Cybersecurity in cyber-physical systems

Digital Substations

Jonas Høsteng Rød

Thesis submitted for the degree of
Master in Electronics and Computer Technology
Program option: Cybernetics
30 credits

Department of Physics
Faculty of Mathematics and Natural Sciences

UNIVERSITY OF OSLO

Spring 2019

Cybersecurity in cyber-physical systems

Digital Substations

Jonas Høsteng Rød

Cybersecurity in cyber-physical systems

http://www.duo.uio.no/

Abstract

This thesis compares conventional and digital substations, and the cybersecurity risk associated with the different substation types.

Statnett's digital substation pilot project at Furuset in Oslo, Norway, is used as basis to investigate possible cybersecurity threats towards cyber-physical systems in general, and furthermore towards digital substations. The specific part of the pilot project modelled in this thesis is the protection and control unit due to its critical functionality and key position in the pilot project's design.

The thesis investigates how cybercriminals can gain access to critical system infrastructure by utilising weaknesses in known industrial standards and how cybercriminals can get access through common cyberattacks.

Statnett is responsible for maintaining, operating and controlling the transmission grid, a part of the Norwegian power grid. A crucial element in the power grid are substations. Substations cover an important functionality in power grids by transforming voltage. The Norwegian power grid consists of several subgrids operating at different voltage levels and are among others connected to the main grid through substations. Modern substations consists of digital and physical elements. A model with coupled components is used to illustrate how a cyberattack can disrupt a coupled system without being detected.

Furthermore, the thesis investigates how typical cyberattacks are accomplished, and the resources and knowledge an perpetrator would need in order to disrupt a modern digitised system.

A modern cyber-secure environment is made resilient and robust by having a well-designed cybersecurity plan which takes into consideration the organisation, digital and analogue components, software and firmware, and the control algorithm including several degrees of redundancy.

Contents

List of Figures

List of Tables

Preface

This thesis is written as a final part of a masters degree in Electronics and Computer Technology, direction Cybernetics, and the course ELD5930 - Master's Thesis, at the University of Oslo.

The purpose of this thesis is to apply knowledge learned throughout the attendance at the university on a relevant industrial challenge.

The final issue was prepared together with Statnett SF, represented by Sonja M. Berljin, SINTEF, represented by Oddbjørn Gjerde and the University of Oslo, represented by Andrea Cristofaro.

Thanks to ABB, ElectraNet and NVE for allowing me to use their figures from related articles that are relevant for this thesis.

A huge gratitude to the following people:

- Rita S. R. Øyen - my beloved sister for helping me with the layout of this thesis and proofreading.
- Josefine R. Magnussen - my beloved girlfriend for motivating and helping me with proofreading of the thesis.
- Mads Magnussen - my extended family, for proofreading the thesis.
- Andrea Cristofaro - my supervisor from UiO, for pointing me in the right direction during this thesis.
- Torbjørn Kringeland - my dearest friend for helping me to understand the complicated dynamics and MATLAB implementation used in this thesis and throughout the study.
- Sonja M. Berlijn - my supervisor from Statnett, for helping me to understand how the Norwegian power grid operates and giving feedback during the process.

Acronyms and requirements

Acronyms

IED	Intelligent Electronic Device
NCIT	Non-Conventional Instrument Transformer
SCADA	Supervisory Control And Data Acquisition
PCU	Protection And Control Unit
CPS	Cyber-Physical System
OSI	Open Systems Interconnection
IT	Information Technology
OT	Operational Technology
PID	Proportional-Integral-Derivative
AC	Alternating Current
DC	Direct Current
DSV	Digital Sample Values
LP	Low Pass
FIR	Finite Impulse Response
RK4	Runge Kutta 4
FOCS	Fiber Optic Current Sensor
HMI	Human Machine Interface
Hacker	A person/group who tries to gain illegal access to a organisation's data using electronic devices
SQL	Structured Query Language - used in databases used to run operations in databases
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SAS	Substation Automation and Protection System
Process bus	Communication bus between measurements and PCUs
Station bus	Communication bus between PCUs and control central
TCP/IP	Transmission Control Protocol/Internet Protocol
NTP	Network Time Protocol
PTP	Precision Time Protocol
Interoperable	The ability to use equipment with different connectors and interface
Predictability	Environment behaving as expected
CPU	Central Processing Unit

Requirements

An updated version of MATLAB to run the simulations of the model used in this thesis.

Part I

Introduction

Chapter 1

Introduction

1.1 Cyber-physical systems

In a historical perspective society have gone from implementing systems using an analogue and mechanical approach, to an electronic and digital approach to meet future demands and development. With the ever increasing demand for electric power in society it is necessary to meet this development with a reliable, secure and robust power delivery system. One important step to achieve this is by exploiting digital technology and to create a more digitized solution of the power grid than today's standard. Transforming the power grid from today's conventional grid to a digitised system can yield huge potential in terms of robustness, accessibility and connectivity when facing the challenges of the future. There are many examples of possible future demands for the power grid such as a higher degree of flexibility where a larger part of the production comes from renewable energy sources and is more interconnected to other power markets in neighbouring countries. For house-holding consumers it may be of interest to buy power when prices are low or to sell power when prices are high by utilising the fluctuating power market. This can for example be charging an electric vehicle or sell solar power from a roof-scale solar grid. These examples illustrate how the power grid of the future needs a higher degree of interconnectivity, reliability and flexibility [55].

Interconnectivity and digitalisation can open for more advanced and sophisticated attacks as already witnessed with the *Stuxnet* virus in Iran which was uncovered in 2010 [56], the malware *Industroyer* in Ukraine [29] or the more recent cyberattack towards the Norwegian company Hydro in March 2019 [33]. These cyberattacks were most likely exploiting specific industrial protocols, combined with detailed knowledge on how the attacked industrial system operates as a way to gain control over the industrial devices and components.

These events represent a cautionary warning of the importance of protecting digital infrastructure through a well-designed cyber-physical security infrastructure.

Cyber-physical systems (CPS) is the terminology used to describe systems containing a cyber and a physical part. A CPS is a network of digital cyber components connected to a network of physical components. A CPS integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world in a real time setting being dependable, safe, secure, efficient and robust. Examples of such systems can be found in the automobile industry, autonomous cars, air traffic control, medical equipment and large industrial systems such as the water grid or the power grid [72].

With the continuous advancements in technology such as IoT (Internet of Things), development in the IT (Information Technology) and OT (Operational Technology), the security aspect of systems combining IT and OT becomes more important than ever before, especially with critical infrastructure. The distinction between cyber and physical elements become more intertwined and harder to separate. This makes it important to implement a framework which clearly defines how the two parts relate, and also how the dynamics of the CPS change due to their complex relationship [10].

In literature there are two general representations when analysing the security aspect. The first one represents the cyber system and how specific attacks affect the cyber system. The second one represents how attacks on the physical system affect the physical system. CPS is one way of representing the overall system, describing a cyber and a physical part as two sub-systems and their interconnection [40].

1.2 Cyber-physical systems in power systems

A modern power grid can be modelled as a CPS. The cyber part describe the digital part of the system. Components in the cyber part often include a combination of sensor(s), transmitter(s), receiver(s), CPU(s) and other necessary components. The physical part of the system are cables, power transformers, current transformers, voltage transformers and other power system components.

Data from sensors form the basis of revealing the present state of the system. Based on the present state, the desired state and the characteristics of the system, active control is applied to the system. In the power grid the measuring components are among others transformers used to measure voltage, current and power. An important functionality in the power grid is the ability to transform voltage levels depending on the voltage level the receiving grid is operating on. This functionality is provided by substations and make out a critical part of the transmission grid, as well as the regional grid and the distribution grid.

A substation can be modelled as a CPS. The cyber part consists of voltage, power and current sensors measuring the voltage, power and current throughput, devices for surveillance, control and security. Data from the sensors originate from the transformers in the substation. The physical parts consists of switches, connectors, cables, circuit breakers, line disconnectors, busbar and so on.

The most likely attack point is to attack physical components through the cyber part of the system. Performing an attack which involves direct contact with substation power components represents a huge risk for the attacker due to the high voltage and current levels passing through the transformers.

The most plausible points of attack in the cyber part are the digital components used for control, storage or communication within the CPS by exploiting undiscovered weaknesses in access points in the software and protocols.

1.3 Purpose and limitations

The purpose of this thesis is to describe and compare conventional and digital substations, and the cybersecurity risks and potential associated with the different substation types.

Statnett is currently studying and exploring digital substations in the power grid through a pilot project at Furuset in Oslo, Norway. The purpose of the pilot project is to investigate different aspects of a digital substation. One important aspect, which will be investigated in this thesis, is cyber-physical systems.

The pilot project *Digitalstasjon – Furuset* is used as a basis in this thesis to describe a digital substation. In this project the protection and control unit (PCU) will be investigated in greater detail due to its key position in the substation design.

A conceptual model will be used to simulate how a cyberattack can influence the PCU to answer the following questions: In what way can a cyber-criminal gain unauthorised access to the data bus, and how can this access be used to disrupt the PCU's functionality to disconnect a line and/or perform an undetectable attack.

This thesis is limited to investigating the PCU and discussing possible ways of gaining access to a substation, and furthermore, the process bus and PCU. In addition, the thesis will investigate possible access points and the probability of successfully performing a cyberattack by exploiting weaknesses related to these access points.

The simulations in this thesis will be used to investigate how a cyberattack can disrupt a digital substation. The model used for simulating cyberattacks are based on a coupled system. The coupled system is based on generators in a power network with coupling effects existing in the system. Furthermore, the simulations will be used to investigate how a cyberattack can disrupt a digital substation with coupling effects between the oscillators in the system.

1.4 Methodology

This section describes the overall methodology used in this thesis.

1.4.1 Literature search

Finding relevant articles, books and related work is the first step towards finding answers to the questions studied in this thesis. Further details of the literature search is in section 5.1.

1.4.2 Modelling the system

Based on the literature search, a model based on a power system was found and used as a basis to describe a system with coupling effects. Details of the modelling is in section 5.3.2

1.4.3 Simulation based on the system model

The simulation of the system is done based on the mathematical model which describes the system. A detailed description of the simulations is in section in section 6.3.

1.4.4 Evaluating the response of the system based on the simulations

The resulting simulated response of the model is described and evaluated. The details of the system response is described in section 7.5.

Chapter 2

Background

The Norwegian power grid is divided into three different grids; the transmission grid, the regional grid and the distribution grid [55].

The transmission grid connects the largest power producers and international connections to related power markets. This grid operates at high voltage levels, usually 420 or 300 kV, with some transmission lines operating at 132 kV.

Statnett SF is the transmission grid system operator responsible for development, maintenance and operation of this grid. The main mission is to secure power supply through operation, monitoring and contingency planning, fascilitate the realisation of Norway's climate goals, and to create value for customers and society[57].

The regional grid connects the transmission grid and the distribution grid. This grid contains consumers with higher power demands such as industrial customers and industrial areas. The voltage level range from 33 kV to 132 kV.

The distribution grid consists of local grids that distributes power to end users such as office buildings operating at lower voltage levels. The voltage level in the distribution grid is up to 22 kV.

An important function in the power grid is the ability to transform voltage levels to limit loss of energy when power is transported over distance. Higher voltage levels lead to less power loss during transportation. In a power grid this functionality is ensured by substations. To enable the required energy transition, digitalisation is necessary. Digital substations are one of the building blocks in the full digitalisation of the Norwegian power system. This thesis investigates the aspect of digitalisation as seen in context of the power grid in figure 2.1.

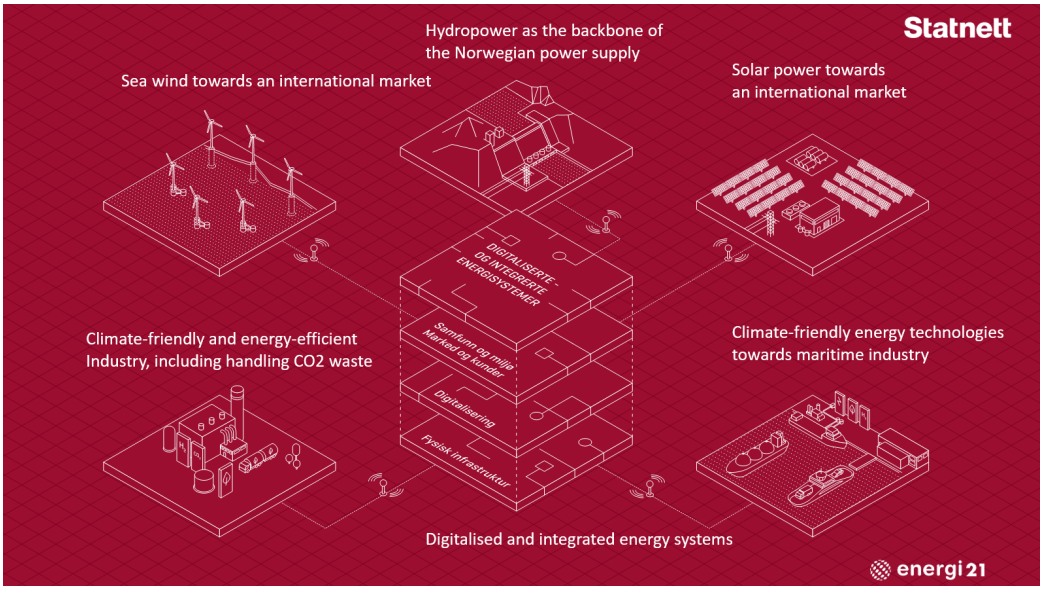

Figure 2.1: Power system of the future [7]

Cybersecurity in substations has become an issue due to the introduction of Ethernet communication protocols, such as TCP/IP, and more open and available access to external networks between automation and control systems [18].

Communication between networks connected to the internet and automation systems like *Supervisory Control And Data Acquisition* (SCADA) has made it easier for unauthorised personnel such as cybercriminals to gain access to critical components used for control and data acquisition. Cyberattacks on automation and control systems have been reported more frequently the past years and often resulted in economic loss and a worst case scenario, loss of human life.

Important characteristics of a cyber secure environment is having a high degree of availability, integrity, confidentiality, authentication, transparency and predictability. These characteristics will be discussed further in section 3.5.

To meet the increasing demand for probabilistic operation and maintenance, the move from conventional analogue implementation and control of such systems towards a digital solution is an important step. A few advantages includes, but are not limited to, increased flexibility, faster response to rapid changes in demand, less system downtime, increased interoperability, better surveillance and performance of the power system.

2.1 Statnett's pilot project at Furuset, Oslo

Layout of Furuset digital substation - the pilot project

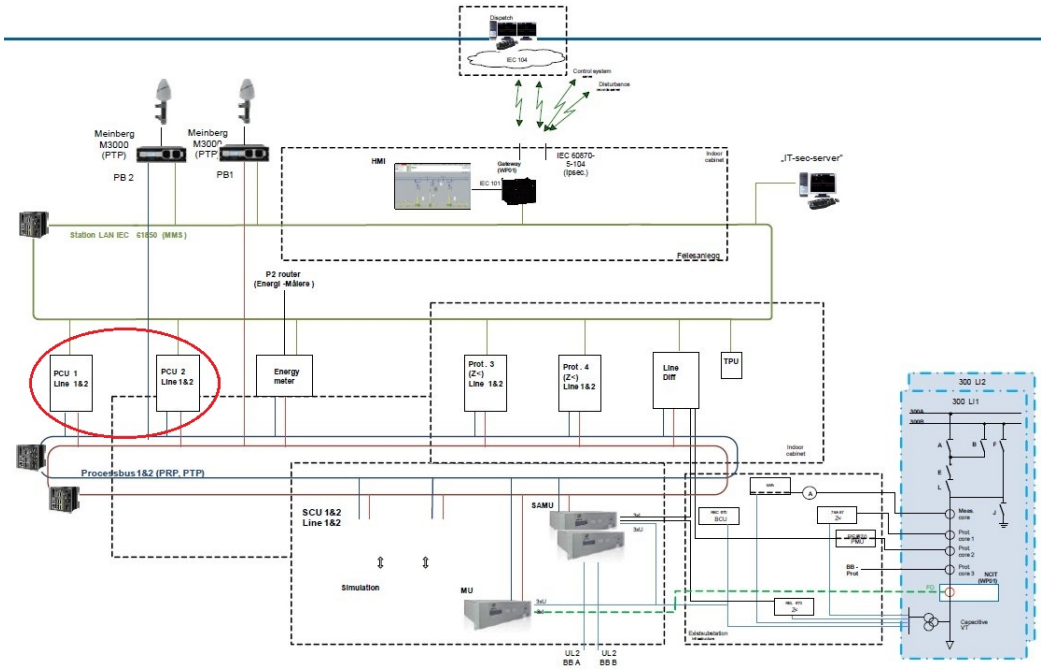

Figure 2.2: The Furuset pilot project with PCUs marked in red [45]

Statnett's pilot project at Furuset in Oslo, Norway, is an important step towards digitising the power grid. The main goal of this pilot is to gain experience and knowledge concerning concepts of a digital substation equipped with a Non-Conventional Instrument Transformer (NCIT) and process bus [45]. Further, the project is used to become familiar with new technology and to investigate possible benefits. The pilot is installed in a live 300 kV line bay in parallel with the already existing Substation Automation and Protection System (SAS) as illustrated in figure 2.2.

Digitising substations can yield many advantages such as reduced costs, increased reliability, productivity and safety, reduced outage time when maintenance or faults occur, and easier access to real-time data produced at each substation. It is of great importance to understand how industrial standards and protocols utilise digital devices to communicate within the digital domain and ultimately ensuring a robust power grid.

Digitising the substations may also give a huge potential in the way substations are controlled, monitored and commissioned in the future. This can lead to less personnel on remote locations as well as making it harder to physically locate the substation. A possible cost of this potential can be an increased number of attack points to the digital domain.

Accessing the digital domain is a challenging task, but if an attacker manages to access one of the communication networks in the substation, the potential for disruption can be very high due to the interconnectivity between digital and physical components in the substation [45][19].

Chapter 3

Theoretical background

3.1 The Norwegian power grid

The Norwegian power grid is a network of interconnected transmission lines as illustrated in figure 3.1. The figure shows how power lines in the transmission grid, marked as red and yellow lines, are connected to substations, marked as red dots, to distribute power in the southern parts of Norway. The substations is an important and critical part of the distribution of power throughout the power grid.

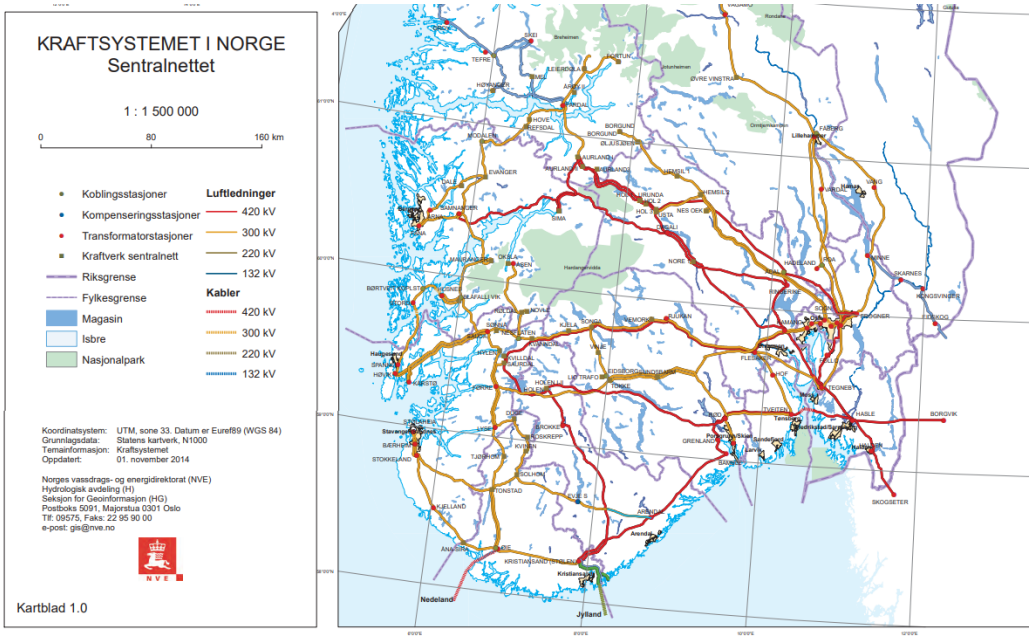

Figure 3.1: Part of the Norwegian power system [31]

3.2 SCADA

Supervisory Control and Data Acquisition (SCADA) is a system of software and hardware elements that allows industrial organisations to control processes locally or remote, monitor, gather and process real-time data, record events into logfiles, interact with devices such as sensors, switches, generators and motors, and more through a human machine interface (HMI) software [68].

SCADA systems are crucial in industrial applications because they enable efficiency, smart processing of data, communication between different parts of the overall system, and well-informed decisions based on real-time data. The sectors using SCADA are among others the energy sector, the oil and gas sector, the manufacturing sector, the transportation sector, the power, water and food production sector.

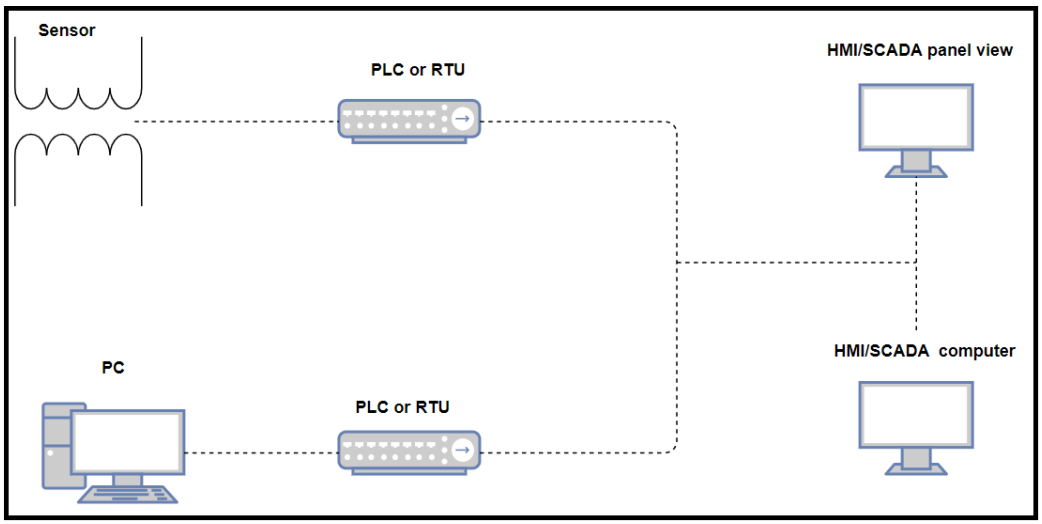

Figure 3.2: Basic SCADA layout

Sensors measure the state of the system and transmits data to Programmable Logic Controllers (PLC) or Remote Terminal Units (RTU). Once the data is processed and handled by the PLC or RTU it is fed throughout the SCADA system. A HMI operator display enables supervision and control from an operational terminal [68]. A basic SCADA layout is illustrated in figure 3.2.

3.3 Cyber-physical systems and cyber threats

A cyber-physical system is a system in which both the cyber part and the physical part are integrated at all levels of the system design [72]. In cyber-physical systems, physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioural modalities, and interacting with each other in ways that change with the context [17].

Figure 3.3: Cyber-physical system layout - cyber and physical part [72]

Based on a cybersecurity perspective, there are at least four important aspects an organisation should consider when investigating cyber threats associated with CPS[10]:

- ***Organisation*** - cybercriminals often attack industrial facilities through exploiting employees without proper training and awareness of cyber threats. E.g. an e-mail which at first glance seems to be trustworthy.
- ***Digital and analogue components*** - exploiting weaknesses in the configuration of components. E.g. opening blocked USB access points and insert a USB drive containing malware.
- ***Software and firmware*** - exploiting weaknesses in IT or OT software/firmware by exploiting undiscovered weaknesses in the software or firmware code. E.g. changing functionality of physical components by altering the firmware.
- ***Control algorithm*** - changing the controllers response to given states of the system. E.g. changing the response rate or delaying the control action which can make the system unstable and unreliable.

3.3.1 Common attacks on cyber-physical systems

The following subsections introduce some typical cyberattacks which will be used in this thesis to discuss ways of gaining access to a cyber-physical system and, furthermore, a digital substation.

3.3.2 DOS attack

A *Denial-of-Service* attack is when a cyberattacker seeks to disrupt the communication between devices by making resources unavailable to the network. The most common types of DOS attacks is TCP SYN flood attack. This attack exploits the buffer space in Transmission Control Protocol (TCP) by sending requests and not responding to the requested data. This causes the attacked device to timeout while waiting for response from the requesting device/sender [6].

Another common DOS-attack is the *Ping of death-attack*, where the attacker exploits the maximum size of an IP packet of 65,535 bytes by sending fragmented packets which when reassembled are larger than the maximum allowed size. When the receiving device defragments the packet, it can experience buffer overflow and other critical system failures.

A *distributed DOS* attack is when the incomming attack originates from several sources making it harder to stop the attack by blocking a single source.

These attacks can be avoided by checking the size of the received packet and/or block the source of the attack by using a firewall.

3.3.3 Phishing

A *phishing attack* is when a cyberattacker attempts to obtain sensitive information by disguising e.g. an e-mail as if it is coming from a trusted source. The main goal is to gain access to data such as usernames and passwords, and/or install malware on the attacked system by exploiting an unaware employee. These attacks are usually conducted through e-mail and can be avoided by investigating the origin and broad use of e-mail filters. The details in the e-mail such as wrong spelled words or company name is a common way to reveal the trustworthiness of the e-mail [67].

One of the most important countermeasures besides continuous updates of software is company awareness of the given threat situation and employees with experience and training in spotting fraudulent content.

3.3.4 Man-in-the-middle attack (MitM)

A *MitM*-attack, commonly known as an eavesdropping attack, is when an attacker intercepts a victims communication without the victim being aware of the ongoing interception. Either the attacker has to be within physical proximity of the target e.g. through an open WiFi network, or the attacker can install malicious software by performing a phishing attack through e-mail. There are several types of MitM attacks such as spoofing or hijacking, both with the intention of pretending to be a trustworthy source, for instance a financial institution or a bank. Spoofing is a situation in which a person or program successfully masquerades as a trustworthy source to gain an illegitimate advantage [54]. Hijacking a situation in which an attacker relays and possibly alters the communication between two parties who believe they are directly communicating through a private connection [36].

Figure 3.4 illustrates how an attacker can monitor a secure session [63] [16].

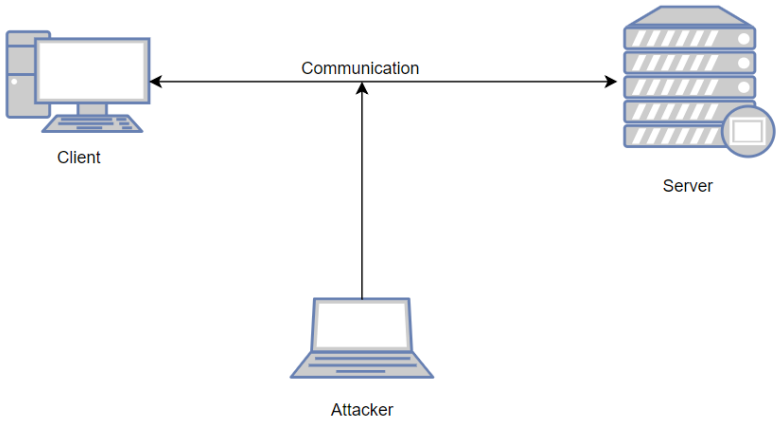

Figure 3.4: Visual illustration of MitM-attack

3.3.5 Malware

Malware describes malicious software such as spyware, ransomware, viruses and worms. The malware exploits weaknesses in a network, typically a user that opens an attachment which installs malicious software. The malicious software will typically block access to key components, install harmful software, obtain information from harddrives or disrupt components resulting in an inoperable system. Users that are exposed to such attacks does not generally become aware of the attack before the malware is deeply integrated with the system if the attack has been successful [65].

3.3.6 SQL injection

A *SQL injection* attack is used to disrupt data-driven applications. SQL-code is injected a server forcing the server to reveal information unintendedly, e.g. by dumping the contents of the database to the attacker [59].

3.3.7 Zero-day vulnerability

A *Zero-day* vulnerability is a software security flaw known to the software vendor, but the vendor have not managed to build and release a patch to fix the flaw. The term zero-day comes from the fact that the vendors software technicians has had zero days to fix the problem.

A zero-day attack is when a cybercriminal manages to exploit a known security flaw before a patch to fix the issue is released and the platform using the software is updated with the new patch [21] [71].

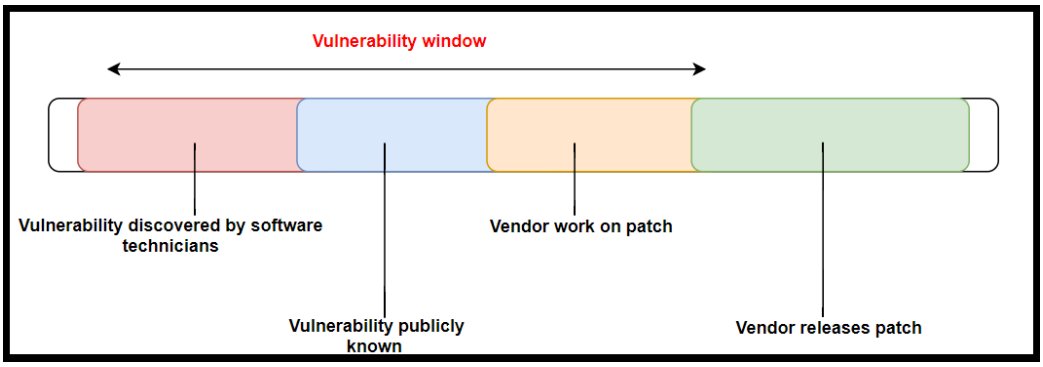

Figure 3.5: Illustration of the vulnerability window

3.4 Substation

A substation is an electrical facility which transforms voltage in the power grid to and from different voltage levels. The most common components of a substation are cables, line disconnectors, voltage transformers, circuit breakers, busbars, current transformers, power transformers and surge arrestors, details can be seen in figure 3.6. Control and measurements in the substation is based on the mentioned components [49].

The substations also have a control building and abilities for remote control. Most substations are designed with a high degree of redundancy in case of failure in the devices and components used in the substation. Redundancy is ensured by having several transformers, transmission lines and grounding cables attached to the busbars. In this way a local or remote control center has the ability to disconnect or reconnect transformers and transmission lines.

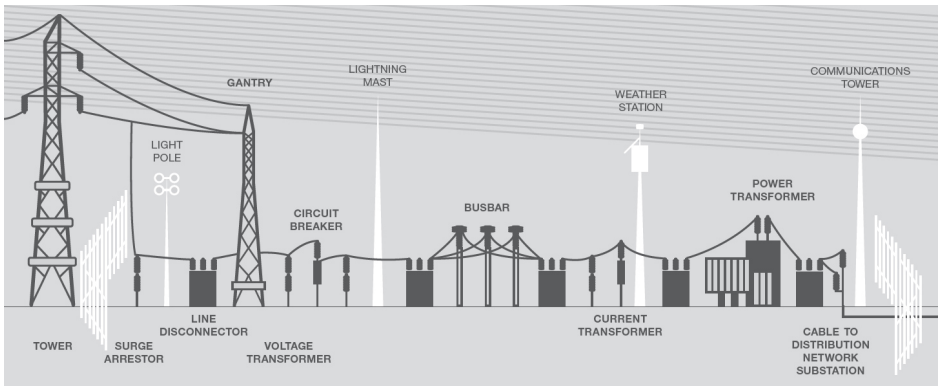

Figure 3.6: Substation power components [58]

Substations can be divided into three categories:

- Substations in the *transmission grid* transform the highest voltages in the power grid, 420 and 300 kV, down to 132 , 66 or 45 kV. The transformers on this voltage level has a capacity per unit of several hundred MW.
- Substations in the *regional grid* transform voltages from 132, 66 or 45 kV to 22 or 11 kV. Transformers on this voltage level has a capacity of 10-25 MW. In small municipalities there is usually only one substation unlike in the bigger cities where there is usually one for each district.
- Substations in the *distribution grid* transform voltage from 22 or 11 kV to 420 or 230 V. Normal outlet-voltage in Norway is 230 V used by house-holding customers and 420 V used by most industrial customers.

Conventional vs. digital substation

In a conventional substation there are several hundred connections, as illustrated in figure 3.7, consisting of copper cables between primary and secondary equipment. Communication and control is made utilising both analogue and digital signals. On process level, each signal for measuring and triggering has a unique copper connection. Communication in the substation is made externally to a SCADA system. In a conventional substation it is hard to use the data from the SCADA system directly [45][20]. Measurements from conventional transformers are connected directly to the substation via copper cables. This results in the same level of voltage inside the substation as in the transmission lines.

In a digital substation the copper cables are replaced by a station bus and a process bus. Communication and control is made by utilising digital signals on both station and process level, both internally and to external systems. Communication and protection commands are sent over highly available fibre optic cables, meaning that both physical and digital access is easy for the organisation. Information is distributed on the communication buses and are made available to the network both internally in the substation, and to external facilities such as a control center.

The digital substation has the ability to communicate between SCADA and other networked systems both internally and externally.
Conventional current and voltage transformers are replaced by
Non-Conventional Instrument Transformer (NCIT) which simultaneously measures current and voltage in the transmission lines and transmits the data via fibre optic cable [64], thus reducing the voltage and current levels inside the substation. Figure 3.7 illustrates the extensive use of copper cables in conventional substations versus using fibre optic process bus and station bus in digital substations.

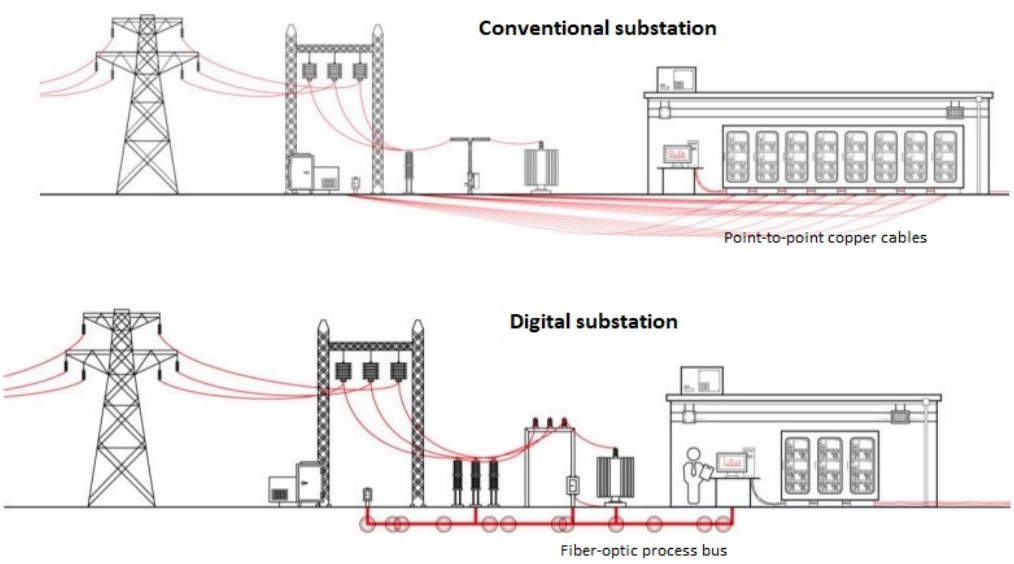

Figure 3.7: Comparison of a conventional substation utilising copper cables and a digital substation utilising a fibre optic process bus for communication [20]

Comparison of substation types			
Type	**Conventional**	**Modern**	**Digital**
Network level	Network management	Network management	Network management, Asset Health Center
Station level	HMI, control board and event recording	HMI, Gateway	HMI, Gateway
Bay level	Hard-wired protection and control	Protection and control IED's	Protection and control IED's
Process level	Air-insulated switch bay	Air-insulated switch bay	Disconnecting circuit breaker with FOCS

Table 3.1: Comparison of the different layers in conventional, modern and digital substations

Comparison of communication medium used in substations			
Communication medium	**Conventional**	**Modern**	**Digital**
Station- and network level	Serial communication	Ethernet communication	MLS-TP, protocol for packet transport
Bay- and station level	Copper cables	IEC 61850 data	IEC 61850 data bus
Process- and bay level	Copper cables	Copper cables	IEC 61850 data bus

Table 3.2: Substation communication medium used on different levels and substation types

3.5 Security zones

A digital substation is protected with a physical perimeter consisting of fences and access control. In addition to the physical perimeter there is also an electronic security perimeter which is the logical border surrounding the network to which critical cyber assets are connected and controlled. The electronic security perimeter is characterised by the following properties [22]:

- *Confidentiality*
  Preventing disclosure of information to unauthorised personnel or systems.
- *Integrity*
  Preventing undetected modification of information by personnel or systems.
- *Availability*
  Ensuring that unauthorised personnel or systems can not deny access or use to authorised users.
- *Authentication*
  Determination of the true identity of a system user by e.g. mapping the identity to a system internal principal (e.g. a valid user account) such as an approved user database.
- *Authorisation*
  Access control, preventing access to the sytem by personnel or systems without permission.
- *Auditability*
  The ability to reconstruct the complete history of the system behaviour from historical records of relevant actions previously executed.
- *Non-repudiability*
  The ability to provide proof of the integrity and origin of the data.
- *Third-party protection*
  The ability to avoid damage done to third-party systems via the attacked network.

Substations are protected with security zones, each being responsible for specific areas of the substation. Figure 3.8 illustrates the different security zones and what type of assets each security zone assures. Protection of assets in a digital substation is ensured by physical security perimeters, electronic perimeters, data protection, encryption of data, secure user accounts, logging and more [18].

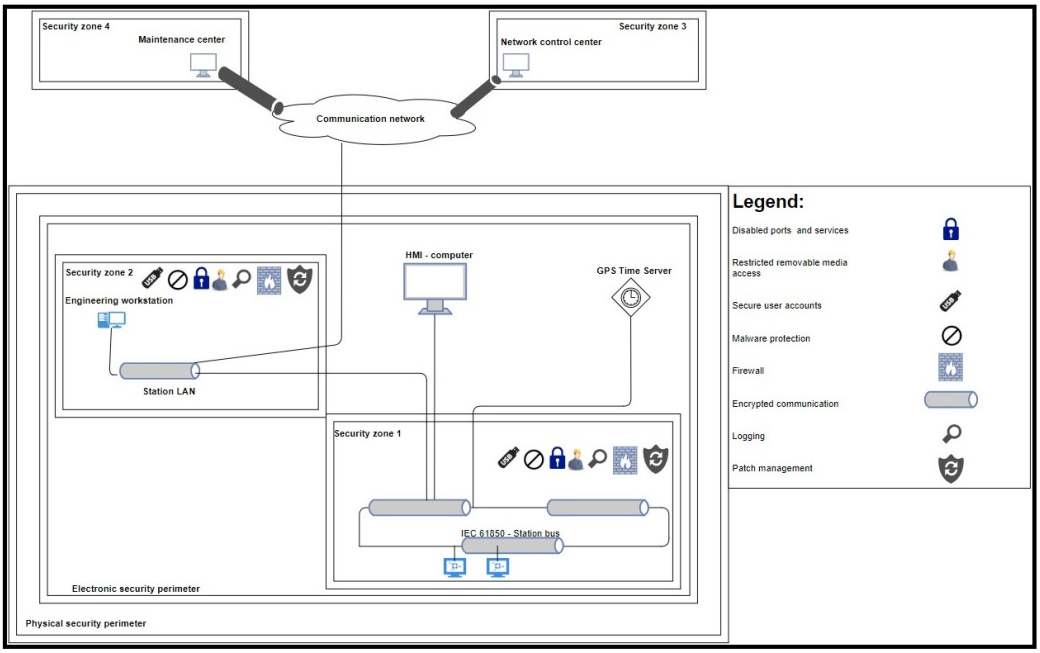

Figure 3.8: Substation security zones [18]

3.6 The OSI model and industrial standards

The *Open Systems Interconnection* model is a conceptual model for data communication in open equipment and vendor independent systems.

The OSI model is an essential part of the standardisation process describing how data is communicated in and between networks. It consists of a framework of seven distinct layers with a common set of protocols describing how communication is ensured. Each layer describes critical communication functionality. The main purpose of the OSI model is to standardise the communication between different systems with standardised protocols such as TCP/IP, NTP and PTP [43][44]. The layers and examples of their functionality is described in table 3.3 and 3.4

OSI model	
Layer	**Functionality**
7 - Application	Running high-level APIs, resource sharing, remote file access
6 - Presentation	Translating data between networking services and applications
5 - Session	Host-to-host communication
4 - Transport	TCP, UDP, SCTP
3 - Network	Controls datatransfer and error handling in the network layer
2 - Data link	Physical addressing of equipment in a computing network
1 - Physical	Defining the equipments physical properties and characteristics

Table 3.3: OSI model - layers and functionality

Layer	**Example**
7	SMTP, web surfing, web chat, virtual terminals
6	GIF, JPEG, HTTPS, SSL, TLS
5	SMPP, SCP and PAP
4	TCP, UDP, SCTP
3	IP, IPsec, DDP
2	Ethernet
1	Multiplexing, circuit switching, optical cable, electrical cable

Table 3.4: OSI model - layers and examples

The application layer makes two or more connections able to communicate directly using protocols such as HTTP, SMTP or FTP. *The presentation* layer makes sure data is presented correctly by e.g. compressing and decompressing data or encrypting data. The *session* layer manages the dialogue over the transport layer between endpoints. *The transport* layer manages the transfer of data in the network layer and handles errors so that higher layers receive data without errors.

The network layer makes sure that data is transmitted and received in correct order, and to the correct receiver. Addressing on this layer is made on logical addresses such as an IP-address representing a node in the network. *The data link* layer handles transfer of data and error handling in the physical layer such as MAC-addressing. *The physical* layer defines all physical properties and signals used in the network such as voltage, physical connectors, cables, radio waves and so on.

Chapter 4

Mathematical theory

This chapter introduce the reader to the mathematical theory and notation used in this thesis.

The system modelling and MATLAB implementation done in this thesis is based on the underlying mathematical principles from this chapter. This is important to be able to determine characteristics of the model such as controllability and observability.

4.1 Notation

$\mathbb{R}$	Set of real numbers
$\mathbb{R}^{mxn}$	Set of matrices with m rows, n columns, and entries in $\mathbb{R}$
$x \in \mathcal{R}^n$	Real-valued column vector of dimension n
x_i	The i-th entry of the vector x
t	Continuous time-constant, real-valued
k	Discrete-time instant, integer-valued
$x(t)$	Continuous-time vector variable
x_k	Discrete-time vector variable
$y \in \mathcal{R}^q$	Real-valued column vector of dimension q
$y(t)$	Continuous-time vector variable
y_k	Discrete-time vector variable
$y(n)$	n-point sample vector variable
$u \in \mathcal{R}^p$	Real-valued column vector of dimension p
$z(t)$	Continuous-time vector variable
$w(t)$	Continuous-time vector variable
$E \in \mathcal{R}^{nxn}$	Descriptor matrix
$A \in \mathcal{R}^{nxn}$	System dynamics matrix
$B \in \mathcal{R}^{nxm}$	Control matrix
$C \in \mathcal{R}^{pxn}$	Sensor matrix
$D \in \mathcal{R}^{pxm}$	Direct term matrix
$E_d \in \mathcal{R}^{nxn}$	Discrete descriptor matrix
$A_d \in \mathcal{R}^{nxn}$	Discrete system dynamics matrix
$B_d \in \mathcal{R}^{nxm}$	Discrete control matrix
$C_d \in \mathcal{R}^{pxn}$	Discrete sensor matrix
$D_d \in \mathcal{R}^{pxm}$	Discrete direct term matrix
$E_N \in \mathcal{R}^{pxn}$	Null space of descriptor matrix E
$A_N \in \mathcal{R}^{nxn}$	Null space of dynamics matrix A
$B_N \in \mathcal{R}^{nxm}$	Null space of control matrix B
$C_N \in \mathcal{R}^{pxn}$	Null space of sensor matrix C
$D_N \in \mathcal{R}^{pxm}$	Null space of direct term matrix D

4.2 Laplace transform

Laplace transform is an integral transform which takes a function, f(t), and transforms it to a complex function F(s). Laplace transform is used to simplify calculations in systems described by large differential equations. The transform is an important part of process control where it is used to examine variables, behaviour and stability of a system [62].

The Laplace transform is mathematically defined as [32][5][34]:

$$F(s) = \int_0^\infty f(t)e^{-st}dt \tag{4.1}$$

where $s = \sigma + i\omega$, σ and ω are real numbers.

4.3 Sine-wave

A sine wave is a continuous mathematical curve that describes periodic oscillations. The wave is defined by an amplitude, frequency and a phase [61][53].

$$y(t) = Asin(2\pi ft + \varphi), \tag{4.2}$$

where $A = amplitude$, $f = frequency$, $t = time$ and $\varphi = phase$.

4.4 The Nyquist Theorem

This theorem is mention in this thesis since it represents an important aspect of digital signal processing.

The Nyquist theorem states that for an analogue-to-digital conversion of a signal, a true representation of the signal is ensured by using a sampling rate that is at least two times higher than the highest frequency occurring in the analogue signal [8][66].

Nyquist frequency:

$S = 2 \times f_{max}$

where S is sampling rate, and f_{max} is the highest occurring frequency in the analogue signal.

4.5 Runge-Kutta

Runge-Kutta is a method for numerically integrating ordinary differential equations [41][60].

The method is mathematically defined as:

$$y_{i+1}^h = y_i^h + h\sum_{j=0}^{m}\beta_j k_j,\ where\ k_j = f(x_i + \rho_j h, y_i^h + h\sum_{l=1}^{m}\gamma_{jl}k_l), \tag{4.3}$$

where m is number of stages, k_j is the number of slopes. The free parameters γ_{il}, ρ_j and β_j must be chosen so the discrete solution problem described in equation 4.3 converges towards a solution to the initial value problem [30].

A more widely used method is the classical Runge-Kutta 4 method which is one of the discretisation methods used in this thesis [27]:

$$y_{i+1}^h = y_i^h + \frac{h}{6}(k_1 + 2k_2 + 3k_3 + k_4) \tag{4.4}$$

$$k_1 = f(x_i, y_i^h) \tag{4.5}$$

$$k_2 = f(x_i + \frac{h}{2},\ y_i^h + \frac{h}{2}k_1) \tag{4.6}$$

$$k_3 = f(x_i + \frac{h}{2},\ y_i^h + \frac{h}{2}k_2) \tag{4.7}$$

$$k_4 = f(x_i + h,\ y_i^h + hk_3) \tag{4.8}$$

4.6 Euler's method

Euler's method is a numerical method to solve first order first degree differential equations with known initial values. The implementation of Euler's method used in this thesis is explicit.

A continuous-time state space model [5]:

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{4.9}$$

$$y(t) = Cx(t) + Du(t) \tag{4.10}$$

can be discretised, assuming each sample is sampled for one sample interval (zero-order-hold) [37]. The discrete state space representation of the continuous system is:

$$x_{[k+1]} = A_d x_{[k]} + B_d u_{[k]}, \tag{4.11}$$

$$y_{[k]} = C_d x_{[k]} + D_d u_{[k]}, \tag{4.12}$$

where x_{k+1} is the discrete solution of $x(t)$ and y_k is the discrete solution of $y(t)$.

An exact solution of the continuous state space representation can be created by using equation 4.13

$$x_{[k+1]} = e^{AT} x_{[k]} + A^{-1}(e^{AT} - I)Bu_{[k]}, \tag{4.13}$$

where T is the discretisation step and k is the discrete sample.

An easy and fast implementation of this method is to approximate a solution to the continuous state state space representation of the system as in equation 4.14 and 4.15.

$$e^{AT} \approx I + AT \tag{4.14}$$

$$x_{[k+1]} \approx (I + AT)x_{[k]} + TBu_{[k]} \tag{4.15}$$

4.7 Moving average filter

The moving average filter is commonly used to remove noise from a sampled signal.

The filter takes in n samples from an input vector x and estimates an average based on a windowsize , resulting in an output vector y. The windowsize determines how many samples the filter uses to average over, this results in a single point based on the average of the input vectors [39][1].

The moving average filter is mathematically defined as:

$$y(n) = \frac{1}{windowsize} \sum_{k=0}^{windowsize} x(n-k) \tag{4.16}$$

where $y(n)$ is the discrete output vector based on an average of the weighted sum of the input vectors, $x(n)$, determined by the windowsize.

4.8 Null space of a matrix

In this thesis the null space of a matrix is used to calculate an augmented attack generating system which produces a dynamic attack that remains undetected on the output of the system.

The null space of an $m \times n$ matrix A, is the set of all solutions to the homogeneous equation $Ax = 0$, $x \neq 0$ [9].

Mathematically defined as:

$Null(A) = \{x \in X | A(x) = 0\}$.

4.9 System modelling

This section describe the mathematical model used to simulate a dynamic power system with coupling between generators in the system.

4.9.1 System model

In control engineering the state space representation is a common way to describe the dynamics of a system based on a set of inputs, outputs and variables describing the state through first order differential equations.

The state space model used in this thesis is a descriptor state space model, which compared to ordinary state space models, contains an additional matrix E. By describing the system as a descriptor state space model, it is possible to perform undetectable dynamic attacks utilising the system transfer function.

State space representation of the PCU is given by the following equations describing the system development as $E\dot{x}(t)$ and the system measurements as y(t):

$$E\dot{x}(t) = Ax(t) + Bu(t) \tag{4.17}$$

$$y(t) = Cx(t) + Du(t), \tag{4.18}$$

where $E\dot{x}(t)$ describes the system development and $y(t)$ the output represented in continuous state space domain.

x: $\mathbb{R} \rightarrow \mathbb{R}^n$
y: $\mathbb{R} \rightarrow \mathbb{R}^p$

are the maps describing the evolution of the system state and measurements, and E, A, B, C and D are constant matrices.

Since E is allowed to be singular the following assumptions hold [46]:
Assumption 1 - The pair (E, A) is regular, that is, the determinant $det(sE - A)$ does not vanish identically.

Assumption 2 - The initial condition $x(0) \in \mathcal{R}^n$ is consistent, that is, the relation $(Ax(0) + Bu(0)) \in Im(E)$ holds.

Assumption 3 - The input signal u is smooth.

These assumptions ensures existence of a unique solution to the model.

The model is from the article *Control-Theoretic Methods for Cyberphysical Security* [46].

4.9.2 Attack model

An attack model is made using the same modelling principles as in section 4.9.

$$E_N\dot{z}(t) = A_N z(t) + B_N w(t) \tag{4.19}$$

$$u_{attack}(t) = C_N z(t) + D_N w(t), \tag{4.20}$$

where

z: $\mathbb{R} \to \mathbb{R}^n$
w: $\mathbb{R} \to \mathbb{R}^p$

$\dot{z}$ and u_{attack} are the state space realisation of the dynamic attack generator. A_N, B_N,C_N,D_N and E_N denote the null space matrices extracted from the system transfer function which is later described in section 5.7.

4.10 Observability

A system is observable if, for any possible sequence of state and control vectors, the present state can be determined in finite time using only the outputs [42][5]. Observability, in other words, describes whether the internal state variables of the system can be externally measured [11].

Observability is determined by:

$$\mathcal{O} = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ C^{n-1} \end{bmatrix} \tag{4.21}$$

where $\mathcal{O} \in \mathbb{R}^{pn \times n}$, $A \in \mathbb{R}^{n \times n}$ and $C \in \mathbb{R}^{p \times n}$.

Observability is an important property of a control system. If a system is observable, it is possible to determine the dynamics of the system based on the measured output.

4.11 Controllability

Controllability is an important property of a control system in terms of stabilising unstable systems by using feedback and/or optimal control.

Controllability is described as the controllers ability to arbitrary alter the functionality of the system plant in a specific way [11]. A system is controllable if and only if the system states can be changed by the system input.

For a discrete time linear state space system the controllability matrix can be described as:

$$\mathcal{C} = \begin{bmatrix} B & AB & A^2B & \dots & A^{n-1}B \end{bmatrix} \tag{4.22}$$

where $\mathcal{C} \in \mathbb{R}^{n \times mn}$ $A \in R^{n \times n}$ and $B \in R^{n \times m}$.

The system is controllable if the controllability matrix has full row rank (rank $\mathcal{C}$ = n). If the system is controllable, $\mathcal{C}$ will have n linearly independent columns. If these n columns of $\mathcal{C}$ are linearly independent, each n states are reachable by giving the system proper control inputs [12][5].

4.12 Controller

A PID controller (or PI controller) is one of the most common controller used in industrial applications and processes [26]. A PID controller is used in the discrete-time model and an PI-controller used in the continuous-time model.

$$u(t) = K_p e(t) + K_i \int_0^t e(t)dt + K_d \frac{de(t)}{dt} \tag{4.23}$$

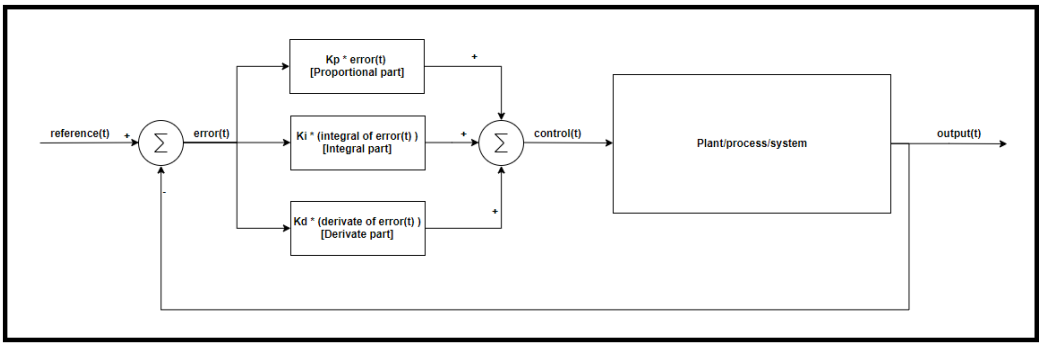

Figure 4.1: PID control calculation

A PID controller calculates control inputs based on the error, $e(t)$, of the past, present and previous state. $e(t)$ is the difference between desired setpoint and measured process state. Corrections to the process is made by adding a proportional gain K_p which is proportional to the error and compensates for the present error, a integral term K_i to compensate for past values and a derivative term K_d to compensate for future trends based on current rate of change [23][25][47]. K_p, K_i and K_d are parameters which are tunable. This enable the system to respond as required depending on the type of system which is controlled.

The PID controller use three control terms (proportional, integral and derivate) to apply accurate control to the system. See details in figure 4.1.

Chapter 5

Detailed methodology

This chapter explains in greater detail how relevant literature has been explored, which premises the PCU model is based on, how the mathematical model can be simulated in MATLAB, and how the results are evaluated.

The goal of the simulations is to determine if it is possible to perform cyberattacks on a cyber-physical system with coupling effects inherent to the system, forcing the disconnection of one or several transmission lines, and/or perform an undetectable cyberattack.

In this section two models will be described. The models use the same mathematical basis. The first model is represented in discrete-time. The second model is represented in continuous-time.

5.1 Literature search

Finding relevant literature by investigating IEEEs website - *the worlds largest technical professional organisation for advancements in technology*, in addition a wide internet search, for relevant topics about cyberattacks, control and industrial systems in substations and power grids.

5.2 Overall system

This section is used to illustrate how a digital substation may receive digital data originating from the transformers, apply active control to the system and feedback the resulting system state.

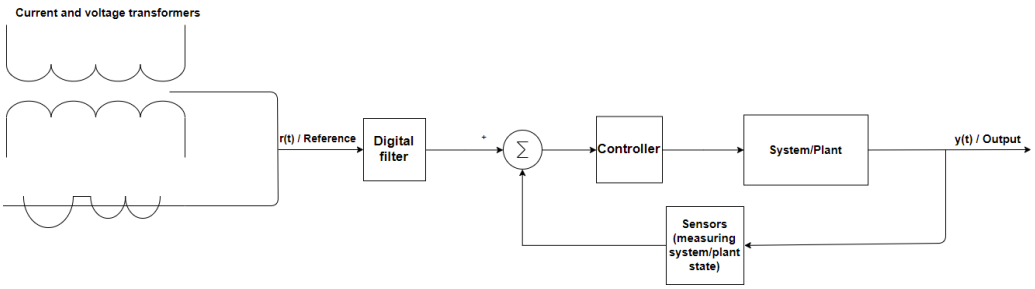

Figure 5.1: Block diagram of the overall system

The block diagram in figure 5.1 illustrate how measurements from the transformers are digitised and filtered. Once the measurements are digitised, they are fed into the system loop and active control is applied to the system using feedback from the output.

5.3 Modelling the states/inputs and the PCU

The following section introduce the reader to how the states and system is mathematically represented and modelled.

5.3.1 Representing the states current, voltage and busbar voltage

System states can be represented as sinusoidal waves as described in detail in section 5.8.1.

By using section 4.2, the input states/signals are simulated as sinusoidal waves using the following parameters:

- Amplitude
- Frequency
- Sampling frequency
- Sampling interval
- Offset
- Noise

5.3.2 Model of the PCU

A mathematical representation of the PCU is made using the Power Network and Attack example from *Control-Theoretic Methods for Cyberphysical Security* [46]. The next step is to illustrate how the model from [46] can be transformed into a mass-spring-damper system which forms the basis of the simulations in MATLAB.

The system model used in [46] (equation 5.2) can be represented as a mass-spring-damper system as shown from equation 5.3 to 5.13.

The Laplacian matrix in equation 5.1 describes the relations between generators and load buses associated with the system.

$$\mathcal{L} = \begin{bmatrix} L_{gg} & L_{gl} \\ L_{lg} & L_{ll} \end{bmatrix} \tag{5.1}$$

The dynamic model of the power network and hence the PCU is modelled as in equation 5.2.

$$\begin{bmatrix} I & 0 & 0 \\ 0 & M_g & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = - \begin{bmatrix} 0 & -I & 0 \\ L_{gg} & D_g & L_{gl} \\ L_{lg} & 0 & L_{ll} \end{bmatrix} \begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ P_\omega \\ P_\theta \end{bmatrix} \tag{5.2}$$

The left side of equation 5.2 is E$\dot{x}$ and the right side is $Ax(t) + F$, where F is a constant known change in the mechanical input power to the generators or real power demand at the loads. In this thesis $F = Bu(t)$.

$$\dot{\delta} = \omega \tag{5.3}$$

$$M_g\dot{\omega} = -L_{gg}\delta - D_g\omega - L_{gl}\theta + P\omega \tag{5.4}$$

$$0 = -L_{lg}\delta - L_{ll}\theta + P_\theta \tag{5.5}$$

θ can be expressed from equation 5.5 as:

$$\theta = L_{ll}^{-1}(-L_{lg}\delta + P_\theta) \tag{5.6}$$

By setting

$$\ddot{\delta} = \dot{\omega}, \tag{5.7}$$

the model can be described as a mass-spring-damper system:

$$M_g\ddot{\delta} = -L_{gg}\delta - D_g\dot{\delta} - L_{gl}\theta + P\omega, \tag{5.8}$$

yields

$$M_g\ddot{\delta} + D_g\dot{\delta} + L_{gg}\delta = P_\omega - L_{gl}\theta, \tag{5.9}$$

Substituting θ with equation 5.6 yields:

$$M_g\ddot{\delta} + D_g\dot{\delta} + L_{gg}\delta = P_\omega - L_{gl}(-L_{ll}^{-1}L_{lg}\delta + L_{ll}^{-1}P_\omega) \tag{5.10}$$

$$M_g\ddot{\delta} + D_g\dot{\delta} + L_{gg}\delta + \delta(L_{gg} - L_{gl}L_{ll}^{-1}L_{lg}) = P_\omega + L_{ll}^{-1}P_\omega, \tag{5.11}$$

Assuming that:

$$L_{gg} - L_{gl}L_{ll}^{-1}L_{lg} < 0 \tag{5.12}$$

Equation 5.11 can be written on a more general mass-spring-damper form:

$$m\ddot{\delta} + b\dot{\delta} + k\delta = F(t) \tag{5.13}$$

where

m = mass,
b = damping and
k = spring constant.

Substituting δ with x yields the familiar mass-spring-damper representation of the system.

$$m\ddot{x} + b\dot{x} + kx = F(t), \tag{5.14}$$

where

m = mass,
b = damping,
k = spring constant,
x = position and
F = force.

Constructing the dynamics matrix, A, based on equation 5.2 as:

$$A = -\begin{bmatrix} 0 & -I & 0 \\ L_{gg} & D_g & L_{gl} \\ L_{lg} & 0 & L_{ll} \end{bmatrix} \tag{5.15}$$

5.4 Discrete-time model

The state space representation of this model is simulated in discrete-time domain. The following matrices originates from [46].

Representing matrices E, A and B based on L_{gg}, L_{gl}, L_{ll} and L_{lg} which describes relationship between generators and the load buses.

$$L_{gg} = \begin{bmatrix} 0.580 & 0 & 0 \\ 0 & 0.0630 & 0 \\ 0 & 0 & 0.0590 \end{bmatrix} \tag{5.16}$$

$$L_{gl} = \begin{bmatrix} -0.0580 & 0 & 0 & 0 & 0 & 0 \\ 0 & -0.0630 & 0 & 0 & 0 & 0 \\ 0 & 0 & -0.0590 & 0 & 0 & 0 \end{bmatrix} \tag{5.17}$$

$$L_{ll} = \begin{bmatrix} 0.2350 & 0 & 0 & -0.0850 & -0.0920 & 0 \\ 0 & 0.2960 & 0 & -0.1610 & 0 & -0.0720 \\ 0 & 0 & 0.3300 & 0 & -0.1700 & -0.1010 \\ -0.0085 & -0.1610 & 0 & 0.2460 & 0 & 0 \\ -0.0920 & 0 & -0.1700 & 0 & 0.2460 & 0 \\ 0 & -0.0720 & -0.1010 & 0 & 0 & 0.1730 \end{bmatrix} \tag{5.18}$$

$$Llg = \begin{bmatrix} -0.0580 & 0 & 0 \\ 0 & -0.0630 & 0 \\ 0 & 0 & -0.0590 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{5.19}$$

$$Dg = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \tag{5.20}$$

where Dg is the system damping coefficients and

$$Mg = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}, \tag{5.21}$$

where Mg describes the system mass coefficients.

Equations 5.16 to 5.19 is originates from [46].

Inserting the matrices in equation 5.15 to obtain the dynamics matrix A which describes the system dynamics (equation 5.22).

$$A = \begin{bmatrix} 0 & 0 & 0 & -1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1.0000 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.0580 & 0 & 0 & 2.0000 & 0 & 0 & -0.0580 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.0630 & 0 & 0 & 2.0000 & 0 & 0 & -0.0630 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.0590 & 0 & 0 & 2.0000 & 0 & 0 & -0.5900 & 0 & 0 & 0 \\ -0.0580 & 0 & 0 & 0 & 0 & 0 & 0.2350 & 0 & 0 & -0.00850 & -0.0920 & 0 \\ 0 & -0.0630 & 0 & 0 & 0 & 0 & 0 & 0.2960 & 0 & -0.01610 & 0 & -0.0720 \\ 0 & 0 & -0.0590 & 0 & 0 & 0 & 0 & 0 & 0.3300 & 0 & -0.1700 & -1010 \\ 0 & 0 & 0 & 0 & 0 & 0 & -0.0850 & -0.1610 & 0 & 0.2460 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -0.0920 & 0 & -0.1700 & 0 & 0.2620 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.0720 & -0.1010 & 0 & 0 & 0.1730 \end{bmatrix} \tag{5.22}$$

Next step is to find an expression for the descriptor matrix E. This is done by inserting equation 5.21 and an identity matrix (size 3×3) in the left side of equation 5.2. This results in equation 5.23

$$E = \begin{bmatrix} 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.23}$$

The next step is to approximate a solution to the set of differential equations by using Euler's method as described in section 4.6.

$$A_d = \begin{bmatrix} 1.0000 & 0 & 0 & 0.0100 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.0000 & 0 & 0 & 0.0100 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1.0000 & 0 & 0 & 0.0100 & 0 & 0 & 0 & 0 & 0 & 0 \\ -0.0006 & 0 & 0 & 0.9800 & 0 & 0 & 0.0006 & 0 & 0 & 0 & 0 & 0 \\ 0 & -0.0006 & 0 & 0 & 0.9800 & 0 & 0 & 0.0006 & 0 & 0 & 0 & 0 \\ 0 & 0 & -0.0006 & 0 & 0 & 0.9800 & 0 & 0 & 0.00059 & 0 & 0 & 0 \\ 0.0006 & 0 & 0 & 0 & 0 & 0 & 0.9977 & 0 & 0 & 0.0009 & 0.0009 & 0 \\ 0 & 0.0006 & 0 & 0 & 0 & 0 & 0 & 0.9977 & 0 & 0.0016 & 0 & 0.0007 \\ 0 & 0 & 0.0006 & 0 & 0 & 0 & 0 & 0 & 0.9967 & 0 & 0.0017 & 0.0010 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.0009 & 0.0016 & 0 & 0.9978 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.0009 & 0 & 0.0017 & 0 & 0.9974 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0007 & 0.0010 & 0 & 0 & 0.9983 \end{bmatrix}, \tag{5.24}$$

where A_d is the discretised state space representation of the continuous state space matrix A.

$$B_d = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.0100 & 0 & 0 \\ 0 & 0.0100 & 0 \\ 0 & 0 & 0.0100 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{5.25}$$

where B_d is the discretised state space representation of the continuous state space matrix B.

$$C_d = \begin{bmatrix} 0.01 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{5.26}$$

where C_d is the discrete-time sensor matrix.

The next step is to calculate the discrete state development of the continuous state space representation, $E\dot{x}(t)$, using equations 5.27 and 5.28.

$$E_d x_{k+1} = A_d x(k) + B_d u(k), \tag{5.27}$$

$$y_{k+1} = C_d x(k) + D_d u(t) \tag{5.28}$$

where $x(k)$ describes the states of the mass-spring-damper system and $u(k)$ the control input. y_{k+1} is the discrete-time output and $D_d = 0$.

5.5 Continuous-time model

The state space representation of this model is simulated using continuous-time domain state space representation.

The matrices describing the generators and the buses are the same as the ones used in the discrete-time model. However, E and Mg are different since the continuous-time model is represented in a continuous time domain.

Representing the implicit matrix E and the matrix containing the masses, Mg as:

$$E = \begin{bmatrix} 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1.0000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.1250 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.0340 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.0160 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.29}$$

$$Mg = \begin{bmatrix} 0.1250 & 0 & 0 \\ 0 & 0.0340 & 0 \\ 0 & 0 & 0.0160 \end{bmatrix} \tag{5.30}$$

5.6 Digraph associated with the continuous-time and discrete-time model

A digraph is a convenient way to represent how the network is connected and is based on the system dynamic matrix A. The digraph eases the understanding of how the cyberattacks transplants throughout the system. Figure 5.2 is the digraph associated with the network model. The red arrows indicates one of the many paths in the system.

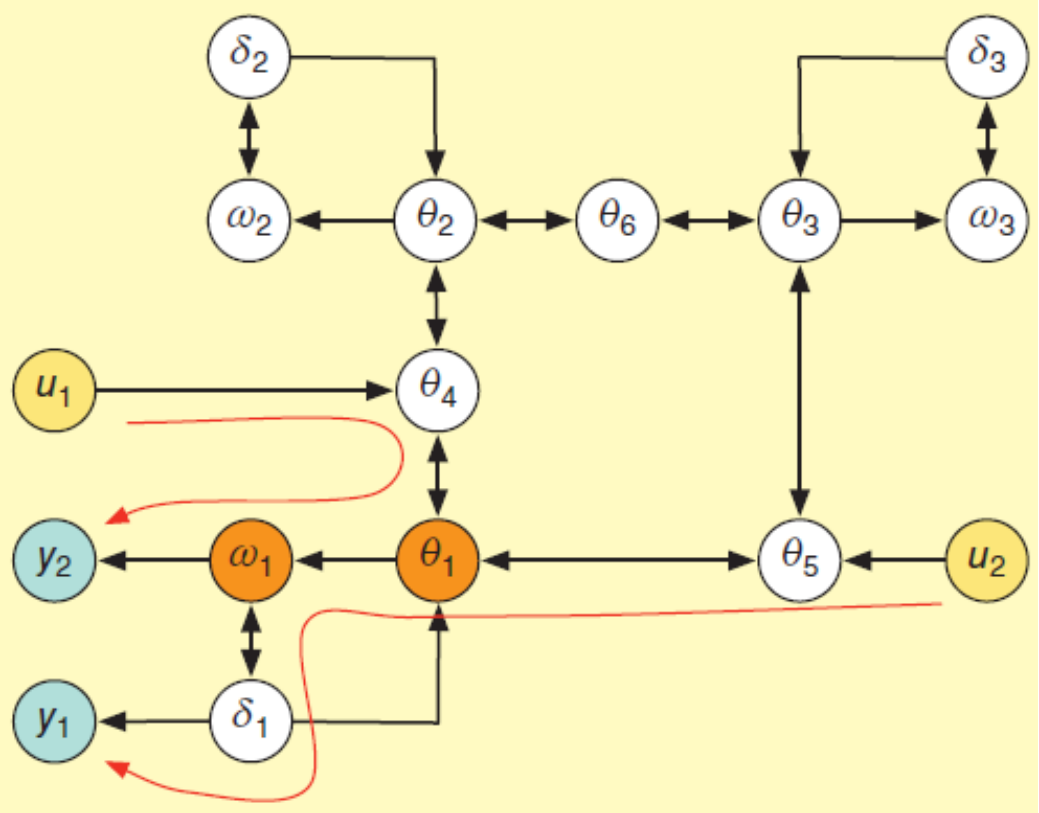

Figure 5.2: Digraph of the discrete-time and continuous-time model. The digraph shows one of the paths the attacks *u1* and *u2* can transplant throughout the system and the point of attack [46].

5.7 Attack generator used for both the continuous-time case and the discrete-time-case

An attack generator is implemented based on section 4.9.2. To simulate the attack generator, the matrices that describe the dynamics of the attack generator has to be extracted based on the model transfer function.

The interested reader is referred to the following papers on how to tackle the problem of output invisible signals; [70], [52], [14] and [28]. The latter paper describes a possible strategy to prevent undetectable attacks.

To simulate how dynamic attacks affect the overall system model, the first step is to find an expression of the system model transfer function, $H(s)$.

By using equation 4.17 and 4.18 from section 4.9.1 and performing a Laplace transform yields:

$$EsX(s) - x(0) = AX(s) - BU(s) \tag{5.31}$$

where the initial condition for $x(0) = 0$.

$$BU(s) = AX(s) - sEX(s) \tag{5.32}$$

$$BU(s) = (A - sE)X(s) \tag{5.33}$$

$$X(s) = (A - sE)^{-1}BU(s) \tag{5.34}$$

Inserting 5.34 in the Laplace transformed version of equation 4.18 and setting $D = 0$, yields the following transfer function:

$$H(s) = C(A - sE)^{-1}B \tag{5.35}$$

which is represented in Laplace domain.

Having obtained the transfer function, the next step is to calculate a function based on the null space of the transfer function,
$N(s) = null(H(s))$.

Then a function $D(s)$ is created, with higher order than $H(s)$, to ensure a proper rational function, and a physically stable and realisable system [37].

$$Attack\ generator\ dynamics = \frac{N(s)}{D(s)} \tag{5.36}$$

Retrieve the descriptor state space model based on the attack generator by utilising the relationship which is described in equation 5.36.

Finally, a dynamic attack model is expressed based on section 4.9.2 and attacks are injected by adding the output of the attack model to the control input to the original system.

5.8 Simulation in MATLAB

This section describes how the mathematical modelling were implemented in MATLAB. In addition, how the signals current, voltage and busbar voltage are simulated and what parameter values which is used.

5.8.1 Current, voltage and busbar voltage as states/inputs

States/inputs are simulated based on section 4.3 with parameters and values listed in table 5.1.

Parameter	Amplitude	Frequency (Hz)	Sampling frequency (Hz)	Sampling interval	Offset
Current	2	50	250	0 to 125001	3000
Voltage	.5	50	250	0 to 125001	300
Busbar voltage	.4	300	250	0 to 125001	300

Table 5.1: Parameters and values used to simulate sinusoidal signals

The simulated values are filtered using a digital filter as described in section 4.16 with a windowsize of 50.

The digitally filtered samples are stored in a vector (DSV).

5.8.2 Model

The model is simulated using the equations and matrices in section 5.3.2. Development of the system is simulated by estimating a control input based on the present state, present time, time step ($\triangle t$) and desired setpoint.

The system development is stored in an output matrix, $y(t)$.

5.8.3 Control of the system

The controller used on the discrete-time system is a PID controller. The controller used on the continuous-time system is a PI controller. Detail of the controller is in section 4.12. The gains Kp, Ki and Kd used the PID controller are listed in table 5.2. The PI controller use the same values as the PID, but the derivative term is removed.

In addition to estimate control inputs for each state, an integral term is calculated which contributes to the overall control input used to drive the discrete-time model to the desired setpoint.

The total error, hence the control input, is calculated based on the control model described in section 4.12.

Parameter		**Kp**	**Ki**	**Kd**
States	**Current**	5	3	3
	Voltage	5	3	3
	Busbar voltage	5	3	3

Table 5.2: Parameters and values used in the PID controller

Table 5.2 contains the values used for the different gain factors in the controller. The gains used in the controller are tuned by first choosing a value for Kp, then adjust the value for Ki and finally adjust the value for Kd.

Part II

Results

Chapter 6

Results

This chapter introduce the reader to the resulting simulation of the system based on the theory and methods described in the previous sections. A description of how the results were obtained is given, before illustrating the resulting system response both with and without attacks present in the system.

The results are presented in the following order:

Flowchart of the MATLAB code

Generation and simulation of simulated transformer signals

Digital filtering of the transformer signals

Model response simulation both with and without present attacks

6.1 Flowchart of the MATLAB code

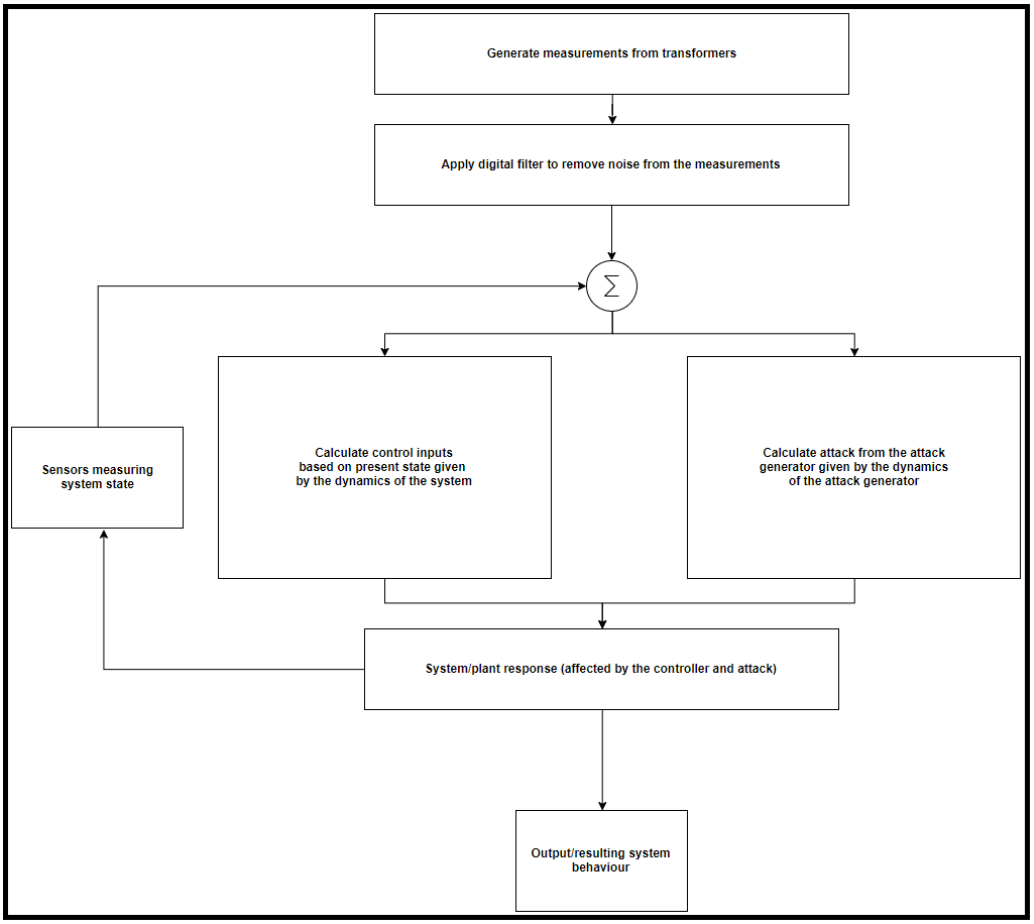

Figure 6.1: Flowchart describing the MATLAB code

Figure 6.1 illustrates how the MATLAB code generates simulated measurements, applies a digital filtering step on the measurements, calculates the state development of the system, and calculates the attack value for the present state using the attack generating model. The state measurements are subtracted from the digitally filtered measurements. This summation is used in the controller to apply accurate control of the system.

6.2 Digital sample values

Digital Sample Values (DSV) are implemented in MATLAB. These values represent current, voltage and busbar voltage as input signals/states to the system. DSV are the digitised states measured by the transformers measuring the present state of the transmission lines.

Generating states for the signals is done by choosing appropriate amplitude, frequency, sampling frequency, offset and a sampling interval. In addition an expression for noise occurring in the states is added by using MATLAB's random number generator. The parameters and values used to simulate current is described in table 6.1.

Next, a moving average filter is implemented as shown in listing 6.1. The filter is used to eliminate noise from the measurements.

Listing 6.1: Moving Average function

```
1  %% FILTERING
2  function y = digital_filter(x,windowsize)
3  %{
4  x: samples to average
5  windowsize: how many samples to average over at each
       time
6  y: vector of averaged elements
7  %}
8
9  N = length(x);
10 averaged = ones(1,length(N));
11 %total_sum = 0;
12
13 for L = 1:(N-windowsize)
14
15 total_sum = sum(x(L:L+windowsize-1));
16 averaged(L) = (1/windowsize)*total_sum;
17 %total_sum = 0;
18
19 end
20 y = averaged;
21 end
```

6.2.1 Simulating current

Parameter and values used to simulate current	
Amplitude	2
Frequency	50 Hz
Sampling frequency	250 Hz
Time step, dt	0.01
Sampling interval	[0:dt:500]
Offset	3000
Noise	8*(random number)

Table 6.1: Parameters and values used to simulate current

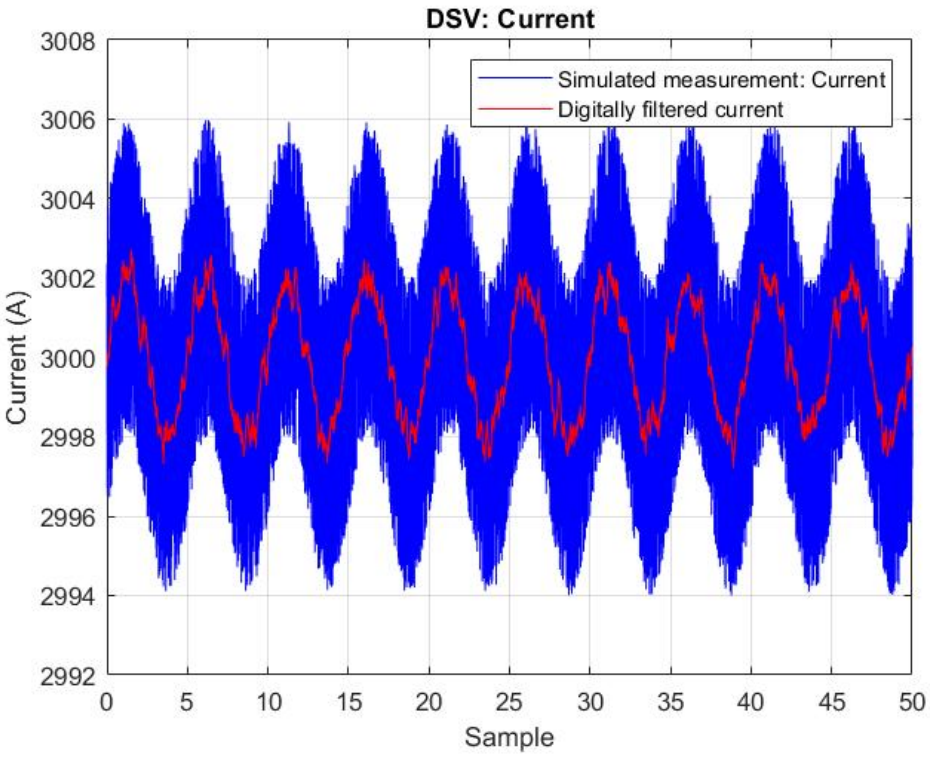

Figure 6.2: DSV: Current simulated in MATLAB

The resulting simulated current originating from the current transformer is shown in figure 6.2. The blue graph illustrates simulated unfiltered measurements originating from current transformers. By filtering the unfiltered data using the digital moving average filter one obtains the red graph. The red graph represents the same states, but with a high degree of noise reduction. As seen in figure 6.2, the filtered signal captures trends and behaviour of the unfiltered measurements and removes noise as intended.

6.2.2 Simulating voltage

Parameter and values used to simulate voltage	
Amplitude	.5
Frequency	50 Hz
Sampling frequency	250 Hz
Time step, dt	0.01
Sampling interval	[0:dt:500]
Offset	300
Noise	.2*(random number)

Table 6.2: Parameters and values used to simulate voltage

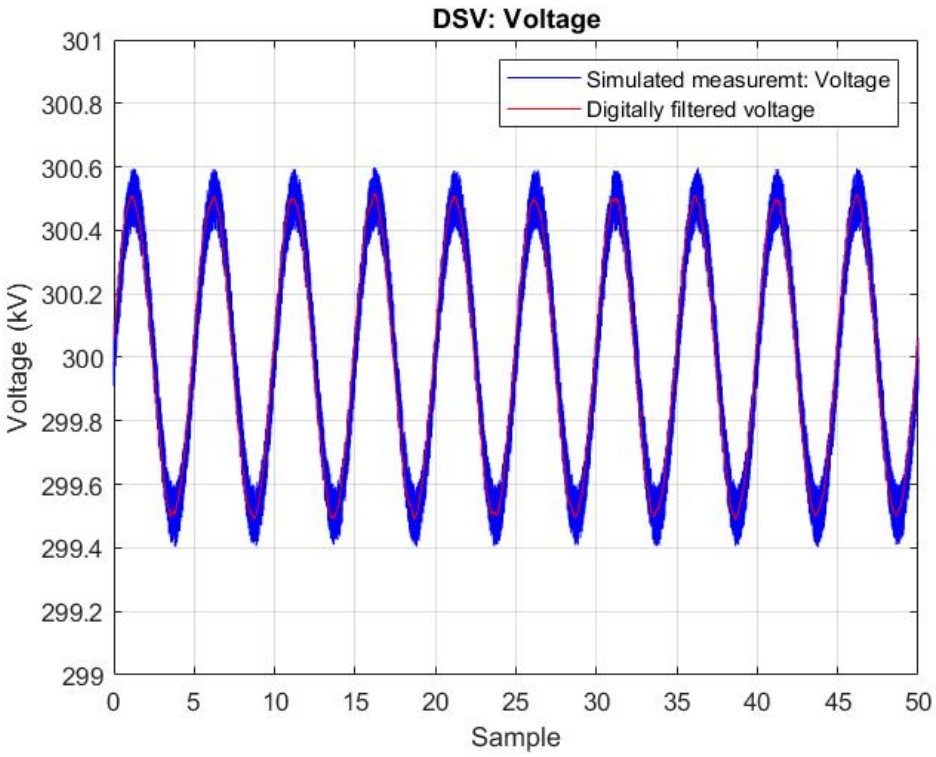

Figure 6.3: DSV: Voltage simulated in MATLAB

The resulting simulated voltage from the voltage transformer is shown in figure 6.3. The blue graph illustrates simulated unfiltered measurements originating from voltage transformers. Applying the digital moving average filter on the measurements to remove noise results in the filtered red graph. The digitally filtered data captures the trends of the measurements and removes noise as intended. Notice that by choosing smaller noise element amplitude the signal becomes less noisy compared to the simulated current.

6.2.3 Simulating busbar voltage

Parameter and values used to simulate busbar voltage	
Amplitude	.4
Frequency	50 Hz
Sampling frequency	250 Hz
Time step, dt	0.01
Sampling interval	[0:dt:500]
Offset	3000
Noise	.39*(random number)

Table 6.3: Parameters and values used to simulate busbar voltage

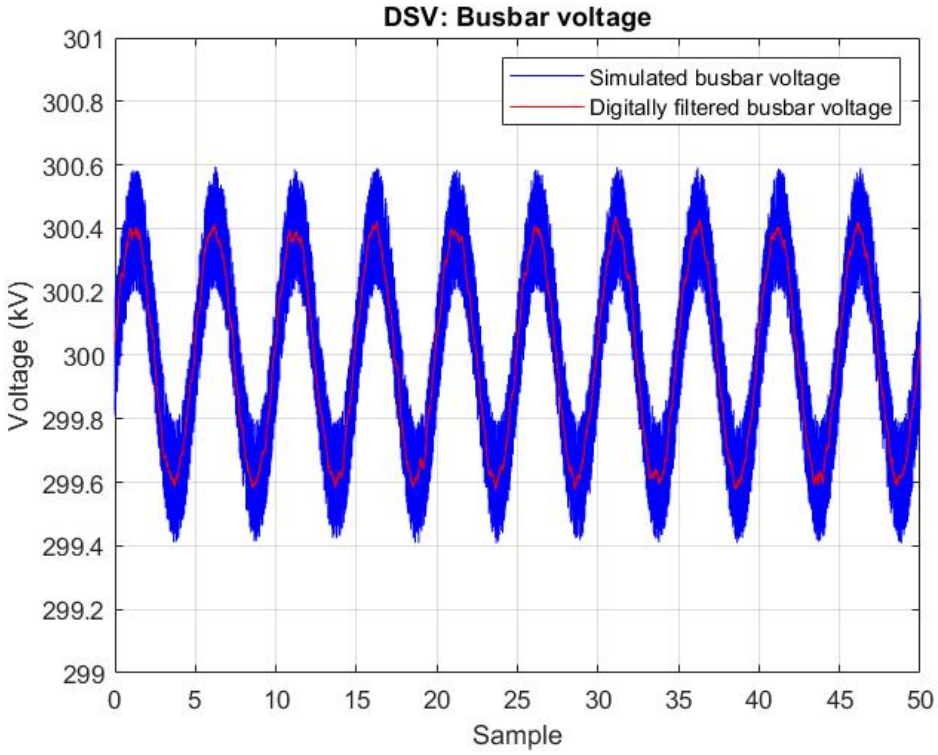

Figure 6.4: DSV: Busbar voltage simulated in MATLAB

The resulting simulated busbar voltage originating from the voltage transformers is shown in figure 6.4. The blue graph illustrates simulated unfiltered measurements measured by voltage transformers. Applying the moving average filter on the measurements results in the red graph. Again the digitally filtered data captures the trends and removes noise as expected. Notice that the simulated busbar voltage has a larger noise element than the simulated voltage.

6.3 Simulating the discrete-time model

The following section describe how the system development is simulated and the resulting response with and without a present cyberattack. This state space model is simulated in discrete-time domain.

First step to simulate the model is to create a function which is used to estimate the development of the state. The function calculates the development based on the matrices A, B, C, D, E, a time step ($\triangle t$), present state and the calculated control inputs from the previous state. The resulting function is illustrated in listing 6.2.

Listing 6.2: Function to simulate state development, discrete-time model

```
1  %% STATEDOT WITH CONTROLLER
2  %STATEDOT with controller
3  function [StateDotControl,z_dot] =
       Derivates_with_control(A,B,C,E, timestep,State,
       ucontrol,time,A_N,B_N,C_N,D_N,E_N,z_state,w)
4      z_dot = A_N*z_state + B_N*w;
5      z_attack = C_N*z_state + D_N*w;
6      P = (eye(12)-A*timestep);
7      R = timestep*B;
8      StateDotControl = P*State + R*(ucontrol+z_attack);
9
10     P = E*P;
11     R = E*R;
12 end
```

A function for simulating development of states without controller is made in a similar way, but with an external force driving the system instead of a PID controller. The resulting function is illustrated in listing 6.3.

The external force used to drive the system is randomly chosen and is based on equation 5.2, random values are chosen as seen in equation 6.1.

$$F_{external} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1.0000 \\ 1.0000 \\ 1.0000 \\ 0 \\ -0.5440 \\ 0 \\ -0.5440 \\ 0 \\ -0.5440 \end{bmatrix}. \tag{6.1}$$

Listing 6.3: Function to simulate state development driven by constant external force, discrete-time model

```
%% STATEDOT withOUT controller
function StateDot = Derivates(A,B,C,E,timestep,State,
    F_external,time)
    P = (eye(12)-A*timestep);
    %F_external is a constant vector with random
        values
    R = timestep*F_external;
    StateDot = P*State + F_external;
    A = E*A;
end
```

Control inputs to the system are calculated based on a PID controller as described in section 4.12.

Listing 6.4: Function to estimate control inputs, discrete-time model

```
%% CONTROLLER
function [ucontrol,integral] = Control(State,dt,
    setpoint, integral)
kp_value = 5;
kd_value = 3;
ki_value = 3;
%Initial values
Kp = [kp_value,      0,              0;
       0,            kp_value,       0;
       0,            0,              kp_value];
Ki = [ki_value,      0,              0;
       0,            ki_value,       0;
       0,            0,              ki_value];
Kd = [kd_value,      0,              0;
       0,            kd_value,       0;
       0,            0,              kd_value];

  %Kp error
error = setpoint(1:3) - State(1:3);
%Ki error
deriverror = setpoint(4:6) - State(4:6);
%Ki error
integral = integral + dt*error;
%Resulting control input
ucontrol = Kp*error + Kd*deriverror + Ki*integral;
end
```

A control input is calculated based on the present state and desired setpoint. The controller takes into account past, present and future development of the states. The elements are multiplied by their respective gain factor and summed to yield a control input to the system, as described in section 4.12 and listing 6.4.

6.3.1 Implementing Runge-Kutta 4 in MATLAB

One of the methods used to solve ordinary differential equations in this thesis is Runge-Kutta 4 (RK4). To simulate system development in MATLAB using RK4, the constants k_1 to k_4 has to be expressed as a function of present state, present time, time step ($\triangle t$) and desired setpoint based on the theory from section 4.5. Further details of the MATLAB calculation is described in listing 6.5.

Listing 6.5: For-loop to estimate state development using RK4, discrete-time model

```
for idx=1:length(time)
    disp(['Simulationstep ',num2str(time(idx)/tfinal
        *100)])
    %Step 1
    u1 = Control(State,time(idx),dt,setpoint);
    k1 = Derivates(State,u1);
    %Step 2
    u2 = Control(State+k1*timestep/2,time(idx)+
        timestep/2,dt,setpoint);
    k2 = Derivates(State+k1*timestep/2,u2);
    %Step 3
    u3 = Control(State+k2*timestep/2,time(idx)+
        timestep/2,dt,setpoint);
    k3 = Derivates(State+k2*timestep/2,u3);
    %Step 4
    u4 = Control(State+k3*timestep/2,time(idx)+
        timestep/2,dt,setpoint);
    k4 = Derivates(State+k3*timestep/2,u4);
    %next estimated state
    next_value = 1/6*(k1 + 2*k3 + 3*k3 + k4); %Her er
        det noe RUSK!
    State = State + next_value*timestep;
end
```

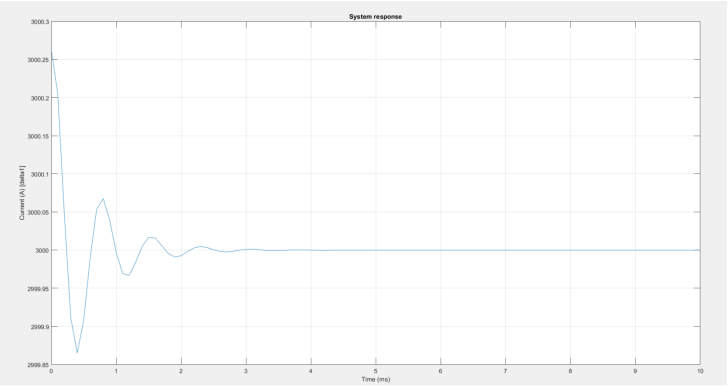

Figure 6.5: System response: RK4, current, delta1

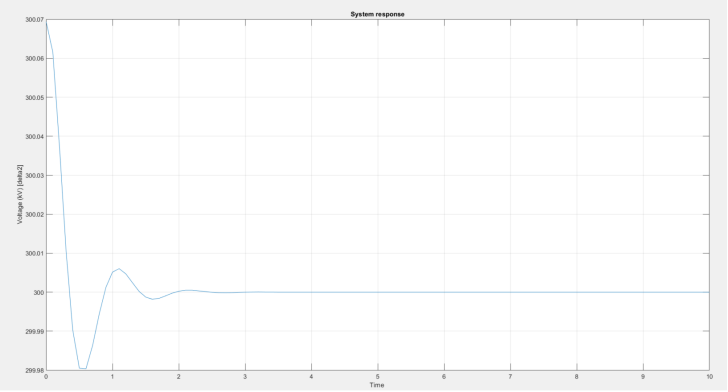

Figure 6.6: System response: RK4, voltage, delta2

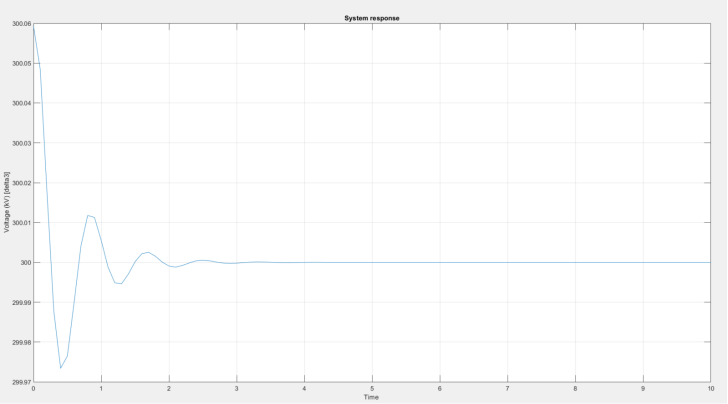

Figure 6.7: System response: RK4, busbar voltage, delta3

Simulation of system response using RK4 and a PID controller is shown in figure 6.7, 6.5 and 6.6. As shown in the figures the controller drives the system to the desired setpoint. The system remains stable.

6.3.2 Implementing Euler's method in MATLAB

One preferred method to iteratively solve differential equations describing a continuous system is Euler's method. Implementing an approximate discrete model using Euler's method in MATLAB is more straightforward than using RK4. To approximate a solution in MATLAB based on Euler's method as described in section 4.6, a time step T and an identity matrix I (same size as the size of A), are implemented in MATLAB. Details of implementation is described in listing 6.2 and 6.6. In addition, initial values for state, control, integral and setpoint have to be chosen.

Listing 6.6: For-loop to estimate state development using Euler's method, discrete-time model

```
1 for idx=1:length(time)
2
3     %Calculate control input
4     [u,integral] = Control(State,dt,setpoint,integral)
          ;
5
6     %Calcualte nexte State and attack generator state
7     [State,z_state] = Derivates_with_control(A,B,C,E,
          dt,State,u,time(idx),A_N,B_N,C_N,D_N,E_N,
          z_state,w);
8 end
```

6.3.3 No cyberattack present in the discrete-time model

Plotting the system response yields a stable system when there is no present cyberattack. The resulting system response is shown in figure 6.8 and 6.9. The generators delta1, delta2 and delta3 representing current, voltage and busbar voltage stabilise at the desired setpoints, driven by the PID controller.

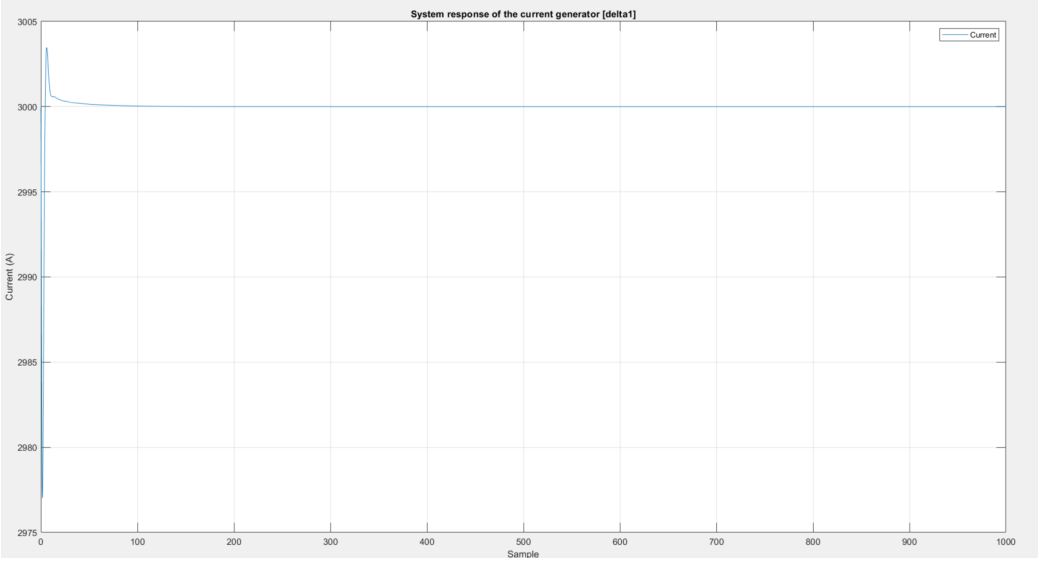

Figure 6.8: System response: No attack on the current generator, delta1

Figure 6.8 shows how the generator for current, delta1, is driven to desired setpoint. The control action results in an overshoot before the generator stabilises.

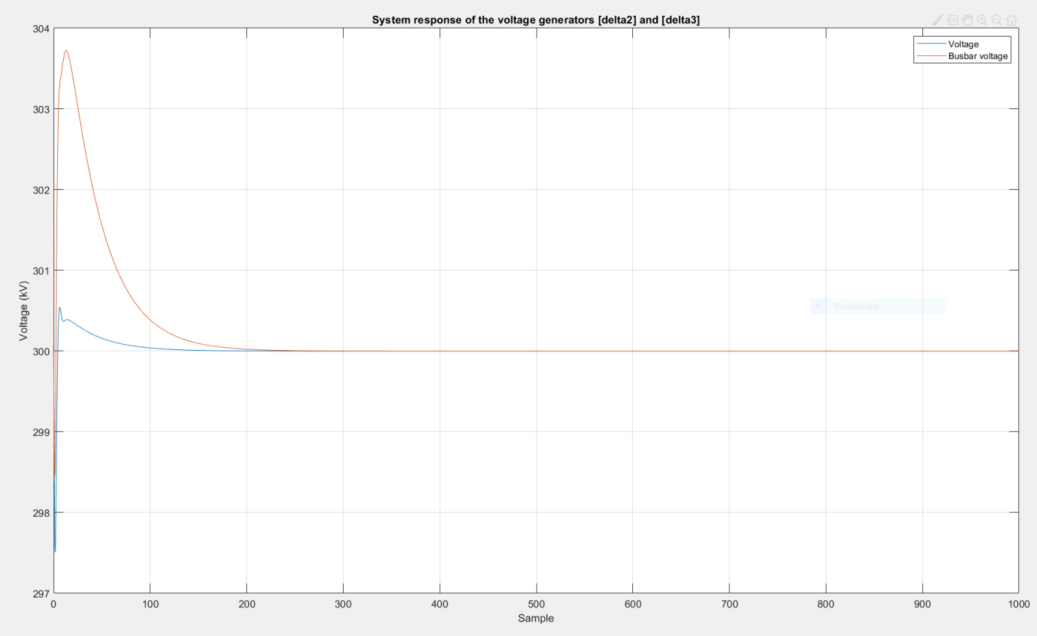

Figure 6.9: System response: No attack on the voltage generators, delta2 and delta3

Figure 6.9 shows how the generators for voltage, delta2 and delta3, are driven to desired setpoint. The control action applied on the voltage generator results in a small overshoot and oscillations before the generator stabilise. The control action applied to the busbar voltage generator results in a larger overshoot before the generators stabilise.

6.3.4 Discrete-time model driven by external force

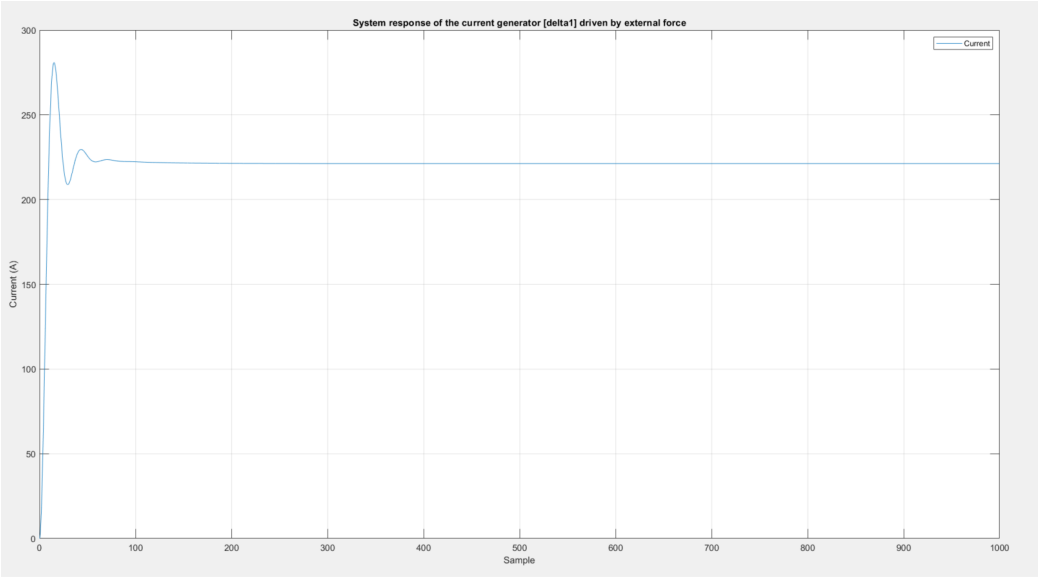

Figure 6.10: System response: The generator for current, delta1, driven by external force

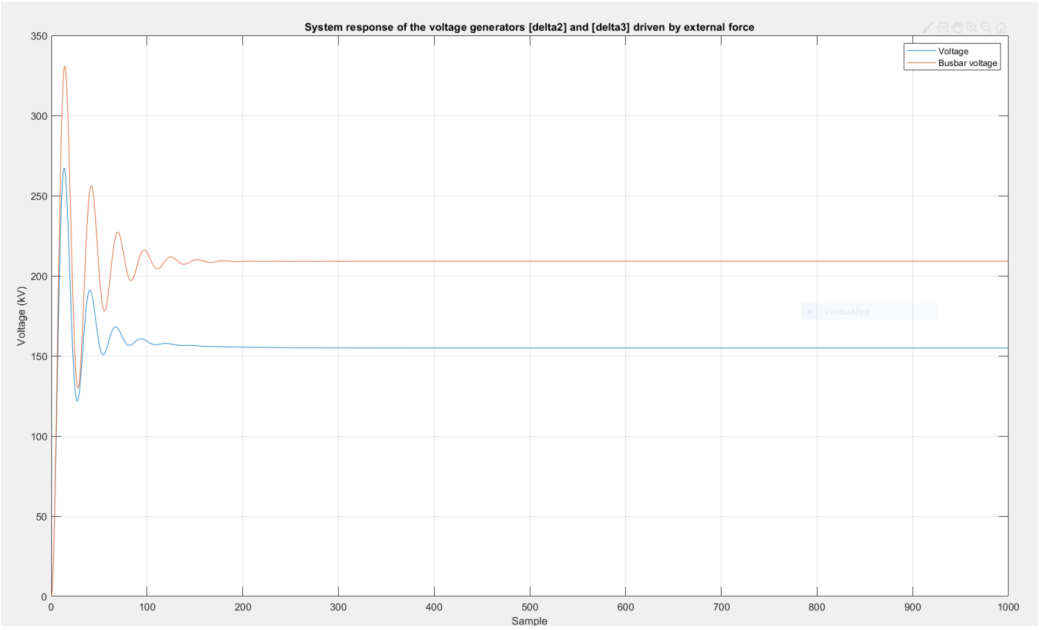

Figure 6.11: System response: The generators for voltage, delta2 and delta3, driven by external force

By applying a randomly chosen constant force to the system it is shown in figure 6.10 and 6.11 that the generators stabilise as expected.

6.3.5 Cyberattack present in the discrete-time model

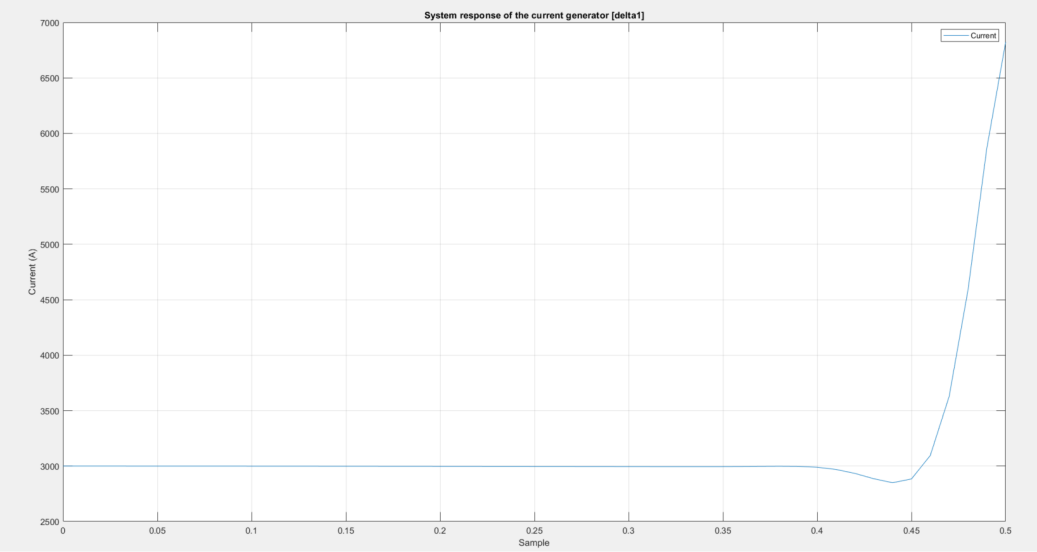

Figure 6.12: Cyberattack present in the generator for current, delta1

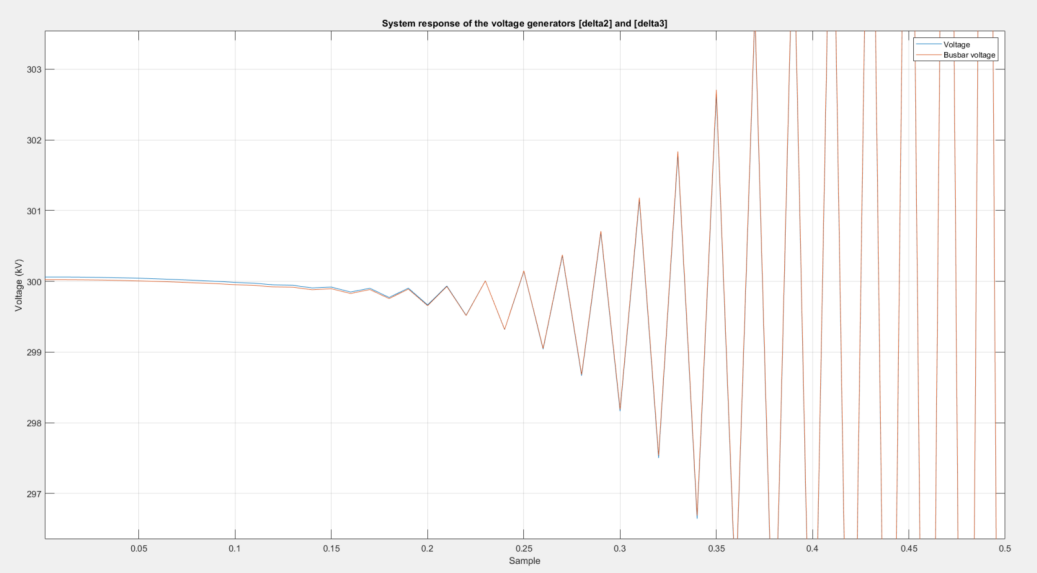

Figure 6.13: Cyberattack present in the generators for voltage, delta2 and delta3

Attacking the system with the augmented attack generating model makes the generators unstable as seen in figure 6.12 and 6.13. The three generators generating current, voltage and busbar voltage are driven unstable. Notice the how rapidly the system is driven unstable.

6.3.6 Observability and controllability

This section describes whether the discrete-time model is observable and controllable or not as described in section 4.10 and 4.11.

The discrete-time model is both controllable and observable since the control matrix $\mathcal{C}$ and the observability matrix $\mathcal{O}$ has full rank n.

6.4 Simulating the continuous-time model

The following section describe how system development is simulated with and without a present cyberattack. This state space model is simulated in continuous-time domain.

Listing 6.7: Function used in MATLAB's ODESolver to estimate the state development of the continuous system

```
function [dxdt, integral] = ODEsolver(t, x, A, B, C, D
    , E, A_N, B_N, C_N, D_N, E_N, dT,K,integral)
    %states of system
    x_state = x(1:12);
    %States of attack generator system
    z_state = x(12+1:end);
    %Setpoint for control
    setpoint = [3000 300 300 0,0,0,0,0,0,0,0]';
    %% Proportional controller
    %Controller u = -Kx
    u = -K*(x_state - setpoint);

    %Attack constant w
    w = [-1 -1]';

    %Attack-generating system
    dz_state = A_N*z_state + B_N*w;
    attack = C_N*z_state + D_N*w;

    %Change attack to attacking delta 2 and 3 instead
%     temp = attack;
%     attack(1) = temp(2);
%     attack(2) = temp(1);
%     attack(3) = temp(1);
    %Include the descriptor matrix E
    dz_state = E_N*dz_state;

    %Output state
    dx_state = -A*x_state+B*(u + attack);
    %Include the descriptor matrix E
    dx_state = E*dx_state;
    %Output
    dxdt = [dx_state; dz_state];
end
```

Listing 6.8: Function ODE45 used to estimate state development for the continuous-time model

```
%Initial states and values
State = zeros(12,1);
z_state = zeros(4,1);
ucontrol = zeros(3,1);
integral = [0,0,0]';
w = [0 0]';
K = [100 50 70 0 0 0 0 0 0 0 0 0]';
t_span = [0 30];
dT = 0.01;
x0 = [DSV(1) DSV(2) DSV(3) 0,0,0,0,0,0,0,0,0, zeros(1,
    size(A_N,1))]';
kp = 500;
kd = 100;
ki = 300;
K = [kp, 0, 0, kd, 0, 0, ki, 0, 0, 0, 0,
    0;
      0, kp, 0, 0, kd, 0, 0, ki, 0, 0, 0,
          0;
      0, 0, kp, 0, 0, kd, 0, 0, ki, 0, 0,
          0];

% Use ode45 to calculate state development
[t,x] = ode45(@(t,x) ODEsolver(t, x, A, B,C, D, E, A_N
    , B_N, C_N, D_N, E_N, dT,K), t_span, x0); %% Sett
    inn A_N, B_N, C_N, D_N
```

Listing 6.7 illustrates how the overall system is implemented in MATLAB. The augmented attack generating system is implemented in the same function used to estimate the state development of the attacked system. This is shown in listing 6.7.

The output of the attack generator is added to the control input. This enables the attack generator to perform dynamic attacks that are undetectable. The attack can be redirected by altering the attack vector to attack the generators for voltage instead of the generator for current.

Listing 6.8 shows the estimation of the system response at each time interval, t, based on the overall system and the augmented attack generating system.

6.4.1 No cyberattack present in the continuous-time model

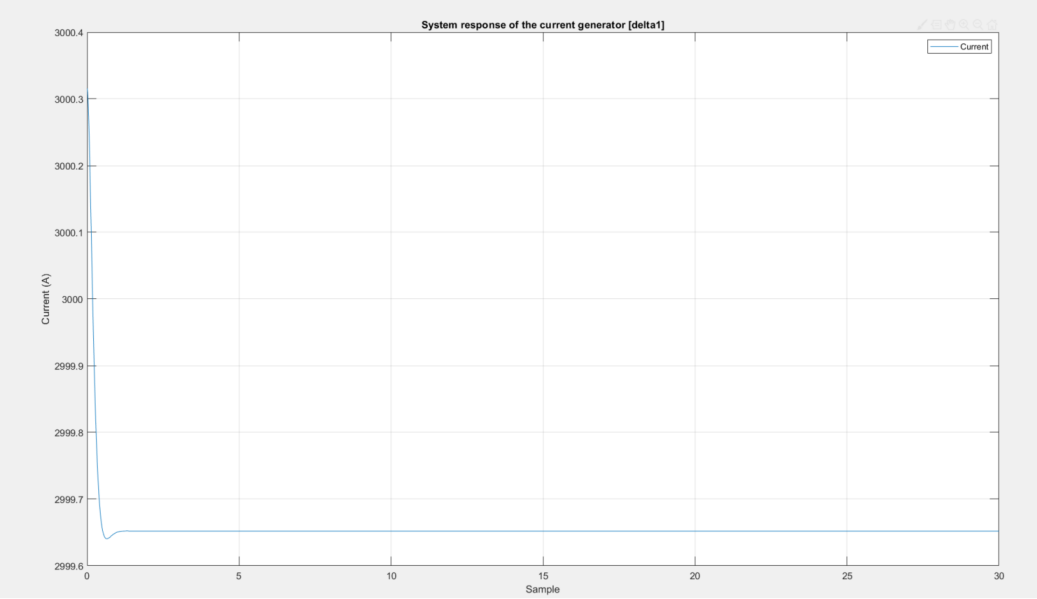

Figure 6.14: System response: No attack present in the generator for current, delta1

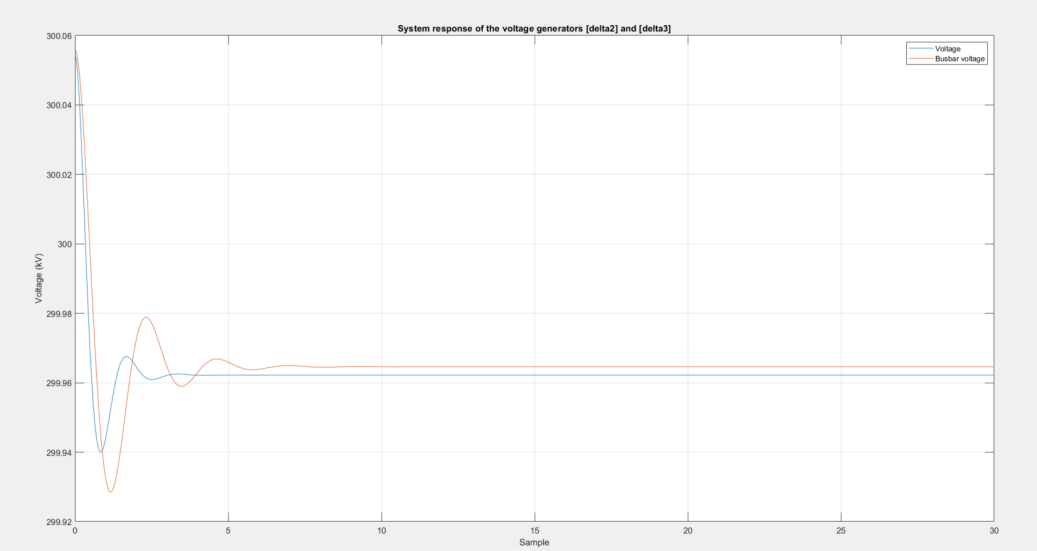

Figure 6.15: System response: No attack present in the generators for voltage, delta2 and delta3

Figure 6.14 shows how the generator for current, delta 1, responds when there is no present cyberattack. The generator stabilise at setpoint, with a small offset. Figure 6.15 shows how the generators for voltage, delta1 and delta2, responds when the is no cyberattack present. The generators stabilise at setpoint with a small offset.

6.4.2 Cyberattack present in the continuous-time model

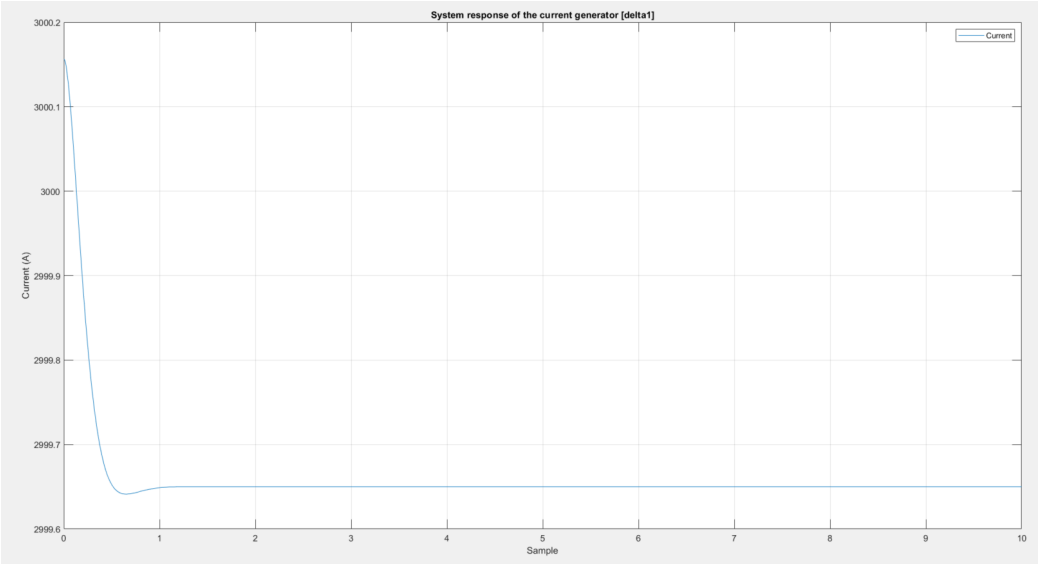

Figure 6.16: Cyberattack present in the system, the generator for current, delta1, not attacked.

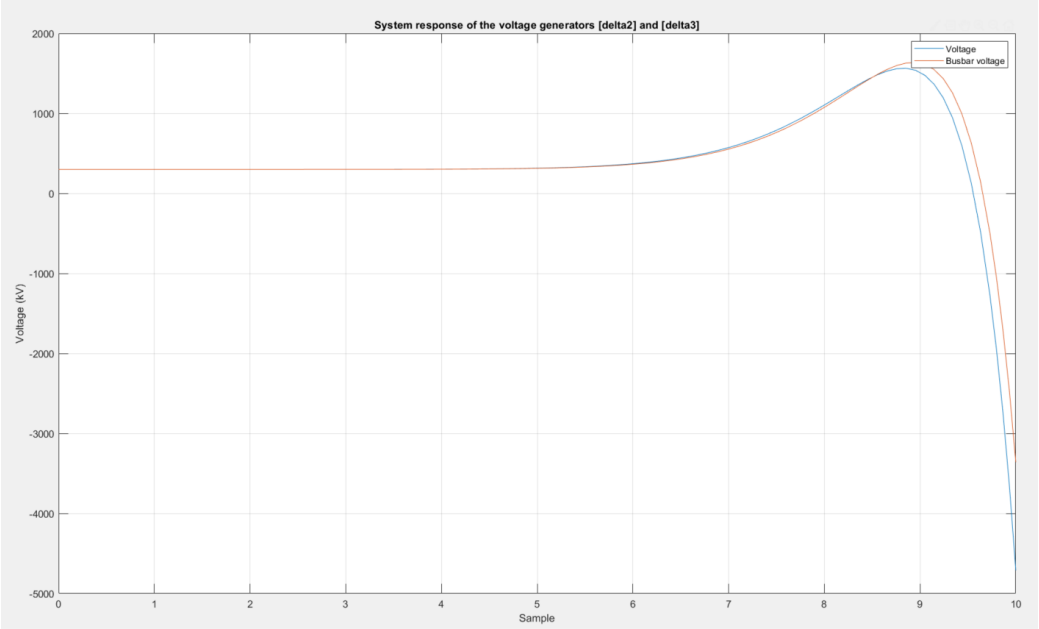

Figure 6.17: Cyberattack present in the system, the attack is directed towards the voltage generators, delta2 and delta3.

Figure 6.16 and 6.17 shows how the generators respond when there is a cyberattack present in the system. Notice how the generator for current, delta1, stabilise and the generators for voltage, delta2 and delta3, diverge.

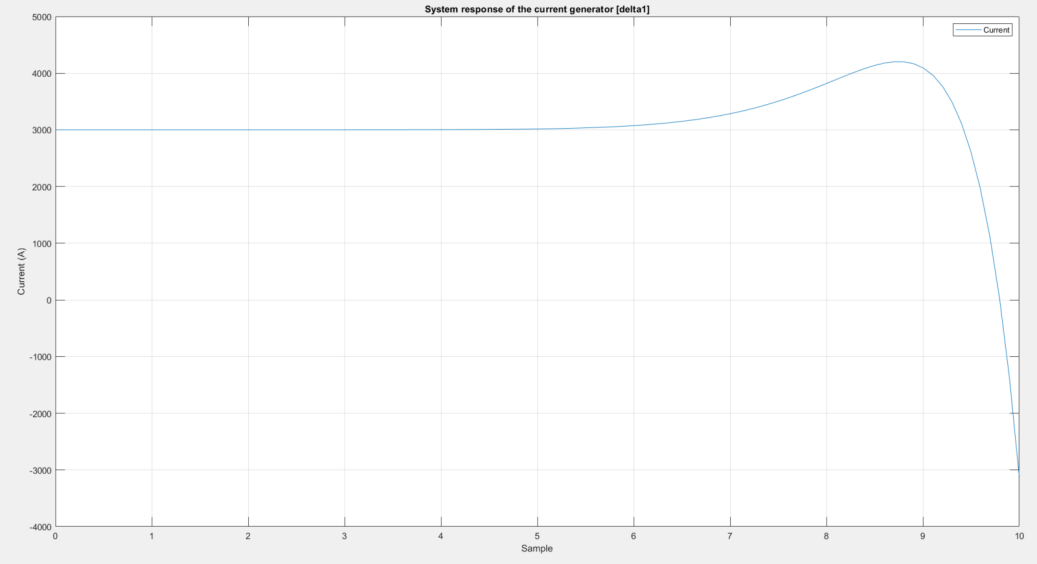

Figure 6.18: Cyberattack present in the system, the attack is redirected towards the generator for current, delta1.

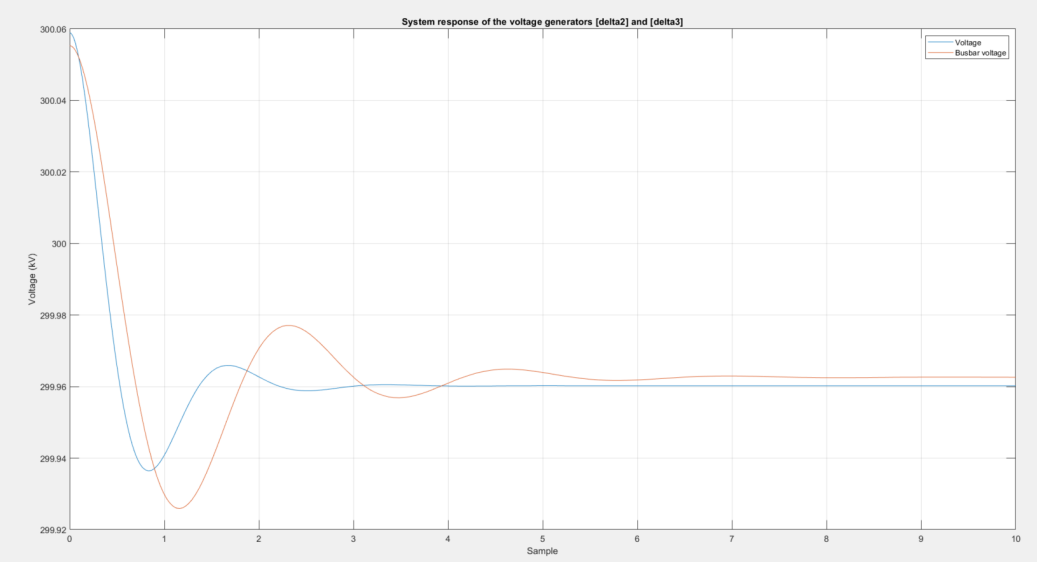

Figure 6.19: Cyberattack present in the system, the generators for voltage are not attacked.

Figure 6.18 shows how the generator for current, delta1, responds when the attack is redirected. Figure 6.19 shows how the generators for voltage, delta2 and delta3, responds to the redirected attack. Notice that delta1 diverge, and that delta2 and delta3 stabilise.

6.4.3 Observability and controllability

This section describes whether the continuous-time domain model is observable and controllable or not as described in section 4.10 and 4.11.

The continuous-time model is both controllable and observable since the control matrix $\mathcal{C}$ and the observability matrix $\mathcal{O}$ has full rank n.

Chapter 7

Discussion

7.1 Advantages and disadvantages of the substation types

A digital substation has the potential for major benefits compared to a conventional substation. The physical location in a conventional substation where the copper cables enter the substation represents danger to employees and nearby equipment due to high levels of current and voltage. The copper cables are directly connected to the transformers and transmission lines outside the substation. The same level of voltage and current present at the transmission lines is also present at the point where the copper cables enter a conventional substation.

In a digital substation conventional transformers are replaced by Non-Conventional Current Transformers (NCIT) and eliminates the dangerous galvanic connection between protection panel, control panel and the switchyard. The measurements from the transmission lines are communicated through fibre optic cables, thus eliminating the dangerous voltage and current levels inside the substation. The NCIT replaces the need for independent transformers for current and voltage by measuring both current and voltage in the same device. The transmitted data from the NCIT is received by a highly interoperable electronic processing unit which provides critical components and devices, such as metering and protection devices with the data via communication buses inside the substation [20][19][49].

In addition, the digital substation is based in accordance with international standards such as the IEC 61850 process bus. This makes the substation more interoperable by being more equipment and vendor independent. Furthermore, replacing communication through copper cables with fibre optics, station buses and process buses results in better area efficiency and intervention in local nearby areas. It can also result in an easier configuration of the substation.

Operational cost will most likely be reduced due to less need of regular maintenance and wider use of industrial standards that are more frequently updated. A digital substation also offers supervision of all exchanged data traffic on the process and station bus. This can enable faster response and identification of failures.

A possible issue with a digital substation are the many connections to different networks both in and between local substation systems and to external networks. The main control central will receive data through a closed and a shared network which makes it exposed to attacks performed by hackers. The digital substation will also be more exposed to occurring data errors than a conventional substation. Since there is a limited amount of digital devices in conventional substations, the possibility of data errors occurring in a conventional substation is more limited.

Implementing a digital substation by using multiple digital devices and components opens for unintentional cascading effects. This is not desired and can be handled by investigating inputs and outputs by simulating the response of each individual device and the overall system. An attacker, with proper knowledge of the system design and protocols used in a digital substation, may be able to attack specific parts of the substation. This attack may result in a malfunction at a completely different physical location than the original point of attack.

The advantages of a digital substation outweighs the disadvantages, thus making it an obvious choice to ensure a robust, reliable and flexible power grid of the future.

7.2 Accessing the substation

Gaining access to a substation is a demanding task that requires detailed knowledge of the system design and protocols used to protect the substation. The most top-secret and critical substations does not appear in public records making it harder to physically locate them.

Each area of the substation is classified within a security zone as described in section 3.5. It is possible to physically access a substation. To do this the attacker have to bypass camera surveillance, fences and electronic access control. The access checkpoints requires privileged user access. Once inside the substation, the attacker has to bypass the digital perimeter, such as bypassing USB ports protected by sticky MAC-addressing. Managing to bypass the mentioned security measures without being detected is not a realistic scenario.

One way of accessing a substation is through the digital domain. Gaining access through the digital domain can be done by utilising undiscovered and unintentional weaknesses in the substation design or industrial standards. The attacker also needs in-depth knowledge of the substation design and functionality. Furthermore, the substation is protected by electronic fences such as firewalls, malware protection and digital access control. One possible way of accessing the digital domain is if a wireless connection is unintentionally activated inside the substation during maintenance. This scenario is plausible, but due to the immense knowledge and resources required, and layers of protection to bypass, it is unlikely to happen.

Another way of gaining access to critical devices inside the substation is by exploiting employees in the organisation that do not have proper cyber threat awareness training. A common way for hackers to gain access to privileged data such as user accounts and passwords, is to perform a phishing attack or a MitM attack through e-mail. These types of attacks attempts to steal sensitive data through installing malware or by eavesdropping a secure connection. The e-mail originating from the hacker have to be concealed by imitating a trustworthy source. The true content of the e-mail have to be hidden from spam filters, firewalls and other cybersecurity measures. A critical part of an attack like this is to make sure that the employee installs the malware included in the e-mail. Once the sensitive data has been exposed, the cybercriminal can use this data to gain access to the digital domain (e.g. a secure IT server) with direct access to the digital substation. Once access to the digital substation has been obtained, the hacker can access the internal communication networks inside the substation and disrupt normal operations. This means that a hacker, in theory, can control parts of the power grid.

The most probable way of gaining access to a digital substation is by taking advantage of the digital domain by exploiting employees without proper cybersecurity awareness training. Although taking into consideration the immense resources needed to do this, it is not a realistic scenario.

7.3 Positioning of devices and equipment

A crucial part of cybersecurity in critical infrastructure is to make sure that devices and components with direct control or access to key functionality is well protected. Transformers and sensors that measures the state of the system must be protected both physically and digitally.

In the future, conventional transformers will most likely be replaced by NCITs. An optical fibre based transformer has a greater need for protection as it does not have the same inherent protection as conventional transformers. A conventional transformer contains high current and voltage levels resulting in a natural protection from physical tampering. It is therefore important to ensure the protection of a NCIT by adding additional security measures such as making it physically out of reach and unavailable. The other devices in a digital substation is protected by being inside the substation within distinct security zones as described in section 3.5.

Ensuring a high degree of redundancy is an important aspect of critical infrastructure to obtain normal operation, even when extraordinary events such as a cyberattack is attempting to disrupt normal operation.

7.4 Additional security

Statnett's pilot project is equipped with several process and station buses which receive current and voltage data originating from the digitised transformer measurements of transmission lines. The buses receive data from SAMU units (Sampling and Measurement Units) and additional MU units (Measurement Units). This ensures redundancy at process level. In addition, there are several cross connected PCUs that receive data from separate communication buses. This ensures additional security in case one of the buses or PCU units are compromised by an attacker.

A conventional substation does not have the same level of redundancy concerning the transformers. Introducing digital substations in the power grid will to a large extent eliminate weaknesses associated with the transformers as NCITs are less expensive and labour intensive to maintain and operate.

Introducing an entirely independent set of sensors and networks to further ensure the redundancy level required should also be considered. Furthermore, making regular back-up of data is recommended. The backups should be tagged with date, logged and stored on independent servers on closed networks. That way, if an attack has disrupted normal operation of a digital substation, existing non-infected backups are available and can be used to reboot the substation. Before rebooting the substation it is important to cut off communication towards outside networks. To the extent possible, having physical hard copies of protocols and operation should also be considered.

7.5 Modelling the PCU

The model used in this thesis exhibit as a proof of concept of how a cyberattack may take place on a cyber-physical system. The model used for simulations in this thesis does not describe the immense complexity of interconnections that is used in the pilot project at Furuset. To gain a more accurate and realistic simulation of how the PCUs actually responds to a cyberattack it is necessary to build a mathematical description/model which thoroughly describes the relationship between all the connections in the digital substation design.

It might be a challenge to obtain exact details of the digital substation design due to the huge cybersecurity risk these details represent. When digital substations gets standardised and installed in live power grids, details of the substation will most likely be restricted to a need-to-know basis due to the potentially catastrophic event of an immense cyberattack that may shut down one or several substations at the same time. On the other hand, it would be beneficial to understand the functionality of the digital substation on a detailed level. Understanding how the complex interconnections in the digital substation operates can make it easier to build a defence strategy against cyberattacks, and furthermore, make the digital substation robust and reliable.

Standardising industrial applications also means to expose details of how components used in critical infrastructure operates. This is one of the negative aspects of standardising. However, standardising leads to an easier integration of components and products used in other related industries. Components and devices will also be more compatible with other systems. Another advantage of standardising is the fact that smaller companies producing components and devices does not have the same resources available to conduct proper studies on different aspects of their product. This can for instance be a wider range of security measures in the product. Most businesses must have a profit, this is done by manufacturing products which are made to work within certain specific requirements. The best solution might be to have a committee or group consisting of representatives from both industry and academia. This will most likely lead to a more robust and secure standard.

The mathematical description used to build a system model of the PCU units are based on generators and their electromechanical characteristics. The PCU units main task is to protect and control the transmission lines by disconnecting and redirecting lines that does not behave as expected. The PCUs also send system diagnostic data to the control center and other relevant systems.

Investigating how a cyberattacker may disrupt normal behaviour of a cyber-physical system is done by using the model of a power network from the article *Control-Theoretic Mehtods for Cyberphysical security* [46]. As previously shown in section 5.3.2, the power network model can be transformed into a general mass-spring-damper system consisting of multiple coupled mass-spring-damper systems. This is done to be able to later build a larger model containing more components and coupled elements. By having a larger, more complex and intertwined model it might be possible to perform more sophisticated attacks. Building a larger model was not possible during this thesis due to a limited amount of time.

There is an analogy between electrical and mechanical systems which makes it suitable to model the PCU units as coupled mass-spring-damper systems [38]. In the mechanical equivalent system, capacitance can be viewed as springs, resistance as friction and inducting elements as mass [4]. Electrical power systems are naturally oscillating systems which makes a mass-spring-damper system suitable as a basis for a conceptual model.

Based on the article *Control-Theoretic Methods for Cyberphysical Security* [46] and equations 5.2 to 5.14, it is illustrated how the system can be transformed into a mass-spring-damper model. The attack simulation in article [46] is based on generator properties such as rotor angles and frequencies, voltage angles and the buses for interconnection between the generators. This makes modelling the overall system as a coupled mass-spring-damper system relevant when investigating how both detectable and undetectable attacks affects the overall system.

The reason for investigating the PCU units, and not other parts of the pilot project design, is the key position the PCUs have in the digital substation design. All communication to external and internal systems goes through the PCUs. Critical data such as voltage and current levels measured by transformers are digitised, distributed on the process bus and sent to the Regional Central (remote control center). The Regional Central makes decisions based on the data from the digital substations, such as the need of adding loads to the system, or the need of adding generators to produce more power. This is done continuously to ensure a stable power grid and distribution [51].

Redundancy in a digital substation is ensured by having multiple digital components and communication networks, both internally and externally. There is also a set of PCUs that communicates between each other on separate process and station buses. The PCUs distribute their health status and the transformer data originating from the transformers.

It is plausible that a cybercriminal may want to manipulate the PCU units by altering the communication as one way to make the substation, and ultimately, the power grid malfunction by disconnecting one or several transmission lines.

7.6 Measuring and sampling continuous signals

An important aspect to be aware of when digitising analogue signals is to use a sampling frequency which enables a full digital description of the analogue signal. If the sampling frequency is to low compared to the frequencies occurring in the analogue signal, unwanted effects such as aliasing can occur in the digitised version of the analogue signal. Aliasing is an effect that causes poorly sampled analogue signals to become impossible to distinguish from one another [2][3]. This can lead to unstable substation performance that affects the power grid in a negative manner.

Attempting to control a system based on aliased signals can lead to irregular system behaviour. This can be solved by ensuring that the sampling device's sampling frequency are based on the Nyquist theorem [37], as described in section 4.4.

The digital sample values used in this thesis represent the states used to drive an actual power network. A power network is in reality driven by the states of the system, although active control of the power network is done by a main control center through operating the substations within the network. A development of the model used in this thesis could be to use the states in this thesis (the DSV states) to drive a new system.

The filter used in this thesis might not be optimal in a real-time setting since it requires logged and stored data. The moving average filter is more suitable for post-processing of data. The trends captured from the post-processed data can be used in future system modelling. A low-pass filter might be a better filter in a real-time setting.

7.7 Euler's method vs. Runge-Kutta

Discretisation of continuous systems is an important part of modelling and simulating real world systems. It is not possible to recreate a full analogue representation on a digital platform due to computational limitations and real-time requirements. By sampling a continuous system, it is possible to obtain a reduced, but accurate description of the system. The discretised representation of the continuous system forms the basis for describing the system and active control applied on the system using this basis. By choosing a correct discretisation step, dt, the discretised representation of the system mimics the continuous system behaviour precisely.

Exact discretisation is often undesirable due to the heavy calculations of matrix exponentials and integral operations. Euler's discretisation method yields accurate results as long as the correct discretisation step is chosen.

Euler's discretisation method is a first order method for solving differential equations. It is one of the most used methods in physically realisable systems due to its simple implementation. The method estimates the next state of a system based on the present state of the system. This method does however not consider the curvature/rate of change of the present state.

Runge-Kutta (RK) is a family of numerical methods that approximates solutions to differential equations. One of the most used RK methods is RK4, described in section 4.5. This method determines the next state based on the present state and a weighted average of four different intermediate increments. An estimation of the resulting curvature is made based on the weighted average. RK methods produce less errors than lower order methods, depending on initial conditions and differential equations used to model the system. This method takes the curvature of the present state into account resulting in a more accurate estimate of the next state than Euler's method.

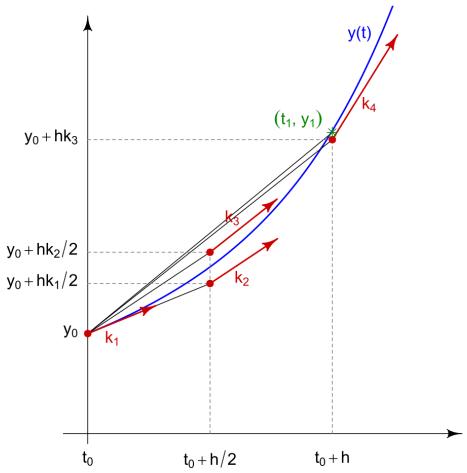

Figure 7.1: RK4 slopes [50]

Figure 7.1 illustrates how the curvature of the next state is taken into consideration when discretising the continuous system. *k1*, *k2*, *k3* and *k4* are the increments based on a chosen step size *h*. The function describing the system must be known as well as the initial conditions.

The computational cost of using RK4 compared to Euler can be extensive when dealing with large systems represented by numerous high order differential equations. By carefully choosing the discretisation step in Euler's method, the resulting estimate will be accurate. Thus concluding that using Euler's method results in the same level of accurate description of the continuous system in the discrete-time domain as RK4 would, as long as the correct discretisation step is chosen.

The smaller the step size used, the more accurate the discrete-time representation becomes. One way to ensure that the sampled signal actually represents the analogue counterpart is by utilising the Nyquist theorem.

Thus concluding that using Euler's method instead of RK4 results in the same level of accurate description of the continuous system in discrete-time domain, simply by choosing correct discretisation step.

7.8 System response, discrete-time model

Creating an augmented attack generator based on the null space of the transfer function of the original system is a critical part of being able to conduct undetectable attacks. The results in section 6.3 reveal that the dynamic attacks become detectable throughout the overall system. The system response is estimated using Euler's method and the null space dynamics matrices are based on a continuous-time representation. This might cause the dynamic attacks towards the system to be detectable. However, this can not be strictly concluded due to the possibility of having represented parts of the state space system in both discrete-time and continuous-time domain. A possible way of utilising the transfer function to design invisible attacks for the discrete-time case, as done in the continuous-time case, is to discretise the continuous-time transfer function. This can be done by using the zero-order hold (ZOH) method [13][5] or a Z-transform [69]. By doing this it might be possible to use numerical methods such as Euler's method to conduct undetectable attacks.

Another possible reason for this result is that the function describing the attack generator is not proper. In other words, the denominator is of lower order than the numerator. It is crucial that the denominator has a higher order. This ensures a stable and physically realisable system.

Simulating the system response of the discrete-time model was made by using a for-loop in MATLAB to estimate control inputs and the next state based on present state.

The discrete-time model stabilises as expected when no attack is affecting the model. However, when an attack is present in the model, the system destabilises. It does not matter which characteristic of the generator that is monitored, the attack will be detected.

The discrete-time model was an important step towards understanding the complex behaviour and mathematics behind the power and network model used in this thesis. The experience gained from the discrete-time model was later used to implement the continuous-time model.

7.9 System response, continuous-time model

The continuous-time model was simulated using the same approach as for the discrete-time model except one significant difference. The continuous-time model was simulated in a continuous-time domain by using the MATLAB's built-in ordinary differential equations solver (ode45).

The augmented attack generating system was created utilising the same approach as for the discrete-time model. The continuous-time model was simulated using MATLAB's built in ODE Solver functionality.

Supposing that a monitoring device only has the capability to monitor either the two generators for voltage or the generator for current makes it possible to conduct an attack which is undetectable. The sensor matrix, C, will have to be constructed so it only measures one of the generators. As shown in section 6.4 it is possible to attack either the generator for current (delta1) or the generators for voltage (delta2 and delta3) with the attack only being visible on the generators for voltage or the generator for current.

The continuous model stabilises as expected when no attack is affecting the model. However, when an attack is present in the network, parts of the power network destabilise depending on which of the generators that are attacked.

The attacks are considered as additional loads for the generator(s) not being attacked.

7.10 Additional aspects

To be able to perform undetectable attacks towards the system it is important that the sensor matrix, C, is unable to measure all states. Performing an undetectable attack on a fully observable system where all outputs and internal states of the system can be measured is not possible. Thus concluding that is is only possible to perform undetectable attacks if the measuring sensor matrix C are not monitoring all states of the system and there exists no undetectable or hidden paths throughout the dynamics of the system. The dynamics describing the attack generator has to be extracted from a proper transfer function to ensure a physically realisable and stable system. This applies to both the continuous-time model and the discrete-time model. Thus concluding that to be able to perform undetectable attacks, the measuring sensor matrix C, cannot monitor all states. Statnett may overcome the issue of detecting undetectable attacks by making sure that there are no hidden paths throughout the digital and physical design. This means that no matter how sophisticated an attack is, it would affect part of the system which is measured directly or indirectly.

To the interested reader, possible strategies of preventing undetectable attacks can be studied in *A saturated dynamic input allocation policy for preventing undetectable attacks in cyber-physical systems* [15].

7.11 Controlling the system

A PID or PI controller is one of the most frequently used controllers in the automation industry [48]. It is a simple and effective controller. As section 6 illustrates, tuning the controller by adjusting the gain factors is an important aspect of obtaining the stability necessary for the overall system. By using a PI controller there is a small offset from setpoint due to the lack of the derivative term. This can be adjusted by tuning the parameters for integral and proportional gain.

The controller enables the system to stabilise at the given setpoint for both models. The system driven by external force settles to a stable value, as expected since the model is a mass-spring-damper system.

The effects of tuning the parameters in the PID controller is described in table 7.1 [47].

Effects of increasing independently increasing parameters					
Parameter	**Rise time**	**Overshoot**	**Settling time**	**Steady-state error**	**Stability**
K_p	Decrease	Increase	Small change	Decrease	Degrade
K_i	Decrease	Increase	Increase	Eliminate	Degrade
K_d	Minor change	Decrease	Decrease	No theoretic effect	Might increase K_d

Table 7.1: PID tuning

Another controller which may be used is an optimal linear-quadratic controller (LQR). Using this may lead to more accurate control and faster response of the system. The LQR controller's main purpose is to control a dynamic system by minimising a cost function associated with a chosen variable in the system [35]. The cost function associates some cost to a given event. Since the LQR controller is an optimal controller it seeks to minimize the cost function.

In general, the controller have to manage to drive the system asymptotically to zero to ensure the stability of the system. This is ensured if the eigenvalues is in the left half plane of the root locus plot.

As the system stabilise when there are no attacks present in the system the control used to regulate the system manages to drive the system towards the desired setpoint. Although the system is stable during normal operation, the PID control gains should be tuned to yield a lesser degree of overshoot. There are many ways to tune a PID controller ranging from Ziegler-Nichols to tuning by trial and error [24].

Thus concluding that the controller used to stabilise and drive the system to the chosen setpoint performs as expected as long as the parameters for gains are chosen correctly.

7.12 Stability, controllability and observability

In control theory and control systems, observability and controllability are important concepts used to measure how accurate internal states of the system can be controlled and observed.

A system can be viewed as a black box (dynamic system), meaning that there is no knowledge of the internal states of the system. By stimulating the black box with an input signal it will produce an output signal. If a system is observable it is possible to determine the outputs based on the dynamics matrix A, and the sensor matrix C, thus indirectly revealing the internal dynamics of the system.

Controllability, on the other hand, is a way to determine if it is possible to control inputs indirectly or directly based on the control matrix B, and the dynamics matrix A.

Notice that results of controllability and observability for the two models in section 6.3.6 and 6.4.3 are controllable and observable. However, since the state space system used in this thesis is a descriptor model, the model is not realistically controllable and observable due to the descriptor matrix E. The descriptor matrix E makes it possible to utilise the null space of the transfer function to generate dynamic and undetectable attacks.

By having a system which is highly interconnected, meaning that the total dynamics matrix A is connected to every input and output variable, leads to a more robust system. This means that it is harder to find hidden paths in the dynamics of the system and ultimately alter the system without being detected.

7.13 Findings during the literature search

A central part of the literature search was to investigate what vendors, such as ABB and Siemens, offers of modern substation automation technology. The IT and OT security part of the thesis was found in a similar way in addition to wide use of SpringerLink which offers literature in book format online. The most yielding result of the literature search concerning digital substations was the *IEEE PES Tutorial on Cybersecurity of the Transmission and Distribution System* [18]. This tutorial covers a huge aspect the distribution systems and digital substations. Furthermore, various cybersecurity organisations offer detailed explanation of the most common cyberattacks.

An interesting discovery from the literature search was an article from February 2015, *Control-Theoretic Methods for Cyberphysical Security* [46]. Page 3 and 4 of this article describes a power network and attack example based on exploiting generator characteristics such as rotor angles, rotor frequencies, and voltage angles.

Part III

Conclusion

Chapter 8

Conclusion

8.1 Summary of the findings of this thesis

By comparing conventional and digital substations it has become clear that replacing conventional substations with digital substations is an obvious choice to ensure a robust, resilient, flexible and secure power grid.

It is possible for a cybercriminal to gain access to critical infrastructure, such as a digital substation, by exploiting industrial standards, unaware employees and unknown weaknesses in the infrastructure design. A substation consists of both digital and physical devices thus being a system where a coupling between different parts of the system occur. The coupling effects in the system design makes it possible to perform undetectable attacks by utilising paths in the system that cannot be monitored.

The PCU units are plausible targets for cybercriminals due to their critical position in the digital substation design. However, a successful cyberattack towards a digital substation requires a tremendous amount of knowledge and specific system understanding few individuals possess. Thus making it possible, but unlikely to access the PCU units and ultimately disconnect one or several transmission lines.

A typical cyberattack is performed by exploiting weaknesses in digital devices, protocols and standards, in combination with manipulating employees without proper cyber threat training to reveal sensitive information through e.g. an e-mail phishing scam.

The resulting simulations based on the model in this thesis reveal that it is possible to perform both detectable and undetectable attacks on a system with coupling effects. The most interesting result is that it is possible to perform undetectable attacks simply by exploiting the null space dynamics of the overall system transfer function.

It is possible to use the digital domain to ultimately perform undetectable attacks based on the model used in this thesis to simulate of the overall system. However, this is unlikely since small deviations from normal operation is detectable in other parts of the power grid.

8.1.1 Discrete-time model

The discrete-time model stabilise to setpoint when no cyberattack is present in the system. This behaviour is expected. However, when an attack is directed towards the system all the generators destabilise. It does not matter which generator is being targeted. A possible reason for this event is that the discrete-time model is discretised using Euler's method and the attack generating model is based on a continuous representation of the system transfer function. Another possible issue is that the function describing the attack generating system in which the null space matrices are extracted from is not proper. This can lead to a physically unstable and unrealisable system.

A possible method that may enable the realisation of undetectable attacks for the discrete-time model is to discretise the continuous-time transfer function. This can be done using the zero-order hold method or a Z-transform.

8.1.2 Continuous-time model

The continuous-time model stabilise to setpoint when no cyberattack is present in the system. There is a small offset from setpoint because the controller used to drive the continuous-time system is a PI controller compared to the discrete-time case using a PID controller. Tuning the gains K_p and K_i might eliminate the offset. However, when an attack is directed towards the system either the generator for current or the generators for voltage destabilise, depending on which of the generators that are targeted by the attack generating system. Supposing that a monitoring device only has the capability to monitor either the two generators for voltage or the generator for current makes it possible to conduct undetectable attacks.

The attack is considered as an additional load for the generator(s) not under attack.

The continuous-time model has been strictly described and simulated in a continuous-time domain to enable undetectable attacks.

8.1.3 Realisation of undetectable attacks

Creating an augmented attack generating system is based on the null space of the transfer function of the original system. This is an important part of being able to conduct undetectable attacks. The dynamics of the attack generating system is extracted based on the null space of the original system's transfer function, $N(s)$, and a stable transfer function, $D(s)$. The relationship $\frac{N(s)}{D(s)}$ is used to extract the attack generator dynamics. It is important to ensure that this relationship is a proper transfer function enabling a physically stable and realisable system.

One way to be able to mitigate or prevent undetectable attacks is to ensure that the dynamics of the system is well-connected. Having a well-connected system might make it more difficult for an attacker to find hidden and undetectable paths throughout the system, if any exists. Having more inputs than outputs in a system might create additional hidden paths which makes it easier to perform undetectable attacks. Other strategies on how to mitigate or prevent undetectable attacks can be studied in the following articles [15] and [14].

8.2 Further work

If the methods used in this thesis are used in a digital substations a study should be conducted where the main goal should be to describe the dynamics of the entire digital substation. Such a study would involve mathematically describing how signals are generated, based on the generators. It could be evaluated how these signals transplants throughout the digital substation. Finally the substation with all interconnections, devices and components affecting the substation, has to be mathematically defined.

Having obtained a full mathematical description of the system, it is possible to apply the suggested methods in this thesis to evaluate a more realistic system response.

Bibliography

[1] *1-D digital filter - MATLAB filter - MathWorks Nordic*. URL: https://se.mathworks.com/help/matlab/ref/filter.html (visited on 04/04/2019).

[2] *Aliasing of Signals - Identity theft in the frequency domain*. AllSignalProcessing.com. 25th Apr. 2015. URL: https://allsignalprocessing.com/aliasing-of-signals-identity-theft-in-the-frequency-domain/ (visited on 07/05/2019).

[3] *Aliasing_wikipedia*. In: *Wikipedia*. Page Version ID: 895614921. 5th May 2019. URL: https://en.wikipedia.org/w/index.php?title=Aliasing&oldid=895614921 (visited on 07/05/2019).

[4] *Analogous Electrical and Mechanical Systems*. URL: https://lpsa.swarthmore.edu/Analogs/ElectricalMechanicalAnalogs.html (visited on 02/04/2019).

[5] Panos J. Antsaklis and Anthony N. Michel. *A linear systems primer*. OCLC: ocm76936056. Boston, Mass. : London: Birkhäuser ; Springer [distributor], 2007. 517 pp. ISBN: 978-0-8176-4460-4.

[6] Maria Bartnes. *tjenestenekt*. In: *Store norske leksikon*. 20th Feb. 2018. URL: http://snl.no/tjenestenekt (visited on 26/03/2019).

[7] Sonja Berlijn. *Kraftsystemet digitaliseres - internal Statnett document*. 2019.

[8] Halvor Bothner-By. *Nyquist_SNL*. In: *Store norske leksikon*. 6th Nov. 2017. URL: http://snl.no/signalteori (visited on 07/05/2019).

[9] Ronald Brown. 'Lecture 8 nul col bases dim & rank - section 4-2, 4-3, 4-5 & 4-6'. Education. URL: https://www.slideshare.net/njit-ronbrown/lecture-8-nul-col-bases-dim-rank-section-42-43-45-46 (visited on 09/05/2019).

[10] Robert M. Clark and Simon Hakim, eds. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*. Protecting Critical Infrastructure. Springer International Publishing, 2017. ISBN: 978-3-319-32822-5. URL: https://www.springer.com/gp/book/9783319328225 (visited on 01/05/2019).

[11] *Control Systems/Controllability and Observability - Wikibooks, open books for an open world*. URL: https://en.wikibooks.org/wiki/Control_Systems/Controllability_and_Observability (visited on 19/05/2019).

[12] *Controllability*. In: *Wikipedia*. Page Version ID: 884512922. 22nd Feb. 2019. URL: https://en.wikipedia.org/w/index.php?title=Controllability&oldid=884512922 (visited on 08/05/2019).

[13] *Convert Discrete-Time System to Continuous Time - MATLAB & Simulink - MathWorks Nordic*. URL: https://se.mathworks.com/help/control/ug/convert-a-discrete-time-system-to-continuous-time.html (visited on 24/05/2019).

[14] A. Cristofaro and S. Galeani. 'Output invisible control allocation with steady-state input optimization for weakly redundant plants'. In: *53rd IEEE Conference on Decision and Control*. 53rd IEEE Conference on Decision and Control. Dec. 2014, pp. 4246–4253. DOI: 10.1109/CDC.2014.7040051.

[15] A Cristofaro, S Galeani and Maria Letizia Corradini. 'A saturated dynamic input allocation policy for preventing undetectable attacks in cyber-physical systems'. In: 2018, pp. 845–850. DOI: 10.23919/ECC.2018.8550352.

[16] *Cyber Attack - What Are Common Cyberthreats? - Cisco*. URL: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (visited on 26/03/2019).

[17] *Cyber-physical system*. In: *Wikipedia*. Page Version ID: 889286908. 24th Mar. 2019. URL: https://en.wikipedia.org/w/index.php?title=Cyber-physical_system&oldid=889286908 (visited on 22/05/2019).

[18] *Cybersecurity of the Electric Power Transmission and Distribution System*. Transmission & Distribution World. 21st Mar. 2018. URL: https://www.tdworld.com/grid-security/cybersecurity-electric-power-transmission-and-distribution-system (visited on 26/04/2019).

[19] *Digital Substation | Energy Topics | Siemens*. URL: https://new.siemens.com/global/en/products/energy/topics/digital-substation.html (visited on 05/04/2019).

[20] *Digital substations*. URL: https://www.tdworld.com/sites/tdworld.com/files/ABBDigitalSubstations.pdf (visited on 06/05/2019).

[21] Henrik Dvergsdal. *sårbarhet – IT*. In: *Store norske leksikon*. 24th Feb. 2017. URL: http://snl.no/s%C3%A5rbarhet_-_IT (visited on 26/03/2019).

[22] D. Dzung et al. 'Security for Industrial Communication Systems'. In: *Proceedings of the IEEE* 93.6 (June 2005), pp. 1152–1177. ISSN: 0018-9219. DOI: 10.1109/JPROC.2005.849714.

[23] Even Fladberg. *PID-regulatoren*. Tu.no. 30th Mar. 2013. URL: https://www.tu.no/artikler/praktisk-reguleringsteknikk-praktisk-prosessregulering-4-8/218514 (visited on 20/05/2019).

[24] Even Fladberg. *Tuning av PID-regulatorer*. Tu.no. 30th Mar. 2013. URL: https://www.tu.no/artikler/praktisk-reguleringsteknikk-praktisk-prosessregulering-7-8/218510 (visited on 24/05/2019).

[25] Jan Tommy Gravdahl. *PID-regulator*. In: *Store norske leksikon*. 12th Mar. 2018. URL: http://snl.no/PID-regulator (visited on 02/04/2019).

[26] Techbriefs Media Group. *The Modern Industrial Workhorse: PID Controllers*. URL: https://www.techbriefs.com/component/content/article/tb/features/articles/20013 (visited on 20/05/2019).

[27] Martin Hermann. *A first course in ordinary differential equations: analytical and numerical methods*. New York: Springer, 2014. ISBN: 978-81-322-1834-0.

[28] *IEEE Xplore Full-Text PDF:* URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7039754 (visited on 24/05/2019).

[29] *Industroyer: Biggest threat to industrial control systems since Stuxnet*. WeLiveSecurity. 12th June 2017. URL: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (visited on 28/03/2019).

[30] A. Iserles. *A first course in the numerical analysis of differential equations*. Cambridge texts in applied mathematics. Cambridge ; New York: Cambridge University Press, 1996. 378 pp.

[31] *Kart over regional- og sentralnettet - NVE*. URL: https://www.nve.no/nytt-fra-nve/nyheter-energi/kart-over-regional-og-sentralnettet/ (visited on 03/05/2019).

[32] *Laplace transform*. In: *Wikipedia*. Page Version ID: 894830561. 30th Apr. 2019. URL: https://en.wikipedia.org/w/index.php?title=Laplace_transform&oldid=894830561 (visited on 09/05/2019).

[33] Henrik Lied. *Skreddersydd dobbeltangrep mot Hydro*. NRK. 19th Mar. 2019. URL: https://www.nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202 (visited on 28/03/2019).

[34] Tom Lindstrøm. *Laplace-transformasjon*. In: *Store norske leksikon*. 24th Jan. 2017. URL: http://snl.no/Laplace-transformasjon (visited on 09/05/2019).

[35] *Linear-Quadratic Regulator (LQR) design - MATLAB lqr - MathWorks Nordic*. URL: https://se.mathworks.com/help/control/ref/lqr.html (visited on 21/05/2019).

[36] *Man-in-the-middle attack*. In: *Wikipedia*. Page Version ID: 897431798. 17th May 2019. URL: https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=897431798 (visited on 22/05/2019).

[37] Dimitris G. Manolakis and Vinay K. Ingle. *Applied Digital Signal Processing: Theory and Practice*. Cambridge: Cambridge University Press. ISBN: 978-0-511-83526-1. URL: http://ebooks.cambridge.org/ref/id/CBO9780511835261.

[38] *Matematisk modellering av kontrollsystem | Mekanisk elektrisk*. URL: https://riverglennapts.com/no/laplace/493-mathematical-modelling-of-control-system-mechanical-electrical.html (visited on 06/05/2019).

[39] Mathuranathan. *Moving Average Filter (MA filter)*. GaussianWaves. 23rd Nov. 2010. URL: https://www.gaussianwaves.com/2010/11/moving-average-filter-ma-filter-2/ (visited on 04/04/2019).

[40] Haifeng Niu and S Jagannathan. 'Optimal defense and control of dynamic systems modeled as cyber-physical systems'. In: *The Journal of Defense Modeling and Simulation* 12.4 (1st Oct. 2015), pp. 423–438. ISSN: 1548-5129. DOI: 10.1177/1548512915594703. URL: https://doi.org/10.1177/1548512915594703 (visited on 03/05/2019).

[41] 'Numerisk løsning av differensiallikninger Eulers metode, Eulers midtpunktmetode, Runge Kuttas metode, Taylorrekkeutvikling* og Likninger av andre orden'. In: (), p. 35.

[42] *Observability*. In: *Wikipedia*. Page Version ID: 888953979. 22nd Mar. 2019. URL: https://en.wikipedia.org/w/index.php?title=Observability&oldid=888953979 (visited on 08/05/2019).

[43] *OSI*. In: *Store norske leksikon*. 28th Oct. 2016. URL: http://snl.no/OSI (visited on 28/03/2019).

[44] *OSI model*. In: *Wikipedia*. Page Version ID: 888673653. 20th Mar. 2019. URL: https://en.wikipedia.org/w/index.php?title=OSI_model&oldid=888673653 (visited on 28/03/2019).

[45] *PAC World magazine : Experience from Statnett R&D Digital Substation Project*. URL: https://www.pacw.org/no-cache/issue/september_2018_issue/lessons_learned/modern_iec61850_based_distribution_feeder_automation_systems.html (visited on 03/05/2019).

[46] F. Pasqualetti, F. Dorfler and F. Bullo. 'Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems'. In: *IEEE Control Systems Magazine* 35.1 (Feb. 2015), pp. 110–127. ISSN: 1066-033X. DOI: 10.1109/MCS.2014.2364725.

[47] *PID controller*. In: *Wikipedia*. Page Version ID: 890074995. 29th Mar. 2019. URL: https://en.wikipedia.org/w/index.php?title=PID_controller&oldid=890074995 (visited on 02/04/2019).

[48] *PID Theory Explained - National Instruments*. URL: http://www.ni.com/en-my/innovations/white-papers/06/pid-theory-explained.html (visited on 20/05/2019).

[49] Knut A. Rosvold. *transformatorstasjon*. In: *Store norske leksikon*. 21st Jan. 2019. URL: http://snl.no/transformatorstasjon (visited on 26/03/2019).

[50] *Runge–Kutta methods*. In: *Wikipedia*. Page Version ID: 894771467. 29th Apr. 2019. URL: https://en.wikipedia.org/w/index.php?title=Runge%E2%80%93Kutta_methods&oldid=894771467 (visited on 21/05/2019).

[51] *Samfunnsansvar — Statnett årsrapport 2014*. URL: http://2014.statnett.no/samfunnsansvar (visited on 24/05/2019).

[52] A. Serrani. 'Output regulation for over-actuated linear systems via inverse model allocation'. In: *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*. 2012 IEEE 51st IEEE Conference on Decision and Control (CDC). Dec. 2012, pp. 4871–4876. DOI: 10.1109/CDC.2012.6426209.

[53] *Sine wave*. In: *Wikipedia*. Page Version ID: 893755745. 23rd Apr. 2019. URL: https://en.wikipedia.org/w/index.php?title=Sine_wave&oldid=893755745 (visited on 05/05/2019).

[54] *Spoofing attack*. In: *Wikipedia*. Page Version ID: 892167635. 12th Apr. 2019. URL: https://en.wikipedia.org/w/index.php?title=Spoofing_attack&oldid=892167635 (visited on 22/05/2019).

[55] *Strømnettet*. Energifakta Norge. URL: https://energifaktanorge.no/norsk-energiforsyning/kraftnett/ (visited on 30/04/2019).

[56] *Stuxnet - an overview | ScienceDirect Topics*. URL: https://www.sciencedirect.com/topics/computer-science/stuxnet (visited on 28/03/2019).

[57] *Systemansvaret*. Statnett. URL: https://www.statnett.no/for-aktorer-i-kraftbransjen/systemansvaret/ (visited on 30/04/2019).

[58] *Transmission Substations*. ElectraNet. URL: https://www.electranet.com.au/our-approach/safety/transmission-substations/ (visited on 28/03/2019).

[59] *Understanding SQL Injection*. Cisco. URL: https://www.cisco.com/c/en/us/about/security-center/sql-injection.html (visited on 26/03/2019).

[60] Eric W. Weisstein. *Runge-Kutta Method*. URL: http://mathworld.wolfram.com/Runge-KuttaMethod.html (visited on 04/04/2019).

[61] Eric W. Weisstein. *Sine*. URL: http://mathworld.wolfram.com/Sine.html (visited on 05/05/2019).

[62] *What are the real world applications of Laplace transform, especially in computer science? - Quora*. URL: https://www.quora.com/What-are-the-real-world-applications-of-Laplace-transform-especially-in-computer-science (visited on 09/05/2019).

[63] *What is a man-in-the-middle attack?* URL: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html (visited on 01/04/2019).

[64] *What is Combined Non-Conventional Instrument Transformer (NCIT)? 3 Minutes with Dr. Thomas Heid (VIDEO)*. Maxwell Technologies. URL: https://www.maxwell.com/blog/combined-non-conventional-instrument-transformer (visited on 28/03/2019).

[65] *What is Malware? - Definition and Examples*. Cisco. URL: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html (visited on 26/03/2019).

[66] *What is Nyquist Theorem? - Definition from WhatIs.com*. WhatIs.com. URL: https://whatis.techtarget.com/definition/Nyquist-Theorem (visited on 07/05/2019).

[67] *What Is Phishing? - Types of Phishing Attacks*. Cisco. URL: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html (visited on 26/03/2019).

[68] *What is SCADA?* Inductive Automation. URL: https://inductiveautomation.com/resources/article/what-is-scada (visited on 23/04/2019).

[69] *Z-transform - MATLAB ztrans - MathWorks Nordic*. URL: https://se.mathworks.com/help/symbolic/ztrans.html (visited on 24/05/2019).

[70] L. Zaccarian. 'On dynamic control allocation for input-redundant control systems'. In: *2007 46th IEEE Conference on Decision and Control*. 2007 46th IEEE Conference on Decision and Control. Dec. 2007, pp. 1192–1197. DOI: 10.1109/CDC.2007.4434679.

[71] *Zero-day vulnerability: What it is, and how it works*. URL: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html (visited on 01/04/2019).

[72] Yan Zhang. 'What are Cyber-Physical Systems?' In: (21st Mar. 2018), p. 44. (Visited on 26/04/2019).