documented the DRV file name. In this case, that period Flamini or variations of previous shows is already active. Most of the infected computer, this software was geography Iran.

3.3.12. Cyber-Attacks on Natural Gas Pipeline Company

In 2012, for 6 months, the identity cannot be determined exactly (being claimed to be from China), a hacker group by the United States to the gas pipeline control systems and continuous cyber-attack was organized in a coordinated manner. Attackers "spearphishing" using the technique of providing access to the pipeline control system were aimed at stealing passwords. When the attackers left, they sent emails pretending to come from a friend or acquaintance of the people they target and attachments in the e-mail it is infected with malware or link opens the target computer.

3.3.13. Ukraine power outage

On December 23, 2015 approximately half of the settlements in Ivano-Frankivsk in Ukraine (1.4 million people) lived a few hours of power outage. The reason for this interruption according to researchers at cybersecurity firm ESET is a cyber-attack (ESET, 2016).

According to ESET employees; attackers unbootable KillDisk components in the way they intended target computer "BlackEnergy" attacks have been carried out using the back door.

BlackEnergy back door, it consists of trojan horse modular structure and uses a variety of downloadable components to carry out specific tasks. In 2014, against several high-profile state institutions in Ukraine are used in cyber espionage activities. In the latest attack against the electricity distribution companies, the KillDisk Trojan horse has been previously downloaded and executed on the infected systems BlackEnergy Trojan horse.

The connection between the first and KillDisk blackenergy November 2015, Ukraine has been reported by CERT-UA. Meanwhile, during the local elections it has been attacked many media organizations in Ukraine. The report on the results of these attacks have been claimed by several video materials and various documents were destroyed.

The variation used in KillDisk carried out attacks against the Ukrainian power distribution company has some additional functions. This special variant of the boot as well as deleting system files to do the code system has been designed to sabotage industrial control systems.

ESET malware analyst Anton Cherepanov; "Aside KillDisk normal function also works to finalize the transaction on the platform commonly used in industrial control systems" says (ESET, 2016).

If this process were found on the target system, Trojan horse not only stop this process but also the author of system executable files on the hard disk with random data related to complicate the work again.

Cherepanov also "Our work on the detected KillDisk malware in several electricity distribution companies in Ukraine in November 2015 shows that the same as the tools used in the attack on the Ukrainian media," he said (Cherepanov, 2016).

The development blackenergy'n 2015

Blackenergy is active, blackenergy variants infected computer in order to assess whether it is desired target allows to control certain criteria. In this case, a normal blackenergy variant of the dropper is pushed into the system.

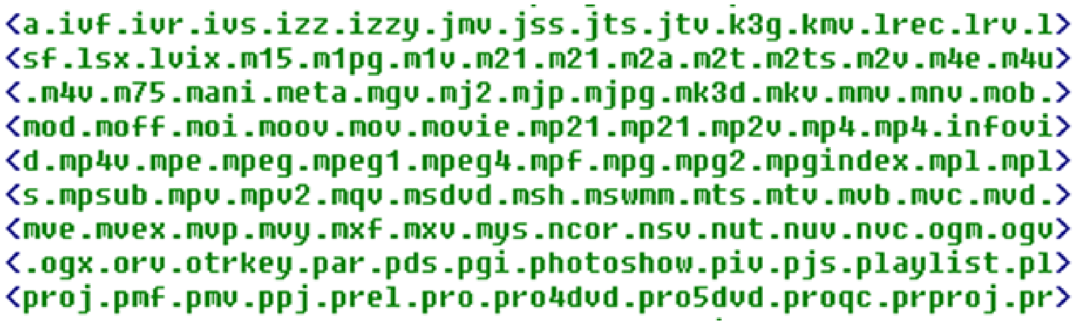
Unlike the C&C server configuration blackenergy "build_id" holds value. This value blackenergy the initiative infection by malicious software or operator is a unique text string that is used to identify individual transmission. The number of combinations of letters and the public can use the information about the target system.

ESET defined in an attack by Ukraine in 2015 "build_id" values are as 2015, khm10, khelm, the 2015telsm, 2015ts, 2015stb, kiev_o, brd2015, 1131526kbp, 02260517e to, 03150618aa, 11131526trk

Some of these values have the meanings given. For example, "2015telsm" value of Russian in Sredstva Massovoj Informaciya (Mass Media, SMI) or the abbreviation "2015." Energy can mean.

KillDisk component

In 2014, some variants blackenergy "DST is" housed plugin designed to bring down the system is infected. In 2015, ESET, blackenergy group of Win32 / killdisk.nbb Win32 / killdisk.nbc and Win32 / disruptive components such as the new Trojan variants has determined that killdisk.nbd use. The main purpose of these components by overwriting with random data and documents operating system is to provide data storage on the computer instead of by preventing damage to boot (Cherepanov, 2016).



```
<a.ivf.ivr.ivs.izz.izzy.jmv.jss.jts.jtv.k3g.kmv.lrec.lrv.l>
<sf.lsx.lvix.m15.m1pg.m1v.m21.m21.m2a.m2t.m2ts.m2v.m4e.m4u>
<.m4v.m75.mani.meta.mgv.mj2.mjp.mjpg.mk3d.mkv.mmv.mnv.mob.>
<mod.moff.moi.moov.mov.movie.mp21.mp21.mp2v.mp4.mp4.infovi>
<d.mp4v.mpe.mpeg.mpeg1.mpeg4.mpf.mpg.mpg2.mpgindex.mpl.mpl>
<s.mpsub.mpv.mpv2.mqv.msdvd.msh.mswmm.mts.mtv.mvb.mvc.mvd.>
<mve.mvex.mvp.mvy.mxf.mxv.mys.ncor.nsv.nut.nuv.nvc.ogm.ogv>
<.ogx.orv.otrkey.par.pds.pgi.photoshow.piv.pjs.playlist.pl>
<proj.pmf.pmv.ppj.prel.pro.pro4dvd.pro5dvd.proqc.prproj.pr>
```

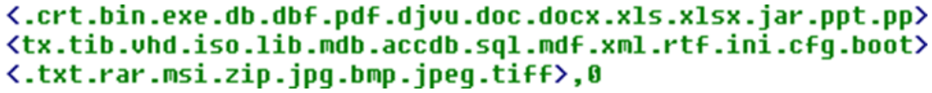
Figure 3.16: List of the Targeted File Extension to Destroy by killdisk.nbb (ESET, 2016)

Contact the company used in the attacks on the Win32 / killdisk.nbb variant is used to destroy many documents and files. There is a long list of file extensions that tries to write on and erase. A portion of the full list of the variant contains more than 4000 of file extensions and file extensions shown on figure 3.16.

KillDisk component used in actual attacks against the energy company in Ukraine is somewhat different. According to the changes in the new version of ESET's analysis:

- The destruction of the active load accepts command line argument to set a specific time delay, if necessary.
- Deletes the Windows event logs: Application, Security, Setup, System

Document deletion is less focused. 35 only the extensions corresponding target file extension is taken is shown in Figure 3.17.



```
<.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pp>
<tx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot>
<.txt.rar.msi.zip.jpg.bmp.jpeg.tiff>,0
```

Figure 3.17: List of File Extensions That are Targeted for Destruction by the New Variant of Killdisk Component (Cherepanov, 2016)

No boot of the side erase system files to do the sequence - such destructive typical functionality for trojan - particularly industrial systems, electrical distribution KillDisk variants detected in the company seeking to sabotage contains some additional functions. When activated, it calls the two variants KillDisk non-standard transactions and ends: komut.exe and sec_service.exe.

The second of these operations (sec_service.exe) of software used in an industrial control system (ASEM Ubiquity or ELTIMA serial-to-ethernet connector) process and malware uses it overwrites the executable but also with random data not only prevents the operation of this embodiment.

The first of these transactions (komut.exe) does not include detailed information about, but in Turkish means the command used instead of command. This situation shows that the targeted Turkish operating system. The above-described "build_id" value of "11131526trk" worth "trk", "Turkey" may be represented as, but "11131525" figures are yet unknown means. in Stuxnet worm 19790509 as the value is significant tension in Iran-Israel relations will be continued research will make any value.

In this part of the thesis of those components will be used in cyber security relationship EMS system, the weakness of these components as a result of threats and possible attacks on these components are mentioned risks that may occur. In addition, the SCADA of the tools used in leak tests of the system and existing SCADA cyber made for this system by mentioning the cyber-attacks on system attacks the result of national security, a possible functional disorder has been emphasized that may even threaten. This section of the Modbus TCP protocol weakness and particularly mentioned attacks on this protocol, Modbus protocol proposed in the following sections of the thesis poses a significant security infrastructure to make it work.

CHAPTER 4
RECOMMENDED STUDY FOR MODBUS TCP PROTOCOL SECURITY

Working Modbus TCP protocol, source IP address control as detailed earlier in this chapter and encryption use vulnerabilities have been shown and interrupt the vulnerability of attack (MITM) with details could appear to be in clear text flowing Modbus packets in simulation environment which will be described in the following sections and to the Metasploit Framework with modules Modbusclient was observed in the same simulated environment can be changed using the read register value. Attack data packets and normal data are sent using Wireshark tool captured data were analyzed and compared. Made in a controlled intermediate layer using the results of this analysis to prevent or mitigate the attack for the Python programming language was developed. The intermediate layer further comprises a control function to control details by the operator that manages the control system will be described in the following sections to deliberate or inadvertent register value to prevent entry value above a predetermined value are added. Thus, the Modbus TCP protocol to communicate with a control by an unauthorized internal or external network for the system data to be entered and one of the threats which are thought to pose the greatest risk of cyber-security community, which in the literature "intruder" as the named disgruntled or malicious employee at a specified value by more than entry It is intended to prevent or alleviate disease

4.1. Scada Testbed

Modbus TCP packets in order to analyze the work done to ensure the security is prepared using a software simulation environment (Witte Software, 2018). This simulation environment is being prepared with the Modbus TCP protocol to communicate over a local network does not have an internet connection. Kali Linux operating system is used to control packets in the intermediate layer and that is running the Python code developed under study Ubuntu operating system is preferred to perform attacks.

The experimental setup for the topology of the proposed security Modbus TCP protocol is given in Figure 4.1. According to the Modbus Master is installed on the

Windows 7 machine as the MTU is running. The default is to send the package via Modbus port 502. Assumptions as control of a nuclear power plant or a manufacturing plant It considered as a central server which manages the system. Modbus RTU as a slave is installed on Windows 7 is running. This machine is listening to stored Modbus communication port 503 is provided via this port. Assumptions as to send a manufacturing plant or a nuclear power plant centrifugation of temperature readings values of rotational frequency can be considered a central server officer of PLC devices. As a control, the intermediate layer was specified during communication between the two devices is controlled to come and outbound packets, it is located on the Modbus TCP protocol security Ubuntu machine is running in order to provide the Python code written. Details of the machine according to the code 503 as described below. At the values entered on the MTU, the control goes to the control middle layer, where the packages with the controls in the control of the packets are sent to the PLC device and written to the registers. There is also a website with experimental setup available for a virtual wireless internet connection developer.

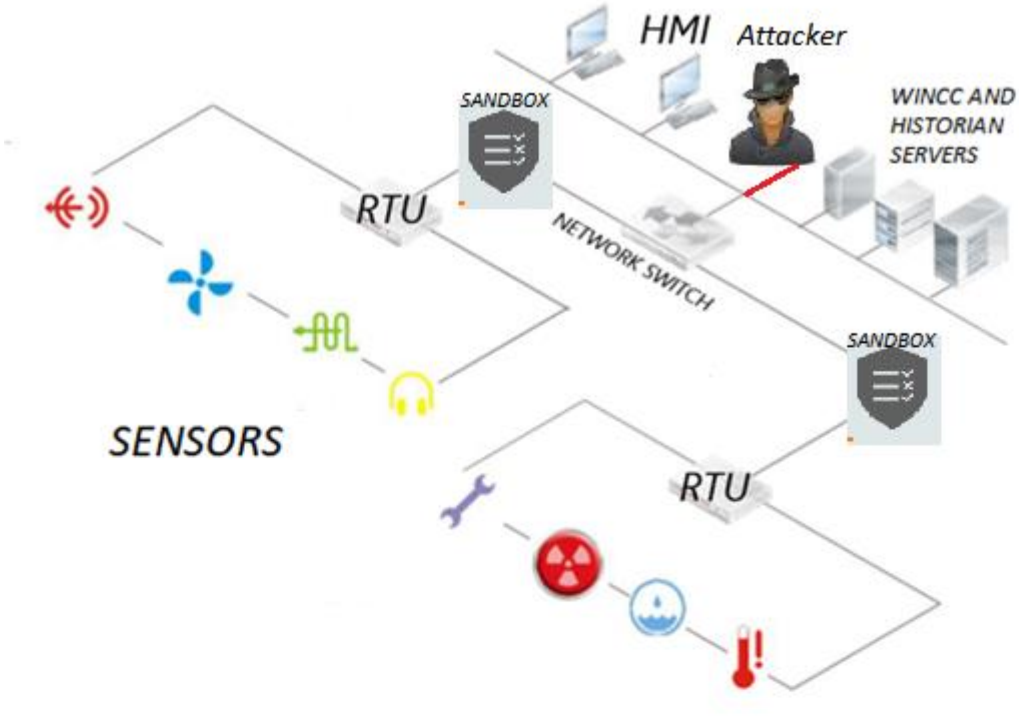
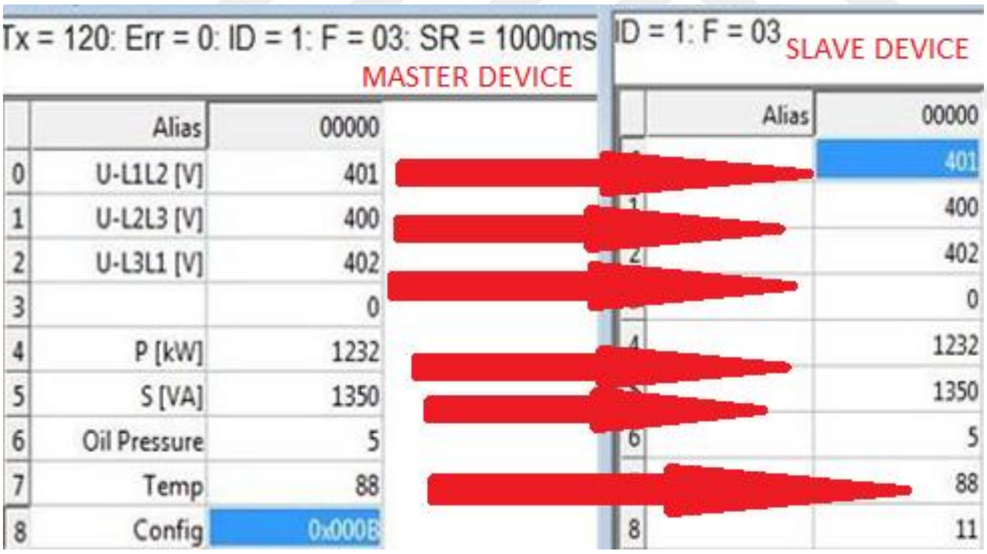


Figure 4.1: Modbus TCP security topology with Sandbox

The simulation environment is designed for a local network, as mentioned ICS. The reason is that use of ex SCADA system, a high percentage of the internet site as an open and a closed network is used for realization of the communication between MTU and RTUs. Thus, the thesis is designed on a local network in order to find solutions to a wider area.

Modbus Master and Modbus Slave simulation environment for the analysis of packet for TCP protocol has been established. Multiple email interface several Modbus slave or data field can be displayed simultaneously. Modbus Slave ID on each screen, function and address can be determined as a special register and read and write operations to be performed.

In the proposed testbed, Modbus Master program is running on the Windows 7 operating system, which earlier this program is working as MTR given details. The Modbus Slave program is running on the Windows 7 operating system is working as RTU. These operating systems that run the Modbus Master and Modbus Slave program is on the same network can communicate with each other. Thus, the values entered in the register values can be written on the Modbus Master Modbus TCP protocol is sent to the registers on Modbus Slave and can be read.



Tx = 120: Err = 0: ID = 1: F = 03: SR = 1000ms

MASTER DEVICE

	Alias	00000
0	U-L1L2 [V]	401
1	U-L2L3 [V]	400
2	U-L3L1 [V]	402
3		0
4	P [kW]	1232
5	S [VA]	1350
6	Oil Pressure	5
7	Temp	88
8	Config	0x000B

ID = 1: F = 03 SLAVE DEVICE

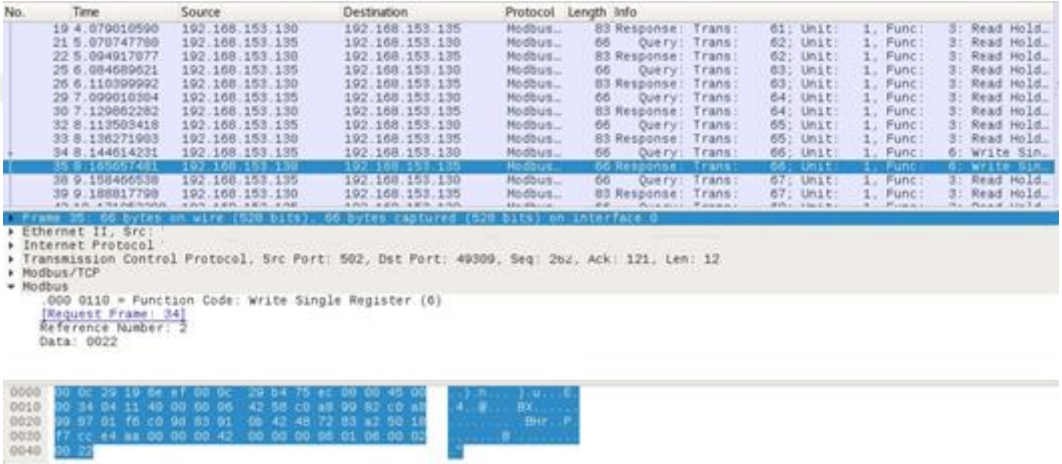
	Alias	00000
0		401
1		400
2		402
3		0
4		1232
5		1350
6		5
7		88
8		11

Figure 4.2: Modbus Master and Modbus Slave

Used in the study in Figure 4.1 Modbus master and slave simulators of screen images is provided. The value entered in the registers Modbus master, Modbus TCP protocol connection between them is written thanks sent to the Modbus Slave registers.

4.2. Analysis of Packages

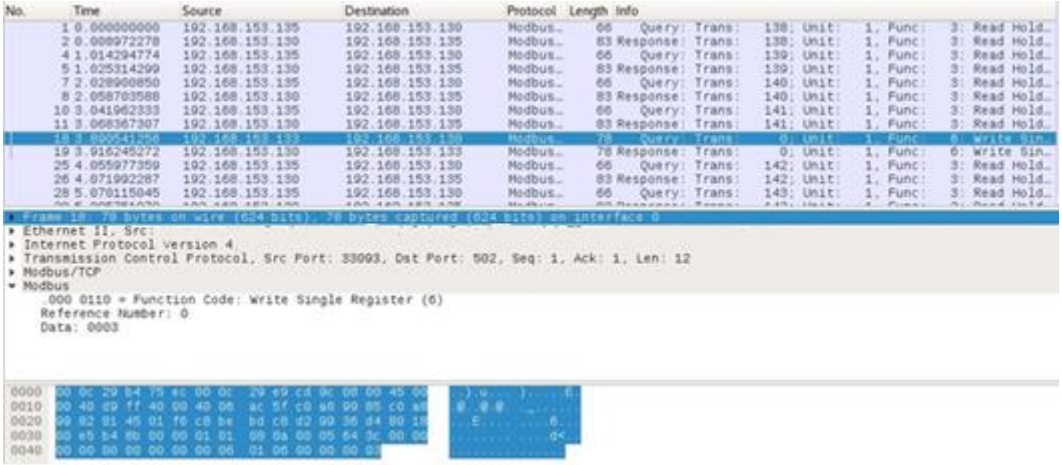
Master Modbus Modbus slave and Modbus TCP packets flowing between captured and analyzed using Wireshark offensive machine tool. Initially Modbus Modbus master and slave machines caught flowing between normal Modbus TCP packets and the attacker machine afterwards Metasploit Framework manipulated Modbusclient module using Modbus TCP packets have been captured. Thus, the normal Modbus TCP packet is analyzed by comparing the manipulated Modbus TCP packets. Figure 5.3 Modbus Modbus master and slave machines Modbus TCP packets flowing between "write_regist" function code captured by the Wireshark tool is shown.



```
No.   Time          Source           Destination      Protocol  Length Info
   19 4.079010590   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:    61; Unit:   1, Func:   3: Read Hold…
   21 5.078747780   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:    62; Unit:   1, Func:   3: Read Hold…
   22 5.094917077   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:    62; Unit:   1, Func:   3: Read Hold…
   25 6.084689621   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:    63; Unit:   1, Func:   3: Read Hold…
   26 6.110399992   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:    63; Unit:   1, Func:   3: Read Hold…
   29 7.099010304   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:    64; Unit:   1, Func:   3: Read Hold…
   30 7.129862282   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:    64; Unit:   1, Func:   3: Read Hold…
   32 8.113503418   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:    65; Unit:   1, Func:   3: Read Hold…
   33 8.136271903   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:    65; Unit:   1, Func:   3: Read Hold…
   34 8.144614231   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:    66; Unit:   1, Func:   6: Write Sin…
   35 8.165657481   192.168.153.130  192.168.153.135  Modbus…   66 Response: Trans:    66; Unit:   1, Func:   6: Write Sin…
   38 9.158466538   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:    67; Unit:   1, Func:   3: Read Hold…
   39 9.188817798   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:    67; Unit:   1, Func:   3: Read Hold…

▸ Frame 35: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src:
▸ Internet Protocol
▸ Transmission Control Protocol, Src Port: 502, Dst Port: 49309, Seq: 262, Ack: 121, Len: 12
▸ Modbus/TCP
▾ Modbus
    .000 0110 = Function Code: Write Single Register (6)
    [Request Frame: 34]
    Reference Number: 2
    Data: 0022

0000  00 0c 29 19 6e ef 00 0c  29 b4 75 ec 00 00 45 00   ..).n... ).u...E.
0010  00 34 04 11 40 00 00 06  42 58 c0 a8 99 82 c0 a8   .4..@... BX......
0020  99 87 01 f6 c0 9d 83 91  0b 42 48 72 83 a2 50 18   ........ .BHr..P.
0030  f7 cc e4 aa 00 00 00 42  00 00 00 06 01 06 00 02   .......B ........
0040  00 22                                              ."
```

Figure 4.3: Normal Modbus TCP packet

Figure 4.4 is manipulated by the attacker machine Wireshark output Modbus TCP packet was sent is displayed.



```
No.   Time          Source           Destination      Protocol  Length Info
    1 0.000000000   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:   138; Unit:   1, Func:   3: Read Hold…
    2 0.008972278   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:   138; Unit:   1, Func:   3: Read Hold…
    4 1.014294774   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:   139; Unit:   1, Func:   3: Read Hold…
    5 1.025314299   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:   139; Unit:   1, Func:   3: Read Hold…
    7 2.028900850   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:   140; Unit:   1, Func:   3: Read Hold…
    8 2.058703588   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:   140; Unit:   1, Func:   3: Read Hold…
   10 3.041962333   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:   141; Unit:   1, Func:   3: Read Hold…
   11 3.068367307   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:   141; Unit:   1, Func:   3: Read Hold…
   18 3.890541256   192.168.153.133  192.168.153.130  Modbus…   78    Query: Trans:     0; Unit:   1, Func:   6: Write Sin…
   19 3.916246272   192.168.153.130  192.168.153.133  Modbus…   78 Response: Trans:     0; Unit:   1, Func:   6: Write Sin…
   25 4.055977359   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:   142; Unit:   1, Func:   3: Read Hold…
   26 4.071992287   192.168.153.130  192.168.153.135  Modbus…   83 Response: Trans:   142; Unit:   1, Func:   3: Read Hold…
   28 5.070115045   192.168.153.135  192.168.153.130  Modbus…   66    Query: Trans:   143; Unit:   1, Func:   3: Read Hold…

▸ Frame 18: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Ethernet II, Src:
▸ Internet Protocol Version 4
▸ Transmission Control Protocol, Src Port: 33093, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
▸ Modbus/TCP
▾ Modbus
    .000 0110 = Function Code: Write Single Register (6)
    Reference Number: 0
    Data: 0003

0000  00 0c 29 b4 75 ec 00 0c  29 e9 cd 0c 08 00 45 00   ..).u... )....E.
0010  00 40 d9 ff 40 00 40 06  ac 5f c0 a8 99 85 c0 a8   .@..@.@. ._......
0020  99 82 81 45 01 f6 c8 be  bd c0 d2 99 36 d4 80 18   ...E.... ....6...
0030  00 e5 b4 8b 00 00 01 01  08 0a 00 05 64 3c 00 00   ........ ....d<..
0040  00 00 00 00 00 00 00 06  01 06 00 00 00 03         ........ ......
```

Figure 4.4: Manipulated Modbus TCP packet

The analysis made by comparing the captured packets x.x.x.135 IP addressing Modbus from the master device x.x.x.130 IP address to the Modbus slave device Modbus TCP packets sending manipulated in the pack has been observed to be sent to the x.x.x.133 IP addressing offensive machine. Packages of other parameters just by changing the source IP address of the packet and that there is no change was observed to be sent in this way. Slave device to control packets from the source IP address that has been noticed him. As a result of this analysis showed that during the communication that occurs between two devices to control the source IP address that sent the Modbus TCP Modbus slave devices to IP-based package for the Windows firewall is used. In addition to Modbus TCP packets flowing between the devices that control over the specified value as threshold value data segments in the packet it is aimed at developing an intermediate layer order cannot be entered. In addition, a safety mechanism will make it possible for the possibility of an attack on the attacker's control middleware has been developed. Thanks to this safety mechanism will be blocked except for requests from the Modbus TCP Modbus Master. Thus, Modbus slave device only accepts Modbus TCP packet from the control middleware to handle their own registers, coming from another IP address after checking Modbus TCP packets in the intermediate layer will be working on their own registers.

4.3. Control Middleware

A control interface has been developed for the control of Modbus TCP packets placed between the Modbus Master and Modbus Slave devices and flowing between the two devices. This control layer is a machine with Ubuntu operating system that runs Python code developed based on work, it receives the Modbus TCP packets flowing on the network itself and can be called as Sandbox because it provides control with the developed control middle layer. The flow diagram of the control intermediate layer is given in Figure 4.5.

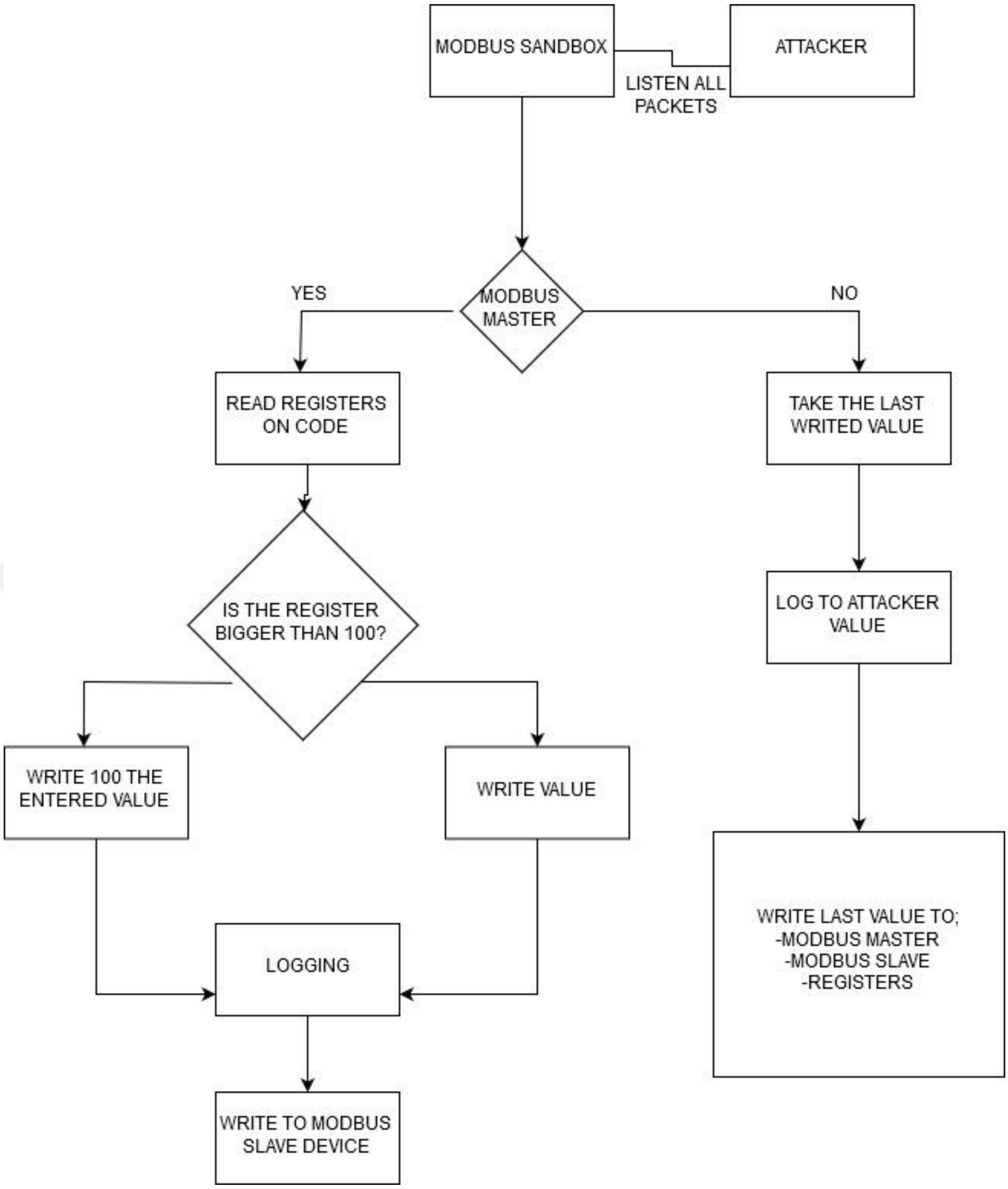


Figure 4.5: Flow Diagram of The Control Middleware

Listens to port 502 and retrieves the source IP addresses of its Modbus packets against the Modbus Master IP address and reads the values in the registers on the code if the IP addresses overlap. If these values are greater than 100, they write 100 as the register value, and if less than 100, they write the value as read. The value 100 specified here is a default value selected in the simulation environment. It can be considered as the temperature value of the medium in a system room or the centrifugal rotation frequency value in a nuclear power plant. Then, register the values in the registers to the desired Modbus log file and write the values to the registers in the Modbus Slave.

If the IP addresses do not match, the code will recognize it as an attack and retrieve the last correct data. Logs the attacker's data in the log file “AttackerModbus” It then writes the last actual data to the registers on the Modbus Master, Modbus Slave and control intermediate layer. With the proposed test setup as a solution for the security of the Modbus TCP protocol, when the attacker attempts to write unauthorized data to the registers of the Modbus Slave using the Metasploit Framework Modbusclient module, the Modbus Slave will be plugged into the IP and port-based firewall in front of it and will not be able to enter unauthorized data. Similarly, when an attacker attempts to enter data into Modbus Sandbox registers, the data threshold of the control interface will be inserted into the control mechanism and will not be able to enter data unauthorized. At the same time, the attacker's actions will be logged on the Sandbox side. However, if you try to write a value over 100 legally on the Modbus Master side, the maximum value of 100 can be entered in the registers. With this limitation, it is made impossible to enter data on a specified value, such as temperature value or centrifugal rotation frequency value, for example in control systems in a generation facility or an electric distribution area.

In this section, instead of using a direct control middleware developed by MTU considered such control can be done over, but the use of such a system will make it impossible to control all traffic on the local ICS network. With the proposed control middleware Modbus field devices and all TCP packets flowing between the central server can be controlled.

4.4. Attack Analysis

A test set is designed as shown in Figure 5.2 in aggressive computer with Kali Linux operating system security test means for using the server and port scan process and the process data section in Modbus packet with the information obtained was tried to change whether manipulated. This scanning and data manipulation operations that are later in this section will be provided with the display images, the first step in the operation illustrated performed without the recommended defense mechanisms, was performed by using defense mechanisms developed through later thesis and the results were analyzed. Thus, the control middleware developed as defense mechanisms will be examined whether the Modbus host Sandbox sheltered weakness.

The simulation environment in MT and RT packets flowing between the aggressive attack scenario that the intervention by the basic level in Figures 5.6 shown. As can be seen; aggressive, RTU sends this data by responding to read messages of MTU devices write their own register written authority outside their own registers data when the simulation environment Send an unauthorized manner Modbus TCP writing the value of the RTU device. As a result, the attacker succeeds manipulation operation and register values on both the MTU and RTU devices are changed by an unauthorized person.

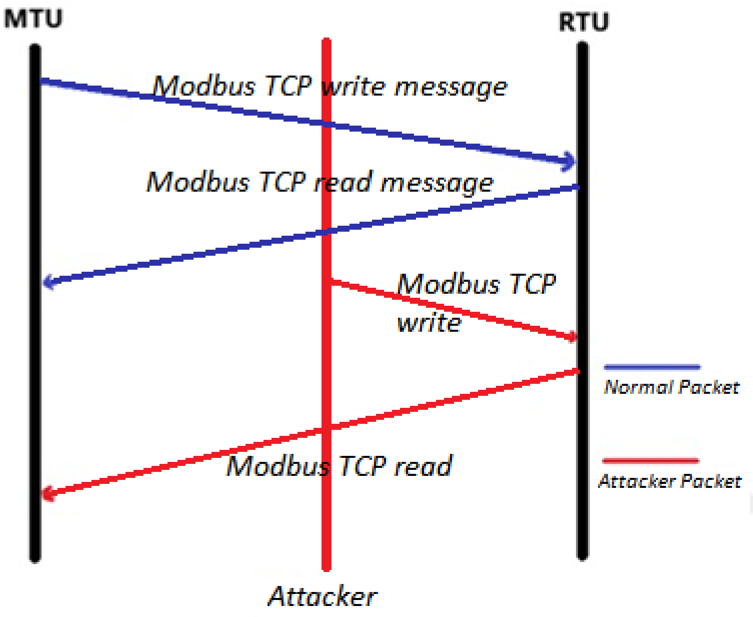
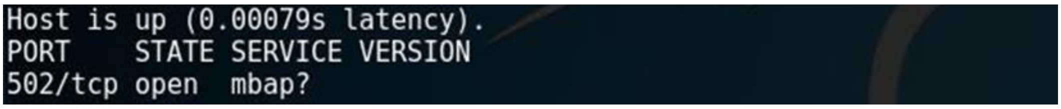


Figure 4.6: Attack Scenario on A Vulnerable System

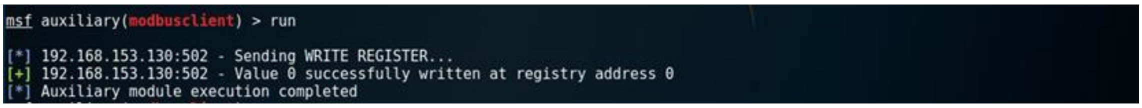
First, check intermediate layer attacks without added only communicate in an environment where no security measures analysis of Modbus Master and Modbus Slave device was performed. For this purpose, initially using nmap scanning tool located in the internal network and the Modbus TCP protocol service that is running on the device operates as the default port 502. Ports were determined. Thus, the targeted device is determined. The port 502 is open at this stage on the Modbus slave device and was monitored on the service that is running. In Figure 4.7 The results of the network scan are shown.



```
Host is up (0.00079s latency).
PORT    STATE SERVICE VERSION
502/tcp open  mbap?
```

Figure 4.7: Nmap Scan on A Vulnerable System

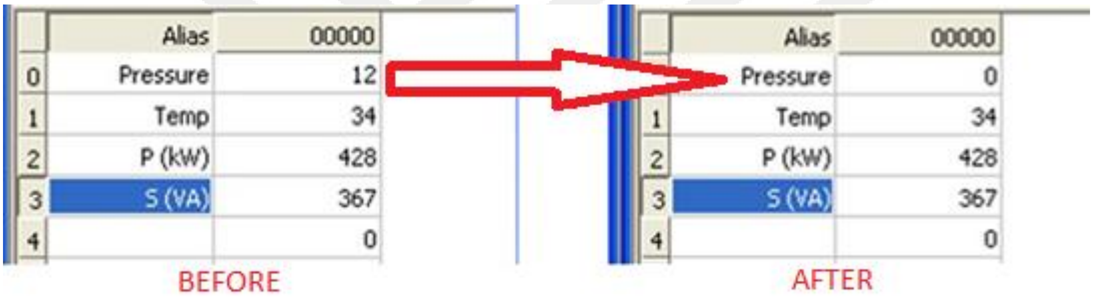
After the scan is previously given details Metasploit Framework modbusclient module register values that are determined to work on the device using the Modbus service is tried to be manipulated. To do this, the register address instead of the address is 0 value is entered by an unauthorized person. Manipulated process Figure 4.8, this results in showing values in Modbus slave device after the attack and attack values before changes in the values in registers on is presented in Figure 4.9.



```
msf auxiliary(modbusclient) > run

[*] 192.168.153.130:502 - Sending WRITE REGISTER...
[+] 192.168.153.130:502 - Value 0 successfully written at registry address 0
[*] Auxiliary module execution completed
```

Figure 4.8: Manipulating the Process in Vulnerable System

As a result of the attack, register 0 is successfully entered address 0 within the abuse module. After manipulation on Modbus Slave device, it has been observed that the change in the register values and the attack have been concluded successfully.



	Alias	00000
0	Pressure	12
1	Temp	34
2	P (kW)	428
3	S (VA)	367
4		0

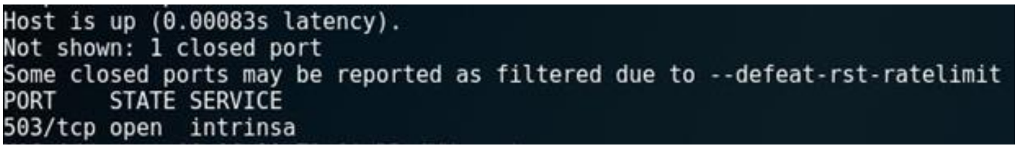
BEFORE

	Alias	00000
	Pressure	0
1	Temp	34
2	P (kW)	428
3	S (VA)	367
4		0

AFTER

Figure 4.9: Modbus Slave Register Value (a) Attacks Before (b) After the Attack

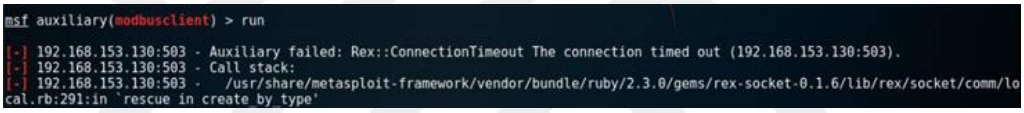
It has been observed that the cyber-attack performed successfully when no control intermediate layer is used in the vulnerable system, i.e. communication between Modbus Master and Modbus Slave devices. In the second stage, the topology shown in Figure 4.2 where Modbus Sandbox and Windows firewall is used as a defense mechanism between Modbus Master and Modbus Client devices was performed and the attack results were observed. In this part of the attack, the Nmap tool is used for network scanning again and the modbusclient module for data manipulation is used as the attack tool. However, according to the network topology, Modbus Slave is communicating over the 503 port, not the default Modbus port. Modbus Sandbox communicates through the default Modbus communication port, i.e. 502 port. In other words, if the attacker scans the servers directly on the network with the Modbus default port open, it will not be able to detect the Modbus Slave devices. This may in some way be considered a security measure because the attacker cannot detect the Modbus device with default attack vectors. In this study, the devices with both port 502 and port 503 open on the network were detected by Nmap scanning and manipulation process was performed on these devices using modbusclient and it was observed that the changes in the values on the registers on Modbus Slave and Modbus Sandbox machines were successful. Figure 4.10 shows the results of the Nmap scan and Figure 4.11 shows the screenshots of the manipulation process.



```
Host is up (0.00083s latency).
Not shown: 1 closed port
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
503/tcp open  intrinsa
```

Figure 4.10: Nmap Scan in Defended System

According to the scanning results, as discussed above in the Modbus slave device 503 port, Modbus sandbox device 502 has been determined that port is open.

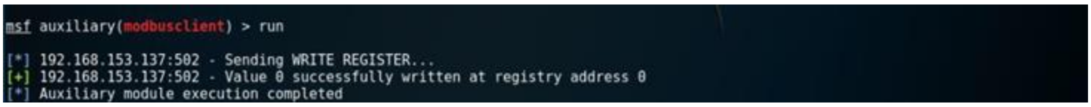


```
msf auxiliary(modbusclient) > run

[-] 192.168.153.130:503 - Auxiliary failed: Rex::ConnectionTimeout The connection timed out (192.168.153.130:503).
[-] 192.168.153.130:503 - Call stack:
[-] 192.168.153.130:503 -   /usr/share/metasploit-framework/vendor/bundle/ruby/2.3.0/gems/rex-socket-0.1.6/lib/rex/socket/comm/lo
cal.rb:291:in `rescue in create_by_type'
```

Figure 4.11: Manipulation Process in Defended System

Using modbusclient module according to Figure 5.11, an unauthorized entry of the value 0 to the register 0 of the Modbus Slave device was attempted, but according to the topology, the IP and Port-based firewall blocked this attack and no intervention was made to the registers in the Modbus Slave.

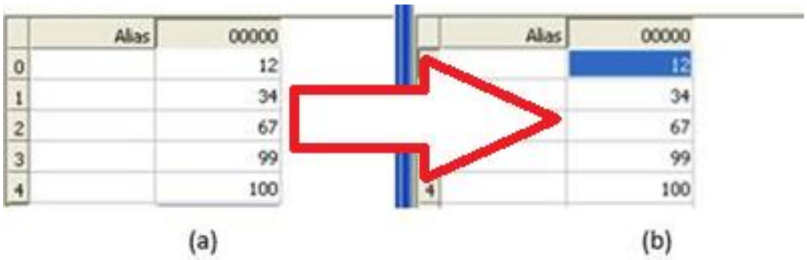
According to the results of the nmap scan, the Modbus Sandbox device whose port 502 is found to be open is manipulated by the control middle layer, whose details are given in the above sections, and blocks the attacker's log in a file named Attacker Modbus. At the same time, if a register value in the Modbus Master device is entered above 100 with the control function in the code, this operation will be blocked, and it will write up to 100 in the register in the Modbus Slave device. Figure 4.12 provides a screenshot of the manipulation process for the Modbus Sandbox.



```
msf auxiliary(modbusclient) > run

[*] 192.168.153.137:502 - Sending WRITE REGISTER...
[+] 192.168.153.137:502 - Value 0 successfully written at registry address 0
[*] Auxiliary module execution completed
```

Figure 4.12: Manipulation Process for A Defended System to Modbus Sandbox

This cyber their attacks option after the attack process as indicated 0. Register address to the value 0 was attempted to be entered in an unauthorized manner and code when attack code to run is stated that the successful work involved writing by the value entered. However, Modbus slave device registers was observed to examine if the attack has failed and changes in register values. Related screenshots are presented in Figure 4.13.



	Alias	00000
0		12
1		34
2		67
3		99
4		100

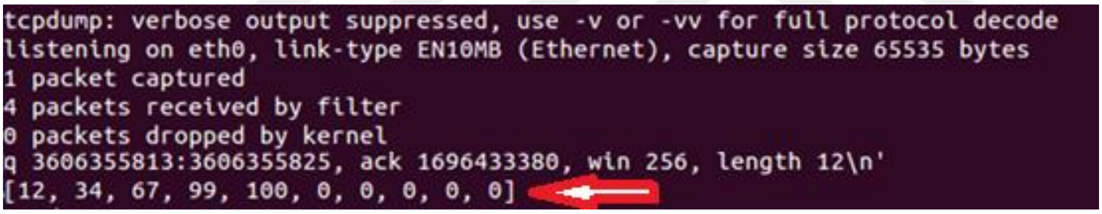
(a)

	Alias	00000
		12
		34
		67
		99
4		100

(b)

Figure 4.13: Modbus Slave Registers Defended System (a) Pre-Attack (b) After the Attack

Figure 4.14 Modbus command line output of register values which flows in the apparatus shown Sandbox.



```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
1 packet captured
4 packets received by filter
0 packets dropped by kernel
q 3606355813:3606355825, ack 1696433380, win 256, length 12\n'
[12, 34, 67, 99, 100, 0, 0, 0, 0, 0]
```

Figure 4.14: Sandbox Device Modbus Register Values

4.5. Evaluation

In this study, it is observed that the Modbus TCP protocol is used half as a result of determining the usage rates of communication protocols in Shodan search engine and ICSs worldwide. In this study, which was put forward as a solution to the security of Modbus TCP protocol, it was shown that cyber-attacks against ICS networks can be prevented and log cyber-attacks can be logged. In addition, it is considered that it will contribute to the studies on the security of critical infrastructures in our country.

4.6. Modbus Sandbox Limitations

It was shown that the source IP address of the Modbus TCP protocol was exploited according to the topology in the experimental setup of this study and that the values in the registers on the field device could be manipulated and a Modbus Sandbox was developed to eliminate this vulnerability. The weakness detected is that the Modbus TCP protocol does not check the source IP address from which the data comes from. Therefore, the source IP address is controlled by the Modbus Sandbox machine and the source IP address from which the data comes from is controlled and when trying to enter data from an IP address different from the IP address specified in the code, the IP and Port based firewall in front of the Modbus Slave device and the Modbus Sandbox prevent it. In this case, the first method that comes to mind to circumvent this security measure is to deceive the Modbus Sandbox machine by making the necessary changes to the Ethernet interface so that the attacker's IP address is the same IP address as the Modbus Master IP address. However, when this method was tried, a Write Error was received on the Modbus Master and the attack was not successful. This is because the IP address of the attacker machine and the IP address of the Modbus Master machine are the same, resulting in an IP address conflict. On the other hand, in order to try to print new data by the attacker before the loop in which the topology devices in the code running in the Modbus Sandbox machine is opened, data can be entered to the registers in Modbus Sandbox and Slave devices without authorization. In this respect, the Modbus Sandbox registers can be successfully attacked by a brute-force attack by the attacker. As a precaution, this attack method can be prevented by the rapid processing of the software by using hardware tools such as FPGA which has fast processing capacity.

CHAPTER 5
CONCLUSIONS AND FUTURE RESEARCH

In this study, security vulnerabilities and attack vectors of SCADA systems and components, which have been one of the most important components of critical infrastructures such as energy, water, transportation, healthcare, banking, nuclear / chemical facilities and communication systems and Industrial Control Systems, have been examined. In addition to this, the most commonly used TCP / IP-based communication protocols in ICS networks have been scanned by Shodan search engine, the results have been analyzed, and statistics have been obtained, and it has been observed that the Modbus TCP protocol has used at a rate of 50% worldwide. In addition to this, the usage rates of these protocols, which have statistics, have been determined by the countries and it has been determined that our country uses ICS communication protocols with 1% among the world countries. According to these results, the most frequently used Modbus TCP protocol with 50% ratio in ICS networks has been focused and a solution proposal has been developed for the security of this protocol.

In this thesis, the security architecture proposed as a solution for the security of Modbus TCP protocol has been realized in Modbus Poll simulation environment with MITM attack. In this architecture, Modbus TCP packets flowing between Modbus Master simulated as MTU and Modbus Slave devices simulated as RTU have been analyzed using Wireshark tool. As a result of the analysis, it has been analyzed that the Modbus TCP protocol did not control the source IP, that the transmitted packets were sent in clear text without encryption, that all packets flowing between the two devices could be read and manipulated on the packets using Metasploit Framework.

In the literature, an additional function has been added to the control interface layer within the proposed testbed environment in order to prevent an undesired employee or an unconscious employee from entering an undesired value in the registers of the ICS devices called under intruder. With this function, a value above the threshold value cannot be entered in the registers of the Modbus-based ICS field devices, and if entered, the maximum threshold value will be written to the registers. However, in order to prevent the attacker from writing unauthorized data to the registers in the control interlayer, all packets coming to the interlayer have been listened and the source IP addresses of these packets have been compared. If the IP addresses of the incoming packets come from an IP address other than the Modbus Master, the system detects this as an attack and the values that are intended to be written to the registers, are not written to the middle layer registers, the last register values are written and the attack packet is logged. Thus, a new solution for data control in Modbus TCP packets flowing in ICS network, which is lacking in literature review, has been proposed and its applicability has been shown.

Risk assessments for critical information systems are another vital element. Risk assessment techniques should be used especially for cyber-attacks against infrastructures of national security.

The three components of information security are privacy, integrity and accessibility. Accessibility is the most important component due to the real-time operation of SCADA systems. It is highly likely that even a time delay of milliseconds during the transmission of data will result in severe disruptions to functional processes. For this reason, it may be inconvenient to perform security tests on real-time SCADA systems. Therefore, it has been concluded that security tests should be performed before the SCADA systems have been commissioned. In this context, it has been observed that some private sector organizations and universities have test setup environments for the security of SCADA systems, but they have been insufficient for national studies. In this respect, it has been suggested that a national research and development laboratory and experimental mechanisms should be established with the cooperation of public, university and private sector in order to secure the national energy infrastructure in our country.

Within the scope of this study, the usage rates of ICS communication protocols and the usage rates of our country in the world have been determined and Modbus TCP protocol has been used in a significant rate of 50%. In this context, the current study provides solutions for the safety of half of the Shodan search results.

Also mentioned first in earlier studies "2013-2014 National Cyber Security Strategy and Action Plan" and the second "2016-2019 National Cyber Security Strategy" scope has been considered to make contributions to the work done to protect the strengthening and critical infrastructure cyber defense.

Proposed for study the main limitations of Python code running on control intermediate layer, making brute-force attack the attacker's security system register values on the field device could be changed by an unauthorized person. This makes parallel processing methods to prevent the attacks and hardware solutions, such as improved FPGA with faster processing power.

As a general conclusion, the loss of functional operations, damage or data transmission occurring manipulations result of the public order, human life, economic loss, national or global level security interrupting could be created awareness of security of critical infrastructure systems, and it has been supposed designed accordingly there is no doubt. Especially in our country, the use of electricity distribution companies to reconsider the control system and communication protocols need to be addressed in terms of cyber security. One of the most important safety systems in the SCADA system for critical infrastructure is of vital importance. Therefore, the communication of SCADA systems has been proposed thesis presented a study for the most commonly used Modbus protocol security. Recommended operating system integrated with the facts of the study; both the internal network will mitigate the impact of cyber-attacks coming from the external network. Thus, with the thesis presented a critical SCADA infrastructure has been expected to contribute to the security of the system.

REFERENCES

Abdelmajid, N. T., Hossain, M. A., Shepherd, S., & Mahmoud, K. (2010). Location-Based Kerberos Authentication Protocol. *SocialCom 2010: 2nd IEEE International Conference on Social Computing* (pp. 1099–1104). Minneapolis: IEEE.

Aloui, N. B. (2016). Industrial Control Systems Dynamic Code Injection. *GreHack.* Grenoble: GreHack.

Alphonsus, E. R., & Abdullah, M. O. (2016). A Review on The Applications of Programmable Logic Controllers (PLCs). *Renewable and Sustainable Energy Reviews*, 1185-1205.

AlShemeili, A., Yeun, C. Y., & Baek, J. (2016). PLC Monitoring and Protection for SCADA Framework. *Advanced Multimedia and Ubiquitous Engineering*, 259-267.

Alves, R. a. (2014). A Summary of Control System Security Standards. *U.S. Department of Energy Office of Electricity*, 1-5.

Amanullah, M. T., Kalam, A., & Zayegh, A. (2005). Network Security Vulnerabilities in SCADA and EMS. *Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference* (pp. 1-6). Dalian: IEEE.

American Petroleum Institute. (2009). *API STANDARD 1164 - Pipeline SCADA Security.* Washington: American Petroleum Institute.

BBC. (2003, 10 17). *Questions cloud cyber crime cases*. Retrieved from BBC: http://news.bbc.co.uk/2/hi/technology/3202116.stm

Beresford, D. (2011). Exploiting Siemens Simatic S7 PLCs. *BlackHat 2011* (pp. 1-26). Las Vegas: UBM.

Bergman, D. C., Jin, D., Nicol, D. M., & Yardley, T. (2009). The Virtual Power System Testbed and Inter-Testbed Integration. *Proceedings of the 2nd conference on Cyber Security Experimentation and Test*, 1-6.

Bhatia, S., Kush, N., Djamaludin, C., Akande, J., & Foo, E. (2014). Practical Modbus Flooding Attack and Detection. . *Conferences in Research and Practice in Information Technology Series* (pp. 57-65). New South Wales: Australian Computer Society Inc.

Bhattacharyya, D. (2008). The Taxonomy of Advanced SCADA Communication Protocols. *Journal of Security Engineering,*, 517-526.

Bolton, W. (2015). *Programmable Logic Controlers, 6th.* High Wycombe: Elsevier.

Bronk, C., & Ringas, E. (2013). *Hack or Attack? Shamoon and the Evolution of Cyber*

Conflict. Houston: Institute for Public Policy Rice University.

Carlson, R. E., Dagle, J. E., Shamsuddin, S. A., & Evans, R. P. (2015). *A Summary of Control System Security Standards Activities in the Energy Sector.* Washington: U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

Centre for the Protection Of National Infrastructure. (2011, 4). *CYBER SECURITY ASSESSMENTS OF INDUSTRIAL CONTROL SYSTEMS.* Retrieved from Centre for the Protection Of National Infrastructure: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf

Centre for the Protection of National Infrastructure. (2014). *Good Practice Guide Process Control and Scada Security Guide 1: Understand the Business Risk.* London: Centre for the Protection of National Infrastructure.

Chabukswar, R., Sinópoli, B., Karsai, G., Giani, A., Neema, H., & Davis, A. (2010). Simulation of Network Attacks on SCADA Systems. *First Workshop on Secure Control Systems.* Stockholm: Carnegie Mellon.

Chandia, R., Gonzalez, J., Kilpatrick, T., & Papa, M. (2007). Security Strategies for. *Critical Infrastructure Protection SCADA Networks*, 117-131.

Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L., & Kundur, D. (2015). Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Testbed. *2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability* (pp. 1-6). Charleston: IEEE.

Cherepanov, A. (2016). *BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry.* ESET.

Chien, E., & O’Gorman, G. (2011). *The Nitro Attacks: Stealing Secrets from the Chemical Industry.* Mountain View,: Symantec Security Response.

Chien, E., O'Murchu, L., & Falliere, N. (2011). *W32.Duqu The Precursor to the Next Stuxnet.* Symantec Security Response.

Ciancamerla, E., Fresilli, B., Minichino, M., Patriarca, T., & Iassinovski, S. (2014). An electrical grid and its SCADA under cyber attacks: Modelling versus a Hybrid Test Bed. *International Carnahan Conference on Security Technology (ICCST)*, 1-6.

CISA. (2012, 10 25). *ICS Alert (ICS-ALERT-12-046-01A).* Retrieved from CISA: https://www.us-cert.gov/ics/alerts/ICS-ALERT-12-046-01A

Clarke, G. R., Reynders, D., & Wright, E. (2004). *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems.* Australia: ELSEVIER.

Clear Energy Pipeline. (2018, 2 3). *Smart Cities in Europe Enabling Innovation.* Retrieved from Clear Energy Pipeline:

http://www.cleanenergypipeline.com/Resources/CE/ResearchReports/Smart%20cities%20in%20Europe.pdf

Cook, B. (2017, 6 24). *modbusdetect.rb.* Retrieved from GitHub: https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/scada/modbusdetect.rb

Dale Peterson. (2012, 12 17). *PROFINET Fuzzer Released*. Retrieved from Digital Bond: https://dale-peterson.com/2012/12/17/profinet-fuzzer-released/

Dondossola, G., Deconinck, G., Garrone, F., & Beitollahi, H. (2009). Testbeds for Assessing Critical Scenarios in Power Control Systems. *International Workshop on Critical Information Infrastructures Security*, 223–234.

Dondossola, G., Garrone, G., Szanto, J., D. G., Loix, T., & Beitollahi, H. (2009). ICT Resilience of Power Control Systems: Experimental Results from the Crutial Testbeds. *Proceedings of the International Conference on Dependable Systems and Networks*, 554-559.

East, S., Butts, J., Papa, M., & Shenoi, S. (2009). A Taxonomy of Attacks on the DNP3 Protocol. *IFIP International Federation for Information Processing*, 67-81.

Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., & Stoddart, K. (2015). A Forensic Taxonomy of SCADA Systems and Approach to Incident Response. *Proceedings of the 3 International Symposium for ICS & SCADA Cyber Security Research* (pp. 42-51). Ingolstadt: BCS Learning & Development Ltd.

Elkin, G. (2016, 09 13). *The evolution of DDoS.* Retrieved from ITProPortal: https://www.itproportal.com/features/the-evolution-of-ddos/

Erickson, K. T. (2010, 11 1). *Programmable logic controllers: Hardware, software architecture*. Retrieved from The International Society of Automation: https://www.isa.org/standards-publications/isa-publications/intech-magazine/2010/december/automation-basics-programmable-logic-controllers-hardware-software-architecture/

ESET. (2016). *ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine.* ESET.

Ettercap. (2015, 6 8). *Ettercap.* Retrieved from Ettercap: https://ettercap.github.io/ettercap/

Fillinger, M. (2013). *Reconstructing the Cryptanalytic Attack behind the Flame Malware.* Amsterdam: Institude for Logic, Language and Computation of Amsterdam University.

Gao, W., Morris, T., Reaves, B., & Richey, D. (2010). On SCADA Control System Command and Response Injection and Intrusion Detection. *General Members*

Meeting and eCrime Researchers Summit. Dallas.

Google. (2012, 9 6). *PLCSCAN*. Retrieved from Google Code Archive: https://code.google.com/archive/p/plcscan/

Gorman, S. (2009, 4 8). *Electricity Grid in U.S. Penetrated By Spies*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/SB123914805204099085

Graham, J. H., & Patel, S. C. (2004). Security Considerations in SCADA Communication Protocols. *Intelligent Systems Research Laboratory*, 1-24.

Hahn, A. (2013). *Cyber Security of the Smart Grid: Attack Exposure Analysis, Detection Algorithms, and Testbed Evaluation.* Iowa: Iowa State University.

Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid*, 847–855.

Hong, S., Oh, M., & Lee, S. (2013). Design and Implementation of an Efficient Defense Mechanism against ARP Spoofing Attacks Using AES and RSA. *Mathematical and Computer Modelling, 58(1)*, 254-260.

Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008). Attack Taxonomies for The Modbus Protocols. *International Journal of Critical Infrastructure Protection*, 37-44.

IDAHO NATIONAL LABORATORY. (2011). *Vulnerability Analysis of Energy Delivery Control Systems.* Idaho Falls: IDAHO NATIONAL LABORATORY.

Industrial Defender. (2012). *Seven Best Practices for Automation System Cyber Security and Compliance.* Foxborough: Industrial Defender.

Information Technology Agreement. (2018, 5 5). Retrieved from World Trade Organization: https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm

Jian, Y. (2009). An Improved Scheme of Single Sign-On Protocol. *5th International Conference on Information Assurance and Security*, 495-498.

Kakanakov, N., & Spasov, G. (2011). Securing against Denial of Service attacks in remote energy management systems. *Annual Jornal of Electronics*.

Kiran, A. R., Sundeep, B. V., Vardhan, C. S., & Mathews, N. (2013). The Principle of Programmable Logic Controller and Its Role in Automation. *International Journal of Engineering Trends and Technology*, 500-502.

Knopová, M., & Knopová, E. (2014). The Third World War? In The Cyberspace Cyber Warfare in the Middle East. *Acta Informatica Pragensia*, 23–32.

Koutsandria, G., Gentz, R., Jamei, M., Scaglione, A., Peisert, S., & McParland, C. (2015). A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid. *Proceedings of the First ACM Workshop on Cyber-Physical Systems-*

Security and/or PrivaCy (pp. 67-68). Denver: ACM New York, NY, USA.

Krutz, R. L. (2005). *Securing SCADA Systems.* Indianapolis: Wiley.

Kuipers, D. G. (2008). *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program.* Washington: US Department of Energy.

Lee, D., Kim, H., Kim, K., & Yoo, P. (2014). Simulated Attack on DNP3 Protocol in SCADA System. *Proceedings of the 31th Symposium on Cryptography and Information Security.* Kagoshima: SCIS2014.

Leverett, E. (2011). *Quantitatively Assessing and Visualising Industrial System Attack Surface.* Cambridge: Advanced Computer Science of University of Cambridge.

Leyden, J. (2010, 10 9). *Stuxnet 'a game changer for malware defence'.* Retrieved from The Register: https://www.theregister.co.uk/2010/10/09/stuxnet_enisa_response/

Lootah, W., Enck, W., & McDaniel, P. D. (2007). TARP Ticket-Based Address Resolution Protocol. *Computer Networks, 51(15)*, 106-116.

Majdalawieh, M., Parisi, F., & Wijesekera, D. (2006). DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework. *Advanced Computer Information System Science Engineering*, 227-234.

Makhija, J., & Subramanyan, L. R. (2003). Comparison of Protocols Used in Remote Monitoring: DNP 3.0, IEC 870-5-101 & Modbus. *Electronics Systems Group*, 1-19.

Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., & Hariri, S. (2011). A testbed for Analyzing Security of SCADA Control Systems (TASSCS). *IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe*, 1–7.

Martin, B., Brown, M., Paller, A., Kirby, D., & Christey, S. (2011). *2011 CWE/SANS Top 25 Most Dangerous Software Errors.* McLean: MITRE.

Mcdonald, J. D. (1993). Developing and Defining Basic SCADA System Concepts. *Rural Electric Power Conference* (pp. 1-5). Kansas City: IEEE.

Mcdonald, M. J., Conrad, G. N., Service, T. C., & Cassidy, R. H. (2008). Cyber Effects Analysis Using VCSE: Promoting Control System Reliability. *Sandia Report*, 1-57.

MODBUS. (2006, 12 28). *MODBUS APPLICATION PROTOCOL SPECIFICATION.* Retrieved from MODBUS: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

MODBUS. (2006, 10 24). *MODBUS Messaging on TCP/IP Implementation Guide.* Retrieved from MODBUS: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_

0b.pdf

MODBUS. (2012, 2 2). *MODBUS over serial line specification and implementation guide*. Retrieved from MODBUS: http://www.modbus.org/docs/Modbus_over_serial_line_V1.pdf

Morris, T. H. (2009). On Cyber Attacks and Signature Based Intrusion Detection for Modbus Based Industrial Control. *The Journal of Digital Forensics, Security and Law*, 37-56.

Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., & Reddi, R. (2011). A Control System Testbed to Validate Critical Infrastructure Protection Concepts. *International Journal of Critical Infrastructure Protection*, 88-103.

Nam, S. Y., Djuraev, S., & Park, M. (2013). Collaborative Approach to Mitigating ARP Poisoning-Based Man-in-the-Middle Attacks. *Computer Networks, 57(18)*, 3866–3884.

NASA. (2015, 5 8). *PROGRAMMABLE LOGIC CONTROLLERS*. Retrieved from NASA: https://engineer.jpl.nasa.gov/practices/ops05.pdf

National Commuication System. (2004). *Supervisory Control and Data Acquisition (SCADA).* Arlington: National Commuication System.

National Cybersecurity And Communications Integration Center . (2013, 9 1). *INCIDENT RESPONSE ACTIVITY.* Retrieved from National Cybersecurity And Communications Integration Center: https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Sep2013.pdf

NIST. (2014). *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.* Gaithersburg: U.S. Department of Commerce. Retrieved from NIST SP 800-53A Revision 4.

NMAP. (2017, 5 5). *NMAP*. Retrieved from NMAP: https://nmap.org/

Nordlander, J. (2009). *What is Special About Scada System Cyber Security ? A Comparison between Existing Scada System Security What is Special about Scada System Cyber.* Stockholm: Royal Institute of Technology.

Office of Energy AssuranceU.S. Department of Energy. (2018, 1 1). *21 Steps to improve Cyber Security of SCADA Networks.* Retrieved from Office of Energy AssuranceU.S. Department of Energy: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Oppliger, R., Hauser, R., & Basin, D. (2006). SSL/TLS Session-Aware User Authentication - Or How to Effectively Thwart the Man-in-the-Middle. *Computer Communications, 29(12)*, 2238–2246.

OUCHN, N. (2015, 11 5). *ICS/SCADA Top 10 Most Dangerous Software Weaknesses.* Retrieved from Tools Watch Hackers Arsenal: ICS/SCADA Top 10 Most Dangerous Software Weaknesses

Pansa, D., & Chomsiri, T. (2008). Architecture and Protocols for Secure LAN by Using a Software-Level Certificate and Cancellation of ARP Protocol. *Proceedings - 3rd International Conference on Convergence and Hybrid Information Technology ICCIT 2008*, 21-26.

Patel, S. C., Bhatt, G. D., & Graham, J. H. (2009). Improving the Cyber Security of SCADA Communication Networks. *Communications of the ACM*, 139-142.

Petrovic, J. D., & Stojanovic, M. D. (2013). Analysis of SCADA System Vulnerabilities to DDoS Attacks. *11th International Conference on Telecommunications in Modern Satellite TELSIKS*, 591–594.

PHOENIX CONTACT. (2010, 5 5). *PROFINET basics.* Retrieved from PROFINET: https://www.switchingonthefuture.be/downloads/manualsfabrikanten/PHOENIX%20CONTACT/Profinet%20Basics/PN_Basics.pdf

PI INTERNATIONAL. (2008). *PROFINET AND IT.* Karlsruhe: PI INTERNATIONAL.

Queiroz, C., Mahmood, A., & Tari, Z. (2011). SCADASim-A Framework for Building SCADA Simulation. *IEEE Transactions on Smart Grid, (2)4*, 589-597.

RACOM. (2014, 2 18). *Protocol DNP 3 for MORSE Distributed Network Protocol*. Retrieved from RACOM: http://www.racom.eu/eng/support/prot/dnp3/index.html

REPUBLIC OF TURKEY Ministry of Transport, Maritime Affairs and Communications. (2014, 1 1). *National Cyber Security Strategy and2013-2014Action Plan.* Retrieved from BTK: https://www.btk.gov.tr/uploads/pages/2-0-1-cyber-security-strategy-and-action-plan-2013-2014-5a3412df707ab.pdf

Risk Based Security. (2015, 12 7). *Our New Year Vulnerability 'Trends' Prediction.* Retrieved from Risk Based Security: https://www.riskbasedsecurity.com/2015/12/07/our-new-year-vulnerability-trends-prediction/

Rodofile, N. R., Radke, K., & Foo, E. (2015). Real-Time and Interactive Attacks on DNP3 Critical Infrastructure Using Scapy. *Conferences in Research and Practice in Information Technology Series*, 67-70.

Russell, A. (2004, 2 28). *CIA plot led to huge blast in Siberian gas pipeline*. Retrieved from The Telegraph: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html

Sanz, R., & Årzén, K. (2003). Trends in Software and Control. *IEEE Control Systems Magazine*, 12-15.

Sayegh, N., Chehab, A., Elhajj, I. H., & Kayssi, A. (2013). Internal security attacks on SCADA systems. *Third International Conference on Communications and Information Technology* (pp. 22-27). Beirut: American University of Beirut.

SCADAhacker. (2015, 5 5). *Metasploit Modules for SCADA-related Vulnerabilities*. Retrieved from SCADAhacker: https://www.scadahacker.com/resources/msf-scada.html

Schaffner, L. G. (2007). *The Function of Corporate Security Within Large Organizations: The interrelationship between Information Security and Business Strategy.* Strasbourg: University of Geneva.

Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2014). The SCADA Review: System Components, Architecture, Protocols and Future Security Trends. *American Journal of Applied Sciences*, 1418–1425.

Shang, W. L., Li, L., Wan, M., & Zeng, P. (2014). Security Defense Model of Modbus TCP Communication Based on Zone / Border Rules. *Network Security and Communication Engineering: Proceedings of the 2014 International Conference on Network Security and Communication Engineering*, 79-86.

SHODAN. (2009, 05 15). *Shodan.* Retrieved from Shodan: https://www.shodan.io/

SIEMENS. (2008, 6 1). *SIMATIC PROFINET System Description.* Retrieved from SIEMENS: http://www.siemens.fi/pool/products/industry/iadt_is/tuotteet/automaatiotekniikka/teollinen_tiedonsiirto/profinet/man_pnsystem_description.pdf

SIEMENS. (2012, 4 1). *Siemens Simatic S7-1200 Programmable Controller System Manual.* Retrieved from SIEMENS: https://cache.industry.siemens.com/dl/files/465/36932465/att_106119/v1/s71200_system_manual_en-US_en-US.pdf

Siven, J. (2015). *Securing Profinet Networks.* Helsinki: Helsinki Metropolia University of Applied Sciences.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *NIST Special Publication 800-82.* Gaithersburg, MD: National Institute of Standards and Technology.

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man and Cybernetics Part A:Systems and Humans*, 853-865.

The Grand National Assembly of Turkey. (2000, 12 6). *T.B.M.M. TUTANAK DERGİSİ.* Retrieved from The Grand National Assembly of Turkey:

https://www.tbmm.gov.tr/tutanak/donem21/yil3/bas/b025m.htm

Tofino Security. (2013, 9 19). *Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting*. Retrieved from Tofino Security: https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting

Turk, R. J. (2005). Cyber Incidents Involving Control Systems. *US-CERT Control Systems Security Center*, 1-58.

UNITED NATIONS OFFICE OF COUNTER-TERRORISM. (2019). *THE PROTECTION OF CRITICAL INFRASTRUCTURES AGAINST TERRORIST ATTACKS.* Brussels: UNITED NATIONS OFFICE OF COUNTER-TERRORISM.

Unver, M., & Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. *Elektrik Mühendisligi Dergisi*, 94-103.

US Department of Energy. (2015, 5 5). *The Smart Grid: An Introduction.* Retrieved from US Department of Energy: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf

Weiss, G. W. (1996, 5 5). *Farewell Dossier.* Retrieved from CIA Library: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a14p.pdf

Williams, M. (2003, 2 3). *Study: Slammer was fastest-spreading worm yet*. Retrieved from Computerworld: www.computerworld.com

Wilshusen, G. C. (2015). Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress. *U.S. Government Accountability Office*, 16-79.

Wireshark. (2013, 9 16). *PROFINET protocol family*. Retrieved from Wireshark: https://wiki.wireshark.org/PROFINET

Witte Software. (2018, 7 5). *MudBus Sim.* Retrieved from ModBusTools: https://www.modbustools.com/download.html

Wu, J. H., Shyan, S., Alexandru, S., Ahmed, F., Ching, L. C., Pavel, G., & Manimaran, G. (2011). An Intrusion and Defense Testbed in a Cyber-Power System Environment. *IEEE Power and Energy Society General Meeting*, 1-5.

Xiong, Q., Liu, H., Xu, Y., Rao, H., Yi, S., Zhang, B., & Deng, H. (2015). A Vulnerability Detecting Method for Modbus-TCP Based on Smart Fuzzing Mechanism. *IEEE International Conference on Electro Information Technology* (pp. 404-409). Dekalb: IEEE.

Yanfei, L., Cheng, W., Chengbo, Y., & Xiaojun, Q. (2009). Research on ZigBee Wireless Sensors Network Based on ModBus Protocol. *Proceedings - 2009 International Forum on Information Technology and Applications, IFITA 2009*, 487-490.

Yang, J. (2010). An Improved Scheme of Single Sign-on Protocol Based on Dynamic Double Password. *International Journal of Intelligent Information Technology Application*, 65-70.

Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E. G., Pranggono, B., & Wang, H. F. (2014). Multiattribute SCADA-Specific Intrusion Detection System for Power Networks. *IEEE Transactions on Power Delivery*, 1092-1102.

Yau, K., & Chow, K. P. (2015). PLC Forensics Based on Control Program Logic Change Detection. *The Journal of Digital Forensics, Security and Law*, 59-68.

Yılmaz, E., Ulus, H., & Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. *Bilişim Teknolojileri Dergisi*, 133-146.

Yun, J. H., Jeon, S. H., Kim, K. H., & Kim, W. N. (2013). Burst-based anomaly detection on the DNP3 protocol. *International Journal of Control Automation*, 313-234.

Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. *IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011* (pp. 380-38). Dalian: IEEE.

APPENDIX 1 – MODBUS SANDBOX CODE

```
{
    /// <summary>
    /// Interaction logic for MainWindow.xaml
    /// </summary>
    public partial class MainWindow : Window
    {
        ModbusClient modbusClient;
        public MainWindow()
        {
            InitializeComponent();
        }

        public bool ConnectToSlave(string IP)
        {
            bool ToReturn = false;
            try
            {
                modbusClient = new ModbusClient(IP, 502);    //Ip-
Address and Port of Modbus-TCP-Server
                modbusClient.Connect();
                ToReturn = true;
            }
            catch (Exception e)
            {
                MessageBox.Show(e.Message);
            }
            return ToReturn;
        }

        //private void btn_Read_Click(object sender, RoutedEventArgs
e)
        //{

        //}

        private void btn_WriteRegister_Click(object sender,
RoutedEventArgs e)
        {
            try
            {
                WriteRegister(int.Parse(tb_Address.Text),
int.Parse(tb_Value.Text));
            }
            catch(Exception ex)
            {
                MessageBox.Show(ex.Message);
            }
        }

        private void WriteRegister(int address, int value)
        {
            if (ConnectToSlave(tb_IPAddress.Text))
            {
                address = address - 1;
                modbusClient.WriteSingleRegister(address, value);
                modbusClient.Disconnect();
            }
        }

        private void btn_Read_Click_1(object sender, RoutedEventArgs
e)
        {
            if (ConnectToSlave(tb_IPAddress.Text))
            {
                int Top = 0;
                int Bottom = 0;
                int startingReg = int.Parse(tb_StartingReg.Text);
                int endingReg = int.Parse(tb_EndingReg.Text);
                int regCount = endingReg - startingReg;
                lbResults.Items.Clear();
                int[] readHoldingRegisters =
modbusClient.ReadHoldingRegisters(startingReg, regCount);
                //int[] readHoldingRegisters =
modbusClient.ReadHoldingRegisters(40005, 2);
                // bool[] readCoils = modbusClient.ReadCoils(6, 1);
                for (int i = 0; i < readHoldingRegisters.Count();
i++)
                {
                    lbResults.Items.Add((startingReg + i +
1).ToString() + " - " + readHoldingRegisters[i].ToString());//
                    if (startingReg + i + 1 == 40007)
                    {
                        lbl_temptest.Content =
readHoldingRegisters[i].ToString();
                    }
                }

                modbusClient.Disconnect();
                //0101110000101001 0100001010010001
            }
            else
            {
                lbResults.Items.Clear();
                lbResults.Items.Add("No Connection, Please Hang Up
And Try Your Call Again...");
            }
        }

        float combinedIntsToFloat(int upper, int lower)
        {
            Int32 top = upper << 16;
            Int32 bottom = lower;
            return (float)(top | bottom);
        }
```