

Mohammad Reza Jafari

Understanding and Simulation of Attacks in Power Networks

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Filip Holik

May 2022

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication
Technology



Norwegian University of
Science and Technology

Mohammad Reza Jafari

Understanding and Simulation of Attacks in Power Networks

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Filip Holik
May 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Understanding and Simulation of Attacks in Power Networks

Mohammad Reza Jafari

2022/01/18

Abstract

The demand for maintenance and reinvestment in the power system grows as power transformers age. To aid decision-making, there is currently a scarcity of suitable data and analysis techniques for estimating condition and residual life-time. Restructuring asset management in order to collect appropriate data and establish new methods for managing and analyzing the data is a difficult task. As a result, the CIA triad — a concept that focuses on the balance between the Confidentiality, Integrity, and Availability of data under the protection of users information security program poses certain problems to Cyber security. These investments replace the old systems to digital substations. The development allows for power industrial operation, real-time functionality, and information access. In DS, ensuring security, and Availability of power systems, as well as interoperability capability for diverse manufacturers, is a major concern. Statnett [1] is studying new functionality advantages and associated costs with international Electrotechnical Commission (IEC) 61850 process buss technology as part of an R&D digital substation pilot project called Engineering and Condition monitoring in Digital Substation (ECODIS). With threat agents becoming more sophisticated by the second, IT security has never been more vital. This causes Cyber community to work extra hard in order to stay up with demand and protect the services.

Sammendrag

Etterspørselen etter vedlikehold og reinvestering i kraftsystemet vokser etter hvert som krafttransformatorene eldes. For å hjelpe beslutningstaking er det for tiden mangel på egnede data og analyseteknikker for å estimere tilstand og gjenværende levetid. Å restrukturere kapitalforvaltningen for å samle inn passende data og etablere nye metoder for å administrere og analysere dataene er en vanskelig oppgave. Som et resultat av dette utgjør Confidentiality, Integrity and Availability (CIA)-triaden – et konsept som fokuserer på balansen mellom konfidensialitet, integritet og tilgjengelighet av data under beskyttelse av brukernes informasjonssikkerhetsprogram, visse problemer for cybersikkerhet. Disse investeringene erstatter de gamle systemene til digitale nettstasjoner. Utviklingen tillater kraftindustri-drift, sanntidsfunksjonalitet og informasjonstilgang. I ds er sikring av sikkerhet og tilgjengelighet av kraftsystemer, samt interoperabilitetsevne for forskjellige produsenter, en stor bekymring. Statnett [1] studerer nye funksjonalitetsfordeler og tilhørende kostnader med IEC 61850 prosessbussteknologi som en del av et R&D-pilotprosjekt for digital transformatorstasjon kalt Engineering and Condition monitoring in Digital Substation (ECODIS). Med trusselagenter som blir mer sofistikerte etter hvert, har sikkerheten aldri vært viktigere. Dette får Cyber-samfunnet til å jobbe ekstra hardt for å følge etterspørselen og beskytte tjenestene.

Preface

The following report is an interdisciplinary work written by Mohammad Reza Jafari, which concludes the bachelor thesis as the final part of the education at Faculty of Information Technology and Electrical Engineering the Department of Information Security and Communication Technology at the Norwegian University of Science and Technology Gjøvik spring 2022.

Firstly, I would like to thank Sule Yildirim representing Norwegian University of Science and Technology (NTNU) IIK for presenting this interesting task. I'd want to express my gratitude to my supervisor, Filip Holik, philosophiae doctor (PhD), for his responsible and professional approach, as well as his patience while I was completing my bachelor's thesis. His insightful remarks and suggestions greatly aided me in improving this thesis.

Filip Holik philosophiae doctor (PhD) at NTNU. He has been the main source of guidance, support and giving a lot of valuable information to improve the end product and feedback throughout the project.

The report is performed in collaboration with InterSecure project. I am very grateful for being a part of this project and giving me the opportunity for joining this journey. This thesis involves understanding and identifying the attacks on a Digital Substation.

Finally, I would like to thank my family and friends for their support and motivation for finishing my thesis.

I thus declare that the bachelor's thesis "Understanding and Simulation of Attack on Power Networks" is the result of my independent effort, and that all sources utilized in the thesis are referenced.

Contents

Abstract	iii
Sammendrag	v
Preface	vii
Contents	ix
Figures	xiii
Tables	xv
Code Listings	xvii
Acronyms	xix
Glossary	xxiii
1 Introduction	1
1.1 Background	2
1.1.1 Roles	2
1.2 Project description	2
1.3 Purpose and approach	3
1.4 Motivation	3
1.5 Target audience	4
1.6 Background and competence	4
1.7 Scope	4
1.7.1 Problem statement	5
1.7.2 Objective and goals	5
1.8 Requirements	6
1.8.1 Functional requirements	6
1.8.2 Operational requirements	6
1.9 Project process and thesis layout	6
2 Literature review and theory	9
2.1 Electrical grid	9
2.1.1 Substations	10
2.2 Control system	14
2.2.1 Topology	14
2.2.2 Types of communication	15
2.2.3 PLC	17
2.2.4 Screen control	17
2.3 Standards	19
2.3.1 IEC 61850	20

2.4	Assets in Digital Substation (DS)	24
2.4.1	Server	24
2.4.2	SCADA	24
2.4.3	HMI	25
2.4.4	IED	25
2.4.5	Gateway	25
2.4.6	MU	25
2.5	Regulations and guidelines	26
2.5.1	Protection of operation control system	26
2.5.2	Internal safety rules	27
2.5.3	Documentation of the OCS	27
2.5.4	Control user access	28
2.5.5	Changes in the OCS	28
2.5.6	Equipment use in OCS	28
2.5.7	Counter measures	29
2.5.8	Mitigation for OCS failure	29
2.5.9	Hiring staff for operation center	29
2.5.10	External connection to the Operational Control System	29
2.5.11	System redundancy in the Operational Control System (OCS)	30
2.5.12	Repealed	30
2.5.13	Protection against EMP and EMI	30
2.5.14	7-14.Special requirements for OCS class 2	30
2.5.15	Special requirements for class 3	32
2.5.16	Protection of power systems	33
2.5.17	Mobile radio network	33
3	Cyber vulnerabilities and cyber threats at digital substations	35
3.1	Cyber attack	35
3.1.1	History	35
3.1.2	Top 20 attacks	35
3.1.3	ICS-cyber incident timeline	36
3.2	Cyber kill chain: 7 phases of APT intrusions	38
3.2.1	Step 1: Reconnaissance	38
3.2.2	Step 2: Weaponization	39
3.2.3	Step 3: Delivery	39
3.2.4	Step 4: Exploitation	40
3.2.5	Step 5: Installation	40
3.2.6	Step 6: Command Control (C2)	40
3.2.7	Step 7: Action objectives	40
3.2.8	Situation overview of cyber attack on Ukrainian power grid	41
3.3	Attack classifications	42
3.3.1	Sophistication	42
3.3.2	Consequences	42
3.4	Cyber risk identification	42
3.4.1	Cyber-attack vectors	42

3.5	Cyber-risk impact	44
3.6	Cyber-attacks on Digital Substation (DS)	45
3.6.1	Infrastructure network attacks	45
3.6.2	Malware injection	46
3.6.3	Intrusion into the physical site:	46
3.6.4	Spoofing attack:	46
3.6.5	Man-In-The-Middle-Attack:	46
3.6.6	Human-factor based attacks:	46
3.7	Cyber-attack map for a pilot DS	46
3.7.1	Communication network:	47
3.7.2	Switch:	47
3.7.3	HMI/SCADA:	47
3.7.4	Intelligent Electronic Devices:	48
3.7.5	Merging Units (MU)s:	48
3.7.6	Physical devices (CT/VT):	48
4	Design	49
4.1	Available solution	49
4.2	Approach design	49
4.2.1	Simulation model design	50
4.3	Infrastructure design	50
4.3.1	Model topologies	50
4.4	Network design	52
4.4.1	Communication emulation	52
4.5	Realization	53
4.5.1	Safe lab	53
4.6	Sequence diagram	54
5	Implementation	57
5.1	Methodology	57
5.1.1	Ethics	57
5.1.2	Work flow	57
5.2	Infrastructure configuration	58
5.2.1	Initial configuration	59
5.2.2	Deployment of instances	59
5.3	Starting VMs	60
5.3.1	Model	60
6	Testing and analysis	61
6.1	Methodology of attacks	61
6.1.1	Pre-engagement phase	61
6.1.2	Information gathering	62
6.1.3	Threat modeling and vulnerability identification	65
6.2	Exploitation	67
6.2.1	Man-In-The-Middle	68
6.2.2	Post exploitation	68
6.3	Analyzing IEC-104 traffic	69

7 Discussion and further work	71
7.1 Decisions	71
7.1.1 Limitations and constraints	71
7.2 Measures for strengthening Cyber security in power networks . . .	71
7.2.1 Communication with third parties	72
7.2.2 SDN	75
7.3 Supply chain attack	76
7.3.1 Software supply chain attack	76
7.3.2 Hardware supply chain attacks	76
7.4 Further work	77
8 Conclusion	79
8.1 Project assessment	79
8.1.1 Work load	80
8.1.2 Learning outcome and evaluation	80
8.1.3 Deviations	80
8.2 Conclusion of the work	81
Bibliography	83
A Additional Material	89

Figures

2.1	Electrical grid sections.	9
2.2	Conventional substation	12
2.3	Digital substation	13
2.4	Control System	14
2.5	modbus communication [34]	16
2.6	PLC-architectrue	17
2.7	SCADA	18
2.8	IEC-61850	19
2.9	SCL	21
2.10	Operational control system and administrative network. Everything within the dotted line is considered an operational control system [52]	26
3.1	Cyber-Attack Vectors	43
3.2	Cyber-Attack Map	47
4.1	Basic topology	51
4.2	Extended topology	52
4.3	InterSecureModel	54
4.4	Sequence diagram	55
5.1	Kanban Board	58
5.2	Deployment of instances	59
6.1	Shodan Search-engine	63
6.2	Shodan Search-modbus	63
6.3	netdiscover scan on the simulation model	64
6.4	nmap scan of a SCADA sytem online	65
6.5	Pcap Investigation from attackers PC	66
6.6	Infrastructure of the model through attackers eyes	66
6.7	Third party Data	67
6.8	DDos Attack	68
6.9	Goose and SV messages	69
7.1	VPN [77]	73

7.2	Secure Bypass with UGW [78].	74
7.3	Example diagram on DMZ with a UGW [79].	74
7.4	Security structure for zones and interconnections	75

Tables

- 1.1 Relevant Competence 4
- 3.1 ICS cyber incident timeline table [56] 37
- 3.2 ICS cyber incident timeline table 38

Code Listings

4.1	Vlan Configuration av Mininet	51
5.1	VM Virtual-box Installation on Linux From Terminal	59
6.1	Active Scan methods	64
6.2	MITM attack using ettercap	68

Acronyms

- AC** Alternating current. 12
- AI** Artificial Intelligence. 77
- APT** Advanced Package Tool. 37–40
- ARP** Address Resolution Protocol. 67
- ASAP** As Soon As Possible. 58
- ASDU** Application Service Data Unit. 23
- CIA** Confidentiality, Integrity and Availability. iii, v, 44
- CIT** Conventional Instrument Transformer. 11
- CPU** Central Processing Unit. 17
- CT** current transformers. xi, 10, 25, 48
- DC** Direct Current. 12
- DIGSEC** Digital Infrastructure and Cyber Security. 4
- DMZ** Demilitarized Zone. xiv, 74
- DS** Digital Substation. iii, vii, x, xi, 1–3, 7, 10, 13, 24–26, 40, 42, 43, 45–47, 61, 64, 77, 79
- DSS** Digital Secondary Substation. 18, 51, 79
- ECODIS** Engineering and Condition monitoring in Digital Substation. iii, v, 2, 3, 71
- EMI** Electromagnetic Interference. x, 30, 32, 33
- EMP** Electromagnetic pulse. x, 30, 32, 33
- FBI** Federal Bureau of Investigation. 41

- GOOSE** Generic Object Oriented Substation Event. 22, 52, 67, 69
- HMI** Human Machine Interface. x, xi, 11, 17, 18, 20, 21, 24, 25, 37, 43, 45, 47, 52
- HVAC** Heating, Ventilation and Air conditioning. 37
- ICS** Industrial control systems. x, xv, 3, 19, 35–38, 42, 44, 72, 74, 75
- IEC** international Electrotechnical Commission. iii, v, ix, xi, 16, 19, 20, 23–26, 51, 69
- IED** Intelligent Electronic Devices. x, xi, 11, 20, 21, 24, 25, 43, 45, 48, 52, 68
- IIK** Information and Communications Security Technology Department. vii, 2
- IP** Internet Protocol. 16, 45, 52, 64, 66, 67
- IT** Information Technology. iii, 3, 4, 36, 71–74
- KBO** Kraftforsyningens beredskapsorganisasjon. 27, 33
- kV** Kilo Volts. 10
- LAN** Local Area Network. 12
- MU** Merging Units. x, xi, 13, 20, 24–26, 43, 48
- NCC** Network Control Center. 11
- NCIT** Non-Conventional Instrument Transformer. 12, 48
- NTNU** Norwegian University of Science and Technology. vii, 2, 4
- OCS** Operational Control System. x, 27–30, 32, 33
- OCT** Optical Current Transformers. 12
- OP** Operator Panel. 17, 18
- OS** Operating System. 40, 59
- OT** Operational technology. 3, 36, 72–74
- OVA** open virtualization format. 49
- PhD** philosophiae doctor. vii
- PLC** Programmable logic circuits. ix, 15–18, 37

- RAM** Random Access Memory. 53
- RTU** Remote Terminal Units. 16, 20, 25, 51, 52, 61, 71
- SAS** Substation Automation System. 11
- SCADA** Supervisory Control and Data Acquisition. x, xi, xiii, 15, 17, 18, 20, 24, 25, 39–41, 43, 45, 47, 61, 62, 64, 65, 71, 74
- SCL** Substation Configuration Description Language. 21
- SCS** Station Control System. 15
- SDN** Software Defined Networking. xii, 75
- SV** Sample Value. 25, 26, 52, 67, 69
- TCP** Transmission Control Protocol. 16, 45, 65
- UGW** Unidirectional Gateway. xiv, 73, 74
- UPS** Uninterruptible power supply. 39
- VM** Virtual Machine. xi, xvii, 49, 52, 53, 58–60
- VPN** Virtual Private Network. 38, 49, 73
- VT** voltage transformers. xi, 10, 25, 48

Glossary

Active footprinting describes the process of using tools and techniques, like using the traceroute commands or a ping sweep – Internet Control Message Protocol sweep – to collect data about a specific target. This often triggers the target’s intrusion detection system (IDS). It takes a certain level of stealth and creativity to evade detection successfully.. 64

Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information [2]. iii

Black-Energy is a Trojan that is used to conduct DDoS attacks, cyber espionage and information destruction attacks. [3]. 39, 40

Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories [2]. iii, 73

Cyber relating to or characteristic of the culture of computers, information technology, and virtual reality.. iii, v, xii, 2–4, 35, 38, 46, 61, 71–73, 77, 79, 81

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.. iii, 1–5, 36

DDoS DDoS (distributed denial of service) assaults are sophisticated attacks that flood a network with unnecessary traffic. A DDoS assault causes either network performance degradation or a complete service interruption of vital infrastructure [4]. xxiii, 39, 45, 68

Emulation is the process of imitating a hardware/software program/platform on another program or platform. This makes it possible to run programs on systems not designed for them.. 49

Ethernet a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.. 12, 16, 17, 20, 75

Hacker is a person who illegally gains access to and sometimes tampers with information in a computer system. . 38, 39

Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality)[2]. iii, 73, 77

Kanban is a popular Lean workflow management method for defining, managing, and improving services that deliver knowledge work. It helps you visualize work, maximize efficiency, and improve continuously. Work is represented on Kanban boards, allowing you to optimize work delivery across multiple teams and handle even the most complex projects in a single environment [5].. 58, 80

Malware (short for “malicious software”) is a file or code, intended to harm or destroy computers and computer systems. The term "malware" refers to malevolent software. Viruses, worms, Trojan horses, spyware, adware, and ransomware are all examples of prevalent malware [6]. 5, 36, 39, 46, 76

Man-In-The-Middle A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway [7]. xi, 46, 47, 68, 73

Mininet Mininet is a software emulator for prototyping a large network on a single machine. Mininet can be used to quickly create a realistic virtual network running actual kernel, switch and software application code on a personal computer [8].. 49, 50, 61

Passive footprinting As the name implies, passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees’ social media profiles, looking at job sites and using Whois, a website that provides the domain names and associated networks

for a specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS [9]. 62

Phishing is a cybercrime technique that uses fraud, trickery, or deception to manipulate you into disclosing sensitive personal information. [10]. 38, 39

Ransomware is a type of malware that encrypts files on a device, making them unusable for the files and the systems that rely on them. Then, in exchange for decryption, malicious actors want a ransom [11]. 36, 77

RAT Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.. 39, 40

RS-485 is an industrial specification that defines the electrical interface and physical layer for point-to-point communication of electrical devices. The RS-485 standard allows for long cabling distances in electrically noisy environments and can support multiple devices on the same bus.. 16

Server A server is a computer program or device that provides a service to another computer program and its user, also known as the client. In a data center, the physical computer that a server program runs on is also frequently referred to as a server. That machine might be a dedicated server or it might be used for other purposes.. x, 24

Social engineering In any security chain, humans are generally the weakest link. While machines can be tricked, people are susceptible to falling for all kinds of manipulative tactics. These tactics are referred to as social engineering.[12]. 38, 39

Taskgiver is equivalent of the norwegian "oppdragsgiver". 2, 4, 79, 80

Threat a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done. 6, 35

Trojan A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. [13]. 39

Zero-day exploit is when hackers take advantage of a software security flaw to perform a cyberattack. And that security flaw is only known to hackers, meaning software developers have no clue to its existence and have no patch to fix it [14]. 36

Chapter 1

Introduction

Utility companies are dealing with an increasing number of aging power transformers in the power grid system, which is necessitating more maintenance and reinvestment. Transformer failures and outages result in a loss of energy supplied as well as a lack of stability and reliability of the power grid, which can result in significant costs as well as societal inconveniences. The companies are upgrading from traditional substations to digital substations with an emphasis on cleaner power, more efficiency, and the use of smart-grid technologies. Electricity transmission and distribution businesses are concerned about maintaining the grid's security and dependability as a result of this change [15]. A major problem in DS is to ensure the security, availability, and dependability of power systems in the same way that they are in traditional systems, as well as interoperability between manufacturers [16].

Power Grid and Cyber security

The electric power system is a network through which generated electricity is transported from power plants to demand centers via transmission lines. In terms of power grid Cyber security, because the system's structure is centralized, it is vulnerable to attack. The interconnectedness of components can cause a chain reaction of failures, potentially bringing the country's financial, communications, traffic, and security systems to a standstill. Both private and public networks are used to communicate between components of a power system. Once the attackers get control of the power system communication networks, they have various possibilities to either access the network and disrupt normal grid operation, or connect to a remote access point, which can lead to major and devastating effects. Cyber security is critical for power grid dependability, and proper study in this field requires the classification of normal and abnormal system activities as well as the identification of system vulnerabilities [17].

Cyber security has emerged as one of the most dynamic and rapidly evolving areas of security research. Almost everything has been digitalized in recent decades, increasing the need to protect vulnerable systems and valuable data. The internet not only provides us with a plethora of options, but it also places us in

a vulnerable position. Cyber threats do not only affect the online world and data on computers, they also pose a threat to the physical, offline world.

1.1 Background

In Gjøvik, NTNU offers a unit dedicated to digital security. At various levels within the organization, this division works pro-actively, actively, and reactively on digital and information security. The Information and Communications Security Technology Department (IIK) performs globally competitive research in a variety of fields, including Cyber security, information security, communication networks, and network services. The department are currently running two research-funded projects, ECODIS and InterSecure Norwegian Council investigates Cyber security of digital networks/substations. Mohammad Reza Jafari would participate in the proposed project by helping to comprehend and simulate attacks in a digital substation and contribute in the importance of these researches. Supervisor Filip Holik will share some background work with the author, and will be expected to analyze the information and identify a few attacks that are likely to occur in a digital environment. Then, in order to determine the impact of such attacks on the substation, a simulation of the attacks will be performed with a report to the significance of simulation model and its need.

1.1.1 Roles

The Taskgiver is Sule Yildirim Yayilgan, who represents the NTNU IIK. Filip Holik, a PostDocs at Norwegian University of Science and Technology (NTNU)'s, is the supervisor. The thesis is written by Mohammad Reza Jafari, where it would be natural to play all the roles related to this bachelor thesis throughout the project.

1.2 Project description

Cyber-attacks are becoming more common by the day, project client Sule Yildirim Yayilgan at NTNU in Gjøvik has assigned the responsibility of evaluating and performing attacks to highlight the importance of Cyber security. The task description states "*Currently we are working on power networks in order to identify threats and attacks, particularly in a DS. Electricity is distributed over power lines, and the control of generation, distribution and storage of electricity is done digitally. The recent years witness more digitalization and hence the analogy networks are being replaced by digital ones stage by stage. The digital networks are referred to as digital substation. Currently we are running two projects, namely ECODIS and InterSecure funded by the research council of Norway in order to investigate into the Cyber security of digital networks/substations. In the proposed project, a student or a group of students will contribute to understanding and simulating attacks in a digital substation. We already have some background work which will be shared with the students, and students are expected to study the material and identify a few attacks that are likely to*

happen in a Digital Substation (DS). Then a simulation of the attacks will be made in order to help identify the impact of such attacks on the substation."

1.3 Purpose and approach

This thesis is divided into two parts. a literature review and a testing/attacking part. Firstly, before presenting the research and literature review portion of the bachelor's thesis, a methodological framework that establishes some ground work for future study is defined to find some answers as conclusion which will be located in the last chapter 8 of this thesis. This bachelor's thesis is based on a qualitative model with a mixture of component based and process based approach [18]. The thesis work began with a literature analysis and an examination of relevant attacks on Digital Substations in order to achieve the specified goals. It was critical to use both Norwegian and international sources and standards to obtain information for this project. Despite the global reach, the attention has been on the Norwegian situation. The main source for collecting information were books, publications, research papers, online pages, and interactions with my supervisor. Statnett, ECODIS, and the intersecure project, as well as the Google academic search engine "Google Scholar" and the IEEE Xplore Digital Library, have all been used to locate pertinent material.

1.4 Motivation

More than 2,500 years ago, the legendary ancient Chinese general Sun Tzu expressed it best *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat"* [19]. Even though the quote is old, but it is still relevant as of today. Malicious attackers can destroy control and safety processes in Industrial control systems (ICS), resulting in costly outages, damaged equipment, hazards to worker safety, and even environmental disasters. This is why it is critical for industries to recognize the importance of securing IT/OT linkages in order to defend these high-risk access points from Cyber terrorism and other attacks. Protecting the industrial network perimeter from hazardous traffic from less trusted external networks is the most critical aspect of power plant in Cyber security. This thesis may be of interest to persons who are interested in power networks, Cybercrime, or criminality in general. Working to make the world a safer place every day encourages many people to pursue a career in information security. By bringing Cybercrime to a more manageable level, being able to make the report gives the impression of contributing to an important community. Moreover, this thesis may be of interest to those interested in using technical skills connected to information security, as it also covers themes such as threat intelligence, ethical hacking, and power networks.

1.5 Target audience

This report's primary audience is the Taskgiver, consumers interested in the power and energy industries, as well as Cyber security students and IT professionals in this field. In order to properly appreciate the project report, the reader should have some prior knowledge of information security and Cyber threats.

1.6 Background and competence

The author in the thesis have prior experience with information security, programming, and networking. He took many relevant courses at Norwegian University of Science and Technology (NTNU) and worked on related projects in their leisure time. These courses cover a wide range of topics, including ethical hacking and reverse engineering.

Below Table 1.1 shows all of the courses that the author took while studying at Norwegian University of Science and Technology (NTNU) which are relevant to this thesis project.

DIGSEC 2019/2022	
Course code	Course name
IDATG2202	Operativsystemer
IMT4116	Reverse Engineering and Malware Analysis
TTM4536	Etical-Hacking Informasjonssikkerhet fordypningsemnet
DCSG1001	Infrastruktur: grunnleggende ferdigheter
DCSG1005	Infrastruktur: sikre grunntjenester
DCSG1006	Datakommunikasjon og nettverk
DCSG2001	Sammenkoblede nettverk og nettverkssikkerhet
DCSG2005	Risikostyring
PROG1001	Grunnleggende programmering
PROG1003	Objektorientert programmering
PROG1004	Porgamvareutvikling

Table 1.1: Relevant Competence

1.7 Scope

This thesis project has a simulation safe sandbox environment that allows attackers to run and execute attacks automatically while receiving important feedback for further study. The project supervisor, Filip Holik, determines which outputs are relevant and specifies them as part of the problem statement. The research question, as well as relevant goals, objectives, and delimitations, will be defined in this chapter to identify the scope of this thesis.

1.7.1 Problem statement

The following problem statement has been produced based on the task description, as well as the project supervisor's instruction and the client's clarifications:

- Importance of Cyber security in power networks
- Use of Simulation model
- Performing attacks and its impact
- Data Manipulation
- Mitigation plans

1.7.2 Objective and goals

This section outlines the immediate and long-term objectives that the project aspires to achieve through this thesis.

Effect goals

The effect goals explain the implementation's long-term impact as well as the possibility for desired changes from the current state of affairs.

- For more effective security assessments, use of the simulation model.
- For the target audience, a detailed study on the importance of Cyber security in power networks
- Further development of the simulation model.

Achievement goals

The term "achievement goals" refers to the objectives that must be met during the thesis project's duration.

- Understanding Power networks
- Security guidelines related to power networks
- Assets and Threats regarding this sector
- Attacking and exploring the Simulation model for analysis

Delimitations

Delimitation's outline the project's target area and bounds using technologies provided by the supervisor Filip Holik, in order to produce an accurate and comprehensive analysis. If active Malware is available, its capabilities could be defined rather than applied in the environment. The project concentrates on the importance of security and analysis, rather than the actual physically attacking the system and its components in power networks, which are highly restricted, confidential and not allowed. Although there are related features simulation model has and acts as the system and components virtually to perform the attacks and analysis, on the other hand, may still be significant for the ultimate conclusion. This

project report will not address actual attacks on power networks physically. The user is solely given information about the Threats, the model's importance, and mitigation's.

1.8 Requirements

This section outlines the functional, operational, and external requirements that must be met in order for the project to be completed and the desired outcomes to be achieved.

1.8.1 Functional requirements

The functional requirements are list of the functions that the solution must offer. The project description outlined the needed functionalities for completing the work, which are described further in this section.

The structure is made to the intended audience. In order to use the output generated by this framework, the user must have prior familiarity with information security analysis. The framework's primary functional needs are:

- Analyzed report about the attacks affected the model.
- Creating an isolated environment in which attacks can be carried out safely.

1.8.2 Operational requirements

Operational requirements are those that must be met in order for the project implementation. Although no operational criteria are included in the project description, certain steps have been taken to make the analysis process as easy as feasible.

- The framework must support OVF file due to simulation model and kali-linux for attacking.
- To execute different types of attacks, the sandbox must support both x86 and x86-64 architectures.

1.9 Project process and thesis layout

This report was produced in \LaTeX , which allows for formatting as well as linking and referencing between chapters. When the reader clicks on an acronym in this report, the entire word appears. If a link appears next to a word in the acronym list, the reader can click it to access a glossary list with an explanation. The glossary contains words that are defined and linked the first time they appear in the context. Other links include places in the report where glossary terminology are mentioned, references, tables, and figures. Footnotes are used in addition to references as tiny comments where a link or brief description is required. More over a quick description of the report's structure below.

The reader will be presented with theories aimed at solving the problem statement, as well as the design and execution procedures used to obtain the desired results. The project starts with a need statement, then moves on to a theory chapter that explains the various concepts and technologies that are employed throughout the thesis.

This section explains how the thesis report is organized for the reader's convenience.

Chapter 1:Introduction

This chapter gives the reader an overview of the thesis, which introduces the project's background, purpose and goals.

Chapter 2:Literature review and theory

This chapter explains the idea behind the many features and technologies employed in this thesis. This section covers detailed theory as well as details of the various technologies needed to understand the simulation part.

Chapter 3:Threat's and attacks to digital substation

This chapter gives the related information to understand the vulnerabilities when it comes to the DS.

Chapter 4:Design

This chapter discusses how the solution has been created for future development, taking into account the defined requirements from chapter 1.

Chapter 5:Implementation

Describes and examines the methodology used and methods utilized to achieve the various results throughout the whole project, as well as the use of the technology gaining the results and how we use it. It also offers instructions for setting up the test environment.

Chapter 6:Testing and analysis

Implementation outlined in Chapter 5 gives an overview of the test environment and as well as describing the thesis's outcomes are covered in Chapter 6.

Chapter 7:Discussion

This chapter reflects on the technology's prospective utility. This entails attempting to quantify the significance in terms of event detection and management. This section will also touch on the theory, past reflections, and project outcomes.

Chapter 8:Conclusion and further work

This chapter will give a brief review of the thesis project, including how it was carried out, the learning outcomes, further work and future considerations.

Chapter 2

Literature review and theory

This section will go through theoretical concepts and technologies that are pertinent to this thesis. The overall goal of this chapter is to prepare the reader for the subsequent chapters by explaining important fundamentals.

2.1 Electrical grid

An electrical grid is a network that connects producers and consumers to distribute electricity. Electrical grids come in all shapes and sizes, and they can span entire countries or continents [20]. It consists of:

- **Power Stations** Frequently found near energy sources and away from densely populated regions Figure 2.1a.
- **Substations** Increase or decrease voltage Figure 2.1b.
- **Electric power transmission** Transport power over large distances.
- **Electric power distribution** Voltage is stepped down to the required service voltage for individual clients.



(a) Power-plant Norway



(b) A digital substation

Figure 2.1: Electrical grid sections.

The area is large enough to encompass all aspects of the electrical grid. Although the substation is part of the electrical grid infrastructure, this section just covers DS, with the rest of the theory focusing on substation-related components.

2.1.1 Substations

Substations are electrical network nodes or junctions that connect generation, transmission, and distribution assets with customers. Substations are vital parts of the electrical grid infrastructure that ensures customers have access to reliable electricity. Transformers, switchgear, circuit breakers, current transformers (CT), voltage transformers (VT), other high-voltage electrical equipment and protection relays are all wired together using copper cables in traditional substations [21]. A substation's primary goal is to convert high-voltage electricity from the transmission system to lower-voltage electricity that can be conveniently distributed to local homes and businesses via lower-voltage distribution lines [22]. The main elements to a substations are briefly described below:

- **Transformers** reduce the high voltage electricity arriving on transmission lines to a considerably lower voltage suited for distribution cables.
- **Circuit Switches** like the switches that turn on and off the lights in your home, direct the flow of electricity.
- **Breakers** When unexpected surges or faults occur, breakers in the main service panel of your home halt the flow of power to protect the system from damage.
- **Capacitors** They smooth out voltage depressions induced by higher loads and "filter out" voltage distortion to improve the quality of the power supply to customers in two ways [22].

Substations have kept up with the evolution of the electrical network to satisfy evolving consumer expectations, combining enhanced technology, engineering, and operational methods to increase the electrical network's availability.

Conventional substations

Transmission substations connect transmission lines and perform critical services such as voltage level transformation, voltage control, reactive power control, and power flow control in transmission networks.[21]

In Energy-laws §1-5, the transmission network is defined as follows.

*“The transmission network comprises of facilities for the transmission of electrical energy at voltage levels of at least 200 kV, and facilities at 132 kV which are of major importance for the operation of these facilities. The transmission network also includes facilities for electrical energy conversion, when the conversion facility is directly connected to facilities for transmission as mentioned in the first paragraph and transforms to a voltage level of at least 33 kV. ...”*¹

¹<https://lovdata.no/dokument/NL/lov/1990-06-29-50>

Transmission substations below Figure 2.2, typically contain a large number of various pieces of equipment that can be split into two categories: primary and secondary. High-voltage equipment such as switching equipment, instrument transformers, power transformers, reactors, capacitor banks, busbars, power cables, and power lines make up the majority of the equipment. The primary equipment is usually organized in high voltage bays in the substation yard. Low-voltage devices for protection, control, and monitoring are included in secondary equipment [4-6]. These instruments are usually found in a control building's control room. These secondary devices, along with the communication networks, make up the Substation Automation System (SAS). SAS has three key functions: to monitor, safeguard, and control the substation's primary equipment [23]. The process level, the bay level, and the station level are the three levels of an SAS architecture. The interface to the principal process is represented at the process level. Data is collected and activities are carried out at this level in order to control the primary process. Equipment such as Conventional Instrument Transformer and various types of switching equipment are included at the process level.

Intelligent Electronic Devices (IED), such as protection Intelligent Electronic Devices and bay controllers, are found at the bay level and fulfill protection and control duties, respectively. Disturbance recorders, electrical energy meters, and quality metering devices are among the other bay level devices. The substation Human Machine Interface and gateways facilitate communication between the substation and the Network Control Center at the station level. The station level sends status data from the substation equipment to the operators for monitoring and control purposes [24]. A connection network known as the station bus connects the station level with the bay level, as depicted in Figure 2.2.

The station bus connects bay level devices to station level devices, allowing communication between the two levels as well as between multiple bay level devices [26]. On the other hand, the connections between the process level equipment and the bay level devices are still hardwired, as shown in Figure 2.2. We can see in conventional substations, a vast number of copper cables flow from the control building to the individual high voltage bays.

This is currently transforming to what is known as the digital substation, thanks to developments in digital technology, connectivity, and standards. The phrase "digital substation" refers to electrical substations in which operation is controlled by distributed Intelligent Electronic Devices (IED)s linked by communications networks. In terms of design and engineering, installation, and operation, the digital substation offers significant advantages. Off-the-shelf solutions may be provided, changes can be made quickly, cabling (and hence costs) can be reduced, and embedded diagnostics can ensure system integrity.² This is an introduction to the digital substation and the various components that make it up.

²<https://electrical-engineering-portal.com/>

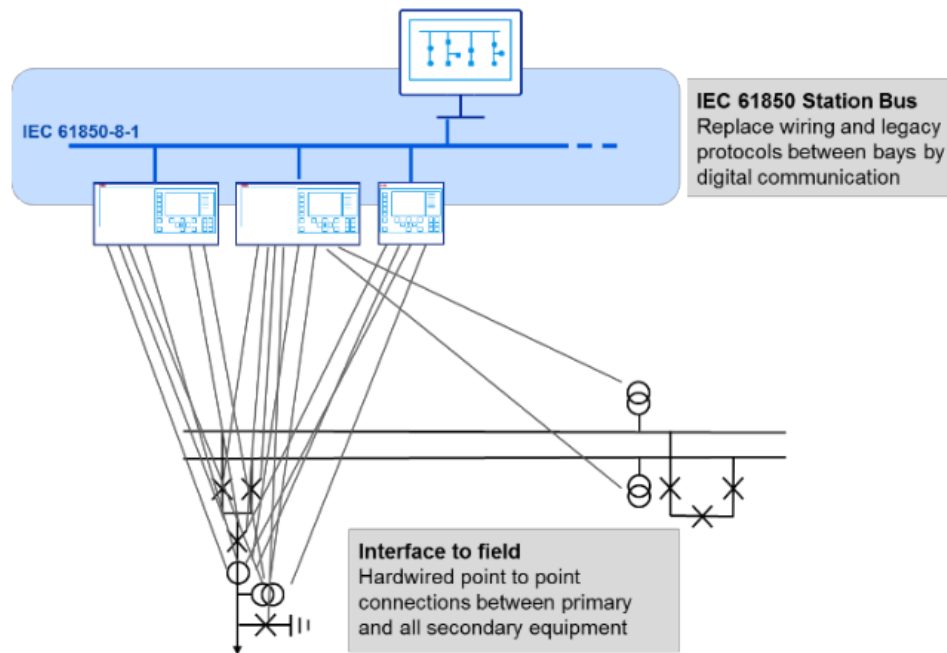


Figure 2.2: Layout of a conventional Substation [25]

Digital substation

The term "digital substation" is used to describe substations where data from process level equipment is digitized at the source. Data, commands, and signals are exchanged between the process level and the bay level via a communication network, with IEC 61850 defining the data format and data access and exchange mechanisms. The Substation levels are explained in 2.3.1. The process bus is the name for this communication network. The process bus is used to distribute an accurate time reference to time synchronize the substation equipment, as well as operational data like as current and voltage measurements, control and protection signals [27].

The process bus is essentially an Ethernet LAN network that substitutes the copper wires that run from the control building to the various high voltage bays in traditional substations for measuring and control circuits. The AC and DC power supply circuits will be the only copper cables left between the control building and the high voltage bays in digital substations.

The station bus is a communication network that connects the station and bay levels. The bay level devices are connected to the station level devices through the station bus, allowing communication between the two levels as well as peer-to-peer communication between bay level devices. The station bus, like the process bus, is an Ethernet LAN network.

Non-Conventional Instrument Transformer (NCIT), such as Optical Current Transformers (OCT), can be used in digital substations to measure current and

voltages using methods other than typical magnetic coupling. Merging Units (MU), which digitize currents and voltages, are required to incorporate traditional instrument transformers into digital substations. Because this occurs close to the field, MUs are discovered in the coupling yard. Figure 2.3 depicts the topology of a digital substation

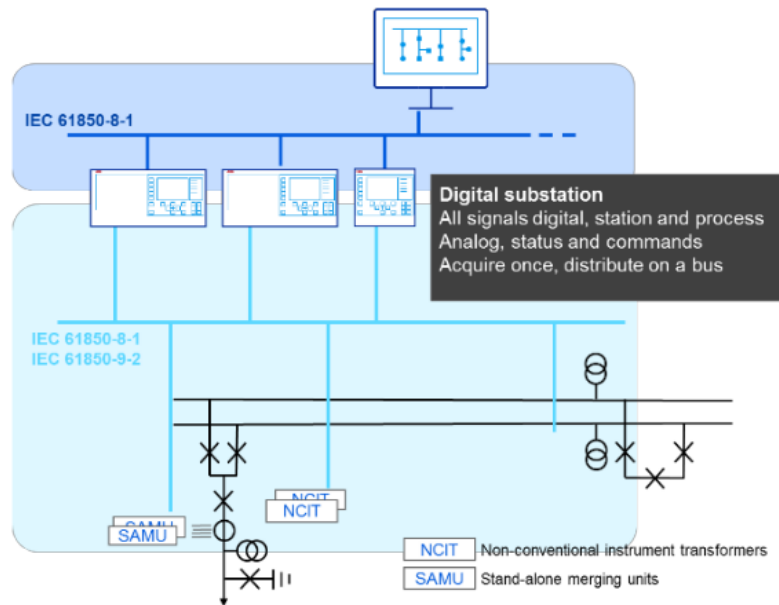


Figure 2.3: Layout of a Digital Substation [25]

Several advantages come with the digital substation which are as follows:

1. Reduces the number of copper cables running between the process and bay equipment.
2. Eliminates high-energy impulses, making the functioning of electrical room panels safer.
3. Reduces the required size of panels in substations, as well as the size of the electrical room.
4. Reduces engineering and construction time, as well as the time and effort required to draft, implement, and test such systems.

Although the concept was introduced more than ten years ago, the Digital Substation is still in its early stages of development, with only a few substations of this type operating today, both in Norway and abroad. However, in Norway, a few prototype DSdigitals are emerging, including Statnett's Furuset substation in Oslo, Skagerak Nett's Trdal substation in Drangedal, and Elvia's Heggdal substation in Asker, as well as a vendor-independent test facility at the National Smart Grid Lab in Trondheim.

2.2 Control system

This section discusses the control system's essential parts in general. During the building of a control system, a number of precautions must be taken depending on the capabilities and limitations of various systems. This section describes the most regularly utilized solutions.

2.2.1 Topology

The Figure 2.4 below depicts a typical ICS control system topology.

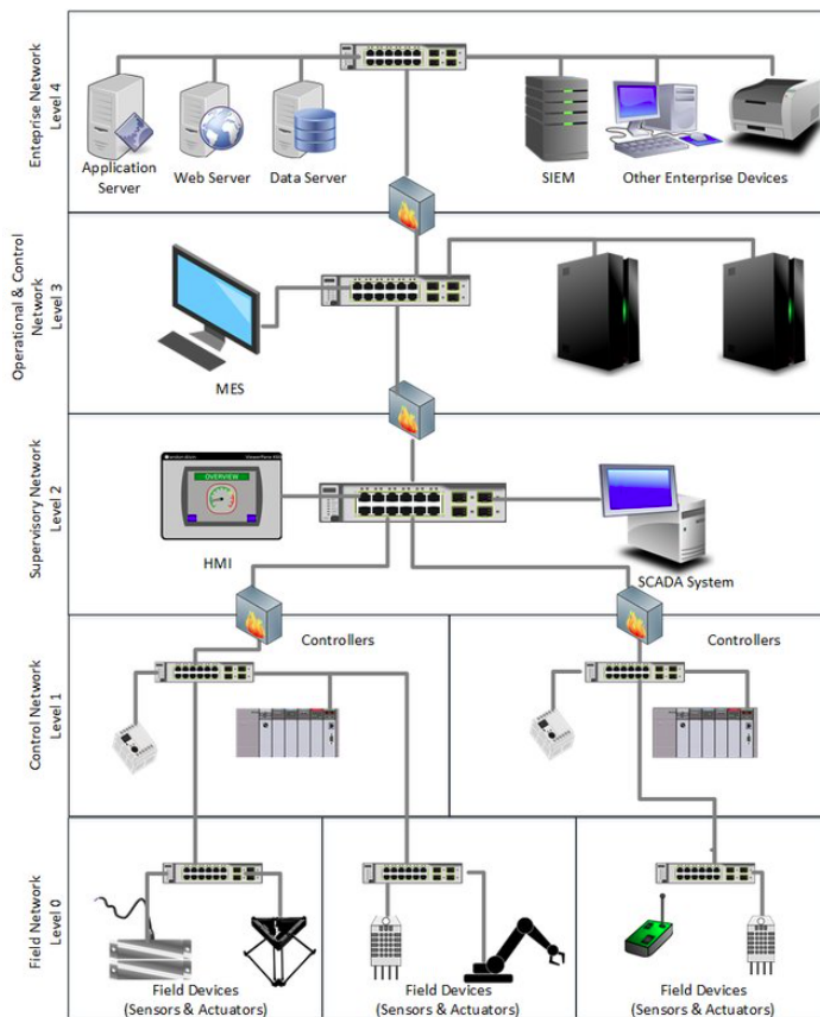


Figure 2.4: An example of general specification for the construction of control systems [28].

Autonomous devices

The control system is broken down into autonomous units, which are self-contained and independent of one another. This is done to reduce the impact of a potential error. The system must also be able to distinguish between minor and major faults. Each autonomous unit must have its own operator interface for local control, as well as a separate control cabinet with its own power supply [29].

Control-level

The control system is divided into 5 control levels Figure 2.4, which are the following:

1. **Vendors/External companies.**
2. **Remote control from operations center:**
An operations center is usually in charge of the power plant.
3. **Control room:**
All systems in the power plant must be able to be operated and monitored from the control room. It is separate from the operations center and must be able to function even if portions of SCS appear out of order level.
4. **Local supervision:** Each autonomous unit is linked to the HMI for local control, allowing the device to be operated and monitored. The panel must have all measurements, indications, and error warnings. The operations center and control room must be independent of the local management.
5. **Direct supervision:** The systems at this level of control are usually set up to be controlled directly and manually. Direct supervision, which is independent of other control levels, is now only utilized for service/maintenance or in special emergencies (class levels 1,2 and 3).

2.2.2 Types of communication

61158 and 61784 define the Profibus and Profinet profiles, respectively. It is a real-time distributed control industrial network system with a way to link instruments with each other.

Modbus is an industrial data transmission standard for linking industrial devices. Modicon, which is now Schneider Electric ³, first introduced the protocol to the market in 1979 for communication between PLCs. Modbus is a free and open protocol that is updated on a regular basis by the Modbus organization due to automation and SCADA products frequently use it [30].

Profibus

Profibus is a fieldbus-based automation standard with a modular structure and a communication protocol at its core. Profibus is connected to controllers or control

³<https://www.se.com/ww/en/>

systems that have decentralized field devices such as actuators or sensors at the field level through a bus connection based on RS-485 that is further connected to controllers or control systems that have decentralized field devices such as actuators or sensors. This allows for consistent data exchanges when using advanced communication methods [31].

Profinet

Profinet is a communication protocol for transferring data between controllers and devices in industrial automation systems. Profinet is the most well-known industrial Ethernet solution available today, and it is based on international standards like IEEE 802, as well as IEC 61158 and IEC 61784. Profinet is an open Ethernet solution, which means that hundreds of manufacturers have created Profinet devices, including PLCs, I/O, diagnostic equipment, and much more, to improve communication between industry equipment [32]. Profinet uses 3 communication channels to ensure appropriate performance, such as TCP / IP, Profinet RT and Profinet IRT. Profinet then has the opportunity to use TCP / IP communication for tasks that are not time-critical, but for time-critical tasks, Profinet uses an RT channel to deliver in a fast and deterministic way.

Modbus

Modbus allows units and equipment to communicate with one another using a master/slave design shown Figure 2.5. A master/slave communication protocol is one in which one or more slaves are controlled by a master. A data exchange between a master and slave consists of requests from the master followed by responses from the slave. The master, which is commonly a PLC, RTU, PC, or DCS, transmits data to the slave's registers, where the slave registers the data and passes it on to the master, who must first recognize the address and then reply within a certain time frame, or the master will receive an error message [33]. The slave cannot send information on his own; instead, the owner must ask him to do so.

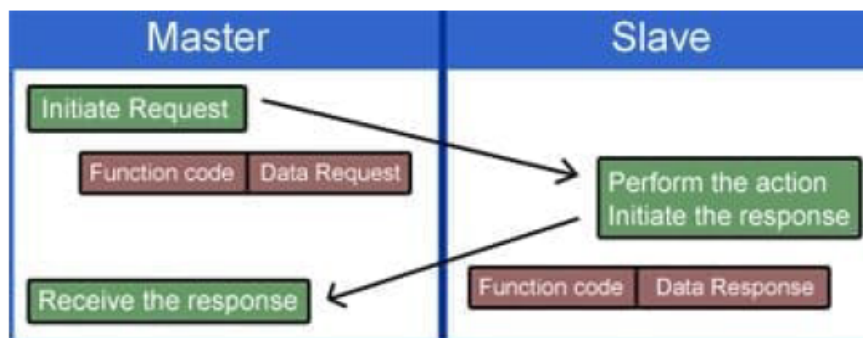


Figure 2.5: modbus communication [34]

2.2.3 PLC

PLC's are commonly referred to as high-level micro controllers. A processing module, a power supply, and I/O modules make up the majority of them. The CPU and memory make up the processor module. In addition to a microprocessor, the CPU has at least one programming interface (USB, Ethernet, or RS232), as well as communication networks [35]. The power supply and the I/O modules are normally separate modules from the processor. Discrete (on/off), analog (continuous variable), and special modules like motion control or high-speed counters are examples of I/O modules. The I/O modules are connected to the field devices.

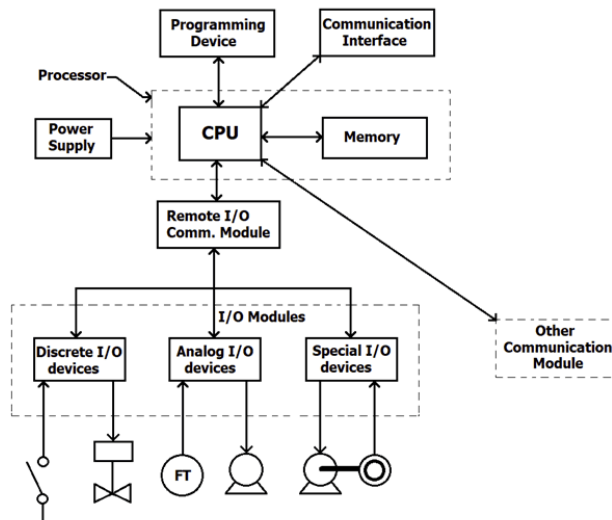


Figure 2.6: Example of an internal architecture of a PLC[35].

2.2.4 Screen control

It is critical to collect the relevant data and create an overview for operating employees in order to operate a electric plant. As a result, the user interface is an integral component of the control system. A power plant can be operated at many control levels in the control system, including direct control, local control, station control, and remote control. These controls have many purposes and are configured in HMI, SCADA and OP-panel user interfaces.

Human Machine Interface

HMI is a data collection and visualization user interface. The station computer in power plants is called HMI. It is kept in the electric plant's control room. The station computer oversees the entire power plant, reading information, warnings, and process trend curves.

SCADA

SCADA is a software and hardware-based automation solution that allows industry groups to control processes locally or through operations centers[36]. The SCADA system uses signals that can communicate over the many channels available to provide the operator control over a system's functioning. A distributed database or a database of tag numbers with distinct codes in the facility can also be implemented by the system [37]. In the control room, the SCADA system represents a basic input or output value that is monitored and/or regulated. The codes that appear are saved in a database with value-time stamp pairs that can be utilized indefinitely or evaluated later. SCADA is widely used in industry because it can gather, monitor, and analyze real-time data for devices like sensors, valves, pumps, and more, and then visualize that data using an HMI. The system aids in maintaining efficiency, processing data for informed decisions, and communicating system issues to minimize downtime.

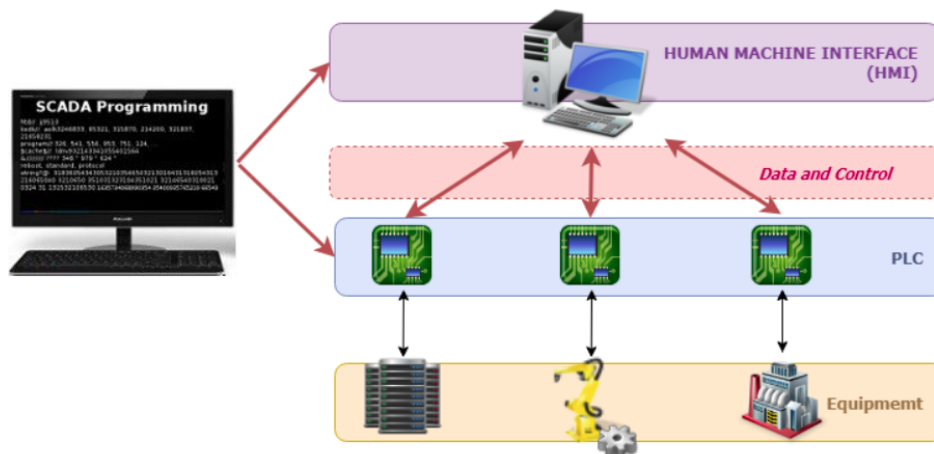


Figure 2.7: Example diagram of the main components of a SCADA system. [38]

Operator Panel

A local user interface connected to and positioned by smaller functional units in the DSS is known as an OP. The panel is a modest HMI with basic capabilities like meter reading and simple start and stop. With an OP, you have limited or no control over the process's settings. This is the lowest control level, with little impact on the overall control system. The function section's local PLC collects I/O, which is then passed to an OP panel to be structured.

2.3 Standards

A standard is a method of doing anything that is repeatable, harmonised, agreed upon, and documented. Technical specifications or other precise criteria are contained in standards, which are intended to be applied consistently as a rule, guideline, or definition. They make life easier by improving the dependability and efficacy of many of the products and services we use [39]. Some of the related standard protocols used in Industrial control systems are as follow.

Topology

The topology depicts a simplified system for a better understanding of the IEC 61850 functionality. As a result, the referred to topology will not be realistic in terms of redundancy or connecting point. The topology is meant to serve as an example of how to comprehend the structure of an IEC 61850 control system. As illustrated in Figure 2.8, the topology is organized by three levels: station, control, and process [40].

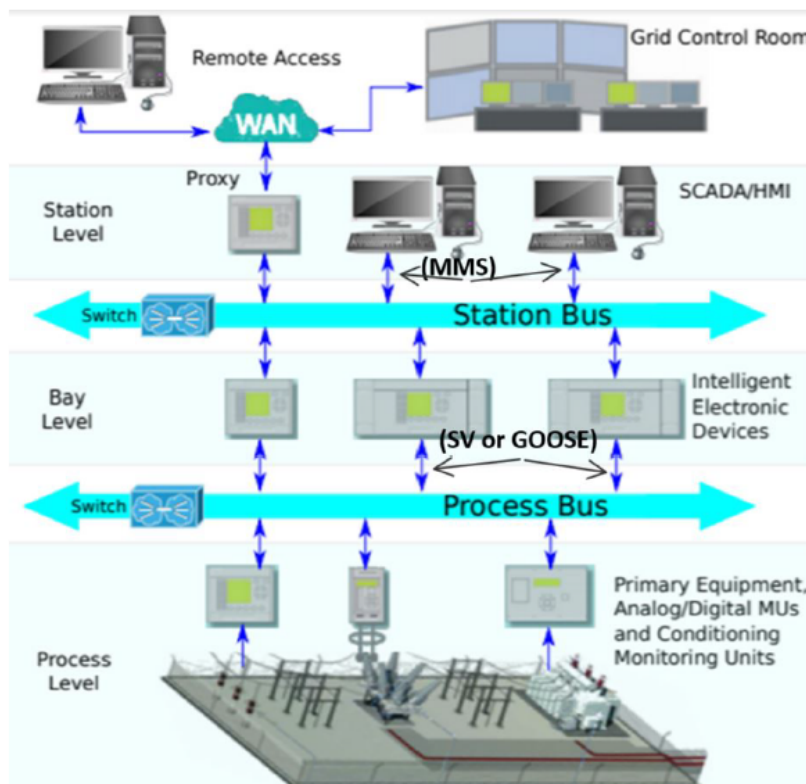


Figure 2.8: Simplified topology for IEC 61850 implemented at switchgear. [40]

2.3.1 IEC 61850

IEC 61850 is an international standard for energy supply automation communication networks and systems. The goal is to provide a standardized communication system based on optical fiber and Ethernet for quick interaction that can be deployed with other standards and is operational across suppliers. This should result in a more efficient operation that is also financially viable for future expansions or repairs. IEC 61850 is an open standard that facilitates the integration of energy system protection, control, measurement, and monitoring [41].

Station level

A station computer, HMI, and SCADA for local control, as well as a firewall that allows external access from the operations center and remote connectivity through gateway, are all found at the station level. IEC 61850 can be used for external connection and control, although other protocols, such as IEC-104, can be mapped for compatibility with a local IEC 61850 system if needed. The gateway is replaced with an RTU in this situation. Since the substations have already transitioned to IEC 61850, it would be beneficial if the entire supply system adopted the same standard for overrides relating to supply network problems.

Control level

The control system of IEC 61850 is based on IEDs at the control level. Intelligent Electronic Devices (IED), provides functions such as measurement, protection, and control. Interoperability between different suppliers will be available since all IEDs will be able to interact with each other using the IEC 61850 standard. To conserve cabling, IEC 61850 provides for a decentralized division, in which IEDs are positioned according to the system part to which they are attached.

Process level

Traditional measuring instruments are connected to MUs at the process level to transform measured values for IEC 61850 communication. These can then be sent to Bay Level through optical fiber or Ethernet. Because the MU transition involves a tiny time delay of 2ms, it has been upgraded to PMU. PMU is an IEC 61850-compliant microprocessor-based intelligent device for measurements that can be linked directly to Ethernet. As a result, in order to transmit time-critical information quickly, this will be desirable.

Process and station buss

On a station and process bus, the levels in the topology are generally connected via Ethernet or fiber optic cable. Process bus is introduced in IEC 61850, where data transfer between MUs and IEDs is controlled by a local switch. The goal of this intermediate link, in comparison to traditional control systems, is to reduce

cabling to measuring devices. Data is transferred between IEDs, station data, HMI, and gateway via the station bus. The Ethernet cables are connected to the buses via switches, which also govern data transmissions. To manage the capacity of data flow, today's Ethernet technology is far ahead, and fiber for process and station bus can be 100Mbit / s or 1 Gbit / s. The way the network is connected is determined by the network's aim for redundancy and speed.

Substation Configuration Description Language (SCL) [42].

1. **Interoperability through XML** IEC 61850 is a data communication system that employs Ethernet or optical fiber for data transfer and is based on the IP protocol. The system's standardized signaling allows different vendors to communicate in the same language, and they can be utilized interchangeably. An IED can accept data in an XML format with a specific tag, translate it to the vendor's own language for internal processing, execute appropriate control or communication operations, transform the data from the vendor language to IEC 61850, and deliver it.
2. **SSD** provides description of the system specification. The single-line diagram, voltages, and essential logic nodes for the power plant and/or switchgear's functionality are described in this file. Based on single-line diagrams and function diagrams, the file is configured in a System Specification Tool (SST).
3. **ICD** An IED's capabilities are described in the ICD. The manufacturer creates an ICD in an IED Configuration Tool (ICT) that incorporates logical nodes, data, and system compatibility.
4. **SCD** The system configuration is described using SCD. This folder contains all ICD files from configured IEDs as well as a description of the communication protocols between them. In the System Configuration Tool, the file is configured (SCT).
5. **CID** The CID is an excerpt from the SCD file that contains the IED settings for each IED individually. Each IED's parameters and settings can be modified here.

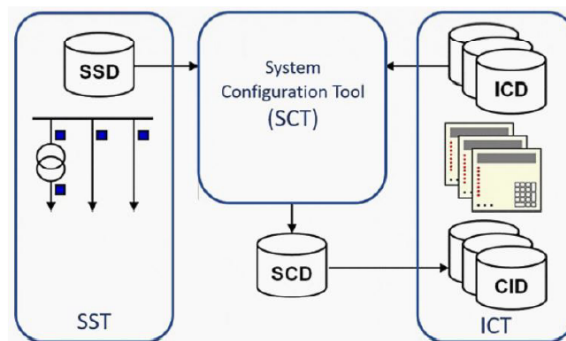


Figure 2.9: SCL

Communication protocols

In the energy industry, a range of specialized standards, technologies, and protocols are used to automate substation control systems. MODBUS, IEC60870, DNP3, and IEC61850 (GOOSE, SV, MMS) are among the most widely used protocols. This section examines and analyzes data communication approaches among the aforementioned protocols, with a particular focus on the current standard IEC61850. The station and process bus are used to communicate between levels. The OSI model separates the functionality between the protocols by using network communication in IEC 61850.

MMS

For a client/server relationship, the station bus uses the MMS protocol. MMS uses the TCP/IP protocol, in which the client asks data from the server, and the server responds with the requested data. MMS is a common data communication mechanism that assures that needed data is received. MMS is used to retrieve information from the server concerning conditions, trends, and other aspects of data collecting and monitoring [43].

SV

Time-critical processes that require immediate response are monitored on the process bus, which connects MUs and IEDs. The protocols SV and GOOSE are employed here, which have tight restrictions for transmission time delays. The protocols are built on publisher/subscriber interactions between IEDs, in which multicast UDP messages are delivered and stored. Numerical values, such as current and voltage level, are transmitted using SV. After a predetermined period, the SV protocol delivers a periodic signal. In a 50Hz system, the standard for protection is 4000 messages per second. Measured values are delivered in real time for monitoring and are not relied on reception verification like MMS [43].

GOOSE

The GOOSE protocol is used to send information about monitoring and control functions, such as switch position. When the state of an output changes, the protocol sends out a multicast message. Because the protocol is not based on receipt verification like MMS, the status change is delivered twice with delays of 4, 16, 100, and 1000 milliseconds. This establishes the groundwork for quick communication between the process and the control level. The multicast message is transmitted at a predetermined period of 1 to 60 seconds in the unaltered state. If the multicast message is not registered after three times the interval time, the relevant IED is marked as non-communicating, and the predetermined position is used instead. It is possible to define the worst-case scenario here for safety reasons [44].

Fixed goose

The GSSE protocol is a fourth protocol for time-critical communication. This is an update to the existing UCA2.0 protocol, which uses a different data set than the regular GOOSE protocol [45]. As a result, GSSE is a faster communication protocol among some IEDs. Because GSSE was not included in IEC 61850, GOOSE

has taken its place as the industry standard. In retrospect, the GSSE dataset uses the GOOSE protocol, therefore Fixed GOOSE can be utilized when it is useful.

IEC 60870-5-104 (IEC 104)

IEC 60870-5-104 is a communication protocol that allows power plants or transformation stations to control their control systems remotely from a central control room [46]. The protocol can also be used for internal communication within the control system of a power plant. Using an uniform protocol allows automated systems from different suppliers to be integrated and controlled without the need for protocol converters or adaptations.

IEC 104 is based on IEC 60870-5-101 (IEC 101), a telecontrol protocol for power system automation applications. IEC 104 gives IEC 101 network access, allowing control rooms and operations centers to communicate via a typical TCP/IP network. This is accomplished by deleting the serial header and replacing it with the proper headers for full duplex TCP/IP connectivity. IEC 101 requires confirmation for each message transmitted, but IEC 104 assumes the channel is stable and allows a maximum number of K-messages to be sent without waiting for confirmation from the opposing station. IEC 104 replaces the serial header with its own APCI header. Three types of frames are identified by the first two bits of the first byte in the APCI header:

U-frame: These control frames oversee the TCP channel's traffic exchange. A start message allows traffic to flow, a stop message prevents further communication, and a test message ensures that the connection is active.

I-frame: These frames carry application data ASDU.

S-frame: The supervision pictures show the opposite station number of the last frame that was received correctly. They are used as a confirmation on a set of messages to indicate that data transmission can continue.

Message types in IEC-104

The protocol defines three primary sorts of messages using the Type field. These types are:

1. **Type U (0x03)** a communication control message with a defined duration START (for connection initialization), STOP (for connection termination), and TEST (for active connection verification) are the three subtypes.
2. **Type I (0x00)** a data transfer message with a changeable length. The payload is in the form of an Application Service Data Unit (ASDU).
3. **Type S (0x01)** a fixed length message used for monitoring and delivering acknowledgements.

Delimitation

The standard's description and application are limited to what is considered important for power plant control systems. IEC 61850-7-3, IEC 61850-7-4, IEC 61850-

7-410, and IEC 61850-7-510 are some of the most important sections. IEC 61850-7-3 addresses communication and data classes, IEC 61850-7-4 addresses communication, logical nodes, and data objects, IEC 61850-7-410 addresses communication for power plant control and monitoring, and IEC 61850-7-510 addresses guidelines and structure.

2.4 Assets in Digital Substation (DS)

This part examines assets and their sophisticated functionality and communications in order to discover cyber-risks in a DS. Figure 3.1 shows the connection between the assets which include SCADA system and servers, HMI, Intelligent Electronic Devices (IED) , Merging Units (MU), switches and gateways are all present in a DS, as indicated in Figure 1. The IEC 61850 process bus in red and IEDs are new assets that are integrated for substation digitization. The following are the functionalities of the assets:

2.4.1 Server

A substation server, used for HMI manages, secures, and delivers substation data to the power utility control system. As detailed below, the server provides substation operators with the information they need to increase operability and reliability [47]:

1. Remote access: specialists can use a secure link to take control of the substation test computer.
2. Multi-function software: delivers data collection, protocol translation, automation logic, and event file collection software to the substation via remote access.
3. Fault record collection and safe file transfer to centralized archive: enables fault record collection and secure file transfer to centralized archive. For third-party conversations, file transfers are encrypted [47].

2.4.2 SCADA

As described in 2.2.4 in a DS, a SCADA system monitors, supervises, and controls power transmission and distribution. SCADA is a control and monitoring system that makes use of hardware such as servers, gateways, and switches, as well as software. A complete system model for power grid automation can be created and used by the monitoring system [48].

1. Remote monitoring: data from the substation is disseminated for DS remote monitoring.
2. Equipment can be controlled remotely from the substation control center.
3. Alarm module: supports analog/digital alarms, allows multiple alarms to be configured, and gives alarm summary and logging.

2.4.3 HMI

HMI process and visualization system that supports the IEC 61850 communication standard and communicates directly with bay units and protective devices.

Monitoring and control: this category contains applications that can monitor and control equipment and supply devices [49].

2.4.4 IED

IED is a microprocessor-based device that connects to substation networks (station bus and process bus) and facilitates communication between components from different suppliers in DS using the IEC 61850 standard. IEDs are essential components of power system automation, serving a variety of functions such as protection and metering. For their settings and configurations, IEDs from various suppliers provide electricity operators with customizable and menu-driven software programming tools [50]. Most Remote Terminal Units are replaced with IED in DS due to their numerous monitoring and protection benefits, as mentioned below.

1. Security function: SVs are employed for real-time DS security processing.
2. Metering and power quality analysis: IEDs are employed for protection in addition to voltage signals (CT/VT).
3. Self-monitoring and circuit monitoring: IEDs can diagnose internal faults at the card level [50]. Inter-face monitoring involves examining and confirming the inputs to IEDs using simple ways
4. Event reporting and fault diagnosis: relay IED monitoring capabilities are used to report events.

2.4.5 Gateway

Gateway is a communication port between a substation and a control center/ SCADA that allows SCADA to monitor and control operations throughout the whole power grid remotely.

Transmission: gateways are used to send substation indications and measurements to the control center/ SCADA, as well as the control center's directives to the grid's substation control systems [51].

2.4.6 MU

For interoperability of substation devices, MU is an interface that connects physical devices (e.g., CT/VT) to the IEC 61850-9-2 process bus and IEDs.

1. Digital interface: The MU measures the current from the transformers, merges them, and sends them in SV, digital format to the protection devices. In the DS [51], it serves as a link between switchyard devices and protection devices.

2. IEC 61850 converter: Event messaging, time synchronization, and sending SV via the process bus are all supported by MU. SVs are sampled and digitalized instantaneous values of analogue signals (voltage, current, etc.) in DS.

2.5 Regulations and guidelines

In order to minimize the societal repercussions, the rules must ensure that the power supply is maintained and that regular supply is restored in an efficient and secure way during and after extraordinary occurrences, as defined in section 1-2 of the Energy Act.

2.5.1 Protection of operation control system

Operational control system Figure 2.10 is defined in §7-1 of these regulations [52]. According to §7-1, operational control systems include operating centers, equipment, networks, computer rooms, communication facilities and other facilities and rooms, systems and components that take care of operational control functions. This definition is broad and when certain requirements are directed at the technical control system, this is commented on separately under each section [52].

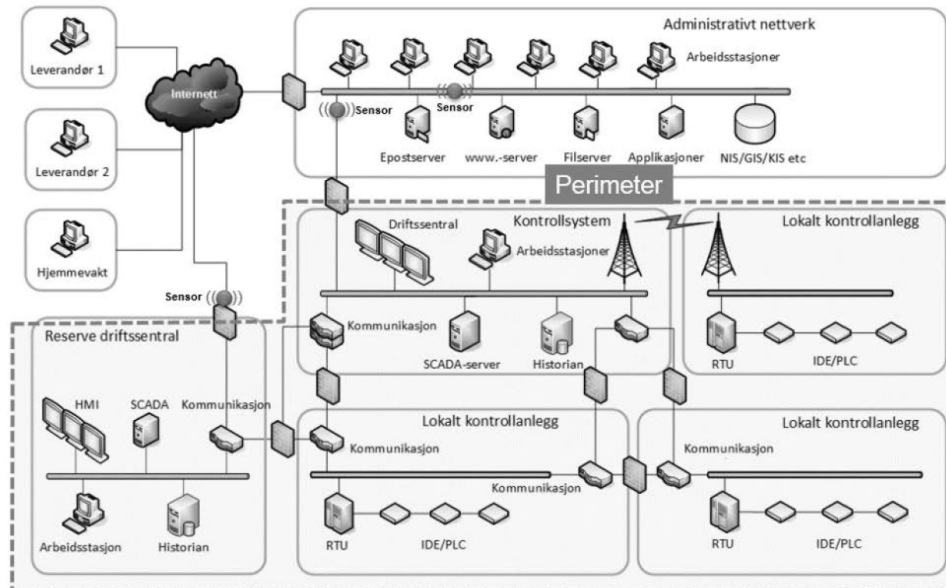


Figure 2.10: Operational control system and administrative network. Everything within the dotted line is considered an operational control system [52]

Operational control systems are essential for situational awareness, efficient operation, handling of extraordinary situations and rapid and safe recovery of faults and other damage to the system and infrastructure. The operational control system must function and provide correct information even in the event of prolonged and extraordinary events. If the operational control system fails, the company must be prepared and plan for alternative operations.

Chapter 7 sets requirements for securing the operational control system against a number of hazards and threats. §7-14 and §7-15 of these regulations sets additional requirements for enterprises with operational control systems in class 2 and 3.

Classes 1, 2 and 3 are used to classify a plant, system, or other item that is critical to the operation, restoration, or safety of production, conversion, transmission, or distribution of electrical energy, or district heating. Where the importance of the power supply is greatest, Class 3 is used.

General duty to protect the Operational Control System (OCS)

§ 7-1. General duty to protect the operational control system

- Businesses with an operational control system must ensure that these always work as intended and must protect the operational control system against all types of unwanted events.
- Operational Control System (OCS) include operations centers, equipment, networks, computer rooms, communication facilities and other facilities and rooms, systems and components that take care of operational control functions. By plant is also meant associated building technical constructions for operational control functions.
- Operational control functions are all organizational, administrative and technical measures to monitor, control and protect facilities in the power supply.
- External suppliers who are not KBO units are not permitted to perform operational control functions in grid plants or production plants.

2.5.2 Internal safety rules

§7-2. Internal safety rules

- Businesses shall lay down safety rules for use, development, operation, system maintenance, securing and more of the operation control system so that monitoring and control of the power supply can be performed in a safe manner.
- Companies must review the safety rules at least annually to ensure that they are complied with and that they provide satisfactory protection.

2.5.3 Documentation of the OCS

§7-3. Documentation of the Operational Control System (OCS)

- Businesses must at all times have updated documentation of the operational control system.

- The documentation must include an overview of all safety measures that have been implemented. The documentation shall also include an updated schematic representation of the operational control system's logical and physical network showing any access points between the operational control system and other networks. The documentation shall also include a complete overview of equipment in the Operational Control System.

2.5.4 Control user access

§7-4. Control user access

- Businesses must check that only legitimate users have access to the operational control system. For this, there shall be control schemes for allocating, changing and deleting user access.
- Businesses must check which user is or has been logged in to the operational control system, even when a remote connection is used.
- The control methods must be reviewed at least annually to ensure that every access rights are correct and at the right level class.

2.5.5 Changes in the OCS

§7-5. Check for changes in the Operational Control System

- Businesses must prevent unintentional errors and new vulnerabilities from being introduced in the event of a change in the operational control system. For this, there must be control schemes for assessment, testing and approval of changes.

2.5.6 Equipment use in OCS

§7-6 Control of equipment in the Operational Control System

- Businesses must ensure that equipment used in the OCS has not been used or is used outside the OCS, not even temporarily.
 - Businesses must prevent unauthorized access between the operational control system and other information systems.
 - Businesses shall prevent unauthorized access to equipment used to establish logical or physical distinctions between the operational control system and other information systems.
 - Businesses must permanently delete all information in equipment that is no longer to be used in the operational control system.
1. It is not permitted to use personally owned equipment in the operation control system.
 2. Data communication in the operations center and data room must be wired.
 3. The emergency preparedness authority may in special cases prohibit the use of certain types of equipment.

2.5.7 Counter measures

§7-7 Handling errors, vulnerabilities and security breaches

- Businesses must handle errors, vulnerabilities in software, security breaches and other incidents that could pose a risk to the operations control system.
 - Businesses shall have access to sufficient personnel with the necessary competence who can handle conditions specified in the first paragraph without undue delay.
 - Businesses must register all security breaches and incidents.
 - Conditions that may constitute an immediate risk to the operation control system's function must be notified and reported to the emergency preparedness authority, cf. §2-5 and §2-6.

2.5.8 Mitigation for OCS failure

§7-8 Emergency preparedness in the event of a failure in the OCS

- Businesses must have preparedness and prepared measures for continued operation of facilities in the event of a failure in the operational control system.

2.5.9 Hiring staff for operation center

§7-9 Staff of operation center

- Businesses must at all times have sufficient and available authorized personnel with the necessary competence, so that the operational control function can be exercised without undue delay.
- The company's risk assessment shall form the basis for choosing the size of the staff and the scope of schemes for calling on additional personnel if necessary, cf. §§ 2-4 and 5-8.

2.5.10 External connection to the Operational Control System

§7-10 External connection to the OCS

- Businesses must have control of external connection to the operational control system.
 - Only authorized users can be given access to the operational control system through external connection. Businesses must have an updated list of all approved users.
 - There must be a separate pre-agreed procedure for external connection to the operational control system.
 - Businesses shall have control schemes for approving, maintaining and terminating schemes for external connection to the operational control system, and for functions for setting protection.
 - Businesses must have control schemes for assessment, allocation, change and withdrawal of user access.

2.5.11 System redundancy in the Operational Control System (OCS)

§7-11 System redundancy in the operation control system

•Businesses must assess the need for redundancy in the operational control system based on local conditions and risk assessment.

2.5.12 Repealed

§7-12 This section has been repealed on 1.1.2019.

2.5.13 Protection against EMP and EMI

§7-13 Protection against electromagnetic pulse and interference

•Businesses should assess the operational control system's vulnerability to EMP or EMI. If vulnerabilities are identified, safety or emergency measures must be implemented in accordance with the importance of the operational control system for safe operation and restoration of function in the power supply.

2.5.14 7-14.Special requirements for OCS class 2

§7-14 7-14.Special requirements for OCS class 2

•In addition to the general requirements for the protection of the operational control system, companies with an operational control system in class 2 must meet the following additional requirements:

1. Backups

The company must regularly test that the restoration of electronic backups works as intended

2. Security audit

The company shall regularly carry out a safety audit and control of imposed protection measures in the operational control system. The purpose of the audit shall be to ensure that the measures are in fact established and function as intended.

3. Monitoring and logging

The company shall have automatic monitoring, logging, analysis and notification in the event of unauthorized use, attempts at unauthorized access, abnormal data traffic or other activity that is not authorized in the operational control system.

4. Unavailable operations center

If the operations center becomes inaccessible, the enterprise must be able to operate and manually control facilities that are part of the enterprise's operations control system. In addition, the company must have plans for alternative operations if the operations center becomes unavailable for a longer period of time.

5. Staffing of operations center

- a. The company shall ensure that all foreseeable extraordinary situations or events in the energy system or in the operational control system are immediately detected and handled without undue delay.
- b. The company must be able to staff the operations center within one hour at the latest.
- c. The company must have a shift system that at all times ensures rapid escalation of staffing when needed.

6. External connection to the operation control system

- a. When connecting from suppliers, the operations center must be staffed
- b. Businesses must have a control system for correct verification of the users who are approved to use an external connection for access to the operational control system. It is not allowed for one user identity to be shared between several people or systems.
- c. Businesses must ensure that external connections are made from a place with a sufficiently safe environment. Businesses should develop internal rules for what is a safe place.
- d. The external connection should only be opened when there is a need to access the operation control system. The connection must be closed when not in use.
- e. There must be a separate written procedure for external connection.
- f. If the KBO unit can manage facilities in the power supply through an external connection, the management shall only take place after permission or guidelines from an authorized person.
- g. Any connection to the operation control system through an external connection must be logged.

7. System redundancy

- a. Connections in the operational control system shall function independently of malfunctions in public electronic communication services or communication networks
- b. The operational control system up to systems in class 2 and 3 shall be redundant up to the local control system. In the local control system, the company must assess the need for redundancy.
- c. Redundant routes for connections and redundant components in the operational control system shall be physically separate and independent so that a single fault or incident does not result in the loss of important functions.
- d. Repair preparedness shall be established for all communications, cf. Chapter 4 and § 7-8.

8. Particularly concerning duplication

By duplication that uses identical technologies and solutions in the operational control system, the company must align itself so that the same system

error does not affect all duplicate systems at the same time, cf. § 7-7

9. Protection against EMP and EMI

Security or contingency measures shall be implemented for the protection of equipment as mentioned in § 7-13 against EMP and EMI for at least one communication road to facilities in class 2 and 3 which the operational control system controls.

10. Secure time reference

Operational control systems that depend on the exact time reference must have reliable sources for time indication

11. Requirements for suppliers

For deliveries to operational control systems, only foreign suppliers from countries that are members of EFTA, the EU or NATO are permitted. A delivery includes delivery of equipment, components, software, data, programming services, updates, bug fixes, service and maintenance.

2.5.15 Special requirements for class 3

§7-15 Special requirements for operational control system class 3

In addition to the general requirements as well as special requirements for the protection of OCS in class 2, enterprises with OCS in class 3 shall meet the following additional requirements:

1. Reserve operations center
 - Businesses must have a reserve operations center that must be located at a safe distance from the ordinary operations center, so that the same incident cannot affect both.
 - The reserve operations center must at all times be ready for use and be equipped so that it can function completely independently of the ordinary operations center and be able to take care of all operations control functions.
 - Undertakings shall at least annually assess whether there is a need to increase staffing or the scope of the on-call scheme for rapid escalation of staffing, §7-9, second paragraph.
2. Staffing of operations center
 - The operations center must be staffed 24 hours a day.
 - It must be possible to step up the staffing within one hour after the call has been made.
 - The company shall at least annually assess whether there is a need to increase staffing or the scope of the on-call scheme for rapid escalation of staffing, §7-9, second paragraph.
3. External connection to the operation control system
 - Connection to grid systems or control of other systems through external connection is not permitted.
4. System redundancy
 - The communication routes in the operational control system shall be con-

structured so safe and robust and with such redundancy and distance that simultaneous or subsequent events such as storms, fire or extensive technical failure do not prevent or damage both routes and other redundant subsystems.

- Up to all facilities in class 3, the company shall have control and control over all components and other technical solutions in at least one communication road, and protect these, cf. Chapter 5.

5. Protection against EMP and EMI

- Security measures shall be implemented for the protection of equipment as mentioned in §7-13 against EMP and EMI for at least one communication road to facilities in class 3 which the OCS controls. The emergency preparedness authority may in special cases approve emergency preparedness measures as an alternative to safety measures.

- In the communication road to facilities in class 2 that the operational control system controls, safety or emergency preparedness measures must be implemented.

6. Determination of special requirements for staffing

- For particularly important operational control systems, the emergency preparedness authority may set special requirements, also for staffing, §section 5-7.

2.5.16 Protection of power systems

§7-16 Protection of power systems in regional and transmission networks.

Communication-based protection systems in transmission and regional networks shall have reliable and secure connections that operate unaffected by fault conditions in the power system, and ensure the transmission of necessary signals and messages to relevant operations centers.

Protection systems must ensure rapid and selective disconnection of the device with malfunction to limit the consequence of faults in the power system.

2.5.17 Mobile radio network

§7-17 Mobile radio network - operating radio.

KBO devices that depend on reliable mobile communications for operation, security or restoration of function shall have access to a mobile communication system. This communication system must:

1. Covered by the general security obligation pursuant to §5-1
2. At all times be kept in working order, be ready for use, and there must be quick access to critical spare parts and expertise in error correction
3. Could be operated by personnel with the necessary competence for use
4. Have a sufficient degree of coverage for the power supply's plant and operation

5. Be able to function independently of malfunctions in public electronic communication services or communication networks
6. Have sufficient emergency power in the event of extensive or prolonged power outages, including an emergency power system with automatic start and a minimum of 48 hours of independent operating time
7. Have the necessary functionality with, among other things, direct device for device communication, group broadcasting and joint calling
8. Be able to act as a reserve connection if another important connection fails
9. Where the radio network uses facilities belonging to a classified operational control system or where it must be considered as part of this, the communication system shall be protected in accordance with the class of the operational control system
10. Where the radio network is digitized and e.g. is based on IP solutions, this must be secured against unauthorized access, spread of unwanted software, unlawful takeover, etc. in accordance with the relevant provisions of these regulations

Chapter 3

Cyber vulnerabilities and cyber threats at digital substations

3.1 Cyber attack

The attacker uses the vulnerabilities of the adversary's machine to deliver a payload during an offensive cyber operation. This means, once the attacker has access to the computer's data and files, this person can do anything that to ensure the operation's success. Cyber attack or exploitation are two terms used to describe offensive Cyber operations, depending on the attacker's aims [53].

3.1.1 History

Malicious Cyber-actors have been focusing their efforts on the Industrial control systems (ICS) that manage our vital infrastructures for years. The majority of these incidents are not publicized, and ICS Cyber-Threats and incidents are less well-known than business cyber-threats and incidents. This section offers a quick look at publicly disclosed cyber-threats to critical infrastructure, shedding light on the growing threat to ICS equipment. It's crucial to realize that this list isn't exhaustive. The events included for this analysis show important threats and incidents to ICS, demonstrating that severe cyber-incidents to ICS devices are increasing in frequency and complexity[54]. The most common and typical cyber attacks ICS are facing on daily basis are listed below.

3.1.2 Top 20 attacks

The Top 20 attacks are presented below, roughly in order of least-to-most-sophisticated. The list includes a variety of industrial cyber threats that can be used to compare security postures across locations and defensive systems. Even if an organization's specialists or experts to create their own list, starting with a standardized list like the Top 20 can help guarantee that the custom assessment process considers a

sufficiently broad spectrum of attacks [55].

- ICS Insider
- IT Insider
- Common Ransomware
- Targeted Ransomware
- Zero-day exploit Ransomware
- Ukrainian Attack
- Sophisticated Ukrainian Attack
- Market Manipulation
- Sophisticated Market Manipulation
- Cell-phone WIFI
- Hijacked Two-Factor
- IIOT Pivot
- Malicious Outsourcing
- Compromised Vendor Website
- Compromised Remote Site
- Vendor Back Door
- Stuxnet
- Hardware Supply Chain
- Nation-State Crypto Compromise
- Sophisticated Credential Insider

3.1.3 ICS-cyber incident timeline

Industrial control systems (ICS) are embedded cyber-devices that run vital infrastructure (e.g energy, water and others). ICS devices are less well-known, and they are usually specific to the cyber-Operational technology framework, which is distinct from enterprise Information Technology. In ICSs, cyber-threats present themselves in a variety of ways. This section shows the numerous forms of ICS threats in this section, including targeted attacks, cyber-intrusion campaigns, Malware, and cyber-threat groups. Table 3.2 below show some of the attacks throughout the total cyber attack history. Directed attacks, cyber-intrusion campaigns, Malware, and cyber-threat groups are among the threat kinds depicted in a chronology. Cyber security companies, independent security researchers, the media, other published publications, and government sources were used to produce this open source analysis[56]. This list is not exhaustive, but it concentrates on the most serious cyber-threats, incidents, and campaigns that have affected ICS equipment and critical infrastructure. Attacks were directed at ICS devices in some situations, while ICS devices were indirectly targeted or harmed in others situations [54].

Table 3.1: ICS cyber incident timeline table [56]

Year	Type	Name	Description
1903	Attack	Marconi Wireless Hack	Morse code was used to hack Marconi's wireless telegraph presentation.
2000	Attack	Maroochy Water	More than 265,000 litres of untreated sewage were released due to a cyber-attack.
2008	Attack	Turkey Pipeline Explosion (Not quite cyber)	Attackers obtain access to a pipeline's control network by exploiting security camera's weakness?
2010	Malware	Stuxnet	The world's first widely publicized digital weapon.
2010	Malware	Night Dragon	Attackers targeted oil, energy, and petrochemical firms with sophisticated malware.
2011	Malware	Duqu / Flame Gauss	Advanced and intricate Malware used to attack specific firms, such as ICS firms.
2012	Campaign	Cyber	ICS-CERT found active series of cyber-intrusions targeting natural gas pipeline sector.
2012	Malware	Shamoon	Malware used to target major Middle Eastern energy businesses like Saudi Aramco and RasGas.
2013	Attack	Target Stores	Target lost \$309 million after hackers obtained access to its sensitive banking systems through a third-party that managed its HVAC ICSs.
2013	Attack	New York Dam	Iran allegedly launched cyber-attack, on the Bowman Dam in Rye Brook, New York, according to the US Justice Department.
2013	Malware	Havex	ICS based malware campaign.
2014	Attack	German Steel Mill	A cyber-attack on a steel factory in Germany resulted in significant system damage.
2014	Attack	Black Energy	Malware that targeted Human Machine Interfaces in Industrial control systems (ICS)s
2014	Campaign	Dragonfly/Energetic Bear No.1	A cyber-espionage effort is now underway, with a focus on the energy sector.
2015	Attack	Ukraine Power Grid Attack No.1	The first successful cyber-attack on a country's power infrastructure has been discovered.
2016	Attack	"Kemuri" Water company	Hundreds of PLCs used to manage control applications were hacked, and water treatment chemicals were tampered with.
2016	Malware	Return of Return of Shamoon	Second Shamoon virus attack knocked down thousands of machines at Saudi Arabia's civil aviation department and other Gulf State entities.
2016	Attack	Ukraine Power Grid Attack No.2	In a second attack, cyber-attackers tripped breakers in 30 substations, cutting out power to 225,000 people.
2017	Malware	CASHOVERRIDE	The malware that caused the power outage in Ukraine has finally been detected.
2017	Group	APT33	A cyber-espionage ring with a focus on the aviation and energy industries.

Table 3.2: ICS cyber incident timeline table

Year	Type	Name	Description
2017	Attack	NotPetya	Malware targeted Ukraine and pretended to be ransomware but didn't allow victims to pay ransom to get their files back.
2017	Campaign	Dragonfly/Energetic Bear No.2	Symantec malware that targeted Ukraine, the energy sector was attacked by sophisticated assault group.
2017	Malware	TRITON/Trisis/HatMan	Sophisticated malware has been targeting industrial safety systems in the Middle East.
2020	Attack	CPC Corp Taiwan	Taiwan's petroleum and natural gas company's payment system crippled by a ransomware attack.
2021	Attack	Colonial Pipeline USA	Hackers accessed company's network by exploiting VPN account with remote access to the computer network.

3.2 Cyber kill chain: 7 phases of APT intrusions

Identifying system flaws needs logical reasoning and the capacity to systematically think through various actions, alternatives, and probable conclusions, regardless of the type of Hacker. The employment of mental models is implied by this mix of reasoning and systematic thinking. To understand the way a Hacker think is easy to follow this method which is common among Cyber crime. It consist of Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command Control, and Action Objectives which are the seven common steps of APT attacks in "Cyber Kill Chain [57]".

3.2.1 Step 1: Reconnaissance

In this step, attackers use a variety of tools and tactics active and passive reconnaissance to obtain as much information as possible about their target. Attackers may use active and passive reconnaissance to obtain information about the target's network (e.g., exposed devices, operating systems, and versions), as well as determine the level of exposure. Are qualifications or information about personnel, for example, freely available? The attackers purpose is to find the target's weakest entry points, which they can or should employ to accomplish their objectives. Individual information is frequently exploited with Social engineering and Phishing attempts[57].

As an example the Ukrainian attack, Hackers started with sending spear Phishing e-mails¹ to three power distribution firms² in the spring of 2015, including Excel files that exploited weaknesses in Microsoft office software (macros particularly). They had to work on getting into SCADA systems despite the fact that networks in Ukrainian distribution centers were separated by a firewall. They could change the Uninterruptible power supply (UPS), the system that provides backup power to the control centers, once they had access to SCADA [58].

3.2.2 Step 2: Weaponization

Based on the reconnaissance phase and chosen tactics, attackers create a specific malicious tool. These tools are often a Remote Access , or RAT, combined with other applications for the exploitation phase and a deliverable payload, such as an infected document (PDF, PPT or Excel file), are frequently used by attackers.

Weaponization, on the other hand, can take many different forms depending on the delivery method, such as exploit kits. In the Ukrainian situation, the attackers do not disguise Malware as a legal file and fool their victim into downloading it.

Instead, the target is urged to visit an infected website, which could result in Malware being "drive-by downloaded" or a susceptible host being directly targeted by attackers.

Overall, the weaponization phase is concerned with how attackers customize malware to the target in order to conceal dangerous code. To achieve the targeted aim, there might be multiple "levels" of weaponization and harmful programs utilized[57]. Malware used during the Ukrainian attack was Black-Energy, attacks, cyber espionage, and data loss were all carried out with the Trojan [3].

3.2.3 Step 3: Delivery

As the attack progresses into a "active" phase, things become more dangerous. This phase relates to the delivery of the tool that was created in the previous phase, which can take a variety of forms. For example, if attackers discovered suitable credentials or unprotected devices on their target's network, they may use their malware to remotely access and exploit the devices. Compelling an employee to disclose access credentials and exploiting weaknesses as they are discovered are two further means of distribution [57].

For targeted attacks, 65% of known APT groups utilized Phishing emails. Through well-crafted phishing emails that employ Social engineering tactics, attackers frequently distribute infected files or links. Email attachments account for around

¹E-mails were sent from address info@rada.gov.ua with subject "Decree of the President of Ukraine No. 15/2015 on partial mobilisation from January 14, 2015" and caused no suspicion. (Prudka 2016)

²Ukraine is divided into 24 self-governing regions, each of which has its own power distribution company.

18% of malware vectors, while email links account for nearly 40%. (from 2020 Data Breach Investigations Report).

Delivery of the weapon can be done by plugging infected USB into HMI, Switch in control center or Digital Substation but most commonly it is down by making others download from a malicious website. The same happened in the Ukrainian attack, Black-Energy got delivered and it started exploiting the SCADA.

3.2.4 Step 4: Exploitation

The exploitation phase might commence once the weapon has been delivered to the target. The goal is for attackers to proliferate over the network, elevate privileges, or do everything else they need to prepare for the next phases.

This stage can cause severe damage to the system and might put the system down for long time.

Malware frequently targets known (Common Flaws and Exposures, or CVEs) or unknown zero-day vulnerabilities in programs or Operating System (OS) (those that have not yet been spotted and patched by the provider of the exploited instance).

3.2.5 Step 5: Installation

As previously said, APTs are frequently about data ex-filtration over a long period of time. The attackers strive to "install" themselves on the network and retain persistence during the installation phase, which frequently involves the use of RATs [59] and backdoors. If one of their access points is found, they can use multiple techniques to offer redundancy.

Black-Energy spread over the network and took over several part of the Ukrainian power plant [60]. The back doors was found later by the response team with the name of "BackBackdoor.Win32.Blakken", "Backdoor.Win64.Blakken", "Backdoor.Win32.Fonten" and "Heur:Trojan.Win32.Generic" [3]

3.2.6 Step 6: Command Control (C2)

A C2 server is used to build a channel between the compromised computers and the malicious actors once the attackers have been "installed" in the network. Intruders can utilize this C2 server to interface directly with their victim, whether to ex-filtrate information or implant fresh malware.

3.2.7 Step 7: Action objectives

After all of the above procedures have been performed, Advanced Package Tool (APT)s can begin working on their initial objectives. Data ex-filtration, remaining undetected until a certain time, installing malware designed to disable or destroy systems, and pivoting toward higher priority targets or systems linked to the system they have infiltrated are just a few examples.

The premise behind the phased method is that if a defense can detect and document one of the phases utilized in an APT assault, a similar intrusion will eventually fail. The same happened in the Ukrainian Power Grid where the attackers developed two SCADA hijacking tactics (one proprietary and one agnostic) and successfully implemented them at three separate firms using different types of SCADA/DMS installations. Finally, the attackers exhibited the capacity and willingness to target field equipment at substations, develop custom malicious software, and render devices inoperable and unrecoverable, such as serial-to-Ethernet converters [60].

A Kill Chain, on the other hand, is just a metaphor for how an intrusion can happen. The Kill Chain is an excellent tool for assisting defenders in mapping specific threat scenarios; nevertheless, it must be tailored to the defender's available resources and applications.

3.2.8 Situation overview of cyber attack on Ukrainian power grid

A cyber-attack disrupted energy to roughly a quarter-million Ukrainians two days before Christmas in 2015. This is the first time a cyber-attack on a power grid has been successful. According to Reuters [61], a power provider in Ukraine's western region experienced a power outage that affected a vast area, including the regional capital of Ivano-Frankivsk. Attackers knocked down power at 30 substations, stranding 230,000 people for up to six hours. SCADA equipment was rendered unusable, and power restoration had to be done manually, which further slowed the restoration process [62]. Investigators revealed that attackers aided the outage by exploiting macros in Microsoft Excel documents with the BlackEnergy malware. Spear-phishing emails were used to infect the company's network with malware. The virus was analyzed by ICS-CERT and US-CERT in collaboration with the Ukrainian CERT and international partners, and it was established that a BlackEnergy 3 variant was found in the Ukrainian power system. The attack was blamed on Russian attackers by the Ukrainian intelligence community. DHS and the FBI have publicly identified BlackEnergy as a member of the RIS GRIZZLEY STEPPE gang [63]. A US interagency team consisting of officials from ICS-CERT and US-CERT, as well as the FBI, and the North American Electric Reliability Corporation, flew to Ukraine at the request of the Ukrainian government to gather information on the incident and identify potential mitigations [54]. This incident demonstrated to the world that a cyber-attack may really do harm to the power grid, and it served as a wake-up call to guarantee that the rest of the world's power grid is fortified against similar attacks. In the instance of Ukraine, the attackers employed crude, low-tech methods to accomplish their goal. The cyber-attack on Ukraine's power infrastructure was a watershed moment in cyber-history.

3.3 Attack classifications

3.3.1 Sophistication

Both the assault and the attacker have a high level of sophistication. Was the attack carried out with off-the-shelf attack tools, professional-grade tools, or custom-built tools? Are the assailants experts in the field of cybercrime? Do they need to comprehend the physics of the industrial process in order to achieve their objectives? Do they need to be able to connect physical consequences with cyber manipulations by understanding the design of important industrial control systems? How much inside information do the attackers require that isn't available from public sources in order to plan and execute their attack? Is there any inside help for the attackers? Or will they be able to carry out the complete attack from outside the target organization? [55].

3.3.2 Consequences

Physical states of the industrial system that we are attempting to avoid are the primary consequences, followed by changes in control system computers. Impaired or poor-quality output, unexpected shutdown of the physical process, damage to physical equipment, harm to personnel at the industrial site, or dangers to public safety are the most common physical effects [55].

3.4 Cyber risk identification

There are many types of risk identification methods used around the world. One of the methods used in order to address cyber-risks in ds is a three-step TO-DO technique is identifying cyber-risks [64].

3.4.1 Cyber-attack vectors

An attacker alters, degrades, or disables at least one component utilized for protection, automation, or control in an ICS during a cyber-attack. When an attacker has control of one or more substations in a power system, it can have disastrous effects for the entire grid. As a result, not only in control centers, but also in substations. Cyber-attack vectors must be identified and appropriate cyber-security measures must be installed [65].

To examine the most relevant cyber-attacks and dangers that are likely to occur in a DS, two assumptions are established to address the cyber-attack vectors. To begin, only authorized individuals are permitted to enter the substation, and only engineers and managers with access to physical equipment are permitted. Second, remote access to the DS is available via remote access software for controlling devices and computers from a distance.

Cyber-attack vectors on a DS are depicted in Figure 3.1. Mobile data storage, engineering PC, test PC, and test set are four devices that can link to DS assets.

According to investigations [65], ds is vulnerable to cyber-attacks via the following five vectors:

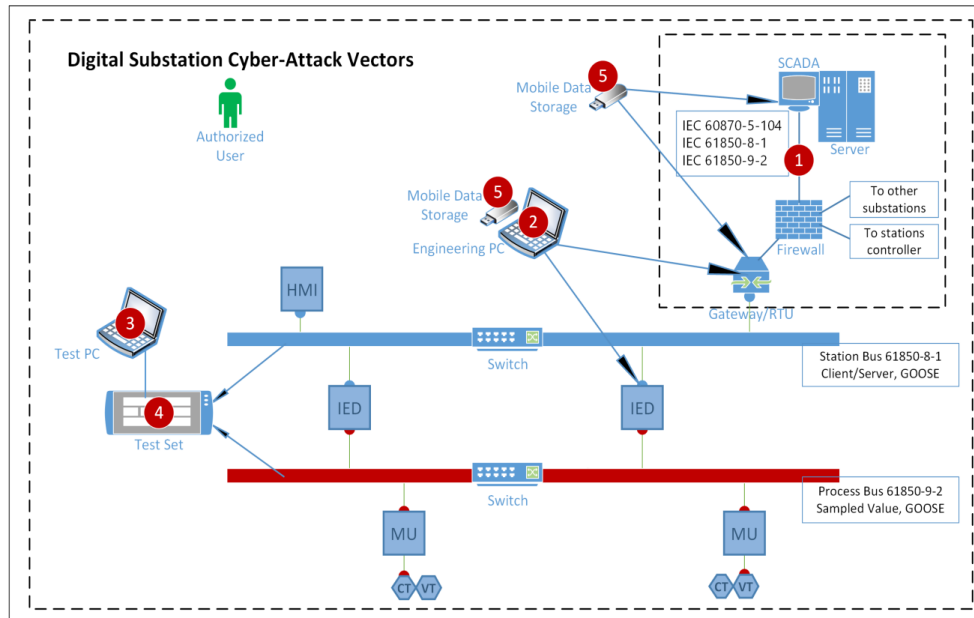


Figure 3.1: Architecture of a DS with assets and corresponding cyber-attack vectors [15]

Path 1: Infiltrate the control center/SCADA system. Unauthorized remote access, server data collecting and modification, and gateway device software manipulation are all cyber-threats that could lead to command and control of the entire substation.

Path 2: Use the engineering PC to attack. Malware can be found on a PC, and by connecting it to a relay, the malware can be executed and installed on IED or SCADA systems. Engineering PC can be used to access device settings, which can be used as a cyber-attack vector.

Path 3: Use the testing PC to launch an attack. A testing PC is connected directly or via a Test Set to the station bus for testing, and this connection poses a risk of infecting substation components such as IEDs, HMIs, and MU. While the Test PC is connected to the station bus or process bus, test documents could be a possible attack vector.

Path 4: Attack through test set can lead the testing devices as entry points to the attackers to exploit which makes it vulnerable.

Path 5: Infiltrate the storage device. Connecting infected devices to asset ports poses a risk of executing malicious software or modifying IED or SCADA system.

3.5 Cyber-risk impact

Cyber-attack vectors may have an impact on the DS's cyber-security measures. The Confidentiality, Integrity and Availability (CIA) [66] is a well known model for developing successful security policy and cyber security measures that is based on three concepts:

1. **Confidentiality:** Security techniques such as username/password, access control models and rules, encryption, and others are used to assure authorized access to sensitive information
2. **Integrity:** Ensuring that information is accurate, consistent, and reliable for its intended purpose, and that information can only be modified by authorized users.
3. **Availability:** Assuring permitted access to information and avoiding service denials[66].

In an ICS environment, MITRE ATT&CK [64] claims that 11 cyber attack strategies, including collection, command and control, discovery, evasion, execution, impact, impair process control, occupy response function, initial access, lateral movement, and persistence, are successful against security measures[67]. These approaches could be used by attackers to alter ICS and one or more CIA measures. According to the tactic's description, lateral movement compromises confidentiality by allowing unauthorized access to the ICS environment and sensitive data as shown in table below.

General Cyber Attack Tactics affecting ICS [15]			
	Tactic	Description	C I A
1	Collection	collect relevant data and domain knowledge	X
2	Command and Control	control and connect with hacked systems, controllers, and platforms	X X X
3	Discovery	determine the ICS environment	X
4	Evasion	avoid getting spotted	X X
5	Execution	execute harmful software	X X X
6	Impact	ICS systems, data, and the surrounding environment can be manipulated, interrupted, or destroyed.	X X X
7	Impair Process Control	Physical control processes can be manipulated, disabled, or damaged	X X X
8	Inhibit Response Function	impede the functions of safety, protection, quality assurance, and operator intervention from reacting to a failure, hazard, or unsafe condition	X X
9	Initial Access	entering the ICS system	X
10	Lateral Movement	browsing the ICS environment	X
11	Persistence	preserve ground in the ICS environment	X X

3.6 Cyber-attacks on Digital Substation (DS)

A cyber attack on a DS could be for a variety of reasons, including hackers demonstrating their ability to breach a system's security or causing damage to substation components. The most significant threats are those that aim to seriously disable the system, such as by generating fake data or attempting to seize control of the system to cause process damage by sending inappropriate control commands or making illegal use of equipment [68]. These attacks necessitate skills, time, system knowledge and a lot of experience. While different vendors DS structures may differ in terms of automation and setup, the following is a list of prevalent cyber threats.

3.6.1 Infrastructure network attacks

These networks are vulnerable and must be protected from outside and inside threats. The system can be made unsafe by a weak firewall, network design, and component configurations. A person on any other system on the network, regardless of how many other computers are between them, could potentially get access to the target system once it is connected to the WAN using TCP/IP transport layer networking[68].

DDoS attack:

By flooding the network with traffic, the attacker tries to render the network unreachable to the intended user. DDoS attacks, which deliver more traffic to the server than it can manage, can help the attacker achieve this.

Scanning ports

To obtain access to the substation, the attacker scans the network and equipment such as switches, IEDs, relays, and the SCADA system for open ports.

Intrusion into the local network on devices

HMI or SCADA systems are impacted by the attacker by following methods:

1. Accessing administrative-level SCADA consoles that are merely secured by a login ID and password.
2. Accessing confidential information.
3. Accessing sensory data.
4. Accessing data from memory and memory corruption.
5. False-data injection.
6. False commands are sent to manipulate the network and electronic equipment such as relays, IEDs, and other sensors.
7. Modifying ID/password files or managing user credentials[69]

3.6.2 Malware injection

Malicious Malware, such as ransomware and worms, are injected into the software components of DS by the attacker. Malicious malware like this can readily infiltrate and spread into the network as well.

3.6.3 Intrusion into the physical site:

The following is how a malicious engineer or technical staff intrudes into the DS:

1. Linking a personnel's mobile device to the Internet.
2. Inserting a virus-infected USB drive or laptop.
3. Manually managing devices
4. Regulating device functioning

3.6.4 Spoofing attack:

To perform operations in the system or obtain access to sensitive data, the attacker or malicious application acts on behalf of another person/device.

3.6.5 Man-In-The-Middle-Attack:

By impersonating SV stream, MMS, and GOOSE messages, the attacker gains unauthorized access to the communication network or between sensors and controllers, causing system failure or unwanted activities.

3.6.6 Human-factor based attacks:

To secure a DS, those who are allowed to enter the physical substation (managers and engineers) should be approved and have limited role-based access to the components depending on their levels of authority. However, an employee may have many roles, resulting in DS vulnerabilities. Assigning numerous roles to the same person frequently results in a permission mix that may allow unwanted authorized access, either due to a combination of permissions across roles or because the individual is allocated a role with more permissions than they require. By mistake or on purpose, an employee could destroy or damage the Cyber or physical system, which is referred to as a "inside job." These actions could also be carried out by former workers of vendors who have access to potentially hazardous information[16].

3.7 Cyber-attack map for a pilot DS

A cyber-attack map based on the DS architecture in Figure 3.2 is shown. An attacker can scan the network for open ports, listen to network traffic, access sensory data, stop/change functionality, reprogram devices, and obtain access to the memory of such devices. These attacks necessitate high-level access as well

as a reasonable amount of system knowledge and skill. Detailed information of component-level vulnerabilities and map popular cyber-attacks to DS are in the following sections, pointing where and how assaults can occur.

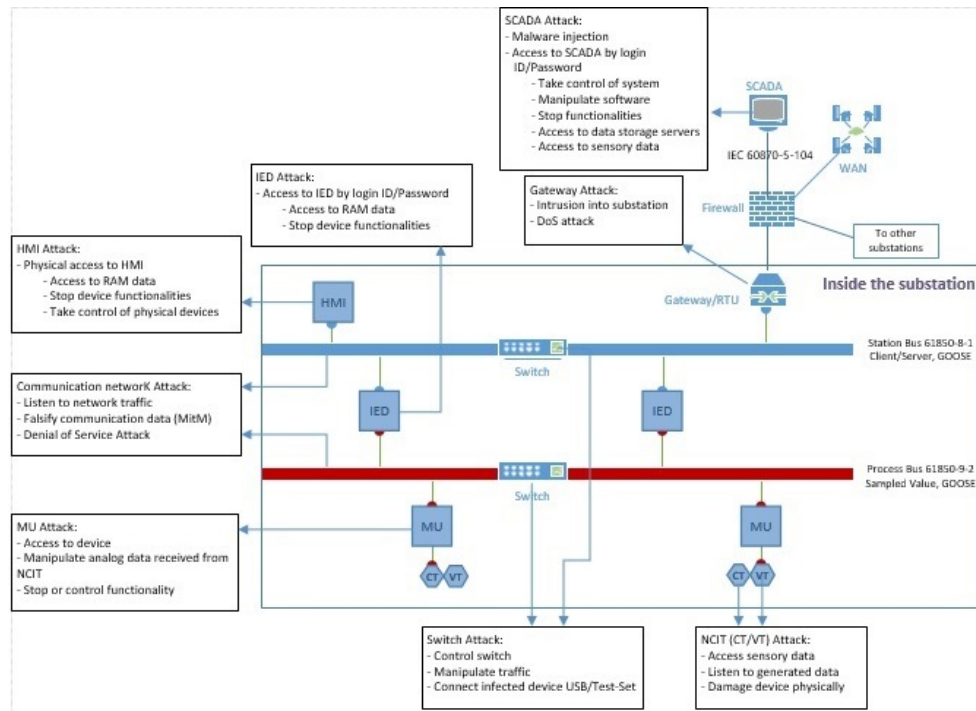


Figure 3.2: Component wise map of potential cyber-attacks to DS[16]

3.7.1 Communication network:

Attacker can listen to network traffic, fabricate communication data (Man-In-The-Middle), and use a attack to locate and exploit weaknesses in communication networks.

3.7.2 Switch:

Attacker can modify switch traffic, operate switches on either bus, and attach an infected device via USB/Test-Set.

3.7.3 HMI/SCADA:

Attacker could infect the SCADA system with malware. To obtain access to the SCADA system, the attacker would typically need to gain access to credentials and login. If the attacker gains access, the attacker may be able to take control of the system, change SCADA software, disable functions, and access data stored on servers and sensory data.

3.7.4 Intelligent Electronic Devices:

By getting login credentials, an attacker can gain access to an IED. If this is the case, the attacker may reprogram the IED, gain access to its data, and/or disable or change the device's functions.

3.7.5 Merging Units (MU)s:

Attacker might acquire access to a MU device and use it to modify analog data received via NCIT, as well as stop and control functions.

3.7.6 Physical devices (CT/VT):

Attacker could get access to sensor data, listen in on measured values, and/or physically harm the device. An assault could have a wide range of effects, from affecting sensors by providing tampered measurements (e.g., sensor spoofing) to causing small performance disturbances to a total takeover of the system. Physical attacks on sensors are also possible.

Chapter 4

Design

This chapter explains how the project's complete framework is created. This chapter will include a description of the tools utilized, as well as the network architecture, application design, and a system overview.

4.1 Available solution

There are numerous types and methods of analysis and simulation available online. Each company involved in this industry has its own approach for testing and analysis. However, due to sensitive data and model designs, obtaining these testing models is quite challenging [70]. A simulation model developed within the InterSecure project (RCN 296381) was provided by the supervisor to conduct attack experiments in order to meet the desired requirements for this thesis. The simulation model is available as an archive in the open virtualization format (OVA). The file is a virtual machine image that can be loaded into virtualization software like VMware Workstation or Oracle VM VirtualBox.

4.2 Approach design

Two approaches of digital substation Emulation are included in the study document [71]. The first way involves using the Mininet network emulator, which lacks some advanced networking functionality such as routing and VPNs but still can swiftly generate the topology quickly. The second method from the document given [72] involves the use of virtual machines, that may be linked together to provide complete functionality, including router devices and VPNs connections. For communication between substations and the control center, an open source library called libIEC60870-5 is employed. The library is examined and compared to data from the Norwegian National Smart Grid Laboratory. The document [72] explains how to alter the library to construct messages that are identical to real-world traffic based on the discrepancies discovered. The supervisor made these

changes because he was the primary source of the model's creation. By producing messages with falsified temperature or multimeter sensor data, these messages can be utilized to validate substation behavior or for security penetration testing.

4.2.1 Simulation model design

The Mininet¹ network emulator is used to develop the model network topologies. The emulator allows users to create network topologies using hosts and switches, and it is very resource efficient thanks to its usage of lightweight virtualization with a common kernel. Open-source libraries² with customized scripts are used to simulate communication.

The following software setup are used in the simulation model:

- **Operating system: Linux Lite 5.2**
- **Mininet network emulator: 2.3.0d6**
- **Libraries for communication emulation**
 - lib60870:2.2.0
 - libIEC61850:1.4.2.1

4.3 Infrastructure design

The Mininet network emulator is an open-source tool used to develop the model network topologies. The emulator allows users to create network topologies using hosts and switches, and it is very resource efficient thanks to its usage of lightweight virtualization with a common kernel. Open-source libraries with customized scripts are used to simulate communication.

4.3.1 Model topologies

Basic and extended topologies are included in the model. These topologies include following sections:

- **Basic topology:**
 - Control center.
 - 2x Digital secondary substations.
- **Extended topology:**
 - 1x Digital primary substation
 - Control center.
 - 2x Digital secondary substations.

¹<https://mininet.org/>

²<https://libiec61850.com/>

Basic topology

Figure 4.1 depicts the basic topology. In the model implementation, all device names are used consistently. Two Digital Secondary Substation (DSS) and a control center are included in the model. A switch is installed between the gateway and the RTU in both substations. The AttackDSS1 and AttackDSS2 switches are configured for external connections. The Internal Network option with the same name can be used to link any other virtual machine to these connections. The section "Connecting an external machine" describes this option. IEC-104 communication is included in the topology.

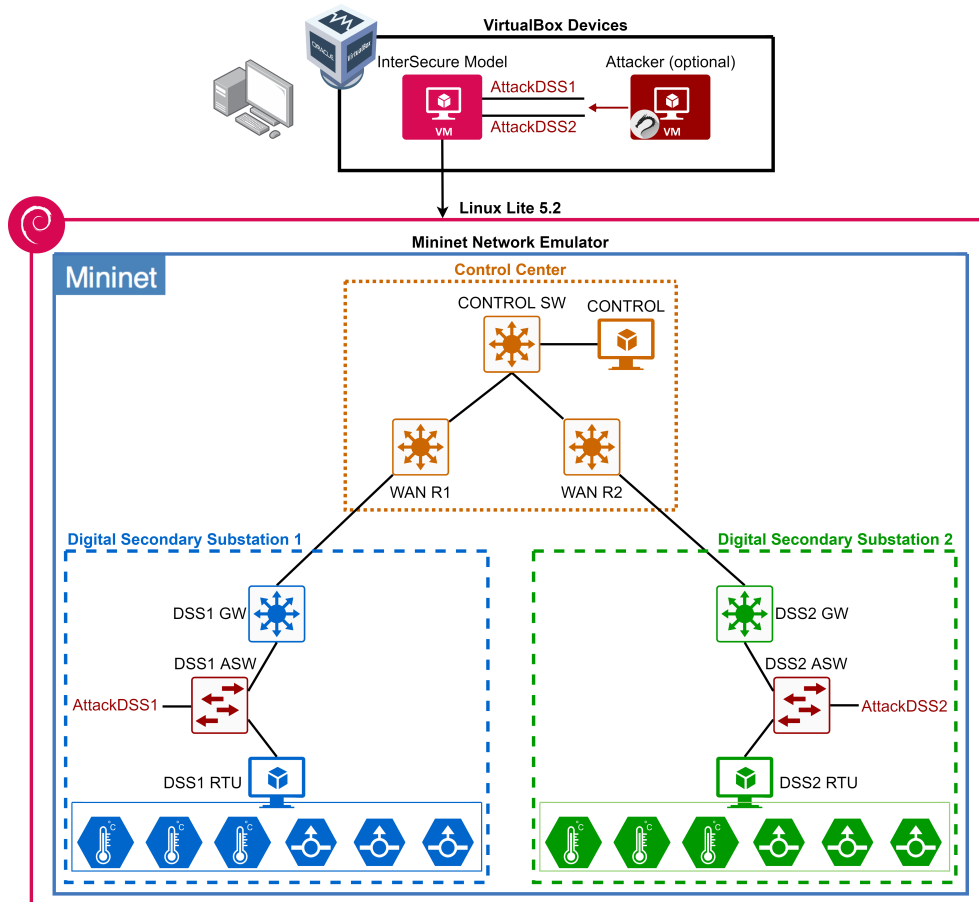


Figure 4.1: Basic topology with two DSS [73]

configuration

For software switches, Mininet does not allow VLAN configuration commands. The configuration must be done outside of the Mininet network. VLAN 10 is assigned to port 1 on switch 1 in the following example:

Code listing 4.1: Vlan Configuration av Mininet

```
sudo ovs-vsctl set port S1-eth1 tag=10
```

Extended topology

As indicated in Figure 4.2, the extended topology includes a digital primary substation. The substation is linked to the control center and incorporates various device kinds (IEDs and an HMI), as well as various connection types (GOOSE, SV).

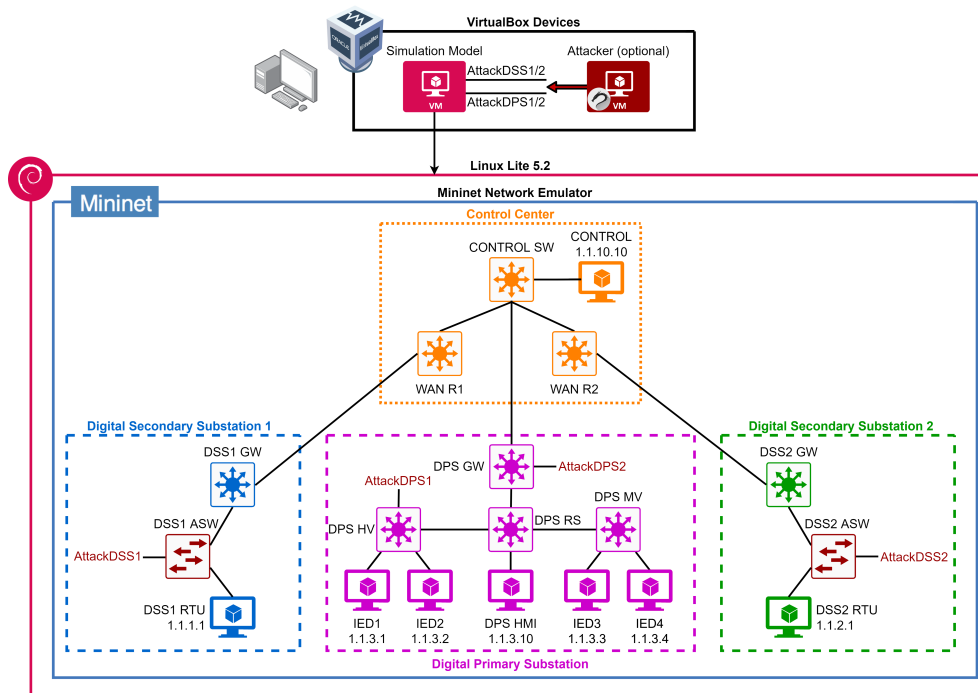


Figure 4.2: Smart Grid topology[73]

4.4 Network design

Network emulation differs depending on the virtualization technology used. To link neighboring devices in Oracle VM VirtualBox, use the internal network adapter option (for example the RTU to the router gateway). On both devices, the network name must be the same. The virtual machines must next configure these interfaces (to set up their IP addresses, network masks and default gateways).

4.4.1 Communication emulation

In both emulation approaches, the library lib-IEC60870-5 is used for communication emulation. The library is built in C and is compatible with all major operating systems, including Linux, Mac OS X, and Windows. This library must be installed on end nodes, which can vary depending on the emulation mechanism chosen. The library can be obtained from the official webpage [74] using either approach.

4.5 Realization

4.5.1 Safe lab

Before launching the attacks, it is crucial to build a secure lab where practicing with the selected tools and procedures are implemented. The best way to do this is to use a virtual environment. It is done by setting up VM-virtualization to run multiple operating systems on the same physical machine.

There are many virtual machine environments to choose from. VMware Workstation, VirtualBox, Parallels, Virtual PC, Xen, ESXi, Hyper-V, and any other virtualization software are examples. The analysis lab will be built up in Oracle's free VirtualBox in this thesis.

Virtual-box configuration

By selecting the InterSecureModel machine and selecting Computer / Settings, the virtual machine may be configured. This will bring up the configuration window, which is divided into numerous sections. The most significant are listed below:

1. RAM and processor are included in the system configuration (number of processors and execution cap). The simulation model should have at least 4 GB of RAM and two processors with a 100% execution limit.
2. Display – this section offers settings for video memory and multiple monitors.
3. Network - comprises virtual network interface cards that can be used to link the model to another (virtual) machine or to the internet.
4. Shared Folders — This section covers the settings for shared folders that can be used to transfer files between the host OS and the virtual machine.
5. User Interface – controls how control components are shown during the VM execution.

Kali linux

Kali Linux ³ is a Debian-based Linux system with a number of security tools pre-loaded, which we'll use during the testing and analysing. Kali Linux comes with hundreds of pre-installed security tools that may be used to test the vulnerabilities of a private network or the internet. The kali-linux-2021.3-amd64 version was utilized throughout and set-up for this penetration testing at the time of writing this thesis. A virtual network laboratory is a suitable best solution for setting up Kali-linux at this time, in order to eliminate or avoid any network vulnerability risk throughout this exercise.

³<https://www.kali.org/get-kali/>

Target system

Any virtualization machine can import the simulation model. The technique is shown in Oracle VM VirtualBox, which is open-source and works with all major operating systems, including Windows, Linux, OS X, and Solaris. In VirtualBox, import the ova file by selecting "File / Import Appliance" and then the ova file. This step will establish a new virtual machine named "InterSecureModel," which will appear in the virtual machine list on the left side of the window, as shown in Figure 4.3.

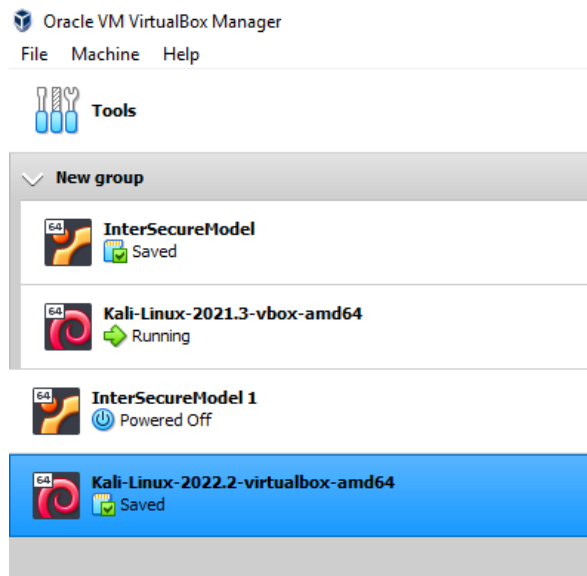


Figure 4.3: InterSecureModel

4.6 Sequence diagram

The Figure 4.4 below depicts how the framework will operate while it is in use, as well as how the framework's many components work together to finish the analytical and testing process. Although the framework has many other options to carry out analysis of the simulation model, but due to sufficient amount of time not all of those can be implemented. The diagram focuses mostly on the project framework's testing and analysis of the components to see its behavior. The returned results and outputs have been depicted in the diagram as a single arrow, but the outputs will also be provided separately for each tool.

The steps done in the sequence diagram are described below. In the sequence graphic, the numbers correspond to an arrow:

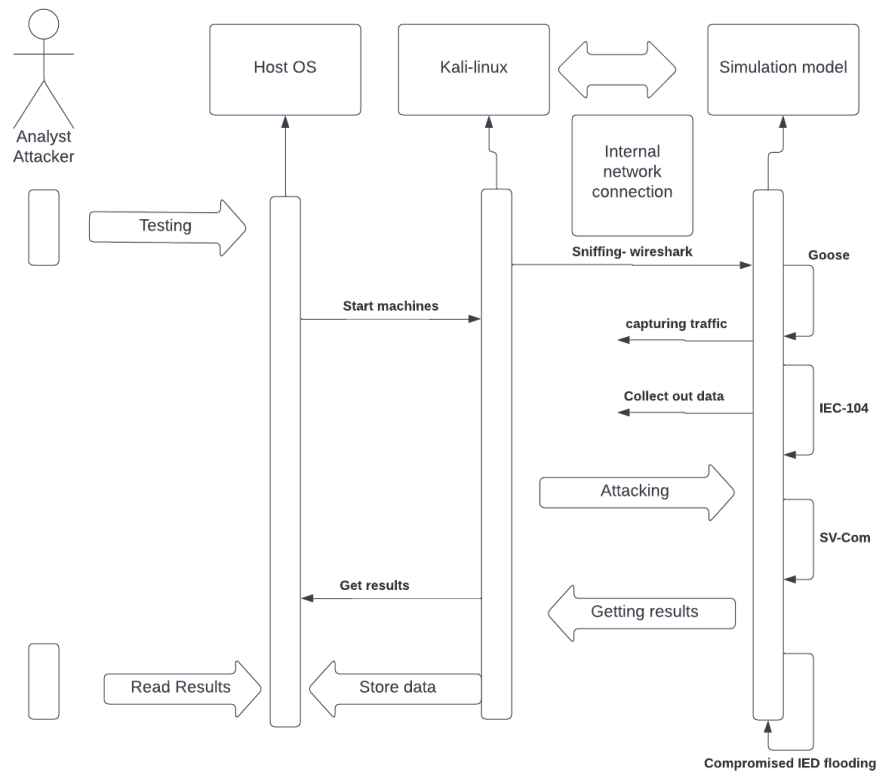


Figure 4.4: Sequence Diagram

Chapter 5

Implementation

This chapter explains how the architecture described in the previous chapter is implemented. Although the chapter focuses mostly on the practical aspects of solving the research topic, the approach technique employed during this thesis project will be briefly discussed. Furthermore, the implementation of the various tools and solutions will be demonstrated and discussed. Each tool is described in detail, along with an explanation for why it is useful in solving the situation at hand.

5.1 Methodology

5.1.1 Ethics

Anyone who unlawfully seeks access to a job meant for automated processing or wrongly edits, eradicates, blocks, or registers for such information is convicted of data breach and faces fines or a maximum sentence of two years in jail, according to Norwegian legislation ¹. As a result, all of the experiments and investigations provided in this thesis were conducted in an isolated home lab environment with no impact on the surrounding networks. All of the data used in this thesis was obtained from a private network for scholarly purposes and analyzed accordingly.

5.1.2 Work flow

The initial plan was to work at school like a normal working hours in any field of work on daily basis even though the author was the only person working on the thesis. It changed during the project as it was more comfortable and easy to work from home. Moreover, the list below shows the tools used to manage the project.

- **Communication:** The main source of communication between the student and supervisor was through emails and Microsoft teams if the meeting went digital due to some issues. Throughout the whole project the student was

¹<https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/norway>

regularly connected with the supervisor through e-mail and physical meetings on Wednesdays each week.

- **File sharing:** File sharing between the student and supervisor were mainly used through Microsoft-teams and E-mails. Moreover the backup was made by the student in OneDrive and Google Docs.
- **Text editor:** The report is written in Overleaf using \LaTeX editor.
- **Work board:** Kanban board used in this thesis represent system, visualize work, maximize efficiency, and improve continuously. It was easier to maintain track and stay motivated with a home-made Kanban board. All report-related tasks were included on the Kanban board. ASAP, To Do, In Progress, Review, and Done are the five sections of the Kanban board. This aided in the organization and prioritization of the appropriate tasks at the appropriate times. The board also served as a project's final checklist. The Kanban board is shown in Figure 5.1.

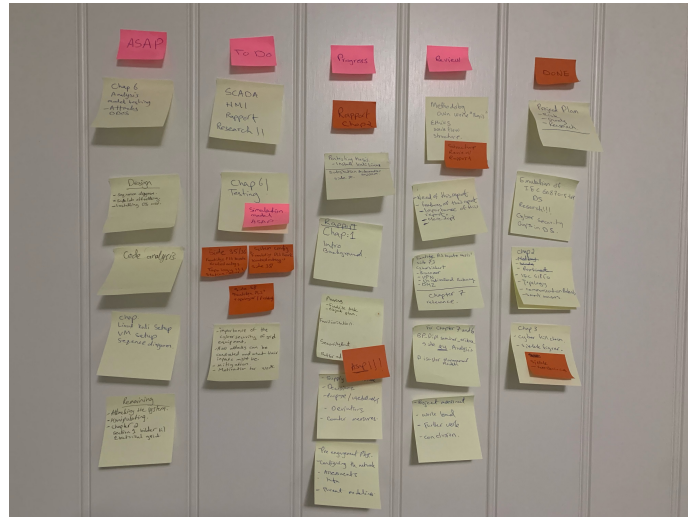


Figure 5.1: Home made Kanban board

5.2 Infrastructure configuration

Simulation can be implemented on any infrastructure that is of interest. This might be a physical system setup, VM virtualization that meets the requirements, or NTNU's Open Stack infrastructure SkyHigh, which has lots of resources available. Regardless of the underlying architecture, VM Virtual Box ² or VMware Workstation ³ are the main interest. VM virtual Box can be found as a free open source edition and is generally used as a hypervisor for the guest OS, so this was an ob-

²<https://www.virtualbox.org/>

³<https://www.vmware.com/no/products/workstation-pro.html>

vious choice for the thesis. The author of the thesis uses Windows 10 and Linux Ubuntu 20.04 LTS OS and configured it on both machines.

5.2.1 Initial configuration

The Initial configuration section covers how to install VirtualBox on an Ubuntu 20.04 LTS machine. The APT package repository is used to install the latest version of VirtualBox.

For Windows machine it can be downloaded on the virtualbox webpage ⁴. Further, follow the steps given to install the VM-box.

Installing Virtual-Box using Ubuntu's APT package repository. The advantage of choosing this approach to install Virtual-Box is that it is very simple and quick to do it. This method has the disadvantage of not updating when a new version is released.

Code listing 5.1: VM Virtual-box Installation on Linux From Terminal

```
sudo apt-get update
sudo apt install virtualbox
sudo apt install virtualbox-ext-pack -y
```

5.2.2 Deployment of instances

Simulation model is configured on an Linux Lite operating system, as mentioned in Chapter 4. In VirtualBox, import the ova file by selecting "File / Import Appliance" and then the ova file. This step will generate a new virtual machine named "InterSecureModel," which should appear in the left-hand window's virtual machine list 4.3. The same method is applied to kali-linux. The setup of the ova file to kali linux is similar as the simulation model.

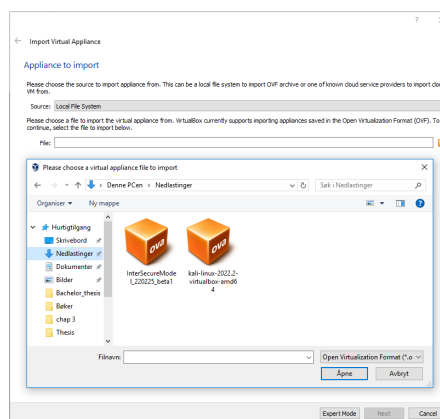


Figure 5.2: Deployment of instances

⁴<https://www.virtualbox.org/>

5.3 Starting VMs

5.3.1 Model

By double-clicking on the InterSecureModel virtual machine in the list, or by choosing it and pressing the green arrow button Start, the virtual computer with the model can be started. A virtual machine window should appear, booting the guest operating system and displaying a login screen. For login, use the following credentials:

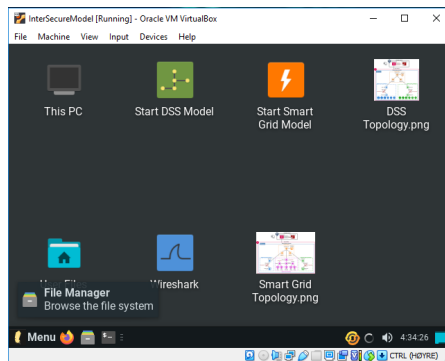
- Username: InterSecure
- Password: intsec

The virtual computer runs Linux Lite's default user interface, Xfce. This is a lightweight, basic, and easy-to-use interface that follows the Windows operating system's structure. Figure 5.3a depicts the primary screen.

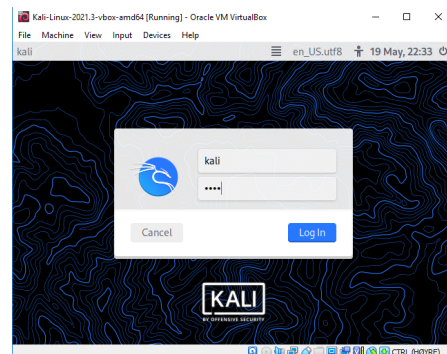
Kali

By double-clicking on the Kali virtual machine in the list, or by choosing it and pressing the green arrow button Start, the virtual computer with the model can be started. A virtual machine window should appear, booting the guest operating system and displaying a login screen Figure 5.3b. Interface of Kali-linux is quite easy as the simulation model. For login, the default credentials are set:

- Username: kali
- Password: kali



(a) User interface of Simulation model



(b) User interface of Kali linux

Chapter 6

Testing and analysis

This chapter provides an overview of the testing environment as well as the various outputs generated during the analysis process. Some components provide theoretical information about the attacking part. A sequence diagram of the framework gives an overview of the practical part.

6.1 Methodology of attacks

A Cyber attack, like any ambitious undertaking, requires meticulous planning and execution to succeed. Advanced threats nest inside organizations for an average of 200 days before being discovered, according to industry studies [75]. That's a lot of time for an attacker to gather sensitive information, monitor communications, and map the network without being detected. The stages required for successful attacks are outlined below, along with the attacks themselves.

6.1.1 Pre-engagement phase

Pre-engagement interactions, also known as scoping, are an often overlooked step in testing. During this phase, the thesis' scope is mostly focused on attacks on power networks. This is where you start preparing and connecting your goals with specific testing outcomes. The second part of this were attacking the network.

The scope and problem description were stated in Chapter 1.2, which was attacking the power network's substation.

Assumptions

- An assumption is made that the attacker, in this case the participant is already in the system and attacks and exploitation's are taken from there.
- The current state of simulation model for DS communication is limited. Only the study and the document [71], with limited knowledge, gives a relevant model of limited elements of the SCADA-RTU communication. The authors utilized Mininet to simulate a network and the 61850 library to generate chosen IEC-104 messages.

6.1.2 Information gathering

The next phase is information collecting also known as reconnaissance for the system under attack. It's important to have as much information about the system as possible because more information leads to more weakness or exploits and this makes attacking and performing operations easier. The main objective is to learn as much about the system or information gained at early stages. Tester acquires information and analyzes openly available sources of data during this step. The first level for collecting information is footprinting. This is the method or technique by which basic information about our simulation model is revealed and collected in order to record its benefits and shortcomings. Footprinting [9] through the collection of data from public or open sources is considered passive, for example, a google search, browsing a company's website, indistinguishing public traffic from ordinary corporate filings, etc., whereas data collection from private or closed sources is considered active, for example, interviews, social engineering, vulnerability scans, ping sweeps, network scans, and so on. This is the method or technique by which basic information about our simulation model is revealed and collected in order to record its benefits and shortcomings. Footprinting through public or open source data collection is considered passive, for example, a google search, browsing a company webpage, distinguishing public traffic from ordinary corporate filing, etc., whereas data collection from private or closed sources is considered active, for example, interviews, social engineering, ping sweep, network scan, and so on [9]. These techniques can be used, for example, to identify network boundaries, network maintainers, and even the operating system and web server software used on the target network.

Passive footprinting

To demonstrate an example of Passive footprinting which is relevant to the thesis like the SCADA section, shodan¹ engine is used to show how many systems are connected online and their protocols. Figure 6.1 and Figure 6.2 below shows SCADA system and their protocols within which country. Moreover communication protocol like modbus with port number 502 can easily seen as a passive reconnaissance approach.

¹<https://www.shodan.io/>

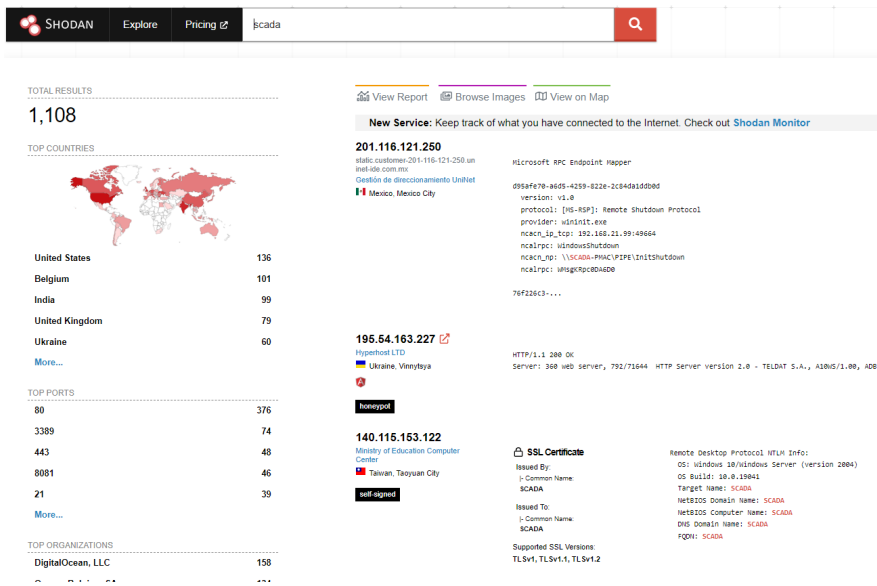


Figure 6.1: Shodan Search-engine



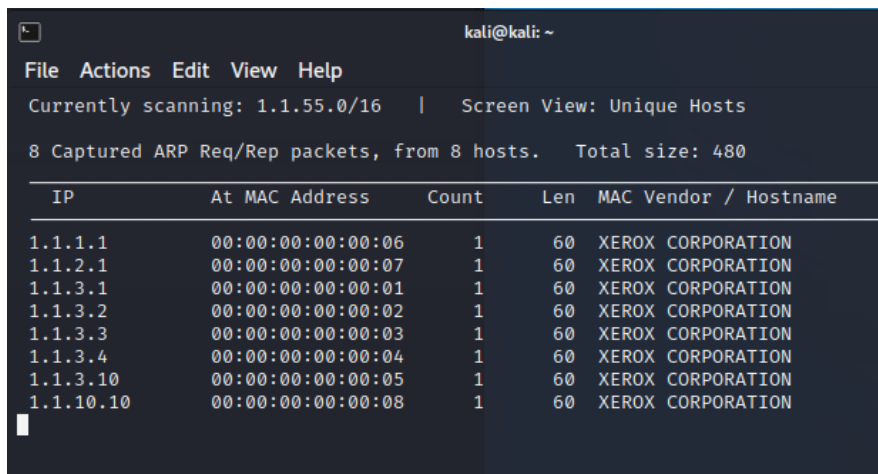
Figure 6.2: Shodan Search-modbus

Active footprinting

Kali-Linux has a lot of tools for attempting active footprinting. Some of those are listed below:

1. Nikto gives full support for SSL, looks for subdomains, supports full HTTP Proxy, outdated component report, Username Guessing
2. Burp Suite highly focused on web application.
3. Nmap is a network discovery tool that finds hosts, ports, and services, as well as their versions.

During the active footprinting on the simulation model all the devices showed up which are relevant to the DS Figure 6.3. It was possible to extract data as it would be useful for an attacker. However, the same IP address was utilized during the passive footprinting to observe the results to illustrate information gathering for SCADA systems Figure 6.4.



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
1.1.1.1	00:00:00:00:00:06	1	60	XEROX CORPORATION
1.1.2.1	00:00:00:00:00:07	1	60	XEROX CORPORATION
1.1.3.1	00:00:00:00:00:01	1	60	XEROX CORPORATION
1.1.3.2	00:00:00:00:00:02	1	60	XEROX CORPORATION
1.1.3.3	00:00:00:00:00:03	1	60	XEROX CORPORATION
1.1.3.4	00:00:00:00:00:04	1	60	XEROX CORPORATION
1.1.3.10	00:00:00:00:00:05	1	60	XEROX CORPORATION
1.1.10.10	00:00:00:00:00:08	1	60	XEROX CORPORATION

Figure 6.3: netdiscover scan on the simulation model

The information gleaned from the simulation model laid the groundwork for gathering and finding more information. IP addresses gave an indication of IP range and use in the system Figure 6.3. A database in the simulation model would have helped in advanced scans to find more data and weak points.

Code listing 6.1: Active Scan methods

```
// scanning the network of the simulation model
sudo netdiscover -i eth0 -r 1.1.10.10/16
```

```
(kali@kali)-[~]
└─$ sudo nmap -sS -Pn 195.54.163.227
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-19 11:05 EDT
Nmap scan report for vds49883ua.hyperhost.name (195.54.163.227)
Host is up (0.13s latency).
Not shown: 984 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https
5120/tcp   open  barracuda-bbs
7001/tcp   open  afs3-callback
8080/tcp   open  http-proxy
8081/tcp   open  blackice-icecap
8181/tcp   open  intermapper
8443/tcp   open  https-alt
8888/tcp   open  sun-answerbook
9000/tcp   open  cslistener
10000/tcp  open  snet-sensor-mgmt
50000/tcp  open  ibm-db2
52869/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 19.19 seconds
```

Figure 6.4: nmap scan of a SCADA system online

6.1.3 Threat modeling and vulnerability identification

Threat modeling identifies any existing vulnerabilities on a target system using the information gathered during the intelligence collection process. When undertaking threat modeling, the attacker will figure out the most effective attack strategy, the type of information they need, and how the target could be attacked.

Threat modeling for the simulation model provided insight into how infrastructure is constructed. Furthermore, the attacker, in this case the author, recognized the model and the data he acquired as being nearly identical. This will be discussed in the following section.

Sniffing traffic with wireshark

Wireshark² is a graphical network protocol analyzer that allows us to look at individual packets as they travel across the network. Wireshark can capture Ethernet, WiFi, Bluetooth, and a variety of additional protocols. It can decode several protocols it encounters. The simulation model revealed data that was not supposed to be seen by the attacker during the collecting of traffic and packets using wireshark Figure 6.5. Following the packets with TCP follow, it shows information which cannot be seen clearly.

For additional analysis and ease, this data was stored as a pcap file format. The author uploaded the pcap file to the internet for analysis, of the methods to get information at apackets³. It revealed a lot of information about the simulation model's relationships with communications between other components within the model.

²<https://www.wireshark.org/>

³<https://apackets.com/>

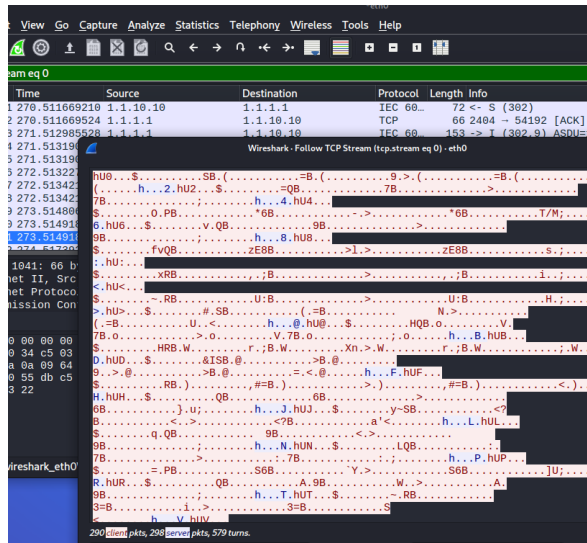


Figure 6.5: Pcap Investigation from attackers PC

Finding vulnerabilities

Testing and analysis begins actively uncovering different vulnerabilities throughout the vulnerability analysis phase. The amount of data gathered from this level provides the attacker, in this case the author, with a better understanding of the model. Here, the infrastructure, traffic, and IP addresses used during communication were revealed Figure 6.6 below shows the connections between the components.

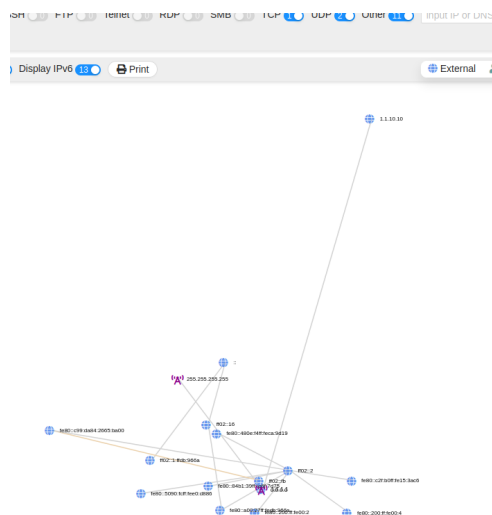


Figure 6.6: Infrastructure of the model through attackers eyes

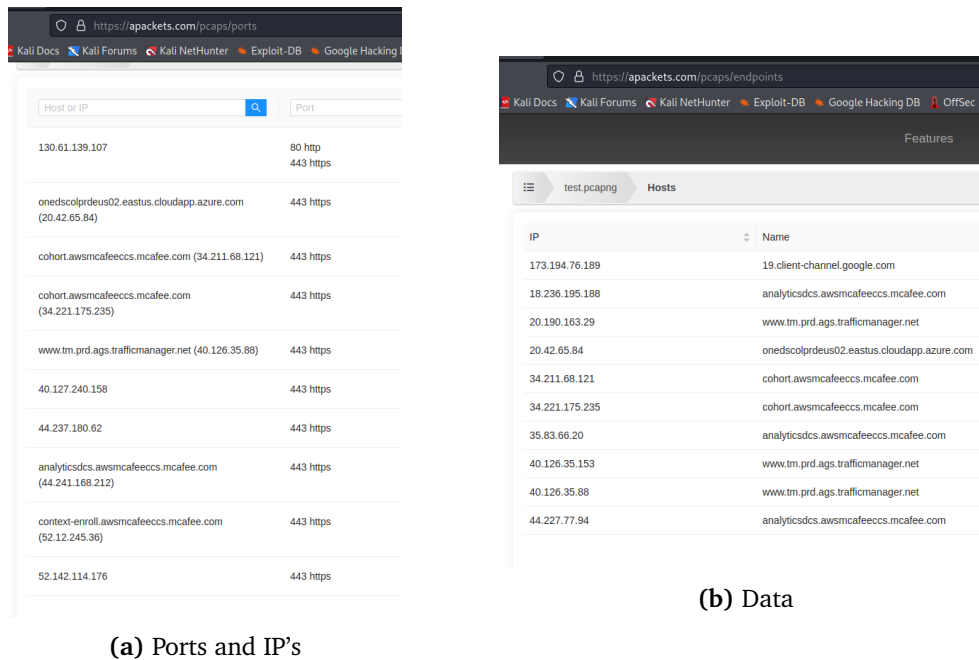


Figure 6.7: Third party Data

The inquiry also reveals further data concerning the collaboration with third-party companies, such as which ports were open during communication and other specifics Figure 6.7a and Figure 6.7b above gives the data related to the attacker.

When vulnerabilities are discovered, the tester can assess the success of various exploitation tactics. Vulnerability scanners employ vulnerability databases and a series of active tests to find vulnerabilities in client systems. If this stage fails, the danger of erroneous exploits being injected increases, and when exploits fail, they can crash services and trigger intrusion-detection alarms. Critical thinking is another crucial tool for a tester to have to perform a successful attack. One of the reasons why many organizations in other nations are hacked but no damage is done is because the attackers maybe use them for their testing area before hitting the real target.

6.2 Exploitation

Exploitation is undoubtedly one of the more attractive aspects of testing, yet it is sometimes carried out blinded rather than accuracy, but it still might be dangerous.

Although the simulation model lacked sufficient data and protection to undertake various types of attacks, certain attacks were viable and some were effective. ARP poisoning, GOOSE and SV data manipulation, and flaws in the model are examples of attacks that could be achievable with enough data. The poisoning

attack and data manipulation were not possible owing to time limits.

The concept for carrying out those attacks came from research and skill the author had which he performed on his local network, but it is theoretically possible to demonstrate the relevance for this thesis.

From attackers pc, DDoS attacks were launched which crashed the simulation model. This shows the attacking methods possible even though the traffic is hidden and not shown to the attackers computer.

```

└─$ sudo hping3 -S -p 80 --flood 1.1.10.10
[sudo] password for kali:
Warning: Unable to guess the output interface
HPING 1.1.10.10 (lo 1.1.10.10): S set, 40 headers + 0 data bytes
[send_ip] sendto: Network is unreachable

```

Figure 6.8: DDoS Attack

6.2.1 Man-In-The-Middle

To apply ettercap attack which is a tool, it can be used to perform the attack as ARP poisoning. The attacker has the information which was retrieved during the information gathering phase.

Code listing 6.2: MITM attack using ettercap

```

//scanning the network of the simulation model,
sudo nmap -sn 1.1.1.1/16
//this shows the mac address and ip addresses of the network
//-T text only -S no use SSL -i interface -M man in the middle attack
sudo ettercap -T -S -i eth0 -M arp:remote /{ip-gateway router} // /targeted ip//

```

Due to constraints and a lack of data, it was not possible to carry out more attacks because many locations lacked data to manipulate.

6.2.2 Post exploitation

After a system has been attacked, the post-exploitation phase begins. In this section, post-exploitation is essential. This is where you'll get thorough information, vital statistics, and testing insight. Post-exploitation focuses on specialized systems, essential infrastructure, and the company's most valuable information or data. The presentation of attacks would have the most impact during the exploitation of one system after another.

The simulation model has some other options to take control over IEDs and misuse the components. A DDoS Attack was launched from the IEDs to show control and misuse of the system ???. An attacker can inject malicious script to control the IEDs or perform more actions to other system.

6.3 Analyzing IEC-104 traffic

The wireshark intercepted the IEC-104 message, SV and GOOSE messages while sniffing the traffic. It demonstrated that it might be useful to the attacker. The attacker then can use other tools to copy, manipulate and resend these messages and the possibility of injecting malicious script to gain its cause. Traffic captured by using wireshark Figure 6.9 below gives the idea to the attacker hva to do next when some data is available.

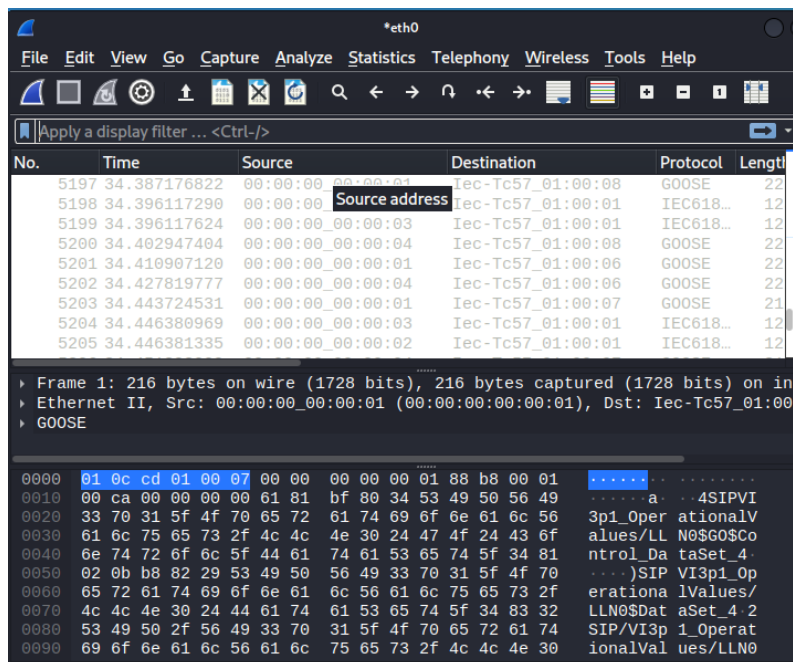


Figure 6.9: Goose and SV messages

It has the possibilities to modify these messages by understanding the system. With enough knowledge, the source code may be rewritten with a malicious script. The document [72], shows the steps of how to change and manipulate these messages.

Chapter 7

Discussion and further work

This chapter expands on the observations and outcomes from Chapter 6: Analysis and Testing. Additional work and suggested measures will be discussed, as well as suggested additions, tweaks, and adjustments that could help with the implementation.

7.1 Decisions

As with any project, decisions and conversations about the best solutions to handle challenges will be made. In this case, they were frequently related to defining criteria, selecting technology, and deciding on an architectural design.

7.1.1 Limitations and constraints

The testing simulation design is relatively limited. The model illustrates that SCADA and RTU have restricted communication. The work on the ECODIS and Intersecure project is being expanded to include the complete substation communication. Further study is needed to confirm the value and utility of emulation models in performing further testing and manipulation.

7.2 Measures for strengthening Cyber security in power networks

The owner of a property bears responsibility for information security under §-7 of the Norwegian Law on Information Security in IT Systems. According to §-7 of the Norwegian Law on the Basic Principles of Security, the owner of essential infrastructure is responsible for the security of IT systems. It is critical to recognize that in several energy sectors in Norway, the appropriate regulatory framework for cyber security is not fully implemented, and there are exceptions to reduce the deviations. These deviations are classified and can not be presented in the thesis.

In the event of a crisis scenario, the subsections will advise on measures to prevent or mitigate attacks.

There are a variety of safe systems for Cyber attacks solutions available, which may be integrated and applied to various situations. In this section, the focus will be on a variety of cyber security solutions, how they function, and how they can be coupled to safeguard the control system while keeping §-7 in mind. Counter measures taken by the ICS are the following.

7.2.1 Communication with third parties

The fact that the world is becoming increasingly digital, including power plant control systems, makes the usage of data from these systems more appealing. It is critical to acquire data and information from the power plant in order to optimize operation, maintenance, and diagnostics. There are a number of security concerns that must be overcome in order to make this information available. This is because a third party connected to the power plant's OT and IT network can be extremely dangerous, since it can be a weak link and thus a back door into the network. This section focuses on safeguarding third-party communication and remote control in the most efficient and secure manner possible.

Firewalls:blacklisting/whitelisting

A firewall is a device that controls network access and protects connected computers from illegal access. The firewall enacts an access policy by employing techniques that either block or allow (blacklisting / whitelisting) specific types of traffic, so controlling the flow of data. When employing whitelisting, all traffic is banned except for approved protocols such as IEC 61850, IEC 104, and others. On the other hand, blacklisting just prohibits communication from specific protocols. The firewall normally allows users inside a protected region to communicate with external services by blocking traffic from outside the protected area to inside the protected area. A firewall's primary functions are to restrict data flow to and from the OT network, log successful and unsuccessful transactions over the firewall, and interface with networks that aren't designed to do so [76]. Figure 7.1 shows use of firewall.

In an Industrial control systems, a firewall is not the answer to all burglary concerns. A firewall's flaw is that it isn't designed for all applications in a control system, making it impossible to adapt the filtering for maximum safety. Firewalls have also evolved significantly, and their design may necessitate specialized knowledge. When using a firewall with a control system, start by configuring the firewall to prohibit all traffic, then look at the traffic that is required and only allow it explicitly. Firewall settings must be kept secret as it can be manipulated. ICS keep their firewalls confidential to prevent manipulation and attacks.

Virtual Private Network (VPN)

A Virtual Private Network is a computer network that sends data across point-to-point connections in the form of a tunnel and encrypts it. This method protects data from the public internet and provides adequate security for standard Man-In-The-Middle. VPNs are commonly used to protect remote access to control systems and data transfer from the OT to the IT networks. Authentication and authorization, Integrity, and Confidentiality are the three security components of a VPN [77]. These components establish the authenticity of a transfer in order to validate the person's authorization, protect information from illegal alteration, and ensure that information is not shared with unapproved people or entities. Figure 7.1 illustrate use of VPN.

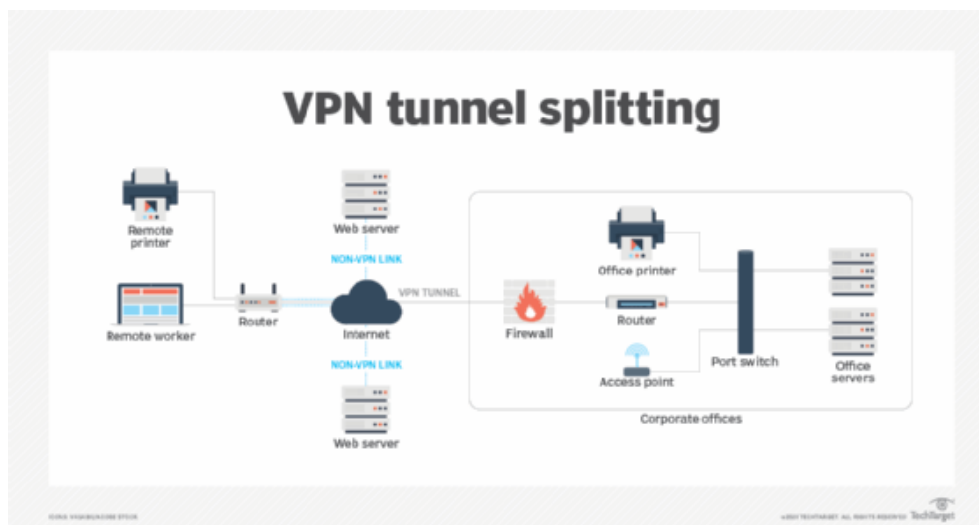


Figure 7.1: VPN [77]

VPN has a variety of flaws and is vulnerable to Cyber attacks because it is a software-based solution. A third party connected for external access can be extremely dangerous in terms of Cyber assaults, as a hacker can gain access through the third party. Once a hacker has gained access, a VPN will not prevent them from accessing additional VPN-connected systems. It can encrypt an attack just like any other piece of data. As a result, VPN can be used by a third party as a backdoor into the OT and IT network. It is still recommended due to it has some security which is better than nothing.

Unidirectional Gateway (UGW)

Unidirectional security gateways allow for secure IT/OT integration, remote access, and real-time monitoring of industrial networks. In an industrial network context, the gateways replace one layer of firewalls, giving industrial control systems complete security from targeted attacks, secure enterprise-wide visibility,

and secure remote access [78]. Figure 7.3 shows an example use of UGW.

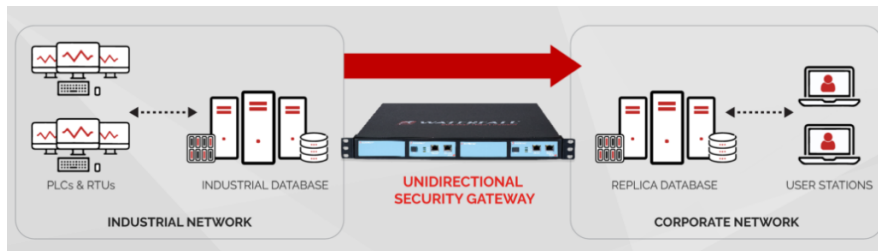


Figure 7.2: Secure Bypass with UGW [78].

Demilitarized Zone (DMZ)

A DMZ, also known as a perimeter network or a protected subnet, is a secure area. It is primarily a network between networks, particularly in the case of OT, ICS, or SCADA, a network layer between them and the less secure IT network [79]. Modern industrial DMZs serve as a zone and line system that secures physical operations while also separating networks based on their various goals, requirements, and hazards. Two firewalls, one between the OT network and the DMZ network, and one between the IT network and the DMZ network, are one approach to create a DMZ. In the event of a hypothetical software fault in the firewall, this design decreases the likelihood of an attack path being opened directly into the control system network. From an attacker's standpoint, stealing a firewall password or a password on the IT network that is trusted for the OT network can be simple, and an attacker can quickly gain access to the DMZ systems. Two firewalls are useless in this situation. An Unidirectional Gateway (UGW), which replicates the OT system to the IT network, is a more current technique to safeguard one side of the IT/OT DMZ. An OT database is replicated and transferred across a unidirectional network to a replica server in the DMZ, which is accessed by the IT network via a firewall. Because two firewalls are insufficient for safeguarding intrusions into the OT network, this will be a considerably more secure option.

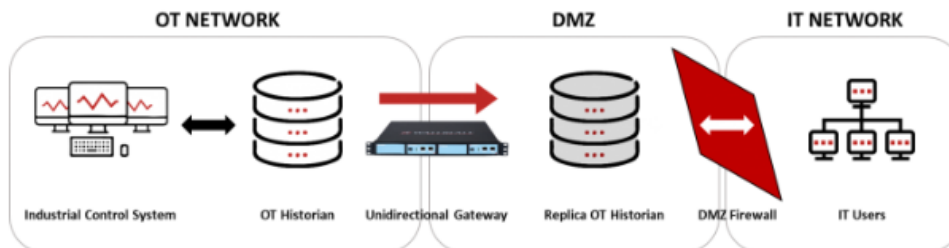


Figure 7.3: Example diagram on DMZ with a UGW [79].

7.2.2 SDN

A SDN is a network administration solution that allows for dynamic and efficient network design. To offer uninterrupted protection, an IEC 61850-based system requires a strong network. SDN is a network architecture that overcomes some of the restrictions of standard Ethernet networks. When compared to a traditional Ethernet switch, the device can repair itself in a matter of milliseconds, handle large amounts of data traffic, and improve cyber security [80]. SDN also improves security by employing a deny-by-default design, in which messages are only routed if they follow a set of tight restrictions. This adds an extra layer of security to the network drive, preventing malicious malware or other unauthorized activity from entering. SDN stops a cyber attack from spreading to other devices linked to the same network.

The diagram below shows an example of a safe security infrastructure for network connections and zones in a ICS sector.

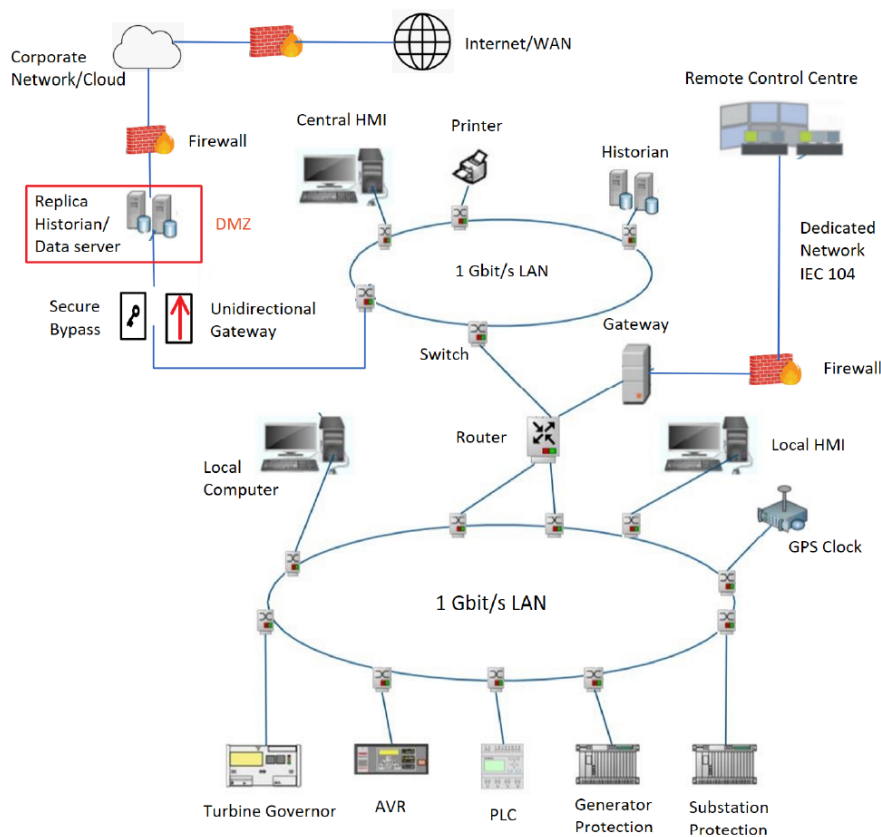


Figure 7.4: Security structure for zones and interconnections

7.3 Supply chain attack

Even if we are securing infrastructure, a key issue is that the components used to construct it can pose a vulnerability, which is known as a supply chain threat. A supply chain threat is a type of cyber-attack that aims to harm an organization by targeting the supply chain's less-secure sections [81]. A supply chain attack can happen in any industry, including the banking, oil, power and government sectors. Software or hardware can be the target of a supply chain attack. By inserting Malware or hardware-based surveillance components, cybercriminals often assault with the manufacturing or distribution of a product [82].

7.3.1 Software supply chain attack

In software supply chain threat, attackers want access to source codes, build processes, and update methods from software developers and suppliers. The attacker wants to infect a legal program and use it to spread malware. Unsecure network protocols, insecure server infrastructures, and risky coding methods are all targets for attackers. They break in, alter source codes, and insert malware. These apps and updates are signed and certified because they are produced and published by reputable vendors [82]. Vendors are likely unaware that their apps or updates are infected with malicious code. The malicious code then runs alongside the program with the same permissions.

Consider what would happen if a free file compression program was tainted and then distributed to users in a country where it was the most popular utility tool. That happened in a previous incident [83]. A popular PDF editor app was targeted by the attackers. They discovered that the vendor is using the server of one of its associate vendors. Attackers created a copy of this server, then updated a single component of the installation package, a fonts pack, to introduce coin miner malware [84]. They got the vendor's website to connect to their server by tricking it. As a result, the app was secretly installed with the poisoned fonts pack file containing malicious coin mining malware. Attacks on the software supply chain have a multiplying impact and software supply chains are quickly becoming a popular method of spreading malware.

Precautions to prevent Software supply chain attack. Implement strict code integrity controls to ensure that only authorized programs are allowed to operate. Using endpoint detection and solutions that can detect and remediate suspicious activity that could indicate a software supply chain assault automatically. A security features in Windows Defender ATP are incorporated into Windows 10 and constitute a unified endpoint security platform to fight against supply chain assaults.

7.3.2 Hardware supply chain attacks

Amazon.com Inc. has been quietly exploring buying Elemental Technologies to help with a major expansion of its streaming video service, now known as Amazon

Prime Video. Elemental's crew packed multiple servers and shipped them to Ontario, Canada, in late spring 2015 for testing by a third-party security firm, according to the individual. The testers discovered a little microprocessor the size of a grain of rice nestled on the servers' motherboards that wasn't intended to be there. When Amazon informed US officials about the discovery, it shook the intelligence community. Investigators discovered that the chips allowed the attackers to build a stealth entryway into any network that featured the altered devices during the subsequent top-secret investigation, which is still ongoing more than three years later. Investigators discovered the chips in factories run by manufacturing subcontractors in China, according to multiple sources familiar with the situation [85].

There are no effective techniques to resist hardware supply chain attacks because the components, systems, distributors, logistics, retailers, and customers are all interrelated, and the region becomes too large to regulate. Still some measures can be done to secure the Digital Substation by following objectives, methods, techniques, and procedures can be used to secure the value chain supply:

1. In the digital value chain, identify security holes, vulnerabilities, and attack vectors
2. Determine which power system components are the most vulnerable and crucial to its operation.
3. Identify relevant hardware reverse engineering tools, methodologies, and methods.
4. Develop organizational policies and procedures to enable the use of technical solutions in the power infrastructure sector.
5. Using components from Elvia's digital substation project, demonstrate and validate the built framework.

7.4 Further work

Cybercrime is strongly increasing, and there are different companies that profit from the distribution of Ransomware. Customers in crisis infrastructure are more vulnerable because their willingness to pay and opportunity are both low. More work should be done to map the security around the rising data flow that is required. As stated in the report, the report serves as a foundation for ongoing research into Cyber security, data processing, and the development of instruments required to regulate for future market requirements and the additional pressure this will impose. Data should be gathered and evaluated in order to create an algorithm that can recognize and predict maintenance requirements. Prioritize a project that focuses on the development and optimization of such an Artificial Intelligence (AI). Smart instrumentation should be implemented to decrease future maintenance costs and ensure the system's Integrity. Work on mapping appropriate media to watch and coordination amongst them could be interesting to look into.

Chapter 8

Conclusion

The reader will get an overview of the thesis project in the following chapter. In addition, the chapter briefly covers accomplishments, how they were achieved, challenges faced during the thesis, further work, closing statement and the overall learning outcome.

8.1 Project assessment

The project assignment began as an open project description with the option of making changes before being finalized. Sule Yildirim, the Taskgiver at , wants to look into the security of Digital Substations by detecting threats, attacks, and analyzing them. Because there was no access to actual substation, the work was done on a simulation model that acted as a control center, a station with substations. Sule wants a document about electricity networks to emphasize the importance and necessity of Cyber security. The requirements for which outputs were relevant were well-defined. Apart from that, the work was difficult due to the information provided for solving the challenge was not enough.

The thesis project began with a thorough examination of the electricity grid. Various relevant articles, Youtube videos, and books were used to gather information and do research. Although thorough understanding of the entire system was outside the scope of the thesis, it may be confusing and challenging for the audience with limited knowledge and background. With that in mind, it will be easier and more pleasant to comprehend the thesis and approach to developing a solution.

The field of requirement specification was large, and it was carried out. It was originally decided to focus on Digital Secondary Substation (DSS), however this was later modified due to the thesis' restrictions and scope, which was more focused on DS. To construct a sandbox and carry out the attacks, the Simulation model was combined with Kali-linux. As a result, the search for current technologies to attack the targeted system began. Several alternative frameworks were available online, but accessing them was challenging due to security and confidentiality concerns.

8.1.1 Work load

Every week, Mohammad worked from Monday to Friday on research and writing. It was difficult to stick to the work schedule and project plan established early on. Because this thesis was handled by one individual, there was no need to register for time. The participant was very motivated and focused on finishing the work throughout the entire thesis process. The assignment itself was intriguing and challenging in terms of what students had learned throughout studies. That is why It was chosen in the priority list from among several other bachelor project task proposals.

8.1.2 Learning outcome and evaluation

In retrospect, some things were kept in mind as to what may have been done better. For example, limiting the scope and scheduling more meetings with the Taskgiver. Working in a group was something that was lacking, and the experience may have aided the project's and students' learning results. It could help with solo challenges and writing the project report. The decision to form a group with classmates to work on bachelor thesis could have been made sooner, but it resulted in solo work and the learning outcomes were much higher. Despite these facts, the Kanban technique performed admirably for a project involving a large amount of individual work.

8.1.3 Deviations

One of the main worries, as noted in the risk assessment section of our preliminary report, was that it might be delayed due to poor planning and incidents faced. The author got infected with Covid-19 virus which kept him away from work over a week. During the month of March, another incident occurred was PC problems. PC used for writing the report and practical experiments had problems with the mother-board which lead to some data loss and total unusable for the thesis. Despite these challenges, the student completed the assignment on time. However, there have been times when it was unclear how much theory should be incorporated. Prioritizing the tasks was difficult, but with the help of the Kanban technique, it became clearer what needed to be done in the short, medium, and long term. The most recent issue occurred when the overleaf program crashed and was unable to generate a PDF file. This added to the author's workload by requiring him to transfer all of the data to a new template.

8.2 Conclusion of the work

The technical implementation began once the systems infrastructure was in place, but the theoretical portion had already been completed during the research phase. As stated in Chapter 6, the project goals listed in Chapter 1.6 were attained and fulfilled. The challenge has allowed to go further into and use technologies and processes that are already familiar with, as well as discover new technologies and combine them with what currently is known.

This project can finally be regarded completed after 5 months of work. The work provided an excellent learning opportunity and put skills and knowledge learned over the previous three years to the test. Even though there were things that could have been done better if there had been more time, the participant is content with the findings of both the testing and the report. Finally, I hope, that findings of this thesis will contribute to vital power networks research in the area of security that is still relatively new and members of our target groups will find the report useful.

Bibliography

- [1] 'Statnett.' Retrived, Feb-2022. (), [Online]. Available: <https://www.statnett.no/en/>.
- [2] 'Cia traid.' Retrieved Feb, 2022. (), [Online]. Available: <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>.
- [3] Visited april 2022. (), [Online]. Available: <https://www.kaspersky.com/resource-center/threats/blackenergy>.
- [4] 'Ddos.' Retrived Mai, 2022. (), [Online]. Available: <https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html?dtid=osscdc000283>.
- [5] 'Kanban.' Retrived, Mai-2022. (), [Online]. Available: <https://kanbanize.com/kanban-resources/getting-started/what-is-kanban>.
- [6] 'Malware.' Retrived Mai, 2022. (), [Online]. Available: <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>.
- [7] 'Mitm.' Retrived, Mai-2022. (), [Online]. Available: <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>.
- [8] 'Mininet.' Retrieved April, 2022. (), [Online]. Available: <https://www.techtarget.com/searchnetworking/definition/Mininet>.
- [9] 'Footprinting.' Retrived, Mai-2022. (), [Online]. Available: <https://www.techtarget.com/searchsecurity/definition/footprinting#:~:text=Footprinting%20is%20an%20ethical%20hacking,best%20methods%20of%20finding%20vulnerabilities..>
- [10] 'Phishing.' Retrieved April, 2022. (), [Online]. Available: <https://www.avast.com/c-phishing>.
- [11] 'Ransomware.' Retrived Mai, 2022. (), [Online]. Available: <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/>.
- [12] 'Social engineering.' Retrieved April, 2022. (), [Online]. Available: <https://www.avast.com/c-social-engineering>.
- [13] Visited april 2022. (Jul. 2020), [Online]. Available: <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>.

- [14] '0-day exploit.' Retrived Mai, 2022. (), [Online]. Available: <https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html>.
- [15] A. Khodabakhsh, S. Yildirim Yayilgan, M. Abomhara, M. Istad and N. Hurzuk, 'Cyber-risk identification for a digital substation,' Aug. 2020. DOI: 10.1145/3407023.3409227.
- [16] A. Khodabakhsh, S. Y. Yayilgan, S. H. Houmb, N. Hurzuk, J. Foros and M. Istad, 'Cyber-security gaps in a digital substation: From sensors to scada,' in *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, 2020, pp. 1–4. DOI: 10.1109/MECO49872.2020.9134350.
- [17] C.-C. Sun, A. Hahn and C.-C. Liu, 'Cyber security of a power grid: State-of-the-art,' *International Journal of Electrical Power & Energy Systems*, 2018.
- [18] 'Qualitative model.' Retrieved Feb, 2022. (), [Online]. Available: <https://www.sciencedirect.com/topics/computer-science/qualitative-model>.
- [19] N. Machiavelli, 'Art of war,' in *Art of War*, University of Chicago Press, 2009.
- [20] S. M. Kaplan, 'Electric power transmission: Background and policy issues,' Library of Congress, Congressional Research Service, 2009.
- [21] B. M. Buchholz and Z. A. Styczynski, 'Modern technologies and the smart grid challenges in transmission networks,' in *Smart Grids*, Springer, 2020, pp. 61–120.
- [22] 'Substations.' Retrived Feb, 2022. (), [Online]. Available: <https://www.enmax.com/generation-wires/transmission-and-distribution/our-system/>.
- [23] M. Golshani, G. A. Taylor and I. Pisica, 'Simulation of power system substation communications architecture based on iec 61850 standard,' in *2014 49th International Universities Power Engineering Conference (UPEC)*, IEEE, 2014, pp. 1–6.
- [24] H. Lei, C. Singh and A. Sprintson, 'Reliability modeling and analysis of iec 61850 based substation protection systems,' *IEEE Transactions on Smart Grid*, vol. 5, no. 5, pp. 2194–2202, 2014.
- [25] S. Kunsman, S. Meier and R. Hedding, 'Protection and control system impacts from the digital world,' in *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, IEEE, 2016, pp. 1–13.
- [26] R. Gore, H. Satheesh, M. Varier and S. Valsan, 'Analysis of an iec 61850 based electric substation communication architecture,' in *2016 7th International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, 2016, pp. 388–393. DOI: 10.1109/ISMS.2016.85.
- [27] L. I. U. Raanaa, 'Condition monitoring of power transformers in digital substations,' M.S. thesis, NTNU, 2020.

- [28] 'Control-system topology.' Retrieved Mai, 2022. (), [Online]. Available: https://www.researchgate.net/publication/329370218_Towards_Industrial_Intrusion_Prevention_Systems_A_Concept_and_Implementation_for_Reactive_Protection/figures?lo=1.
- [29] 'Control-system topology.' Retrieved Mai, 2022. (), [Online]. Available: https://library.e.abb.com/public/18f20edbb8069e5c1257b4a004a943c/Industrial%20Smart%20Grid_EN.pdf.
- [30] 'Modbus.' Retrieved, Mai-2022. (), [Online]. Available: <https://modbus.org/faq.php>.
- [31] 'Profibus.' Retrieved, Mai-2022. (), [Online]. Available: <https://www.profibus.com/technology/profibus/overview>.
- [32] 'Profinet.' Retrieved Feb,2022. (), [Online]. Available: <https://us.profinet.com/profinet-explained/#:~:text=>.
- [33] 'Modbus.' Retrieved Feb,2022. (), [Online]. Available: https://www.csimn.com/CSI_pages/Modbus101.html?.
- [34] 'Modbus protocol.' Retrieved Feb,2022. (), [Online]. Available: <https://www.rtautomation.com/technologies/modbus-rtu/>.
- [35] 'Plc.' Retrieved, Mai-2022. (), [Online]. Available: <https://circuitdigest.com/article/microcontroller-vs-plc-detailed-comparison-and-difference-between-plc-and-microcontroller>.
- [36] 'Scada.' Retrieved April, 2022. (), [Online]. Available: <https://inductiveautomation.com/resources/article/what-is-scada#:~:text=SCADA%20Explained,and%20process%20real%2Dtime%20data>.
- [37] 'Scada.' Retrieved April, 2022. (), [Online]. Available: <https://no.answersexpress.com/an-introduction-scada-systems-99185>.
- [38] 'Scada.' Retrieved, Mai-2022. (), [Online]. Available: <https://www.dpstele.com/scada/how-systems-work.php>.
- [39] 'Standards.' Retrieved March,2022. (), [Online]. Available: <https://www.irena.org/inspire/Standards/What-are-Standards>.
- [40] H. León, C. Montez, O. Valle and F. Vasques, 'Real-time analysis of time-critical messages in iec 61850 electrical substation communication systems,'
- [41] 'Iec 61850.' Retrieved Feb,2022. (), [Online]. Available: https://www.gegridolutions.com/multilin/iec_innovations.htm.
- [42] 'Functional testing of iec 61850 based substation automation systems.' Retrieved March,2022. (), [Online]. Available: <https://electrical-engineering-portal.com/functional-testing-iec-61850-based-substation-automation-systems>.

- [43] H. León, C. Montez, O. Valle and F. Vasques, 'Real-time analysis of time-critical messages in iec 61850 electrical substation communication systems,'
- [44] 'Iec 61850.' Retrived, Mai-2022. (), [Online]. Available: <https://www.youtube.com/watch?v=ahd0V8qwbPY>.
- [45] 'Gsse.' Retrived, Mai-2022. (), [Online]. Available: <http://sclmanager.blogspot.com/2012/09/generic-substation-state-events-gsse.html>.
- [46] 'Iec-104.' Retrived, Mai-2022. (), [Online]. Available: <https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard/>.
- [47] Visited February 2022. (), [Online]. Available: <https://www.gegridsolutions.com/>.
- [48] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, 'A review of cyber security risk assessment methods for scada systems,' *Computers Security*, vol. 56, pp. 1–27, 2016, ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2015.09.009>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404815001388>.
- [49] E. Csanyi. 'Four design criteria for human machine interface (hmi) in a substation.' (2017), [Online]. Available: <https://electrical-engineering-portal.com/design-human-machine-interface-hmi-substation>.
- [50] E. Csanyi. 'Ied (intelligent electronic device) advanced functions that make our life better.' (2019), [Online]. Available: <https://electrical-engineering-portal.com/>.
- [51] GE. 'Ge grid solutions.' (2020), [Online]. Available: <https://www.gegridsolutions.com/>.
- [52] 'Guidelines and rules.' Retrieved Mai, 2022. (), [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157#KAPITTEL_7.
- [53] 'Offensive cyber operations and the use of force.' Retrieved Feb, 2022. (), [Online]. Available: https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
- [54] K. E. Hemsley, E. Fisher *et al.*, 'History of industrial control system cyber incidents,' Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2018.
- [55] Visited February 2022. (May 2018), [Online]. Available: <https://waterfall-security.com/20-attacks/>.
- [56] '2022 cyber attack statistics, data, and trends.' (Apr. 2022), [Online]. Available: <https://www.makeuseof.com/cyberattacks-on-industry-hackers/>.
- [57] Visited. (Apr. 2022), [Online]. Available: <https://cybelangel.com/blog/steps-in-the-cyber-kill-chain/>.

- [58] Visited april 2022. (Dec. 2016), [Online]. Available: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
- [59] 'Rat.' Retrived March,2022. (), [Online]. Available: <https://www.techopedia.com/definition/4077/remote-access-trojan-rat>.
- [60] Visited march 2022. (Mar. 2016), [Online]. Available: <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>.
- [61] Visited march 2022. (Dec. 2015), [Online]. Available: <https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231>.
- [62] Visited march 2022. (Jan. 2016), [Online]. Available: www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.
- [63] Visited march 2022. (Dec. 2016), [Online]. Available: www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC.
- [64] MITRE. 'Systems engineering guide: Risk management.' Retrieved April, 2022. (2020), [Online]. Available: <https://bit.ly/3byYPAA>.
- [65] Y. Cherdantseva and J. Hilton, 'A reference model of information assurance & security,' in *2013 International Conference on Availability, Reliability and Security*, IEEE, 2013, pp. 546–555.
- [66] J. H. Saltzer and M. D. Schroeder, 'The protection of information in computer systems,' *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975.
- [67] O. Alexander, M. Belisle and J. Steele, 'Mitre att&ck® for industrial control systems: Design and philosophy,' *The MITRE Corporation: Bedford, MA, USA*, 2020.
- [68] W. T. Shaw, *Scada system vulnerabilities to cyber attack*, Oct. 2004.
- [69] N. Moreira, E. Molina, J. Lázaro, E. Jacob and A. Astarloa, 'Cyber-security in substation automation systems,' *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1552–1562, 2016.
- [70] 'Simulation model siemens.' Retrieved Feb, 2022. (), [Online]. Available: <https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/pss-software.html>.
- [71] S. Y. F. Holik D. Abraham, 'Emulation of iec 60870-5-104 communication in digital secondary substations,' 2021.
- [72] Y. Yayilgan, 'Emulation of iec 60870-5-104 communication in digital secondary substations,'
- [73] F. Holik. 'Simulation model documentation.' Initial version. (Feb. 2022).

- [74] 'Libiec61850 / lib60870.' Retrieved April, 2022. (), [Online]. Available: <https://libiec61850.com/libiec61850/about/>.
- [75] 'Attack steps.' Retrived Mai,2022. (), [Online]. Available: <https://www.information-age.com/7-steps-hackers-take-execute-successful-cyber-attack-123460872/>.
- [76] J. Nivethan and M. Papa, 'On the use of open-source firewalls in ics/scada systems,' *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 83–93, 2016.
- [77] 'Vpn.' Retrived May,2022. (), [Online]. Available: <https://www.techtarget.com/searchnetworking/answer/Can-you-have-two-VPN-connections-to-the-same-machine-simultaneously>.
- [78] 'Ugw.' Retrived, Mai-2022. (), [Online]. Available: <https://waterfall-security.com/unidirectional-security-gateways/>.
- [79] 'Dmz.' Retrived, Mai-2022. (), [Online]. Available: <https://waterfall-security.com/dmz-the-industrial-context/>.
- [80] 'Sdn.' Retrived May,2022. (), [Online]. Available: <https://selinc.com/mktg/132609/>.
- [81] 'Supply chain attacks.' Retrived, Mai-2022. (), [Online]. Available: <https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html>.
- [82] 'Supply chain attacks.' Retrived, Mai-2022. (), [Online]. Available: <https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide>.
- [83] 'Software supply chain attacks.' Retrived, Mai-2022. (), [Online]. Available: <https://www.securityweek.com/software-supply-chain-attacks-tripled-2021-study>.
- [84] 'Coin miner.' Retrived, Mai-2022. (), [Online]. Available: <https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/coinminer-malware?view=o365-worldwide>.
- [85] 'Hardware supplychain attack.' Retrived May,2022. (), [Online]. Available: <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>.

Appendix A

Additional Material

Approved by the Pro-Rector for Education 10 December 2020

STANDARD AGREEMENT

on student works carried out in cooperation with an external organization

The agreement is mandatory for student works such as master's thesis, bachelor's thesis or project assignment (hereinafter referred to as works) at NTNU that are carried out in cooperation with an external organization.

Explanation of terms

Copyright

Is the right of the creator of a literary, scientific or artistic work to produce copies of the work and make it available to the public. A student thesis or paper is such a work.

Ownership of results

Means that whoever owns the results decides on these. The basic principle is that the student owns the results from their own student work. Students can also transfer their ownership to the external organization.

Right to use results

The owner of the results can give others a right to use the results – for example, the student gives NTNU and the external organization the right to use the results from the student work in their activities.

Project background

What the parties to the agreement bring with them into the project, that is what each party already owns or has rights to and which is used in the further development of the student's work. This may also be material to which third parties (who are not parties to the agreement) have rights.

Delayed publication (embargo)

Means that a work will not be available to the public until a certain period has passed; for example, publication will be delayed for three years. In this case, only the supervisor at NTNU, the examiners and the external organization will have access to the student work for the first three years after the student work has been submitted.

1. Contracting parties

The Norwegian University of Science and Technology (NTNU) Department: <i>Information Security and Communication Technology</i>
Supervisor at NTNU: <i>Filip Holik</i> email and telephone: <i>filip.holik@ntnu.no</i>
External organization: Contact person, email address and telephone number of the external organization:
Student: <i>Mohammad Reza Jafari</i> Date of birth: <i>16.05.1998</i>
Other students, if applicable ¹

The parties are responsible for clearing any intellectual property rights that the student, NTNU, the external organization or third party (which is not a party to the agreement) has to project background before use in connection with completion of the work. Ownership of project background must be set out in a separate annex to the agreement where this may be significant for the completion of the student work.

2. Execution of the work

The student is to complete: (Place an X)

A master's thesis	
A bachelor's thesis	X
A project assignment	
Another student work	

Start date: <i>11.01.2022</i>
Completion date: <i>20.05.2022</i>

The working title of the work is: *Understanding and Simulation attacks in Power networks.*

¹ If several students co-author a work, they can all be listed here. The students then have joint rights to the work. If an external organization instead wants a separate agreement to be concluded with each student, this is done.

The responsible supervisor at NTNU has the overarching academic responsibility for the design and approval of the project description and the student's learning.

3. Duties of the external organization

The external organization must provide a contact person who has the necessary expertise to provide the student with adequate guidance in collaboration with the supervisor at NTNU. The external contact person is specified in Section 1.

The purpose of the work is to carry out a student assignment. The work is performed as part of the programme of study. The student must not receive a salary or similar remuneration from the external organization for the student work. Expenses related to carrying out the work must be covered by the external organization. Examples of relevant expenses include travel, materials for building prototypes, purchasing of samples, tests in a laboratory, chemicals. The student must obtain clearance for coverage of expenses with the external organization in advance.

The external organization must cover the following expenses for carrying out the work:

Coverage of expenses for purposes other than those listed here is to be decided by the external organization during the work process.

4. The student's rights

Students hold the copyright to their works². All results of the work, created by the student alone through their own efforts, is owned by the student with the limitations that follow from sections 5, 6 and 7 below. The right of ownership to the results is to be transferred to the external organization if Section 5 b is checked or in cases as specified in Section 6 (transfer in connection with patentable inventions).

In accordance with the Copyright Act, students always retain the moral rights to their own literary, scientific or artistic work, that is, the right to claim authorship (the right of attribution) and the right to object to any distortion or modification of a work (the right of integrity).

A student has the right to enter into a separate agreement with NTNU on publication of their work in NTNU's institutional repository on the Internet (NTNU Open). The student also

² See Section 1 of the Norwegian Copyright Act of 15 June 2018 [Lov om opphavsrett til åndsverk]

has the right to publish the work or parts of it in other connections if no restrictions on the right to publish have been agreed on in this agreement; see Section 8.

5. Rights of the external organization

Where the work is based on or further develops materials and/or methods (project background) owned by the external organization, the project background is still owned by the external organization. If the student is to use results that include the external organization's project background, a prerequisite for this is that a separate agreement on this has been entered into between the student and the external organization.

Alternative a) (Place an X) General rule

<input type="checkbox"/>	The external organization is to have the right to use the results of the work
--------------------------	---

This means that the external organization must have the right to use the results of the work in its own activities. The right is non-exclusive.

Alternative B) (Place an X) Exception

<input type="checkbox"/>	The external organization is to have the right of ownership to the results of the task and the student's contribution to the external organization's project
--------------------------	--

Justification of the external organization's need to have ownership of the results transferred to it:

6. Remuneration for patentable inventions

If the student, in connection with carrying out the work, has achieved a patentable invention, either alone or together with others, the external organization can claim transfer of the right to the invention to itself. A prerequisite for this is that exploitation of the invention falls within the external organization's sphere of activity. If so, the student is entitled to reasonable remuneration. The remuneration is to be determined in accordance with Section 7 of the Employees' Inventions Act. The provisions on deadlines in Section 7 apply correspondingly.

7. NTNU's rights

The submitted files of the work, together with appendices, which are necessary for assessment and archival at NTNU belong to NTNU. NTNU receives a right, free of charge, to use the results of the work, including appendices to this, and can use them for teaching and research purposes with any restrictions as set out in Section 8.

8. Delayed publication (embargo)

The general rule is that student works must be available to the public.

Place an X

<input type="checkbox"/>	The work is to be available to the public.
--------------------------	--

In special cases, the parties may agree that all or part of the work will be subject to delayed publication for a maximum of three years. If the work is exempted from publication, it will only be available to the student, external organization and supervisor during this period. The assessment committee will have access to the work in connection with assessment. The student, supervisor and examiners have a duty of confidentiality regarding content that is exempt from publication.

The work is to be subject to delayed publication for (place an X if this applies):

Place an X		Specify date
<input type="checkbox"/>	one year	
<input type="checkbox"/>	two years	
<input type="checkbox"/>	three years	

The need for delayed publication is justified on the following basis:

If, after the work is complete, the parties agree that delayed publication is not necessary, this can be changed. If so, this must be agreed in writing.

Appendices to the student work can be exempted for more than three years at the request of the external organization. NTNU (through the department) and the student must accept this if the external organization has objective grounds for requesting that one or more appendices be exempted. The external organization must send the request before the work is delivered.

The parts of the work that are not subject to delayed publication can be published in NTNU's institutional repository – see the last paragraph of Section 4. Even if the work is subject to delayed publication, the external organization must establish a basis for the student to use all or part of the work in connection with job applications as well as continuation in a master's or doctoral thesis.

9. General provisions



This agreement takes precedence over any other agreement(s) that have been or will be entered into by two of the parties mentioned above. If the student and the external organization are to enter into a confidentiality agreement regarding information of which the student becomes aware through the external organization, NTNU's standard template for confidentiality agreements can be used.

The external organization's own confidentiality agreement, or any confidentiality agreement that the external party has entered into in collaborative projects, can also be used provided that it does not include points in conflict with this agreement (on rights, publication, etc). However, if it emerges that there is a conflict, NTNU's standard contract on carrying out a student work must take precedence. Any agreement on confidentiality must be attached to this agreement.

Should there be any dispute relating to this agreement, efforts must be made to resolve this by negotiations. If this does not lead to a solution, the parties agree to resolution of the dispute by arbitration in accordance with Norwegian law. Any such dispute is to be decided by the chief judge (sorenskriver) at the Sør-Trøndelag District Court or whoever he/she appoints.

This agreement is signed in four copies, where each party to this agreement is to keep one copy. The agreement comes into effect when it has been signed by NTNU, represented by the Head of Department.

Signatures:

Head of Department: Date:		
Supervisor at NTNU: Date:		31.1.2022
External organization: Date:		
Student: Date:		26-01-2022
Other students, if applicable		

Bachelor Thesis Confidentiality agreement

Bachelor thesis title: Understanding and simulation attacks in power networks

Author: Mohammad Reza Jafari, mohammaj@stud.ntnu.no

Supervisor: Dr. Filip Holik, filip.holik@ntnu.no

Applicant: Prof. Sule Yildirim Yayilgan, sule.yildirim@ntnu.no

I, **Mohammad Reza Jafari** agree to keep the details and materials provided from the ECODIS and InterSecure projects confidential and will not discuss them with any other person outside the projects research group and persons reasonably involved with the thesis. This involves presentation materials, publications, data, and developed tools (simulation model).

Further, I will not undertake a similar project to ECODIS and InterSecure in the following three years (that would permit it to be undertaken from the 1st of February 2025).

In the event that I do undertake an independent project based wholly or substantially on this work following the expiry date of this agreement (1st of February 2025), I undertake to offer all members of the research team who participate in the mentioned projects the opportunity to be involved in it at principal level.

Signature: 

Date: 16-02-2022

Witnessed: 

Date: 16.02.2022

Bachelors-Prosjekt Plan

mohammaj

January 2022

1 Goals and Scope

1.1 Background

Background for this project is to identify threats and attacks particularly in a digital substation. Electricity is distributed over power lines and the control of generation, distribution and storage of electricity is done digitally. Since the digitalization has taken over the analog types, more challenges have been created due to cyber attacks.

1.2 Goals

The goal of this thesis is to understand and simulate attacks in power networks. Documents which were given to me for research and updating myself to the project are the following:

- Emulation of IEC 60870-5-104 communication in digital secondary substations
- Security and Privacy issues in IoT-Based smart grids: a case study in a digital substation
- Cyber-security gaps in a digital substation:from sensors to SCADA
- Cyber-Risk Identification for a digital substation
- An industrial trial of an approach to identification and modelling of cybersecurity risks in the context of digital secondary substations
- A Detailed analysis of the GOOSE message structure in an IEC standard based substation automation system.
- Sikkerhet i digitale verdikjeder presentation document.

As it is under research with two projects ECODIS and InterSecure, it is a huge opportunity to learn more about this on a high scale. Material issued to me

1.2.1 Research on goals

- Reading and research of materials provided by team members
- Research of threats on substation and selection of specific ones for simulation
- Research and hands on experience with the simulation tool provided from team members
- Attend the meetings with others team members

1.2.2 Result goals

- Describe functionality of digital substations
- Describe threats of digital substations

- Identify threat(s) suitable for the simulation testing
- Test the selected threat(s) in the simulation tool
- Complete and deliver the thesis.

1.3 Scope and limitations

This section describes the planned scope of the project. The scope is focused only to the threats identification and their simulations.

2 Resource available

If the project needs any cloud environment, NTNU's openstack is available. In addition to that the simulation tool for attacking is available to perform any activities for the project.

3 Workflow

This thesis is specific as it includes only one person. This workflow excludes formal group rules or role assignment of group members. That's why the part like agreement, rules and agreement has been removed from this section, the rest of this section however details the planned workflow and timeline for the project.

3.2 Status meetings

M.Reza will have weekly meetings with his supervisor Filip Holik and some other meetings with Sule Yildirim and Doney Abraham if possible. Meetings with Filip will be held around 13:00 every Wednesday as agreed.

During the status meetings Reza will present his work done each week and get feedback from the mentor, these meetings will also likely influence what Reza will be working on the following week.

3.3 Journal

Reza will keep a personal log/journal for the work he does every week as well as notes of all the meetings he has conducted. This will help him with the reflection note at the end of the project.

3.4 Quality assurance

In addition to the status meetings Reza will send at occasion drafts of the final document to his mentor for quality assurance, the majority of these will likely only concern certain pieces of the report however a final draft of the entire report is planned towards the end of the April.

3.5 Project Timeline

A simple project timeline is written below. This gives a brief and easy plan to follow during the whole project.

Planning from week 1 to week 5

- Meetings, future work

Familiarization week 4 to week 7

- Research and data collection

Implementation week 8 to week 13

- Identification of threats

Testing part week 13 to week 15

- Implementation of attacks and testing.

Buffer and polish week 14 to week 21

- Manuscript preparation, polishing the theory part in the thesis

4 Risk Analysis

Risk	Likely	Consequence	Mitigations
Member becomes sick	Medium	High	Limit exposure risk, Wash hands and use alcohol hand spray Wear face mask when meeting people
Mentor becomes sick	Medium	Medium	Use email, digital meetings If the mentor feels well enough to respond on another date.
Loss of work	Low	High	Daily backups, online backups such as git or other platform, extra pc for the work
Major changes to workflow	Low	High	Limit the scope to only specific versions If not too much has changed go back and revisit the affected sections to save the work.
Wasting time	High	Medium	Limit the scope to specific plan Ask the mentor for a crash course or help when stuck on a specific problem.

