DNV·GL

Thesis

Cyber Security for Power System Operators

Author: Casper van der Sluis
Student number: 15049558
University: The Hague University of Applied Sciences
Education: Electrical Engineering
University supervisors: 1st Ben Kuiper
2nd Paul Witte
Company: DNV GL Singapore PTE. LTD.
Company supervisor: Gary Chee Kiong Ang

Date: 31 - May – 2019

1.0	Final	Casper van der Sluis	31-05-2019
0.2	For review	Casper van der Sluis	15-05-2019
0.1	First draft	Casper van der Sluis	04-02-2019
Revision	**Description**	**Name**	**Date**

COLOPHON

Title

Cyber Security for Power System Operators – Detection of intrusion within a SCADA system

Version

1.0 Final

Author

Name: C.M. (Casper) van der Sluis
Student number: 15049558
Address: Hof van Azuur 44
Postcode: 2614 TB Delft, The Netherlands
E-mail: caspervdsluis@live.nl
Phone number: +31 (0)6 22259475

Company

Company: DNV GL Singapore PTE. LTD.
Address: 16 Science Park Drive DNV GL Clean Technology Centre
Postcode: 118227 Singapore
Supervisor: Gary Chee Kiong Ang
E-mail: gary.chee.kiong.ang@dnvgl.com
Phone number: +65 97864559

University

University: The Hague University of Applied Sciences
Address: Rotterdamseweg 137
Postcode: 2628 AL Delft, The Netherlands
1st supervisor: Ben Kuiper
E-mail: b.kuiper@hhs.nl
2nd supervisor Paul Witte
E-mail: p.m.witte@hhs.nl

PREFACE

In front of you is my thesis "Cyber Security for Power System Operators – Detection of intrusion within a SCADA system". This bachelor thesis is the final assessment for the dual bachelor's Programme Electrical Engineering at The Hague University of Applied Sciences in Delft, The Netherlands. The graduation internship is performed at DNV GL Singapore PTE. LTD. located in Singapore.

During the first 3 years of my dual bachelor Electrical Engineering I worked at Movares, a Dutch market-orientated consultancy and engineering company. During that time, I was able to visit multiple locations and work on interesting projects which thought me a lot about the electrical power grid. My original interest toward Electrical Engineering, however, was the vastness of subjects as well as the broad international implementation. With the lack of international work at Movares, I figured out that I wanted to expand my knowledge abroad using my graduation internship.

Together with Gary Chee Kiong Ang a research toward cyber security for electrical power grid operating systems was formed. With this research I was able to enhance my knowledge about the electrical power grid. As well as to learn about the important and hot topic of cyber security.

I would like to express my gratitude to my company supervisor Gary Chee Kiong Ang as well as all members of the Intelligent Network and Communications team for their guidance and support.

I would also like to thank several experts with hands-on experience in the implementation of physical and cyber security for industrial control systems. I highly appreciate their responsiveness on mails and involvement through calls.

Thereafter, I would like to express my gratitude to the people who initiated me with the opportunity. Firstly, Rik Luiten my manager during my time at Movares. He connected me with Maurice Adriaensen, who introduced me to DNV GL and reached out to Leo Akkerman situated in Singapore. From there the exploration for a suitable graduation project unfolded.

Furthermore, I like to thank all employees from the company DNV GL who contributed to giving me this opportunity.

I would like to thank Ben Kuiper from The Hague University of Applied Sciences. For his enthusiasm, input and support during his role as first university supervisor.

Finally, I would like to thank my parents for their continued support and care provided during my study.

Casper van der Sluis
Singapore, May 2019

SUMMARY

Industrial control systems are essential for the functioning of our society since they control our electricity, water, agriculture, health, communication, transportation, emergency service and financial service. In the digital age of big data and data analytics these so-called critical infrastructures are also digitalizing, to keep up with the customer demand of data analytics and reliability. For the digitalisation of the electrical power grid, the increasing implementation of renewables also plays a role. The implementation causes the energy flows to become bidirectional. To manage and control these bidirectional power flows, more intelligent electronic devices must be implemented. All these field devices are connected to a centralized control centre, which contains the Supervisory Control and Data Acquisition (SCADA) servers. These servers collect the data and provide it to the operators to manage the electrical power grid and keep the energy supply stable and reliable. These systems are managed and controlled by utilities. They also use the data for data analytics, forecasting and further development of their infrastructure.

The digitalization provides a lot of benefits in terms of management and control for the electrical power grid. However, with the digitalization and increasing cases of cyber-attacks the threat of cyber-attacks becomes more and more relevant. This is obvious from the first known successful cyber-attack on the Ukrainian electrical power grid. Whereby an adversary was able to control the electrical power grid from a remote location causing power outage to a large number of customers. In addition, the increasing appearance of malware specially designed to target industrial control system. Therefore, our critical infrastructures and society are at risk.

The research question for this thesis is formulated as: **How to detect a high-risk cyber-attack intrusion?**
Several sub-questions have been formulated to be able to answer the main research question.

Firstly, the configuration of an electrical power grid control system is researched. The electrical power grid control system can be separated into 3 categories: Power substations, telecommunication network and SCADA network. A comprehensive overview is presented for each of these infrastructures, explaining their function and evolution through their implementation.

Thereafter, to understand the methods adversaries use for cyber-attacks, two historical cyber-attack cases on industrial control systems are researched and evaluated. This results in an understanding of how cyber-attacks unfold and provides a lesson learned. To further expand understanding of methods adversaries might use, research into attack vectors or methods for adversaries to infiltrate into the network are evaluated. Measures against several of the attack vectors are researched and evaluated. With the first three chapters a detailed electrical power grid control system (shown in Figure 2.1 and attached as Appendix C) is created whereby modern cyber security solutions are implemented.

This detailed electrical power grid control system is the basis whereupon cyber-attack scenarios are researched. 12 cyber-attack scenarios are presented and categorised in malware, compromised vendor and compromised remote location. A risk assessment evaluates each of the 12 cyber-attack scenarios. Concluding that a sniffing & replay cyber-attack is the highest risk cyber-attack scenario. The sniffing & replay attack is simulated on a local private network to see the ease and the result of such a cyber-attack. A simulation also provides insight into a possible detection method. The results show, assuming that the adversary is able to infiltrate himself into the network that the detection method should focus on the process of the monitoring and control of the electrical power grid. The simulation also provides process data to understand the communication between devices.

To answer the main research question, an algorithm method is created and presented, this algorithm detects abnormal process data from normal process data by comparing the interactive real time data against a certified data set, the benchmark. The biggest conclusion however is that an intrusion detection system is not necessarily the best solution against a sniffing & replay attack, since the attack already happened. Proactive or preventive cyber security measures prevent the cyber-attack from happening. Encryption or authentication implemented within network traffic would be solid solution for preventing any cyber-attack related to manipulating network traffic. The intrusion detection algorithm should be used as a last resort, when the proactive measures fail. When intrusion is detected, further spread can be prevented if acted adequately to the alarms provide by the intrusion detection system. Reactive measures are not discussed in this thesis but are essential as well. This shows that just one category of measures is insufficient, the combination of measures is essential for a cyber resilience system.

SAMENVATTING (DUTCH SUMMARY)

Industriële controlesystemen zijn essentieel voor het functioneren van onze samenleving, omdat ze onze elektriciteit, water, landbouw, gezondheid, communicatie, transport, hulpdiensten en financiële dienstverlening beheersen. In het digitale tijdperk van big data en data-analyse zijn deze zogeheten kritische infrastructuren ook aan het digitaliseren, zodat zij kunnen blijven voldoen aan de vraag van klanten voor data-analyses van hun verbruik en betrouwbaarheid van hun energievoorziening. De toenemende implementatie van hernieuwbare energiebronnen speelt ook een rol in het digitaliseren van het elektriciteitsnet en zorgt ervoor dat de energiestromen bidirectioneel worden. Om de bidirectionele energiestromen te beheren, moeten meer intelligentere elektronische apparaten worden geïmplementeerd. Al deze veldapparaten zijn verbonden met een gecentraliseerd controlecentrum dat de SCADA-servers (Supervisory Control and Data Acquisition) huist. Deze servers vezamelen de gegevens en verstrekken de data aan de operators zodat zij het elektriciteitsnet kunnen beheren en de energievoorziening stabiel en betrouwbaar kunnen houden. Deze systemen worden beheerd door utiliteitsbedrijven. Zij gebruiken de gegevens voor gegevensanalyse, prognoses en verdere ontwikkeling van hun infrastructuur.

De digitalisering biedt veel voordelen voor het beheer van het elektriciteitsnet. Met de digitalisering en toenemende gevallen van cyberaanvallen wordt de bedreiging van cyberaanvallen echter steeds relevanter. Dit blijkt ook uit de eerste bekende succesvolle cyberaanval op het Oekraïense elektriciteitsnet. Bij deze aanval was een aanvaller in staat om het elektriciteitsnet vanaf een externe locatie te besturen, waardoor voor een groot aantal klanten stroomuitval het gevolg was. Daarbij is er een toename van malware die speciaal ontworpen wordt om industriële controlesystemen te raken. Daarom lopen onze kritieke infrastructuren en onze samenleving risico.

De hoofd onderzoeksvraag luidt: **Hoe kan een hoogrisico cyber-aanval worden gedetecteerd?** Verschillende deelvragen zijn geformuleerd om de hoofdvraag te kunnen beantwoorden.

Allereerst wordt de configuratie van het regelsysteem van het elektriciteitsnet onderzocht. Het regelsysteem voor het elektriciteitsnet kan in 3 categorieën worden onderverdeeld: onderstations, telecommunicatie netwerk en SCADA-netwerk. Voor elk van deze infrastructuren wordt een uitgebreid overzicht gepresenteerd, waarin hun functie en ontwikkeling worden uitgelegd aan de hand van hun implementatie.

Daarna worden twee historische gevallen van cyberaanval op industriële controlesystemen onderzocht en geëvalueerd. Dit om de methoden te begrijpen die aanvallers gebruiken voor cyberaanvallen. Dit resulteert in een goed begrip van hoe cyberaanvallen zich ontvouwen en biedt leermomenten. Om de methoden die aanvallers gebruiken nog beter te begrijpen, wordt onderzoek gedaan naar eventuele methoden die gebruikt worden door aanvallers om een netwerk te infiltreren. Dit zijn zogeheten aanvalsvectoren. Maatregelen tegen verschillende aanvalsvectoren worden onderzocht en geëvalueerd. Met de eerste drie hoofdstukken wordt een gedetailleerd regelsysteem van het elektriciteitsnet (zowel weergegeven in figuur 2.1 als bijgevoegd in bijlage C) gecreëerd. Daarbij is moderne cyberbeveiliging geïmplementeerd.

Dit gedetailleerd regelsysteem van het elektriciteitsnet is als uitgangspunt genomen voor onderzoek naar cyberaanval scenario's. 12 scenario's voor cyberaanvallen worden gepresenteerd en gecategoriseerd in malware, aangetaste leverancier en aangetaste externe locatie. Een risicobeoordeling evalueert elk van de 12 cyberaanval scenario's en concludeert dat een sniffing & replay cyber-aanval de meest risicovolle cyberaanvalscenario is. De sniffing & replay-aanval wordt gesimuleerd op een lokaal privaat netwerk om het gemak en het resultaat van een dergelijke cyberaanval te beoordelen. Een simulatie biedt ook inzicht in een mogelijke detectie methode. De resultaten laten zien dat de detectiemethode zich zou moeten concentreren op het proces van het elektriciteitsnet, ervan uitgaande dat de aanvaller in staat is zichzelf in het netwerk te infiltreren. De simulatie biedt ook proces gegevens om de communicatie tussen apparaten te begrijpen.

Om de belangrijkste onderzoeksvraag te beantwoorden, wordt een algoritmemethode gecreëerd en gepresenteerd. Dit algoritme detecteert abnormale procesgegevens van normale procesgegevens door de interactive realtime geveven te vergelijken met een gecertificeerde gegevensset, het criterium. De grootste conclusie is echter dat een indringingsdetectiesysteem niet noodzakelijk de beste oplossing is tegen een sniffing & replay-aanval, aangezien de aanval al is gebeurd. Proactieve of preventieve cyberbeveiligingsmaatregelen zijn een betere oplossing omdat ze voorkomen dat de cyberaanval überhaupt plaatsvindt. De implementatie van versleuteling of authenticatie in het netwerkverkeer zou een solide oplossing zijn voor het voorkomen van cyberaanvallen gerelateerd aan het manipuleren van netwerkverkeer. Het algoritme voor indringingsdetectie zou als laatste redmiddel moeten worden gebruikt, wanneer de proactieve maatregelen falen. Wanneer indringing wordt gedetecteerd, kan verdere verspreiding worden voorkomen als adequaat gereageerd wordt op de alarmen van het indringingsdetectiesysteem. Reactieve maatregelen worden niet besproken in deze scriptie, maar zijn ook essentieel. Dit toont aan dat slechts één categorie maatregelen onvoldoende is. Juist de combinatie van maatregelen is essentieel voor een cyber-veerkrachtig systeem.

Table of Contents

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
ADMS	Advanced Distribution Management System
AMI	Automatic Meter Infrastructure
AMR	Automatic Meter Reading
API	Application Programming Interface
ARP	Address Resolution Protocol
BCU	Bay Control Unit
CA	Contingency Analysis
CM	Crew Management
DC	Data Concentrator
(D)DoS	(Distributed) Denial of Service
DMS	Distribution Management System
DPI	Deep Packet Inspection
DTS	Dispatcher Training Simulator
DUT	Device Under Test
ED	Economic Dispatch
EMS	Energy Management System
EUS	External User Support
FEP	Front End Processor
FLISR	Fault Location Isolation and Service Restoration
FR	Feeder Reconfiguration
GIS	Geographic Information System
HTTPS	Hypertext Transfer Protocol Secure
ICCP	Inter-Control Centre Communication Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
INC	Intelligent Network and Communication
IPS	Intrusion Protection System
IS&R	Information Storage & Retrieval
IT	Information Technology
LAN	Local Area Network
LFC	Load Frequency Control
MAC	Media Access Control
MITM	Man-In-The-Middle
MMI	Man-Machine Interface
MMS	Market Management System
NCIT	Non-Conventional Instrument Transformer
OLE	Object Linking and Embedding
OLTC	On-Load Tap Changers
OMS	Outage Management System
OPC-UA	Object Linking and Embedding for Process Control - Unified Architecture
OPF	Optimal Power Flow
OSI	Open System Interconnection
OT	Operational Technology
PDS	Program Development System
PF	Power Flow
PLC	Programmable Logic Controller
QAS	Quality Assurance System
RAT	Remote Access Trojan
RM	Reserve Monitoring
RTU	Remote Terminal Unit
SAN/NAS	System Area Network/Network Attached Storage
SCA	Short Circuit Analysis
SCADA	Supervisory Control and Data Acquisition
SCUC	Security Constraint Unit Commitment
SE	State Estimation
SFTP	Secure File Transport Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol

SMV	Sample Measured Values
SIEM	Security Information and Event Management
TC	Trouble Call
TCP/IP	Transmission Control Protocol/Internet Protocol
TDoS	Telephonic Denial of Service
UART	Universal Asynchronous Receiver/Transmitter
UC	Unit Commitment
USG	Unidirectional Security Gateway
VCS	Vendor Control System
VPN	Virtual Private Network
VVC/O	Volt/VAr Control/Optimization
WAN	Wide Area Network

1 INTRODUCTION

This chapter provides an introduction to the company DNV GL and their expertise. As well as Supervisory Control and Data Acquisition (SCADA) used for Energy Management Systems (EMS) and Distribution Management Systems (DMS). It also summarises current changes in SCADA/EMS/DMS architecture and clarifies the essence of cyber security. This chapter is concluded with an informative outline of the thesis.

1.1 Company

DNV GL [1] was created from of a merger between Det Norske Veritas (DNV) and Germanischer Lloyd (GL) in 2013. Previously, in 2008 GL acquired Advantica to broaden GL's service scope to consultancy services in the oil and gas sectors. Followed by a merger with Noble Denton in 2009 which further expanded it activities in offshore technical services. GL shortly after acquired Garrad Hassan, the world's largest wind energy consultancy firm. DNV and KEMA joined forces in 2012 to create a world-leading consulting, testing and certification company for the global energy sector. These main companies presented in Figure 1.1, merged to what is now DVN GL.

Figure 1.1 DNV GL merger [1]

DNV GL is a global leading quality assurance and risk management company. Driven by the purpose of safeguarding life, property and the environment, DNV GL enables organisations to advance the safety and sustainability of their businesses. They provide classification, technical assurance, digital solutions and independent expert advisory services to the maritime, oil & gas, power and renewables industries. As well as certification, supply chain and data management services to customers across a wide range of industries. Operating for over 150 years, with 12500 employees located in more than 300 offices across 100 countries.

DNV GL Energy represents over 20% of the turnover in DNV GL and is expected to grow. A subsection of DNV GL Energy is the region Advisory Asia Pacific which includes countries such as Australia, China, Singapore, India, Japan, Korea and Thailand. Clean Technology Centre (CTC) in Singapore is the head office for Advisory Asia Pacific and seen as the hub to the Asia Pacific countries. DNV GL Energy Singapore is divided in two departments, Energy Advisory and Renewables Advisory. Under Energy Advisory is the department Intelligent Network and Communication (INC) which is led by Gary Chee Kiong Ang, my company supervisor. Intelligent Network and Communication is active amongst Protocol Competence Testing, Power System Operation, Cyber Security, IEC61850 Substation Automation, SCADA/EMS/DMS Digital Transformation and System & Component Level.

1.2 Background

Modern Supervisory Control and Data Acquisition (SCADA) systems are essential for monitoring and managing power systems. The power system operators control their SCADA systems from a central point, the control centre and use it as an Energy Management System (EMS) or Distribution Management System (DMS) to manage the energy flows within their network. These systems were designed for reliability, not security. [2]

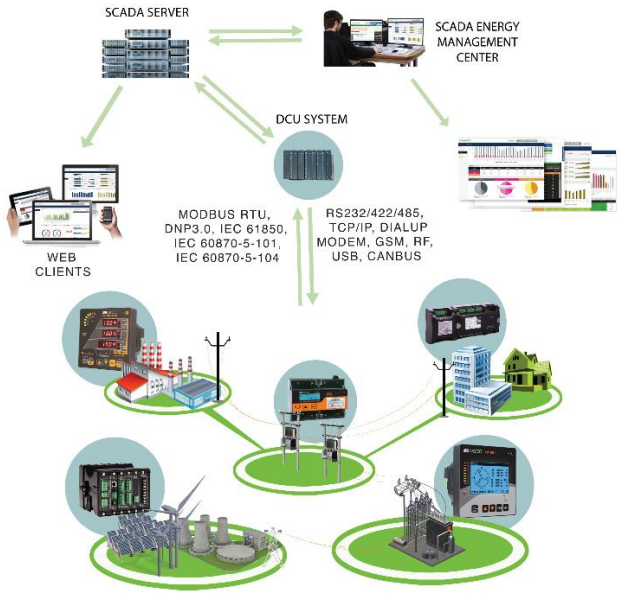


Figure 1.2 Electrical power grid control system [3]

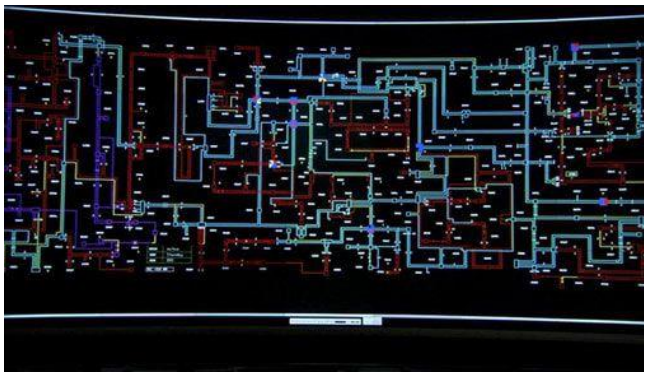


Figure 1.3 Control centre console overview [4]

Due to the digitalisation of the electrical power grid for autonomous operation, communication between smart protection relays, meters and sensors which are Intelligent Electronic Devices (IEDs) is essential. The implementation of IEC61850 (will be further explained in chapter 2.1.1) requires more IEDs which control and monitor all sorts of equipment using optimisation algorithms for load configuration. These IEDs will be able to communicate with each other over the power substations Local Area Network (LAN). Therefore, the merging of Operational Technology (OT) and Information Technology (IT) systems is inevitable. Digitalisation brings a lot of advantages for monitoring and controlling the electrical power grid, however, it also creates cyber security concerns.

The standardization and implementation of open communication protocols is an upward trend. With these standardized protocols utilities are not dependent on the proprietary communication protocols from vendors. Therefore, they are free to determine with which vendor they do business. This creates a competitive tender market whereby no vendor has a monopoly. However, all these open communication protocols are publicly available to adversaries as well. Therefore, an adversary can easily gather knowledge about a certain open protocol which is broadly used. Since the utilities infrastructure increasingly resemble each other, this knowledge can be used to attack a lot of different utilities. Therefore, cyber security for these communication protocols is increasingly important.

The ongoing digitalisation and standardization are also required for the energy transition, towards a more renewable energy infrastructure. The implementation of renewable generation as well as local renewable generation and power storage changes the way of the power flows within the power systems. Traditionally the power flows from the generators to the end users as shown on the left side of Figure 1.4. In the near future end users consist of consumers with solar generation and power storage including an optimization system which will constantly determine the optimal energy consumption. Besides the small consumers, the renewable generators in combination with energy storage systems will charge and discharge determined by their optimisation systems. The implementation of renewables and energy storage changes the power flows within the electrical power grid. The power flow becomes bidirectional as shown on the right side of Figure 1.4. To manage these increasingly complex systems more IEDs must be implemented, whereby cyber security plays an important role for reliability and security of the system.

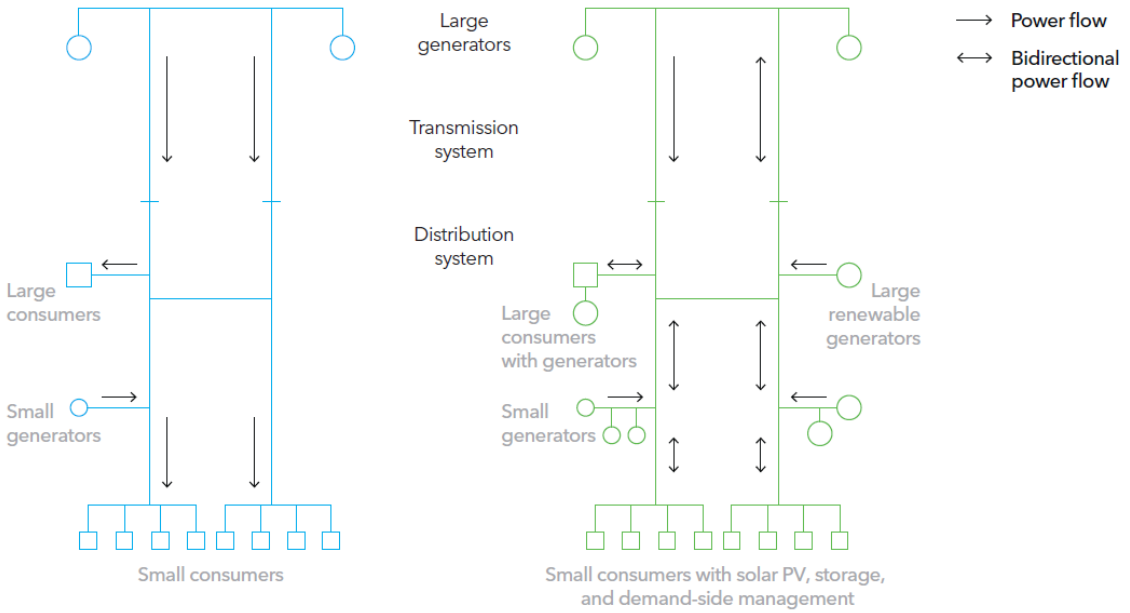


Figure 1.4 Traditional and new electricity system architecture [5]

Another reason showing the essence of security and reliability within the electrical power grid is the electrification of society. It is becoming a more common practise to replace gas for electricity, for instance for heating or cooking in households. As well as for our transportation by electrical vehicles. These changes together with the implementation of renewable energy generation are required to obtain the set climate goals of the reduction of greenhouse gasses. However, these changes will increase the electricity demand wherefore the electrical power grid becomes even more critical to our society.

Besides the ongoing changes in the electrical power grid infrastructure, the electrical power grid is part of the critical infrastructures. Critical infrastructures are described as assets that are essential for the functioning of society and economy. A few other critical infrastructures are water, agriculture, health, communication, transportation, emergency service and financial service. [6, 7] Since the critical infrastructures are essential for society they could be targeted by adversaries with intent driven by money, politics, religion, activist causes, recreation, recognition or simply malevolence. [8] To prevent chaos such as recently seen in Venezuela's power outages [9], maintenance and cyber security of these critical infrastructures are essential. Since SCADA is broadly used in critical infrastructures research into this topic could be useful to other SCADA controlled critical infrastructures as well. Figure 1.5 shows the percentage of cyber-attacks per critical infrastructure, whereby the energy industry is targeted 54% of the time.

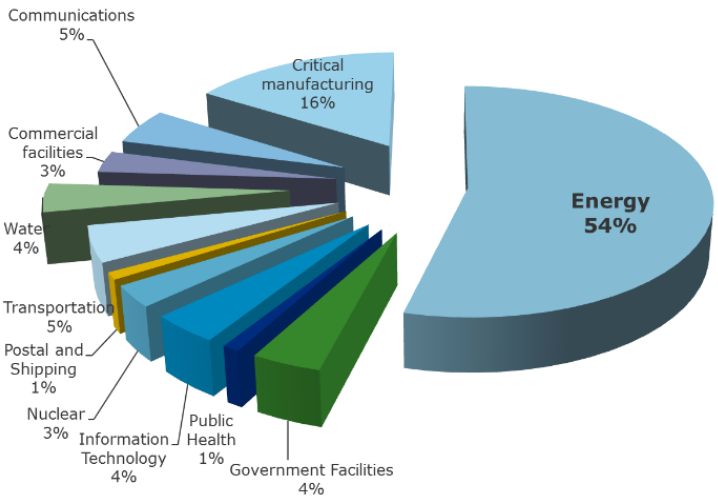


Figure 1.5 Percentage of cyber-attacks per critical infrastructure [6]

1.3 Research objective

This research shall focus on the detection of intrusion within the SCADA network of a power system operator. Creating an algorithm for a high-risk cyber-attack scenario. Therefore, the algorithm should be able to detect given cyber-attack scenarios with the provided variables by the system.

A big part of this research shall focus on the understanding of the SCADA configuration. As well as a general view of cyber security in operational technology. The end result being an algorithm which should be able to detect a given cyber-attack scenario. This algorithm will be presented in the form of a flowchart diagram and does not include programming of any code. A SCADA network will be simulated and researched for possible algorithm methodology creation.

Cyber security has a wide spectrum, the focus is on the aspect of a cyber-attack, detecting intrusion in the network. Therefore, chapters will limit to only relevant information for this research. Topics of physical security, social engineering and response towards cyber threats will not be discussed.

The main research question is formulated as: **How to detect a high-risk cyber-attack intrusion?**
Sub-questions to answer the main research question are:

- What is the network configuration of an electrical power grid infrastructure?
- How did historical cyber-attacks on industrial control systems (ICSs) unfold?
- What are the attack vectors for these electrical power grid infrastructures?
- Which measures for cyber security are available?
- What cyber-attack scenarios are possible and what is their potential risk?

By answering the sub-questions in the following chapters, the answer for main research question will become clear. Several research methods are used, including desk research into the energy sector, SCADA/EMS/DMS applications, historical cyber-attacks, attack vectors and measures. As well as several interviews with experts in the field about cyber and physical security. And lastly an experiment using simulation for verification and validation purposes.

1.4 Outline of the thesis

Chapter 2 consists of an in-depth research about the configuration of the SCADA network architecture as well as the functionalities and application running on top of the network. Chapter 3 focusses on historical cyber-attacks on ICSs to create a better understanding of methods used by cyber criminals. Chapter 4 investigates possible security breaches as well as security measures. These measures reflect to the detailed electrical power grid control system provided in chapter 2, which is used as base point for the cyber-attack scenarios. These risks and cyber-attack scenarios are described and evaluated in chapter 5. The highest risk cyber-attack scenario has been investigated and simulated in chapter 6, whereby mitigating measures and an additional algorithm for detection are proposed. This thesis is concluded with chapter 7. The structure of the thesis is also illustrated in Figure 1.6. The project execution plan is attached in Appendix A and a competence accountability report is attached in Appendix B.

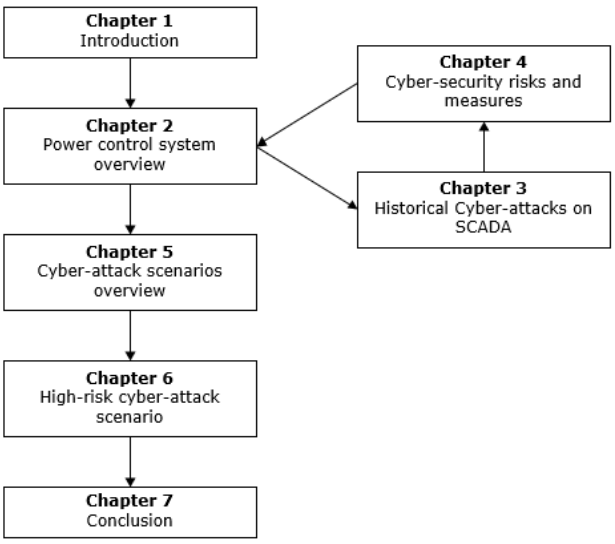


Figure 1.6 Thesis outline map

2 ELECTRICAL POWER GRID CONTROL SYSTEM OVERVIEW

In order to get an understanding of an electrical power grid control system, which comprises of power substations, telecommunication network and SCADA network. Comprehensive research into the network configuration is fulfilled. SCADA is a broad term and can be used for a lot of different types of infrastructures which include control and data acquisition. This research focusses particularly on the configuration of the SCADA system used for the electrical power grid control and monitoring. Electrical power grid control systems themselves vary a lot due to the topology of a country, the different political relations of countries, the variety of vendors to choose equipment from, the year of construction and the desired design philosophy finding a balance between reliability, security and cost. Therefore, there cannot be one description of an electrical power grid control system used by power system operators. The following chapter will describe the different infrastructures of the electrical power grid control system and will create a broad overview of network components used for the monitoring and control of an electrical power grid. All presented information has been generalized and cannot be connected to any specific utility.

2.1 Electrical power grid control system network

A broad overview of a complete power system network is shown in Figure 2.1 and is also attached as Appendix C. Figure 2.1 shows from the device level in the power substation's bay through the telecommunication network all the way up to the SCADA network. The network is a general setup of an electrical power grid control system network used for EMS or DMS functionalities. [7, 10, 11, 12]

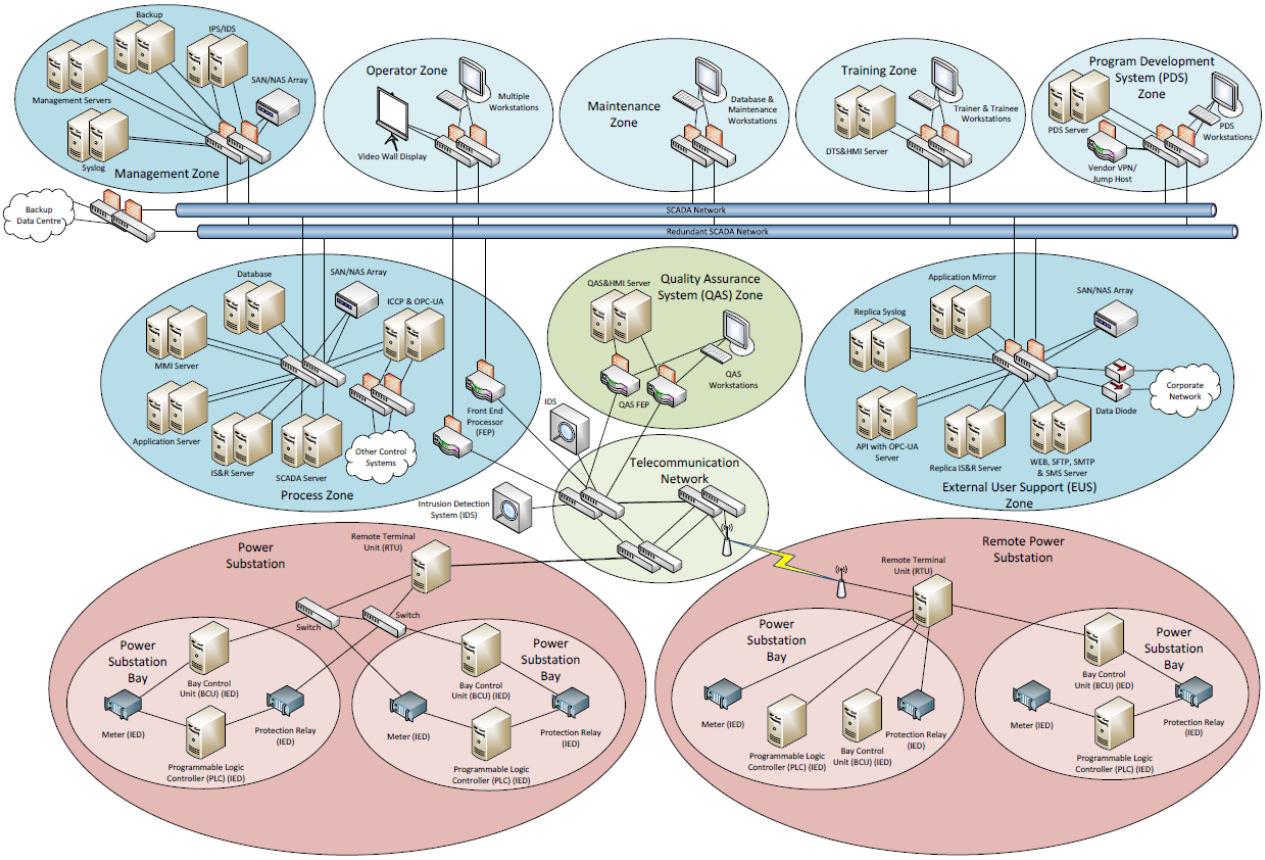


Figure 2.1 Detailed electrical power grid control system overview

The biggest changes in electrical power grid configurations through the years have been the integration of IT into OT, the additional software and communication protocols. Due to the addition of IEDs with additional communication structures. IEC Technical Committee 57 is one of the technical committees of the International Electrotechnical Commission (IEC). Technical Committee 57 is responsible for the development of standards for information exchange for power systems. The following paragraphs will discuss from bottom up, the evolution of each of the infrastructures, to complete a broad overview of an electrical power grid control system network.

2.1.1 Power substation network

High voltage power substations generally make use of a double busbar system. The connecting circuits or bays could connect to either one of the busbars. Two general configurations of a line/cable bay are shown in Figure 2.2. For each bay there is a Bay Control Unit (BCU) which measures the voltage and current for each circuit. As well as the positioning of all the switching gear and important events & alarms. The switch gear in the bay can be controlled locally by the Human-Machine Interface (HMI) on the panel. As well as from the control centre, both actions will send commands to the BCU. The BCU is the interface between the switching gear and control systems and will control switching component. Apart from the BCU each bay hosts several IEDs. IEDs are microcontroller-based controllers, devices as BCU, protection relays, meters and Programmable Logic Controllers (PLCs). All these devices control and measure bay components such as circuit breakers, transformers and switching gear. All required data for the control centre will be collected by a Data Concentrator (DC) or Remote Terminal Unit (RTU) via the bay IEDs. These DC and RTU devices are the interfaces between the control centre and the power substations. [13]

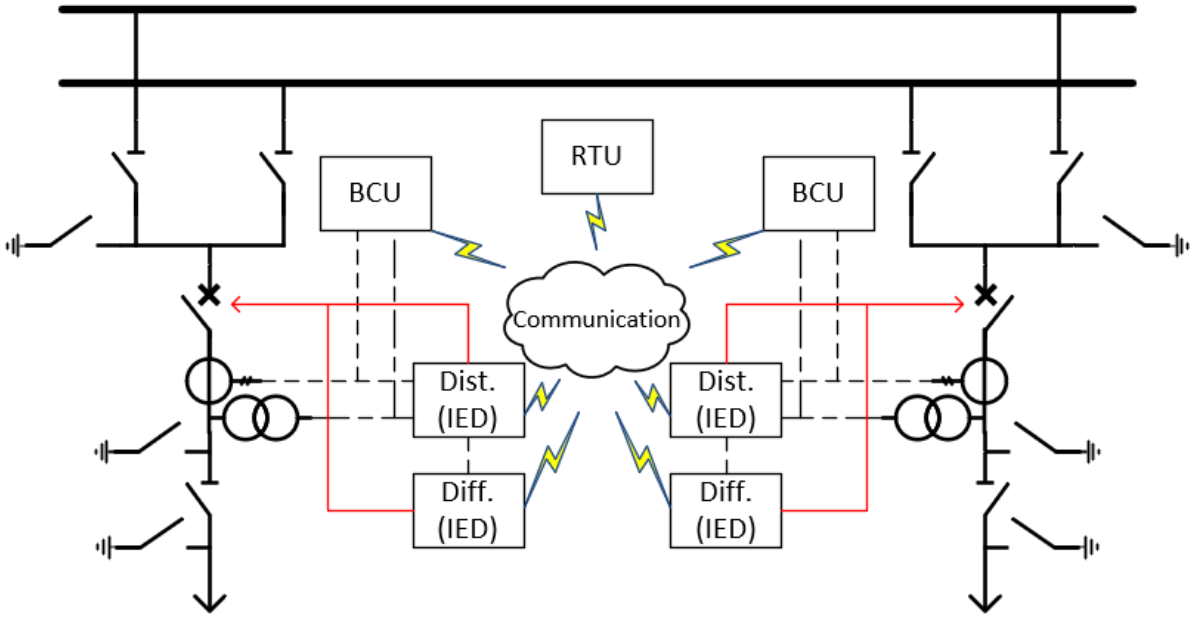


Figure 2.2 General bay configuration

Through the years several communication protocols between IEDs are standardised. These communication standards require different network configurations. Figure 2.3 zooms in on the two substations, which shows several common communication network configurations. Multiple communication protocols can be implemented at these different communication network configurations.

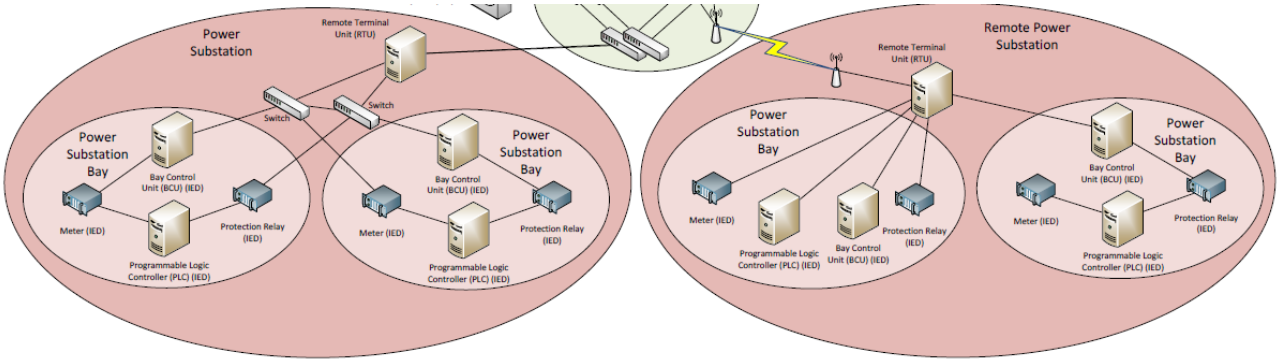


Figure 2.3 Communication within power substation TCP/IP (left) & serial (right)

The "Remote Power Substation" shown on the right in Figure 2.3 could be seen as a conventional type of power substation. These are still being built by corporations who are conservative to use more digitalized technologies for the sake of security. These power substations make use of serial communication protocols. The serial communication could be either star or open loop configured. The star configuration is shown in the left bay of the remote power substation, using RS-232 serial communication architecture to transfer data between the IEDs and the DC or RTU, point-to-point. The open loop serial communication is shown in the right bay of the remote power substation, using RS-485 multidrop serial communication architecture. RS-485 uses master-slave configuration, the drivers use three-state logic allowing individual nodes to be deactivated. This allows linear bus topology using two wires. At the end of the open ring the two wires are connected by a so-called termination resistor, filtering signal reflection which could cause data corruption.

Both serial communication configurations are broadly implemented in built power substation. Both configuration lack redundancy, as can be seen from Figure 2.4. The star configuration of RS-232 is single wired. If there is something wrong with the connection, communication to the device is lost. The open ring configuration of RS-485 means if a connection between two devices is disrupted all communication to underlaying devices is lost. Open application protocols such as Modbus, IEC60870-5-101 and DNP3.0 all support serial communication on RS-232 and RS-485 configuration. Some vendors develop proprietary protocols which are also capable of running on these configurations. Since RS-485 uses multiple slaves a form of addressing is done whereby each slave holds a byte address which the slave device will react to. For the datalink layer Universal Asynchronous Receiver/Transmitter (UART) interfacing is used to convert the serial bit stream. Lastly for the physical layer either copper of fibre cables could be used.

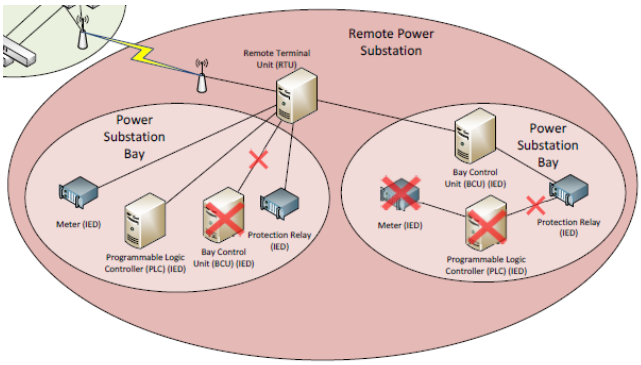


Figure 2.4 Serial connection failure

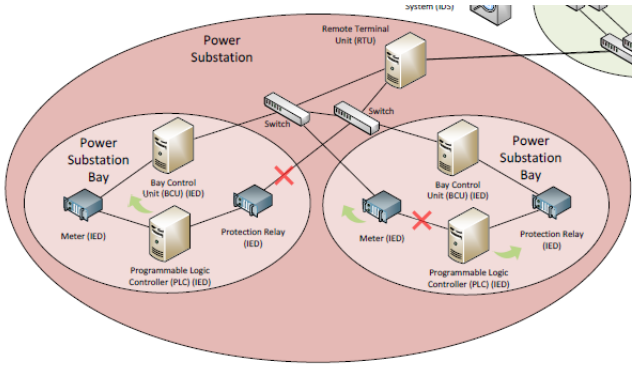


Figure 2.5 TCP/IP connection failure

The "Power substation" shown on the left in Figure 2.3 could be seen as a more digitalized and modern power substation. Here, if a connection fails, communication via the other side remains, as shown in Figure 2.5. The communication within the substation and bays is done using Transmission Control Protocol/Internet Protocol (TCP/IP) communication protocols. These TCP/IP protocols use closed ring structures, meaning all IEDs form a closed loop connecting to redundant switches. This redundancy provides a more reliable and secure network. The open application protocols, Modbus TCP/IP, IEC60870-5-104 and DNP3.0 as well as proprietary application protocols all support TCP/IP communication in closed loop architecture. TCP/IP uses a four-layer structure, based on the seven-layer Open System Interconnection (OSI) model [14]. Whereby the TCP protocol is used in the transport layer for reliable communication. The IP protocol is used in the network layer to communicate between devices. Ethernet IEEE.802.3 protocol is used for the datalink and physical layer.

Future substations will be fully set up according to the application protocol IEC61850. The IEC61850 protocol is used for power substation automatization. The protocol uses TCP/IP configuration and is standardized so IEDs and RTU from different vendors could directly communicate using a variety of protocols. The Non-Conventional Instrument Transformer (NCIT) [15] is a great example of the use of the IEC61850 protocol. This transformer simultaneously measures voltage and current and transmits this data via fibre optic cables. The current fibre optic measurement does not reach saturation by high currents and is therefore ideal for measuring short circuit currents. The measurements of the current and voltages can be directly sent to the required IEDs in the network using one of IEC61850 protocols: Sample Measured Values (SMV).

2.1.2 Telecommunication Network

The telecommunication network connects all the RTUs and DCs and provides data throughput for communication between substation and SCADA system. The telecommunication network is a private Wide Area Network (WAN), a computer network spanning large regions to transmit data over long distances and between different substation LANs. The general hardware equipment used for a telecommunication network are routers, modems, hubs and switches. The wide spanning telecommunication network is usually segmented into regions for security. Therefore, if an adversary has compromised a part of the network he will not be able to directly reach all of the telecommunication network.

The mediums which could be used for communication are power line carrier, pilot cable, telecom cable, fibre optic, microwave radio, 3G/4G GSM network. [16] In case the topology of a country does not allow a directly wired connection or the cost for one would be excessive, a connection to the isolated or remote location of a substation could be made by a dedicated wireless telecommunication connection through a microwave channel. This telecommunication could be leased or bought from a telecom provider or even be part of a utilities own private infrastructure. Another option could be satellites to span an even wider connection.

The communication used in the telecommunication networks could be either serial or TCP/IP. For serial communication the application protocols used could be again the open protocols Modbus, IEC60870-5-101 and DNP3.0 or proprietary protocols. For TCP/IP communications the open application protocols are Modbus TCP/IP, IEC60870-5-104 and DNP3.0 or proprietary protocols. Most telecommunication network are TCP/IP nowadays because of the communication structure and data transfer speed. Although there are still utilities who stick to serial communication. A comparison of the OSI model versus the RS-232, RS-485 and TCP/IP configuration is shown in Figure 2.6.

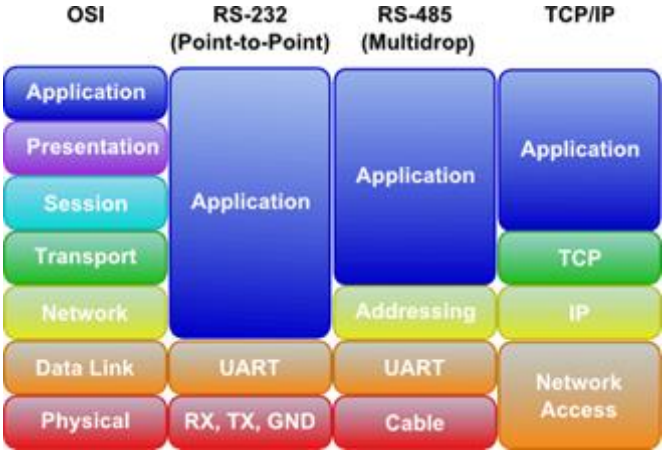


Figure 2.6 OSI model vs RS-232, RS-485 and TCP/IP configuration [17]

On the distribution level wireless communication is often used due to the size of infrastructure. The wireless communication is broadcasted and encrypted through modems. This encryption however is over the communication line and is not end-to-end encryption between the devices. The cost for creating a wired infrastructure in urban areas is often very high. With the integration of renewable generation as well as the digitalisation, more IEDs must be implemented, to monitor and control the network, the telecommunication network is an ever-extending infrastructure to connect those devices into one network.

The utilities configure their network in such a way, that no direct RTU to RTU communication is possible on the application protocol level: every communication is initiated from central SCADA to the RTU in the substation. Meaning that if an RTU would communicate to another RTU the communication would go through the central SCADA. There are protection relays (IEDs) which sometimes communicate to other protection relays located in another substation. This is for instance for line or cable protections, where for each bay the current is measured. The differential protection relay needs two currents to measure a difference. Therefor the current measures and trip signals are communicated between protection relays located in different power substations. These communication links between protection relays are not connected over the telecommunication network but are usually hard wired dedicated serial connections from protection relay to protection relay.

2.1.3 Supervisory Control and Data Acquisition Network

The Supervisory Control and Data Acquisition network processes the interactive real time data which is used for energy management applications. The SCADA takes care of the interactive real time data, performs data analytics and provides the data via the video wall display and operator workstations to the operators. The operators can perform switching actions, the SCADA system will therefor send a command to the telecommunication network which will provide the command to the right device in a substation. Such action will receive confirmation by the updated data and the status of the component in the substation, e.g. the position of a field switch.

The network is fully redundant for reliability purposes and is connected to at least one exact copy of the SCADA server's data centre. In operation, depending on the setup of the servers, the main server is active while the backup is on hot-standby meaning it can take over immediately because they are synchronised. Another setup could be active-active were both servers are running with the capability to immediately take over each other's processes. Additionally, in case of an emergency the power system operators could move the whole operation to the replica control centre. The SCADA network has several functions spread over different servers. The SCADA network can therefore be divided into several zones with each a different purpose and privilege to the system. [18]

Figure 2.7 Quadrant for Advanced Distribution Management Systems [19]

There are many different vendors offering their SCADA solution based on their own created platform, the ranking is shown in Figure 2.7. The SCADA network as well as the segmented zones shown in Figure 2.1 are based of the SCADA solutions vendors such as Schneider Electric [20], GE [21], Siemens [22], ABB [23] and OSI [24] offer, as well as internal documentation used for consultancy towards utilities. Each vendor developed its own software and functionalities. Of course, the functionalities are based on the same underlaying theory. As seen in Figure 2.1 each zone is segmented using firewalls to prevent unauthorised access. Below every zone including its server's functionalities will be described.

Process zone
The process zone is the main zone of the SCADA infrastructure. The data from power substation field components gets acquired through the DCs and RTUs, telecommunication network and Front End Processors (FEPs). The data gets stored and processed in the process zone, the FEPs provide a firewall between the SCADA network and telecommunication network. The FEPs could also be used to convert communication protocols, for instance if the telecommunication network still uses serial communication while the SCADA network is of course TCP/IP. The following servers are generally located in the process zone:

SCADA server
The SCADA server is the main server for the SCADA network and processes the incoming and outgoing data to the RTUs. The SCADA server communicates the data to the required servers.

Information Storage & Retrieval (IS&R) server
The IS&R server is a storage database which holds the SCADA process data for an amount of time, varying from one month up to one year. The stored data is used by other servers to calculate trend analyses and create energy consumption forecasts.

Application server
The Application server is a server which hosts all the SCADA applications and functionalities for the network. These servers could also be called according to their function like EMS, DMS or OMS server. The application server retrieves the required data from the SCADA server for its calculations, these results will trigger certain actions within the SCADA system or will present information to the operators.

Man-Machine Interface (MMI) server
The MMI server processes the interactive real time processed data from the SCADA server so it can be displayed at the operator zone. The relevant data of the network will be real time presented to the operators through the video wall display and the operator workstations.

Database server
The database stores the structures of the electrical power grid configuration. These structures will be presented at the video wall display and operator workstations together with the interactive real time network data.

System Area Network/Network Attached Storage (SAN/NAS) Array
System Area Network (SAN) & Network Attached Storage NAS both provide networked storage solutions. A NAS is a single storage device while a SAN is a local network of multiple devices. Either method can be chosen, a utility uses SAN/NAS of a longer-term storage. The SAN/NAS array stores process data for multiple years.

ICCP & OPC-UA server
These are communication servers, for which Inter-Control Centre Communication Protocol (ICCP) is used to connect to other utilities control centres. And hence creating an inter-utility real time data exchange, which is necessary for interconnected systems.
OPC-UA is a standard regarding Object Linking & Embedding (OLE) for Process Control – Unified Architecture. Meaning it is possible to implement on any platform and therefore able to connect Microsoft and Linux operated systems together.

Quality Assurance System (QAS) zone
The Quality Assurance System is just like the Process zone directly connected to the telecommunication network through its own FEPs. The QAS zone is used for testing of the communication to the substation. The QAS and Human Machine Interface (HMI) server provides a stand-alone SCADA environment with the facilities for testing. Testing happens when a new substation gets connected or changes to a substation's communications are made. After validation of a proper communication the communication gets switched over to the actual SCADA network.

External User Support (EUS) zone
The EUS or also called Demilitarized Zone (DMZ) is the connection between the SCADA network and the corporate network or OT/IT. A DMZ usually has a firewall on both sides for extra security. SCADA data will be copied to the EUS zone, wherefrom the corporate users can use the data for their application. Therefore, the corporate users do no directly retrieve data from the operational SCADA.

WEB, SFTP, SMTP & SMS Server
These servers provide data and messaging towards the corporate network. The WEB server provides interfacing with the application mirror through Hypertext Transfer Protocol Secure (HTTPS) functions for secure browsing. The Secure File Transport Protocol (SFTP) provides data transfers between the SCADA data and external applications. The Simple Mail Transfer Protocol (SMTP) server is used to facilitate the sending of emails from the SCADA system when certain alarms occur. The Short Message Service (SMS) gateway can send SMS text messages to personnel for specific user defined alarms.

Replica IS&R Server
The replica IS&R server is a replication of the IS&R deployed in the process zone. Thereby, the corporate users are facilitated with historical data.

API with OPC-UA Server
The Application Programming Interface (API) server provides a series of APIs for corporate users, external systems or applications accesses. The OPC-UA makes is once again possible to connect different platforms.

Replica Syslog
The replica syslog server captures all the logs from the management zone. The syslog of EUS can be connected to a Security Information and Event Management (SIEM) system in the corporate network.

Application Mirror
The application mirror server mimics the data and functionalities of the application server situated in the process zone. Therefore, the EUS zone is not directly connected to the SCADA system. The application mirror will provide real-time analyses and alerts from the applications to the corporate users.

Management zone
The management zone comprises servers and functions that facilitates the management of the entire SCADA system. It provides centralized management including services for the configuration, control, and monitoring of SCADA resources such as processors, network devices, applications and databases. The following servers are generally located in the management zone

Syslog server
The syslog server or system logger logs two types of data. Both on operating system level and SCADA level. This data can be used to evaluate events within the system.

Management Servers
The management servers contain the following functionalities:

- Account management: for user login access of operator workstations.
- Network & System management: for management of the network framework and configurations.
- Configuration management: Domain Name System (DNS) server for network configuration and restorage of the IP configuration.

Backup
The backup provides a backup of the whole system and stores all types of data. Daily, weekly and monthly backups are created is case of needed restoration of the system.

Intrusion Protection and Detection System (IPS/IDS) Server
The IPS/IDS server or software acts as a firewall to monitor the system for malicious activity or policy violations access. IPS/IDS will be further explained in chapter 4.2: Cyber security measures.

System Area Network/Network Attached Storage (SAN/NAS) Array
System Area Network (SAN) & Network Attached Storage NAS both provide networked storage solutions. A NAS is a single storage device while a SAN is a local network of multiple devices. Either method can be chosen, a utility uses SAN/NAS of a longer-term storage. The SAN/NAS array stores process data for multiple years.

Operator Zone
The operator zone is where the grid gets monitored and controlled by operators. Usually there is a video wall display which shows the whole electrical power grid and main parameters such as frequency. The video wall display provides the operators of an overview, indicates events using varies colours and alarms. The control of an electrical power grid is usually separated into smaller areas. For each of these areas there are several operator workstations in place showing the areas networks and events. The architecture for the grid as well as the shown data is provided by the MMI server and Database from the Process & Management zone.

Maintenance Zone
The maintenance zone is used to implement data changes through several database & maintenance workstations.

Training Zone
The training zone is a dedicated, stand-alone operator training simulator. The Dispatcher Training Simulator (DTS) is capable of simulating SCADA with its applications. The DTS equipment is isolated from the production zone with a firewall. There are both trainer and multiple trainee workstation available.

Program Development System (PDS) zone
The program development system zone is a stand-alone SCADA with its application. The program development zone is used to test applications, database, displays and reports. The PDS shall be used to aid in problem resolution, development and preliminary testing of new applications. Remote Virtual Private Network (VPN) or jump host access to the PDS is available. These connections are commonly used by vendors to assist.

The network is built on reliability through redundancy of servers and data centres. Security is implemented thought the different zones by segmentation using firewalls. The firewalls prevent unauthorised communication between zones. If one zone is corrupted, spreading by itself will be prevented by these firewalls. These zones all serve their purpose and communicate with each other like a LAN computer network, to provide data from and to each other. In the design shown in Figure 2.1 the corporate network only receives data from the SCADA network, which can be used for analytics. The data diode creates a unidirectional data stream, therefore if the corporate network is corrupted the infection is not able to spread to the OT network. However, it unsure if the data diode is a sustainable feature due to the increasing interest of data sending from the corporate network into the SCADA network, used particular for the smart meter infrastructure. For this research the data diode is implemented to showcase its result for cyber security of the network.

2.2 Functionalities

The functionalities of the SCADA system lay in the software application which processes the provided interactive real time data. Therefor the SCADA system is the infrastructure, where the applications of Energy Management System (EMS) and Distribution Management system (DMS) run on. EMS/DMS serve the same purpose which is maintaining stable operation of the electrical power grid. EMS is used to manage transmission system and generation while DMS is used to manage distribution systems. For that reason, these systems have some different software applications.

An EMS/DMS is a collection of computerized tools used to monitor, control, and optimize the performance of generation and transmission systems. This intelligent energy management software control system is designed to reduce energy consumption, improve the utilization of the system, increase reliability and predicts power system performance as well as optimize energy usage to reduce cost. EMS/DMS application use real-time data such as frequency, actual generation, power flows through transmission lines and plant unit's controller status to provide system changes.

There are primary, secondary and tertiary objectives for an EMS/DMS. The primary objective is to maintain the security and stability of the system. While the secondary objective focusses on the economic operation and control, the tertiary objective is optimization of operation. [25]

Primary objective:

- Maintaining the frequency within allowable limits.
- Maintaining the power flows in the transmission lines to the scheduled values.

Secondary objective:

- Economic operation of the power system through real time dispatch and control.
- Optimal control of the power system using both preventive and corrective control actions.
- Real time economic dispatch through real power and reactive power control.

Tertiary objective:

- Optimization of the power system for normal and abnormal operating scenarios.
- Maintenance scheduling of power system.

The primary objective is automatically controlled by a closed loop system without intervention of an operator, the secondary and tertiary are performed by the operators.

2.2.1 Energy Management System (EMS)

The functionalities can be divides into three categories: generation, network and forecast. [26]

Generation:

- Load Frequency Control (LFC)
- Economic Dispatch (ED) or Security Constraint Unit Commitment (SCUC) depending on the Market Management System (MMS)
- Reserve Monitoring (RM)

Network:

- State Estimation (SE)
- Power Flow (PF)
- Optimal Power Flow (OPF)
- Contingency Analysis (CA)
- Short Circuit Analysis (SCA)

Forecast:

- Generation & Load Forecast
- Unit Commitment (UC)

Load Frequency Control (LFC)
The Load Frequency Control function consist of primary and secondary frequency control. The primary control will act if there is a deviation in frequency meaning that there is a deviation in load and generation. The primary control will rebalance the load and generation by sending a new setpoint to the generators. Thereafter the secondary control will recover the frequency by controlling the generators to rebalance the power flow over tie-lines between areas. [27]

Economic Dispatch (ED) or Security Constraint Unit Commitment (SCUC)
Depending on the electricity market of a country there will either be an Economic Dispatch or Security Constraint Unit Commitment functionality in place. If a government company runs all aspects of the electricity market: generation, transmission, distribution and retail, there is a natural monopoly. The control centre will have an ED in place to determine the optimal output of their assets at the lowest possible costs.

If the electricity market is privatized meaning generation, transmission, distribution and retail are separate private entities there will be a SCUC in place. The generation companies will bid their electricity price for their unit commitment each time period, making it a competitive market between different generators. Which hopefully results in more efficient processes and cheaper electricity prices.

Reserve Monitoring (RM)
The Reserve Monitoring function will monitor the reserves, which in case of peak load should contribute to the generation. Reserve can be divided into two categories:

- Spinning reserve which is extra generator capacity that is available by increasing the power output of generators that are already connected to the power system.
- Non-spinning reserve applying generators which are currently not connected to the power system but can be brought online after a short delay.

State Estimation (SE)
The State Estimator (SE) function incorporates both measured and modelled information and dynamically estimates the states of unmonitored portions of the system. It shall be used for estimating active power and losses, reactive power and losses, voltage and current of all network components such as buses, transformers, lines, distributed generation and loads in the network. SE information is used by the other applications of EMS in actively managing the system in real time.

Power Flow (PF)
The power flow function calculates the state of the power system with input from the SE function. Data are displayed on the video control wall and operator workstations.

Optimal Power Flow (OPF)
The Optimal Power Flow function minimalizes power losses and costs and maximize system performance by calculating the optimal configurations for the electrical power grid. The calculations will be evaluated by the system operators, if granted they will make the switching actions.

Contingency Analysis (CA)
The function Contingency Analysis is a major function which calculates if the power system will remain within the operational allowance when an element of the electrical power grid fails. The element could be a generator, transmission line, transformer of whole substation. The contingency analysis calculates what the effect would be if such an event would occur. The system should be redundant meaning n-1 and remain operational if an element fails.

Short Circuit Analysis (SCA)
The Short Circuit Analysis function evaluates the fault current level of a short circuit case within the modelled power system, by specifying the fault type on the given equipment such as bus or line. It can calculate fault current of fault types including but not limited to three-phase, three-phase-to-ground, line-to-ground, line-to-line and line-to-line-to-ground fault. In addition, SCA should be able to calculate the impedance at each point.

Generation & Load Forecast
The generation and load forecast system receive input from weather forecast and uses historical data to determine the generation capacity and load expectancy. The weather forecast is especially important when large generation comes from renewables. The type of day in relation to the energy demand will be evaluated against the historical data to determine the load expectancy.

Unit Commitment (UC)
Unit Commitment is part of the generation forecast and is an operational planning which tells which unit will generate at a given time period. This is determined once again depending on the electricity market of the country.

The applications can be divided into two types: real-time and off-line. Real-time application will handle situation instantly while off-line applications are used for scenario determination. [26]

2.2.2 Distribution Management System (DMS)

DMS application is very similar to EMS however, DMS systems control the distribution of power instead of the transmission and generation. Hence, there are some differences, DMS only have one generation application which is RM, this application is used for monitoring small generator facilities and renewables which are connected to the distribution grid.

For network applications distribution it also uses SE and PF of display purposes. The OPF function can be divided into 2 functions: Feeder Reconfiguration (FR) and Volt/VAr Control/Optimization (VVC/O). Another additional function is Fault Location Isolation and Service Restoration (FLISR). Distribution forecast is the same as EMS but on a smaller scale.

Feeder Reconfiguration (FR)
Feeder Reconfiguration function provides optimal network configuration required for eliminating negative operating conditions such as overload at the line or transformer. The function will provide a set of switching procedures that reduce system losses and apply feeder reconfiguration for balancing the loads of primary stations to the operator. Consequently, the line and transformer loads shall be changed by transmitting the loads on one feeder to the other feeder.

Volt VAr Control/Optimization (VVC/O)
The Volt VAr Control/Optimization is an integrated solution throughout the entire distribution network. By automatically sending various control signals to switchable shunt capacitor banks to manage the VAr (the reactive power) within the network. The voltage gets controlled by automatically send control actions to tap positions of regulators and transformer On-Load Tap Changers (OLTCs). These controls will make sure that a variety of defined goals such as limit reactive power flows, reduce losses and control voltage within limits in the distribution system.

Fault Location Isolation and Service Restoration (FLISR)
The Fault Location Isolation and Service Restoration function can detect, in an expeditious and reasonably accurate manner, serves for fault evaluation and determination of fault location in the distribution network when network disturbances occur, and develop solutions (e.g. a switching procedure) for isolation and restoring service.

These additional functions are typical for the distribution level of the electrical power grid, where the infrastructure consists of loops whereby the optimal configuration for the feeders as well as optimization of reactive power provides less losses and optimal power flows. Since the distribution infrastructure is huge and complex, the FLISR provides fast analyses for the fault location as well as restoration by redirecting power to decrease power outage effects.

2.2.3 Outage Management System (OMS)

The OMS is a system used to assist in restoration of power after a power outage as well as managing planned outages for maintenance. The OMS include a Geographic Information System (GIS) system which gives an overview of the power network. Integrated systems are Automatic Meter Infrastructure (AMI), Trouble Call (TC) and Crew Management (CM). The OMS system is separated from the EMS/DMS systems and managed by the corporation receiving relevant information from the SCADA system.

Automatic Meter Infrastructure (AMI)
The Automatic Meter Infrastructure is an integrated system of smart meters, communication networks and data management systems. With the data from the smart meters, utilities can better determine the location and consequences of the outage.

Trouble Call (TC)
Trouble call is another system used by utilities to better determine the location of the outage. When customers experience an outage, they call the utility for answers. With the locations of the customers the utility can determine the location and consequences of the outage.

Crew Management (CM)
The Crew Management will send a service crew to the location based on the received information from the AMI and TC systems. The crew will try to locate the outage and conduct maintenance if required to get the power back on line as fast as possible.

Each utility is accountable for their outage times whereby significant bonusses or fines play a role depending on their performance. A team dedicated to outage management has a set of tools to resolve a power outage as fast as possible. As well as plan repair or replacement works to keep their infrastructure reliable.

2.2.4 Advanced Distribution Management System (ADMS)

An ADMS is the integrated combination of DMS and OMS in one system. An ADMS is not a one size fits all solution for utilities. Instead utilities can pick modules to create their own optimized system. This allows utilities to prioritize implementation with consideration to cost and benefits. Many additional modules are available, each value of a module depends on the individual utility's needs and infrastructure. [28] Utilities invest into ADMS because they are required by their customers who demand higher reliability, improved power quality, renewable energy sources, security of their data, and resiliency to natural disasters and other threats that disrupts the flow of power and their lifestyles.

Utilities that are pioneering ADMS are investing in this technology because they believe the capabilities it enables are essential to the future of their business. As technologies mature and distributed energy resources approach parity with traditional generation sources, customers are installing rooftop solar photovoltaic systems, electric vehicles, and other grid-connected devices that the utilities must accommodate. At the same time, regulators are developing policies that increase reliability and renewable energy portfolio standards, and they are discussing fundamental changes to how distribution utilities are regulated to encourage the integration of renewables and overall grid efficiency. Utilities that are investing in ADMS view it as necessary to stay relevant in the changing electricity business. [29]

3 HISTORICAL CYBER-ATTACKS ON ICS

To further understand the process of a cyber-attack on a SCADA system, research has been done into known cyber-attacks on SCADA and ICS. Looking at Stuxnet [30], a well-known malware causing physical damage to its targets as well as the first known successful cyber-attack on an electrical power grid: Ukraine 2015 [31].

3.1 Stuxnet

Stuxnet is a computer worm discovered in 2010 affecting Iran's nuclear program. The Stuxnet worm is written in several programming languages. It exploited four zero-day vulnerabilities in Microsoft's Windows operating system to spread and infect other computers. A zero-day exploit is a security software flaw that is unknown to the software vendor. Therefore, it has the potential to be exploited. [32] The four zero-day exploits used in Stuxnet are:

1. Automatic process from connected USB drives thereby spreading through USB drives.
2. Exploit of print spooler service by being able to create files and therefore copying itself to other devices.
3. Privilege escalation to execute software in computers.
4. Privilege escalation exploit to gain complete control over the affected system.

The Stuxnet worm originally spread from Iran, it is believed that Iran's nuclear program was its target. Since the Iranian nuclear powerplant was an isolated network someone must have infiltrated and inserted the infected USB to start the attack. The worm thereafter spread over the internet, probably because of personal using their laptop within the LAN of the plant as well as at home the worm spread through the internet infecting devices. After the Stuxnet worm settled in a system, it searched for Siemens Simatic WinCC/Step-7 software. Which is a program used to control industrial equipment. By effecting files used by this software the worm was able to access and control the PLC. Then Stuxnet would launch its attack by changing the speed of the centrifuges used in the nuclear facility, causing irreparable damage. The Stuxnet worm is a highly complex worm with probably a lot of resources invested. The creators of the worm had extensive knowledge about the Iranian powerplant. And probably the resources to test and verify their design. Additionally, the worm would connect itself to two servers located in Denmark and Malaysia in order to be updated. [30]

Things to note from the Stuxnet cyber-attack is, to prevent vulnerability to zero-day exploits as good as possible. Updating the operating system software with latest security patches is essential. The aspect of social engineering played its role in the Iranian powerplant as well. Personal and visitors should be checked according to G50 security clearance of a high category, in order to therefor minimise the risk of infiltration. Besides, personal should be trained according to security guidelines to prevent the chance of infected USBs being inserted into the systems network. The adversary was very knowledgeable about the installation and system. Therefore, he could launch an accurate attack specifically focussed on the type of PLC controlling the centrifuges. Information about the installation and its systems should be kept classified and stored in a secure manner. Making it harder for the adversary to do reconnaissance. The adversary might implement a broader cyber-attack to gain information, which could be detected in earlier stages.

3.2 Ukraine electrical power grid cyber-attack

Ukraine is the first known successful cyber-attack on an electrical power grid. On December 23, 2015, the regional electricity distribution company reported service outages. The outages were due to a third party's illegal entry into the company's computer and SCADA/DMS systems. Seven 110kV and 23 35kV substations were disconnected for three hours. Later was revealed that three regional electricity distribution companies were attacked. Resulting in several outages that caused approximately 225.000 customers to lose power across various areas. [31]

The adversary showed the capability to infiltrate into the SCADA system, bypassing all securities, block out the operator and take over full control, all from a remote area. Consequently, the adversary was able to perform a phase 2 cyber-attack according to ICS cyber kill chain. The Phases are shown in Figure 3.1 and Figure 3.2.

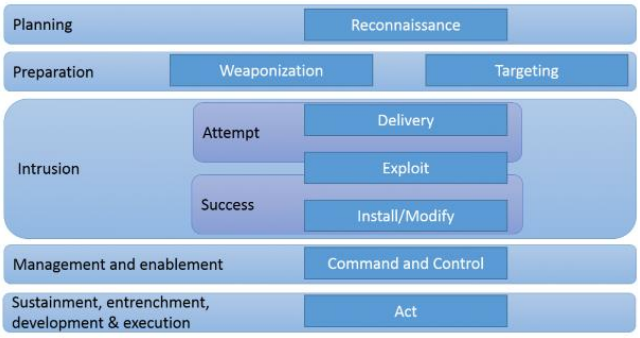


Figure 3.1 Phase 1 of ICS Cyber Kill Chain [33]

Figure 3.2 Phase 2 of ICS Cyber Kill Chain [33]

The adversary followed the ICS Cyber Kill Chain accordingly and started off by infiltrating the corporate network using varies methods, including spear fishing emails, BlackEnergy 3 malware and including malware into Microsoft Office documents. These methods were effective and granted him access in the IT network of the utility. They got hold of credentials and VPN access by which they could enter the SCADA network to harvest information and gain command and control and thereby completing phase 1.

The adversary leaned to interact with the DMS environments using remote workstation access as well as creating malicious firmware for communication devices. The adversary likely had systems in his organisation that they were able to evaluate and test his firmware against prior to execution. In preparation for the attack the adversary installed the malicious firmware in communication devices. He also installed malicious software identified as a KillDisk across the environment, which wiped workstations, servers and HMIs. Besides the adversary disconnected UPS system to cause backup failure. To complete the phase 2, attack the adversary executed the attack on the SCADA system by opening the circuit breakers through HMIs in the SCADA environment causing the power outage. Thereafter the adversary uploaded the malicious firmware to cause communication failure for the operators with the field devices. At the same time the adversary launched a Telephonic Denial of Service (TDoS) to the call centre so impacted customers could not report the outages. [31]

Things to note from the Ukraine cyber-attack is, the actual cause of the outage was the manipulation of the SCADA system itself and the loss of control. The BlackEnergy 3, KillDisk and malicious firmware were all tools used to gain access and delay the restorations procedure. The aspect of social engineering played its role to gain access into the IT network from which the adversary could exploit the utilities network.

According to the Ukraine report the amount of VPN connection into the OT network was excessive. Utilities should evaluate the need for each VPN access connection since each bring security concern. Beside the many VPN connection, they also lacked 2FA and hence with the stolen credentials access was easy to obtain.

4 CYBER SECURITY RISKS AND MEASURES

The mentioned examples in the previous chapter are very informative and provide good insight in how cyber-attacks unfold. It must be kept in mind, that the attacks took place 9 and 4 years ago respectively and that the digitalization of all kind of processes is accelerating in a high pace, together with the increasing threat for cyber-attacks. Due to the digitalization and energy transition of electrical power grids, the Operational Technology (OT) systems are becoming more of an Information Technology (IT) system. Additionally, causing the implementation of a lot of smart electronic devices communicating with each other using a variety of communication protocols. These additions and implementations have new cyber security risks associated. However, these newer devices are more cyber security focused and offer standard implemented security measures. Wherefore the older systems are not cyber security focused and hence lacking encryption or security measures. The following paragraphs will focus on vulnerabilities in the form of attack vectors as well as cyber security counter measures. [34]

4.1 Attack vectors

The definition of attack vectors is a path or means by which a hacker can gain access to a computer, device or computer network to gain access or transmit malicious software. Attack vectors in cyber security exploit vulnerabilities. [35]

Phishing

Attack vectors used to infiltrate into the corporate IT network as seen in Ukraine 2015 cyber-attack [31] are based around social engineering. Involving the manipulation of people into clicking malicious files or links attached in a corporate email.

These so-called phishing emails are disguised as legitimate message. The goal is to lure individuals into opening malicious software (malware) which disrupts computer operation, gather sensitive information or gain unauthorised access to computer systems. Or have the individuals click on a link to a malicious login webpage, which looks legitimate. However, the webpage is been domain shadowed by an adversary, meaning the IPs are redirected. Consequently, the adversary will receive the user credentials which could be used to exploit the network. [36]

Sniffing/Replay

An attack vector directly threatening the SCADA network and trying to infiltrate the communication devices on the SCADA to RTU level, would be sniffing. Sniffing is capturing of data traffic using a sniffer, an application aimed at capturing network packets. This can be done when data is transmitted across networks. Both for serial as TCP/IP communication protocols. Serial communication will likely go through a fibre optic connection between modems. De packets will be encrypted when in between the modems. The sniffer will not be able to read the encrypted packets from the modem communication. Neither will the sniffer will be able to resend the sniffed packets when using modern encryption protocols. However, the packets between field device and modem are not encrypted and consequently, the sniffer is able to duplicate, manipulate and resend the sniffed packets. For TCP/IP communication protocols sniffing is also possible. Default TCP/IP communication packets are not encrypted, which poses a potential risk. However, encryption between devices is possible, especially with the addition of smarter IEDs. Encrypted communication between devices could also be established by a VPN or tunnel connections to created secure encrypted communication. These packets could contain certain switching commands alarms and other sensible data. To be able to connect the sniffer to the system, you must physically connect your device on location to the modem or switch. If the communication is wireless, you would need a device with the right settings to be able to also receive packets. [37]

Man-In-The-Middle (MITM)

A MITM attack is an advanced sniffing attack where the adversary sets himself up between the two communication devices. Firstly, the adversary will let the system know that he is the actual device, the other device should communicate with. This is done by repeatedly sending Address Resolution Protocols (ARPs) to the other devices, poisoning their ARP caches in such a way that the adversary places himself between the two devices. From there the adversary can read, manipulate and control the communication between the devices. Even if the communication packets are encrypted, since the adversary's device is part of the trusted connection. Just like sniffing you must physically connect your device on location to the modem or switch or be able to receive packets wireless through a rightly configured device. [38]

(Distributed) Denial of Service (D)DoS
Denial of Service is when a network device is getting spammed with packets which will cause the device to overheat and malfunction. Since the buffers of the device gets filled, new packets will be dropped. The communication channels will be flooded, and critical information will not receive its destination. A DoS attack is initiated by a compromised field device which floods the network with packets. If multiple devices are compromised and all send packets into the network flooding an even greater area of the network it is called a DDoS, a DoS distributed over several compromised devices. For an adversary to be able to perform a (D)DoS the adversary must have access to the network either by directly connecting his device to the SCADA network or wirelessly be able to send packets from a remote location to flood the network. [39]

Zero-day exploit
As mentioned in chapter 3.1 about Stuxnet [30], zero-day exploit could be catastrophic for a system. A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in software or hardware and create complicated problems well before anyone realizes something is wrong. A zero-day attack happens once that flaw of software or hardware is exploited and attackers release malware before the developer has an opportunity to create a patch to fix the vulnerability hence zero-day. [40]

Remote Access Trojan (RAT)
A Remote Access Trojan is a type of malware that lets an adversary take control of your device. Once the RAT is installed the adversary may carry out several spying activities such as exploring files and harvesting login credentials. The adversary may also perform illegal activities using your device. Using the devices IP addresses while attack and infecting other devices. [41] If a RAT infects and OT network of an electricity utility, the adversary might be able to take over full control of the operation.

Software update with malicious software
To update the OT system, an update can be downloaded from the vendors website. This is done in the corporate network, the file will be scanned for malware or viruses. However, there is a possibility that a sophisticated adversary managed to compromise the vendors website. Thereby planting undetectable malware in the software update by using zero-day exploits. Once the update file looks alright the utility will start the update procedure by inserting the update file via USB into the OT system. Wherefore the malware will spread through the SCADA system with all possible consequences.

Third party vendor vulnerability
Utilities rely on vendors and other third-party service and product providers. Therefore, the zone Program Development System (PDS) shown in Figure 2.1 provides a VPN or jump host connection. Vendors can connect so they can assist when required. If the vendors security is insufficient and an adversary manages to hack into their network, a potential backdoor to the SCADA network is created. [34] An adversary could further exploit the connection by harvesting data stored in the PDS zone. If the adversary can breach the firewall, he will have direct access to the SCADA network.

Besides the above described attack vectors there are for sure a lot more attack vectors which threaten industrial control systems. The mentioned attack vectors are all cyber based while there are a lot of physical attack vectors as well. This research is limited to cyber based attack vectors since if focusses on cyber-attack intrusion detection. Therefor this list represents a relevant and diverse list of cyber-attack vectors threatening the electrical power grid control system.

4.2 Cyber security measures

Because of the known attacks and mentioned attack vectors in the previous paragraph, protection measures are needed. Deployed measurement for cyber security could be separated into a few categories, proactive, interactive and reactive. Most cyber security measurement are proactive measures which are preventive measures, securing all known vulnerabilities of the system so adversaries do not get the chance to exploit any vulnerability. Proactive measures are network segmentation, firewalls, unidirectional security gateways, port security and ARP protection. Interactive cyber security consists of monitoring the network. Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) are being more implemented. Reactive measures focus on responding towards a cyber-attack. Knowing your week spots and have actions plans thought out. [42]

Network segmentation
As seen in Figure 2.1 the SCADA system is separated into several segments or zones. Each being its own LAN hosting and having its own function in the SCADA system. The zones are connected to each other through firewalls. Thereby, preventing unauthorised access and communication from one to another. If one segment of the network gets compromised there is still a firewall preventing the instruction to spread. The Demilitarized Zone (DMZ) between the SCADA network and corporate network provides information used for corporate applications as well as an extra buffer between the internet and the SCADA network. [43]

Firewall
A Firewall monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between segments to prevent unauthorised access and communication from one to another. A Firewall analyses incoming traffic based on pre-established rules and filters traffic coming from unsecured or suspicious sources. Firewalls guard traffic at a device's entry point, called ports. If a malicious device wants to make an unauthorised connection to a port which the device should not have access to the firewall will block the connection. Firewalls can be either software of hardware. Software firewall is a program installed on each computer or device and regulates traffic through port numbers and applications, while a physical firewall is a piece of hardware installed between networks. [44]

Unidirectional Security Gateway (USG) or Data Diode
A unidirectional security gateway [45] or data diode [46] creates a one-way connection between two segments in the network. This would be deployed between the corporate network and the DMZ. The DMZ would only have a transmit module connecting to the corporate's receiver module. By not connecting the transmit module from the corporate network to the receiver module in the DMZ. The connection will be one way and the corporate network will only be able to receive data from the DMZ. Thanks to that, if the corporate network gets compromised there is no way to penetrate the DMZ and SCADA because the physical connection to transmit data into the DMZ is not made.

Port security
Port security are settings within network devices that restrict input to an interface by limiting and identifying MAC addresses of devices that are allowed to access the port. When a port has an assigned group of secure MAC addresses, the port will only forward packets from those MAC addresses and drop packets with source addresses outside of the defined group. This will protect the network from unauthorised devices trying to send packets through the network. [47] However, MAC spoofing could easily manipulate MAC addresses in packets.

ARP protection
To prevent a MITM attack, switches offer ARP protection. This is a setting which prevents ARP poisoning by saving its ARP cache therefore knowing IP and MAC addresses of devices. An ARP attack from a malicious device telling the network that that device holds the actual IP and MAC address combination will not be effective. Thanks to that, ARP protection can prevent MITM attacks. [48]

Interactive cyber security measures are Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS). They are constantly monitoring and analysing network traffic for signatures that match known cyber-attacks. IDS and IPS are both part of the network infrastructure, they compare packets to known cyber threats and flag any matching packets. The difference is that IDS is a monitoring system and IPS is a control system. An IDS does not modify the network packets in any way, whereas IPS prevents the packets from delivery based on contents in the packets. [49]

Intrusion Detection System (IDS)
An IDS analyse and monitor network traffic for signs that indicate that adversaries are using known cyberthreats to infiltrate or steel data from the network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviours like security policy violations, malware and port scanners.

Intrusion Protection System (IPS)
An IPS is placed in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively denies network traffic based on a security profile if that packet represents a known security threat.

There are many cyber security measures for IT systems which allows networks to be more secure or encrypted. However, and OT network does not have the same process power as an IT network to perform complex encryption and decryption calculations. If implemented, it could cause hiccups in the OT network and reduce the reliability of operation. Therefore, relevant cyber security measures are mentioned above. By implementing these proactive and interactive measures, the overall protection towards cyber threats can be greatly improved. And lots of attack vectors can be countered. However, adversaries are creative and will always try to come up with new attack vectors.

5 CYBER-ATTACK SCENARIOS OVERVIEW

The following chapter will provide an overview of possible cyber-attack scenarios. These cyber-attack scenarios are based on a combination of attack vectors earlier stated. As well as the cyber-attacks of Stuxnet [30] and Ukraine [31]. Some cyber-attack scenarios are already defeated by implementing variations of the above-mentioned cyber security measures. A risk assessment is done on each of the cyber-attack scenarios to determine their impact level to the electrical power grid control system shown in Figure 2.1. The risk assessment has determined how high the potential risk for each cyber-attack scenario case is. The risk assessment is done according to NESCOR's Electric Sector Failure Scenarios and Impact Analysis [8]– High Level Ranking Method. This method is chosen because this report particularly focusses on cyber security in the electric sector and provides guidelines for risk assessments in a wide variety of scenarios. After the risk assessment the highest risk cyber-attack scenario is chosen and further researched and evaluated.

5.1 Cyber-attack scenarios

To determine the threats the SCADA system faces, a base point for the SCADA network infrastructure must be determined. Therefore, the base point of the SCADA network is the one presented in Figure 2.1. This particular design on the SCADA level is a very modern solution, which already defeats several cyber-attack scenarios, or at least prevents spreading to the critical infrastructure. Whether the design with the data diode is sustainable for the future is unsure, due to the increasing interest to send data from the corporate network to the SCADA network, used particular for the smart meter infrastructure as earlier stated. Nevertheless, the presented configuration of Figure 2.1 will be used including the data diode. A list of cyber-attack scenarios is presented to show the effectiveness of certain cyber security measures implemented in the SCADA design. The scenarios can be divided into 3 made up categories; malware, compromised vendor and compromised remote site as shown in Figure 5.1.

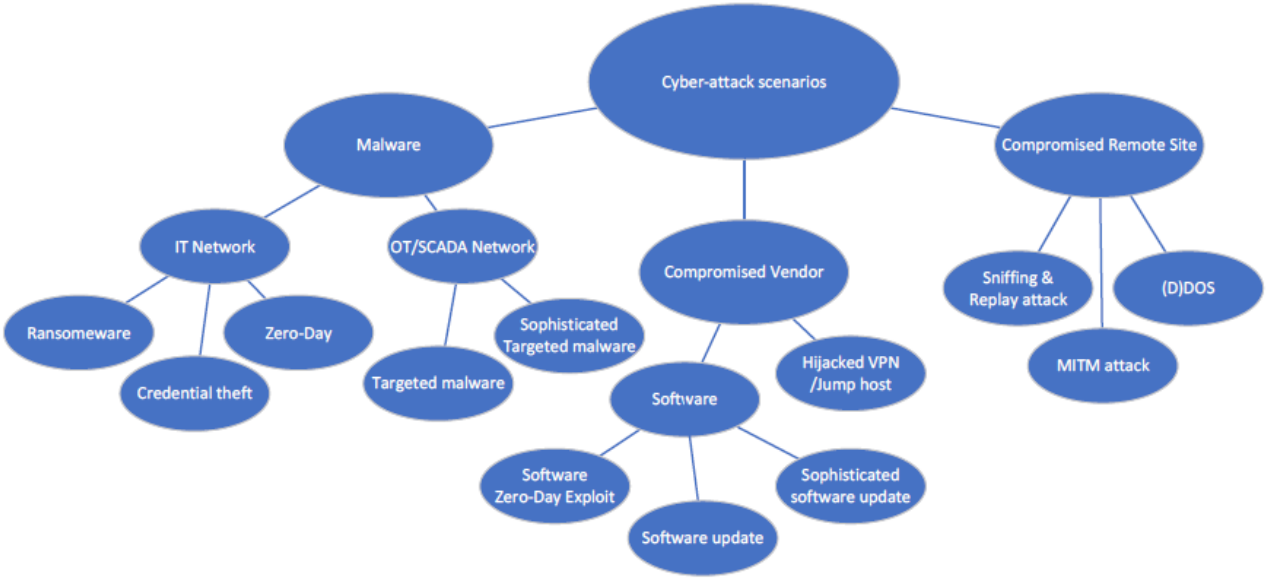


Figure 5.1 Cyber-attack scenarios overview tree

Malware

1. Common ransomware infection into corporate IT network.

Corporate IT users receive phishing mails attached with ransomware which infects the corporate IT network. Encrypting documentation and holding computers hostage till a certain pay sum is paid. This will affect the operation in the corporate network of the utility but will not be able to reach the OT network because of the data diode between the corporate network and the DMZ. Therefore, power management can continue in normal operation.

2. Credentials theft of corporate users.

Corporate IT users receive legitimate looking phishing mails attached with malware and malicious login links. Once logging in by the links credentials are send to the adversary. The malware and credentials will be used to exploit the corporate network further looking for sensitive data and a way into the SCADA network. However, once again the data diode prevents further infiltration into the OT network. Nevertheless, critical information could be stolen and used for a more sophisticated attack.

3. Zero-Day malware using varieties of exploits.

This is another type of malware which could infiltrate the IT network through the internet or mailing. Since the zero-day malware exploits vulnerabilities in the software and with that bypassing firewalls and other cyber security measures. The zero-day malware changes settings in the IT network of the corporation and is thereby detected. The zero-day malware is unable to spread to the OT network because of the data diode, leaving the SCADA network unharmed. However, it zero-day malware causes some chaos in the IT network configuration of the corporate network.

4. Targeted malware infection into SCADA network.

A malware, possibly using zero-day exploits is directly infecting the SCADA network. This could be because an employee's laptop got infected through phishing mails or internet. The employee thereafter connects his laptop with the SCADA network spreading the malware into the SCADA network, which then activates the malware functionalities. Infection could also happen through an infected USB which has been plugged into the SCADA network by an insider or employee, either intentionally or without knowing the USB is infected with SCADA targeted malware. The malware reconfigured certain equipment causing operation malfunction and power outage.

5. Sophisticated Targeted malware infection into SCADA network.

A more sophisticated malware, possibly using zero-day exploits is directly infecting the SCADA network. This could be again because an employee's laptop got infected through phishing mails or internet. The employee thereafter connects his laptop with the SCADA network spreading the malware into the SCADA network which then activates the malware functionalities. Infection could also happen through an infected USB which has been plugged into the SCADA network by an insider or employee, either intentionally or without knowing the USB is infected with SCADA targeted malware. The adversary was very much aware of the electrical power grid infrastructure, therefore knowing how to cause damage. The malware is targeting protection relays and OLTCs. Changing the settings so the protection relays do not trip and reconfiguration the tap changers, so the transformers voltages rise or dip. This causes malfunction in the electrical power grid and damage to equipment. Circuit breakers are not being activated by the protection relays, eventually physical equipment breaks causing outage with severe damage to expensive and critical equipment. As well as possible life-threatening situations.

Compromised vendor

6. Adversary exploits software of vendor.

Each vendor has its own unique software for SCADA development and configuration. A vendor does not release its source code for its provided SCADA system solutions, for several reasons. First one being, the source code is intellectual property and developed with vendor's resources. Second is the access for adversaries to analyse the software for vulnerabilities and zero-days. However, an adversary manages to get access to the source code and found vulnerabilities. These vulnerabilities could be exploited by every utility the vendor supplies. The adversary manages to gain access to the SCADA network of the utility and exploits the found vulnerabilities to exploit authorisations and control. Worst case would be causing physical damage and life-threatening situations.

7. Malicious software update from compromised vendor website.

From time to time the SCADA software must be updated. The vendor provides the available update file on their website. The utility will download the file from their corporate network. An adversary was able to hijack the vendors site and upload a custom update file including malware which will harm the OT network. Even though the utility scanned the file for viruses of malware, the adversary was sophisticated enough to be able to hide his malware from cyber security measures. The malware reconfigured certain equipment causing operator malfunction and power outage.

8. Sophisticated malicious software update from compromised vendor website.

A sophisticated adversary was able to hijack the vendors site and upload a custom update file including malware which will harm the OT network. Even though the utility scanned the file for viruses of malware, the adversary was sophisticated enough to be able to hide his malware from cyber security measures. The adversary was very much aware of the electrical power grid infrastructure, therefore knowing how to cause damage. The malware is targeting protection relays and tap changers. Changing the settings so the protection relays do not trip and reconfiguration the tap changers, so the transformers voltages rise or dip. This causing malfunction in the electrical power grid and damage to equipment. Circuit breakers are not being activated by the protection relays, eventually physical equipment breaks causing outage with severe damage to expensive and critical equipment. As well as possible life-threatening situations.

9. Hijacked VPN/Jump host access from vendor.

The vendor is able to make a direct connection with the SCADA system through a VPN or Jump host. This connection enters the SCADA network in the Program Development System (PDS) zone. The cyber security of the vendor is insufficient, and an adversary manages to acquire credentials with VPN or Jump host remote access. Once the adversary manages to hijack a remote access connection into the PDS zone. There is still a firewall to the SCADA zone. The adversary manages to breach the firewall and is able to manipulate data or load malware into the SCADA network. Worst case would be sophisticated malware causing physical damage and life-threatening situations.

Compromised remote site

10. Sniffing & replay attack.

Remote sites are mostly unmanned, an adversary manages to break into a physical power substation location and connect his device to the SCADA network. Or the adversary manages to capture wireless communication over the SCADA network, breaching the encryption security measures. The adversary sniffs the packets send between the SCADA system and RTU and manages to determine what type of command a packet has. For instance, a packet could be a circuit breaker opening command. After some time, the adversary will replay the packets and therefor open the circuit breaker. This would cause outage as well as confusion. The adversary could randomly trigger the circuit breaker to trip and the utility will be clueless.

11. MITM attack manipulating packets.

An adversary manages to break in into a physical power substation location and connect his device to the SCADA network. Or the adversary manages to capture wireless communication over the SCADA network, breaching the encryption security measures. The adversary will perform a Man in The Middle attack, which means interfering with the communication between the SCADA system and the RTU. The adversary will be able to manipulate packets to the RTU causing outage while sending packets back to the SCADA system that everything is fine.

12. DoS or DDoS.

An adversary manages to break in into a physical power substation location and connect their device to the OT network. Or the adversary manages to capture wireless communication over the OT network, breaching the encryption security measures. This time the adversary sends loads of request to a DC or RTU, flooding its communication channels. Consequently, the communication from the SCADA system to the RTU will be disturbed. The operators will not be able to communicate with the RTU which could cause mismanagement of the electrical power grid.

5.2 Risk assessment

The risk factor will be assigned according to NESCOR's Electric Sector Failure Scenarios and Impact Analyses [8] – High Level Ranking Method. The two criteria which will be factored in are "impact, considering all types of impacts" and "cost to the adversary, considering the overall difficulty and cost to the threat agent to carry out the failure scenario." The overall ranking is then calculated as impact divided by the cost to the adversary, as shown in eq. 5.1. The two criteria used for this method correspond to the composite values of "impacts result" and "effects on likelihood and opportunity result". Assigning a score of 0,1,3 or 9 to represent the impact of the failure scenarios, as it ranges from none to physical damage. Assigning a score of 0.1,1,3 or 9 to represent the cost and difficulty to the threat agent to carry out the failure scenarios is low to highly sophisticated. Each scenario will be discussed and evaluated.

$$Impact\ result = \frac{Impact}{Cost\ to\ the\ adversary} \tag{5.1}$$

Cost and difficulty of the adversary are represented by "sophistication" rating:

- Low 0.1
- Medium 1
- High 3
- Highly 9

The impact on the SCADA system is determined by the consequences described:

- None 0
- Malfunction 1
- Outage 3
- Physical damage 9

1. Common ransomware infection into corporate IT network.

Low sophistication, such ransomware is very common and could be bought online. The infection into the IT network is unfortunate and annoying. The adversary is probably out to get the pay sum and is not targeting the SCADA infrastructure.
The consequences are annoying and will take a few hours or a few days to restore the systems and load backups. Or could be expensive if the utility decides to pay the pay sum to the adversary, where there are no guarantees for actual restoration. However, no SCADA process is harmed because the ransomware could not spread to the OT network thanks to the data diode. The data diode is a hardware solution and prevents spreading to the OT network. Therefore, the impact on the SCADA system is none.

2. Credentials theft of corporate users.

Low sophistication since those tools are available online. Without monitoring of network traffic, the spyware can be roaming around the network for a long time. Stealing all sorts of corporate and personal data.
Consequences are that the adversary will be able to extract a lot of information which could be used for a follow up cyber-attack or a physical attack on infrastructure. This could be seen as a reconnaissance [33] phase of a cyber-attack, just like in Ukraine [31]. However, thanks to the data diode the data harvesting was limited to the IT network. Therefore, the impact on the SCADA system is none.

3. Zero-Day malware using varieties of exploits.

High sophistication, finding zero-day exploits requires specialist and lots of resources. The zero-day malware requires complex programming to hide the payload while using the zero-day vulnerabilities to breach security measures.
The consequences remain within the IT network thanks to the data diode, even though the zero-day ransomware can breach every firewall.

4. Targeted malware infection into SCADA network.

High sophistication since the adversary is aware of the critical infrastructure and knows which components to target to cause outage. Besides social engineering is done to insert an infected USB into the system.
The consequences are hiccups in operations with possible opening of circuit breakers and consequently power outage. The backup network components will take control over, therefore the redundancy. The corrupted network has to be isolated once detected. An expert will have to investigate the network components, the corrupt SCADA components must be replaced or restored if possible. Such attack could cause a short hiccup in operation including possible power outages.

5. Sophisticated Targeted malware infection into SCADA network.

Highly sophisticated since the adversary is aware of the critical infrastructure and knows which components to target as well as how to manipulate the controller software in a way to damage the targeted components. Besides social engineering is done to insert an infected USB into the system.
The consequences are huge, wrongly configuration network components causing damaging to expensive equipment. The replacement of equipment could take a long time. Depending on the redundancy of the destroyed infrastructure it is possible some customers will be left without power for longer periods of time. Besides the physical damage, the breach in the SCADA network has to be isolated and components have to be replaced or restored.

6. Adversary exploits software of vendor.

Highly sophisticated, since the software source code is not published. Acquiring the source code is one thing, probably by infiltrating the corporate network. Finding valuable vulnerabilities and testing them costs a lot of resources. Thereafter the adversary requires access to a SCADA network to actually exploit the found vulnerabilities to disrupt power control.
The consequences depend on the found vulnerabilities as well as how sophisticated the adversary is. Worst case would be, takeover of full control and cause physical damage to equipment as well as power outage. Since this exploit exists in all other SCADA systems the vendor provided, the attack could be carried out to other utilities as well.

7. Malicious software update from compromised vendor website.

High sophistication, the adversary was able to compromise the vendors site, unpack the latest update for the SCADA software and insert a small script. Thereafter presenting a legitimate looking update file which would bypass virus scanners. The creation of the malicious update file requires understanding of the property software used by the vendor and of resources to produce.
The consequences are hiccups in operations with possible opening of circuit breakers and consequently power outage. The backup network components will take over control. For this reason, redundancy is required. Once detected the corrupted network has to be isolated. An expert will have to investigate the network components, the corrupt SCADA components must be replaced or restored if possible. Such attack could cause a short hiccup in operation including possible power outages. The above mentioned could apply to every utility who uses the targeted vendor SCADA solutions.

8. Sophisticated malicious software update from compromised vendor website.

Highly sophisticated, the adversary was able to compromise the vendors site, unpack the latest update for the SCADA software and insert a small script. Thereafter presenting a legitimate looking update file which would bypass virus scanners. The creation of the malicious update file requires understanding of the property software used by the vendor and of resources to produce. Besides the adversary is aware of the critical infrastructure and knows which components to target as well as how to manipulate the controller software in a way to damage the targeted components.
The consequences are huge, wrongly configuration network components causing damaging to expensive equipment. The replacement of equipment could take a long time. Depending on the redundancy of the destroyed infrastructure it is possible some customers will be left without power for longer periods of time. Besides the physical damage, the breach in the SCADA network has to be isolated and components have to be replaced or restored. The above mentioned could apply to every utility who uses the targeted vendor SCADA solutions.

9. Hijacked VPN/Jump host access from vendor.

Highly sophisticated, the adversary needs to gain access to the vendors network. This would probably be performed by phishing mails including custom Remote Access Trojan (RAT) malware, to gain remote access to the technical support workstations of the vendor. Thereafter once the vendor establishes a remote access session with a utility through either VPN or Jump host, the adversary is able to hijack the connection. The adversary is only able to Remote Access when the vendor sets up the connection first, due to the two-factor authentication. To hijack the 2FA as well the adversary needs heavy investment in developing such tools. The connection reaches into the PDS zone of the SCADA network, but from there the adversary still must penetrate a firewall to reach the process zone of the SCADA network.
The consequences after a successful penetration to the SCADA network could be severe because the adversary needs to invest a lot of resources for the attack; it will only be deployed in case on can cause severe physical damage.

10. Sniffing & replay attack.

Medium sophistication, all tools are easily accessible online in order to perform a sniffing & replay attack. However, to gain access to the utilities network the adversary will need to perform some actions, entry points could be either breaking into a substation and physically connecting a malicious device or connection through wireless communication directly used for the communication between SCADA and RTU communication. These wireless connections are usually protected using encryption through a tunnelling method like VPN. Therefore, physical breach is probably easier and more likely. Once access is acquired the adversary is able to sniff packets and replay them.

The consequences are sudden opening of circuit breakers or other changes in the electrical power grid causing power outage.

11. MITM attack manipulating packets.

High sophistication, all tools are easily accessible online in order to perform a man in the middle attack. However, MITM attack is an advanced sniffing & replay attack whereby the adversary hijacks the communication between the SCADA and RTU. To gain access to the utilities network the adversary will need to perform some actions, entry points could be either breaking into a substation and physically connecting a malicious device or connection through wireless communication directly used for the communication between SCADA and RTU communication.

The consequences are that the adversary can intercept communication and is able to control the power substation. As well as manipulate or drop alarm messages sent from the substation intended for the SCADA system. This could cause mismanagement of the electrical power grid as well as intended power outages while the operator is not aware of what is happening at the substation level.

12. DoS or DDoS.

Medium sophistication, all tools or services are easily accessible online in order to perform a (D)DoS attack. However, to gain access to the utilities network the adversary will need to perform some actions, entry points could be either breaking into a substation and physically connecting a malicious device or connection through wireless communication directly used for the communication between SCADA and RTU communication. Once access is acquired a (D)DoS attack could be easily performed.

The consequences will be that the operator will not be able to receive field information since the network is getting flooded. This will cause malfunction of the SCADA system and mismanagement of the electrical power grid.

5.3 Risk assessment result

The risk assessment is done using my own interpretation and knowledge of the electrical power grid for each cyber-attack scenario. Someone else's interpretation of a case could be different, whereby the result of the whole risk assessment could be different. Anyhow each utility should perform their risk assessment on their own infrastructure since no infrastructure is alike.

Table 5.1 shows an overview of the scores of the risk assessment. Whereby the collected scores are calculated using eq. 5.2.

$$Impact\ result = \frac{Consequences}{Sophistication} \tag{5.2}$$

Table 5.1 Overview of risk assessment

Scenario	Sophistication	Consequences	Result
#1	0.1	0	0
#2	0.1	0	0
#3	3	0	0
#4	3	3	1
#5	9	9	1
#6	3	3	1
#7	3	3	1
#8	9	9	1
#9	9	9	1
#10	1	3	3
#11	3	3	1
#12	1	1	1

Because of the various preventive cyber-attack measures, several of the mentioned cyber-attack scenarios are defeated. Or at least are not able to spread to the OT network, therefore having no effect on the SCADA system. Access to the SCADA system can only be acquired by direct access to the OT network e.g. direct malware infection into the SCADA network or connection to the SCADA network. The physical access could be established from anywhere in the OT network. Power substation are mainly unmanned and could be at a remote location.

Therefore, cyber-attack scenario number 10: Sniffing & replay attack has a result score of 3, which is the highest. A sniffing & replay attack at any remote location is the highest risk cyber-attack scenario due to its medium sophistication, but high possible consequences with significant impact causing outages and malfunction. With the earlier stated digitalisation of the electrical power grid the entry points for adversaries are increasing. Therefore, the risk for a cyber-attack targeting a local substation will increase. Chapter 6 will focus on the methods used in the execution of the scenario as well as precautions and measures to decrease vulnerability and detect intrusion.

6 HIGH-RISK CYBER-ATTACK SCENARIO

The result of the risk assessment in chapter 5 shows that cyber-attack scenario 10: Sniffing & Replay attack has the highest result because of its low sophistication and high possible consequences. The sniffing & replay attack is described in detail below. To see the ease to perform a sniffing and replay attack as well as to see what happens to the network. A network is simulated whereby a sniffing and replay attack is performed. These results provide insight from where possible measures as well as an intrusion detection algorithm method can be researched.

6.1 Scenario overview

Cyber-attack scenario 10: Sniffing & Replay attack. This attack is focussed on disrupting the control process of the electrical power grid. Every attack starts of in the reconnaissance phase, where the adversary plans out his attack. The adversary is aware of the infrastructure and examines the weak spots of the electrical power grid e.g. lack of redundancy, critical tie-line connections or very remote locations on either low of high voltage level. Once determining the target location, the adversary needs an entry point to gain access to the OT network. There are two options: wireless connection or wired connection. The entry point will be determined in the preparation phase.

With the increasing implementation of IEDs and an ever-expanding OT network, more entry points for adversaries appear on a local scale. Often these devices are wireless and situated in urban areas making them interesting and accessible. These IEDs control and monitor low to medium voltage equipment used for distribution. The impact of a malfunction due to cyber-attack is less catastrophic but could still impact communities.

Wireless connection is rarely used in high voltage substation, more so in medium to low voltage due to the size of infrastructure. Disruption in high voltage causes more chaos over medium to low voltage. These wireless connections could be 3G/4G leased lines from a telecom provides. Whereby the utility usually applies end to end encryption to the communication as well as a VPN. If the adversary manages to configure his malicious device to the right channel as well as gain access to the VPN, the adversary is able to receive and resend packets. However, if encryption is used the adversary will not be able to make sense out of them. Also, without knowing the encryption resend packets will not be received by the targeted field devices.

For a wired connection the adversary needs physical access to the power substation. He must breach the building which stores the monitoring and control panels. Once inside he must physically connect his malicious device to the network. However, the ports of the devices are hardened, and non-used port should be deactivated. Therefore, just connecting the malicious device to an open port would not work. By adding a hub in between the connection from SCADA to RTU, the adversary can connect his malicious device to the hub. A hub broadcasts the packets to every port therefore the malicious device is able to sniff all the network traffic which is communicated over the connection. The adversary needs to make sure the MAC address of his malicious device does not get detected. By properly hiding the malicious device in the control cabinet as well as in the configured network the connection is established. Which completes the intrusion phase. A physical breach would probably be detected and investigated. Since no equipment is missing and the network is still functioning properly the physical breach is labelled as vandalism.

After the attention about the event has decreased, the adversary sets himself up near the substation and connects to his device. The adversary will perform scanning of the network to know which devices he can reach and get an understanding of the OT network. By monitoring the packets stream and understanding the application protocol used with the variety of commands.

The management and enablement phase is next and includes establishing the right commands used for physical switching actions within the substation. After that the adversary has a broad list of useful commands for command and control. The adversary is ready to randomly replay a packet causing some malfunction in the OT system of the substation. Or to replay a circuit breaker opening command to cause outage. The utility operator might think this is a malfunction of the circuit breaker or other equipment while the adversary just randomly disrupts equipment. Causing outage, loss of trust by customers, loss of revenue due to compensation and loss of reputation.

6.2 Simulation

A simulation of the network traffic during a normal circumstance and during a sniffing and replay attack is essential for the development of a possible algorithm. To simulate the sniffing & replay attack a local network is created. Using a variety of software, a SCADA to RTU communication can be simulated and disturbed. It turned out the first simulation method did not work, in the configured method. Therefore, a second simulation method has been created using a different configuration and other simulation software. The two methods are explained below via Setup 1 and Setup 2.

6.2.1 Simulation method 1

For the first simulation method the application communication protocol used is IEC60870-5-104, this open protocol is broadly used for electrical power grid control. The following equipment and software are used for the simulation setup:

- Laptop x2
- Achilles Test Platform [50]
- Achilles Client
- ASE2000 V2 Test Set Client x2 [51]
- ASE2000 Licence Dongle
- TP-Link USB 3.0 to Gigabit Ethernet Network Adaptor UE300 [52]
- Ethernet Cable x3
- Wireshark software [53]

To give an impression of the practical side of the research Figure 6.1 and 6.2 show the setup and the wiring. The black box, where a laptop is standing on is the Achilles Test Platform (ATP), which is a device created by Wurldtech a General Electric Digital company. The ATP is created as a cyber security testing platform and can perform robustness and penetration testing on ICS networks. The ATP can be used to directly test RTUs or other IEDs on known and unknown vulnerabilities with its extensive number of tests, supporting a wide variety of protocols.

Figure 6.1 Simulation setup 1 display

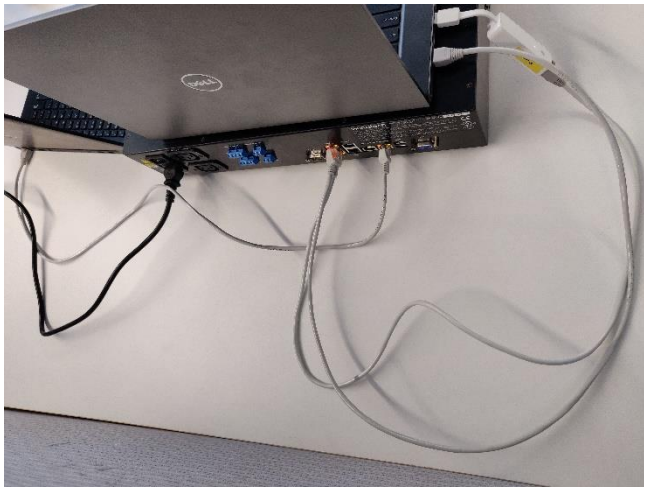


Figure 6.2 Simulation setup 1 wiring

The laptop on the right in Figure 6.1 is connected to the management port of the ATP and is running the Achilles client. The Achilles client is used for monitoring the data traffic and executing interfering communications. The other laptop (on top of the ATP) hosts two ASE2000 V2 Communications Test Set clients, one in master simulation mode and one in RTU simulation mode. These two clients have established a communication and are functioning as SCADA master and field RTU just like in Figure 2.1, a connection between de SCADA server in the process zone and the RTU of a power substation. The communication is through the ATP were the two ports are bridged. Shown in Figure 6.2 are the two ethernet cables connected to the ATP. The top one is the Device Under Test (DUT) port and the bottom one is the Vendor Control System (VCS) port. To create an extra ethernet connection for the laptop the TP-Link is used. In Figure 6.3 a schematic configuration of the simulation is shown.

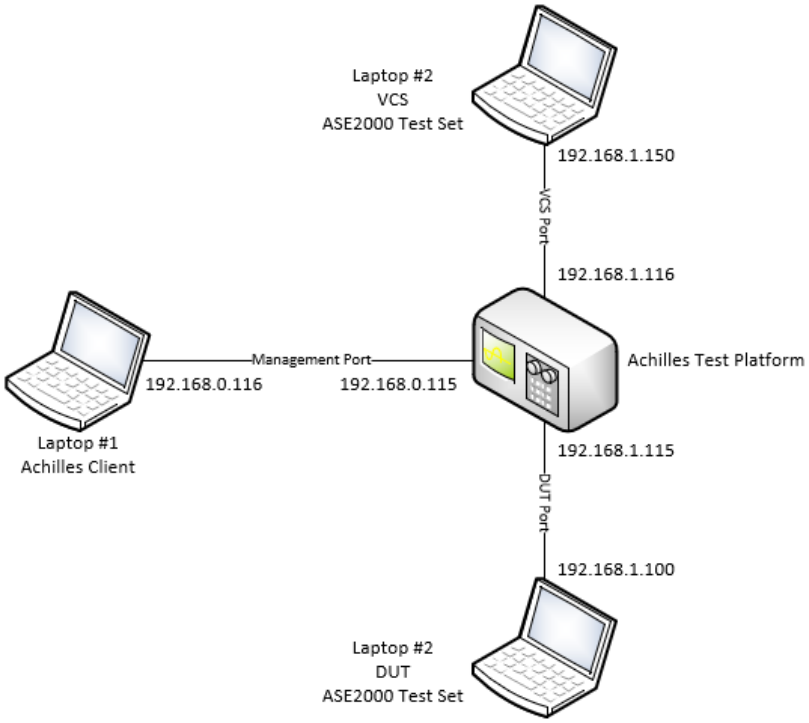


Figure 6.3 Schematic configuration of simulation setup 1

The ATP is able to perform a replay attack test: 9.1 Packet Capture Replay (over TCP). This can send captured packets into the communication. Wireshark would be used for the capturing of packets traffic between the SCADA and RTU clients. However, because the two clients are running on the same device the packets will never reach the physical transport layer. Therefore, there is no traffic to be captured and resend. Because there is only one licence dongle for the ASE2000 software available, hosting a client on another laptop is not possible and this method will not work for this purpose. However, in cyber-attack scenario the SCADA and RTU will be two separate physical devices and this method is perfectly feasible.

6.2.2 Simulation method 2

As mentioned in simulation method 1, there must be two physical devices in order to capture network traffic. Therefore, simulation software of SCADA and RTU must be run two on separate devices. The only thing that stopped that in simulation method 1, was the simulation software. Therefore, free Modbus tools are used for the second simulation. The application communication protocol is Modbus TCP/IP, this communication protocol is more used in industry ICS then utility but is still relevant for the elaboration of the algorithm.

The physical equipment for the second simulation remains the same, the configuration and software is different and stated in the following list:

- Laptop x2
- Achilles Test Platform [50]
- Achilles Client
- Modbus Poll Client [54]
- Modbus Slave Client [54]
- TP-Link USB 3.0 to Gigabit Ethernet Network Adaptor UE300 [52]
- Ethernet Cable x3
- Wireshark software [53]

To give an impression of the practical side of the research Figure 6.4 and 6.5 show the setup and the wiring. The black box, where a laptop is standing on is once again the Achilles Test Platform (ATP), which is a device created by Wurldtech a General Electric Digital company. The ATP is created as a cyber security testing platform and can perform robustness and penetration testing on ICS networks. The ATP can be used to directly test RTUs or other IEDs on known and unknown vulnerabilities with its extensive number of tests, supporting a wide variety of protocols.

Figure 6.4 Simulation setup 2 display

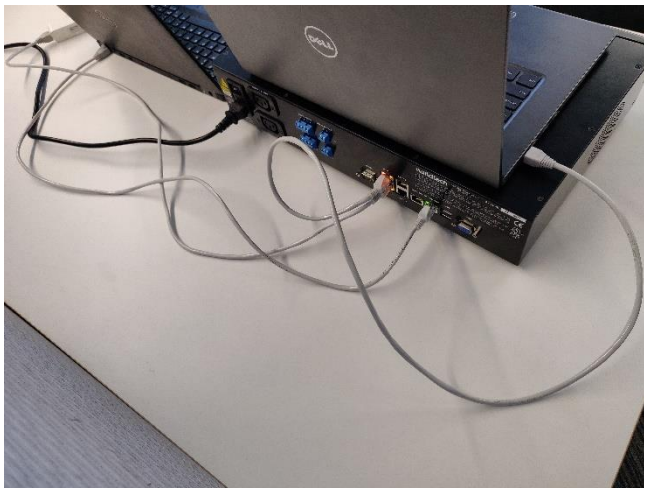


Figure 6.5 Simulation setup 2 wiring

The configuration is almost the same as the one in simulation 1. One laptop is connected to the management port of the ATP and is running the Achilles client. But not also hosts the Modbus Poll Client which acts as a SCADA component. The Achilles client is used for monitoring the data traffic and executing interfering communications. The other laptop now just hosts only one Modbus Slave Client which serves as the RTU. To enable communication between these two devices the firewall had to be disabled on Laptop #2. Thereafter the two clients have established a communication and are functioning as SCADA master and field RTU. The communication is through the ATP were the two ports are bridged. Shown in Figure 6.5 the two ethernet cables connected to the ATP. To create an extra ethernet connection for the laptop the TP-Link is used. In Figure 6.6 a schematic configuration of the simulation is shown.

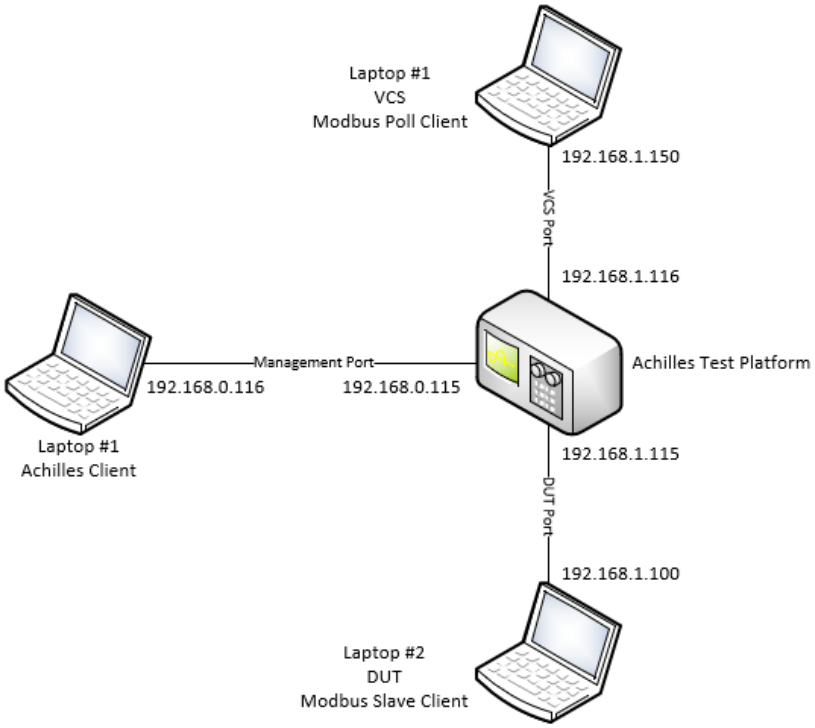


Figure 6.6 Schematic configuration of simulation setup 2

With this configuration the traffic between the SCADA and RTU can be captured using Wireshark. Thereafter the capture file can be loaded into the ATP, so the ATP is able to perform a replay attack test: 9.1 Packet Capture Replay (over TCP).

Firstly, a normal communication between the SCADA and RTU will be monitored. Modbus function 03: Read Holding Registers makes it possible for the SCADA as well as the RTU to change parameters. The SCADA will constantly read the RTU, if the SCADA wants to change a parameter in the RTU, it will do so by sending a write command to the RTU as seen in Figure 6.7. The changing of parameters can be seen as certain commands for switching actions or field measurements. So, the changing of a parameter could be a circuit breaker opening command with the effects of and outage.

10 3.072578	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 401; Unit: 1, Func: 3: Read Holding Registers
11 3.087553	192.168.1.100	192.168.1.150	Modbus…	83	Response: Trans: 401; Unit: 1, Func: 3: Read Holding Registers
12 3.127995	192.168.1.150	192.168.1.100	TCP	54	54267 → 502 [ACK] Seq=49 Ack=117 Win=251 Len=0
13 4.088691	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 402; Unit: 1, Func: 3: Read Holding Registers
14 4.103470	192.168.1.100	192.168.1.150	Modbus…	83	Response: Trans: 402; Unit: 1, Func: 3: Read Holding Registers
15 4.143785	192.168.1.150	192.168.1.100	TCP	54	54267 → 502 [ACK] Seq=61 Ack=146 Win=251 Len=0
16 5.104122	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 403; Unit: 1, Func: 6: Write Single Register
17 5.119269	192.168.1.100	192.168.1.150	Modbus…	66	Response: Trans: 403; Unit: 1, Func: 6: Write Single Register
18 5.165855	192.168.1.150	192.168.1.100	TCP	54	54267 → 502 [ACK] Seq=73 Ack=158 Win=251 Len=0
19 6.130546	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 404; Unit: 1, Func: 3: Read Holding Registers
20 6.150288	192.168.1.100	192.168.1.150	Modbus…	83	Response: Trans: 404; Unit: 1, Func: 3: Read Holding Registers
21 6.190778	192.168.1.150	192.168.1.100	TCP	54	54267 → 502 [ACK] Seq=85 Ack=187 Win=251 Len=0
22 7.151460	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 405; Unit: 1, Func: 3: Read Holding Registers
23 7.165840	192.168.1.100	192.168.1.150	Modbus…	83	Response: Trans: 405; Unit: 1, Func: 3: Read Holding Registers
24 7.206636	192.168.1.150	192.168.1.100	TCP	54	54267 → 502 [ACK] Seq=97 Ack=216 Win=251 Len=0

Figure 6.7 Captured network traffic between SCADA and RTU

This capture can be saved as a Wireshark Capture File (.pcap). Thereafter attached in the 9.1 Packet Capture Replay (over TCP) test. By resending the TCP confirmation send from the SCADA to the RTU after the initial Write Single Register command, the parameter will be changed.

To see what happens to the RTU during the execution of the attack, the network traffic is monitored from laptop #2 which hosts the Modbus Slave Client using Wireshark. The result is shown in Figure 6.8. An Achilles Report of the sniffing & replay attack is attached as Appendix D.

4 1.015725	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 14; Unit: 1, Func: 3: Read Holding Registers
5 1.027564	192.168.1.100	192.168.1.150	Modbus…	83	Response: Trans: 14; Unit: 1, Func: 3: Read Holding Registers
6 1.069874	192.168.1.150	192.168.1.100	TCP	60	57641 → 502 [ACK] Seq=25 Ack=59 Win=254 Len=0
7 1.874383	192.168.1.115	192.168.1.100	TCP	74	49064 → 502 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=6091924 TSecr=0 WS=64
8 1.874537	192.168.1.100	192.168.1.115	TCP	74	502 → 49064 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=24585685 TSecr=6091924
9 1.875423	192.168.1.115	192.168.1.100	TCP	66	49064 → 502 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=6091924 TSecr=24585685
10 1.877199	192.168.1.115	192.168.1.100	Modbus…	78	Query: Trans: 403; Unit: 1, Func: 6: Write Single Register
11 1.877370	192.168.1.115	192.168.1.100	TCP	66	49064 → 502 [FIN, ACK] Seq=13 Ack=1 Win=5888 Len=0 TSval=6091925 TSecr=24585685
12 1.877435	192.168.1.100	192.168.1.115	TCP	66	502 → 49064 [ACK] Seq=1 Ack=14 Win=66560 Len=0 TSval=24585688 TSecr=6091924
13 1.918088	192.168.1.100	192.168.1.115	Modbus…	78	Response: Trans: 403; Unit: 1, Func: 6: Write Single Register
14 1.918672	192.168.1.115	192.168.1.100	TCP	60	49064 → 502 [RST] Seq=14 Win=0 Len=0
15 2.030886	192.168.1.150	192.168.1.100	Modbus…	66	Query: Trans: 15; Unit: 1, Func: 3: Read Holding Registers
16 2.043311	192.168.1.100	192.168.1.150	Modbus…	83	Response: Trans: 15; Unit: 1, Func: 3: Read Holding Registers
17 2.086627	192.168.1.150	192.168.1.100	TCP	60	57641 → 502 [ACK] Seq=37 Ack=88 Win=254 Len=0

Figure 6.8 Captured network traffic during the attack

The first thing which is observed is the source IP changes to the one of the ATP. Which makes sense since the packets are injected by the ATP. The ATP performs the Three-Way Handshake to establish a connection. This is done by the ATP which sends a SYN for Synchronisation packet to the RTU. The RTU will replay with a packet were both the SYN and ACK for Acknowledgement bit are set. Hereafter the ATP confirms the connection by sending an ACK packet. In this 3-way handshake the two devices agree on the set parameter for the connection like the maximum segment size as well as if they would use the selective acknowledgement mechanism for their packet's communication.

Thereafter, the captured Write Single Register packets is sent with the changed parameter which could act as a circuit breaker opening command. Right thereafter, the ATP sends a packet stating, "that's all I have to send", the FIN for finish and ACK bit are set. The RTU will respond with an ACK to confirm the preparation for the closure of the communication. The RTU confirms the change of the parameter back to the ATP. The ATP hereby sends an RST reset packet to close the communication. Thereafter the communication between the RTU and SCADA continues whereby the SCADA reads the changed parameter of the RTU. A schematic communication of the attack is shown in Figure 6.9.

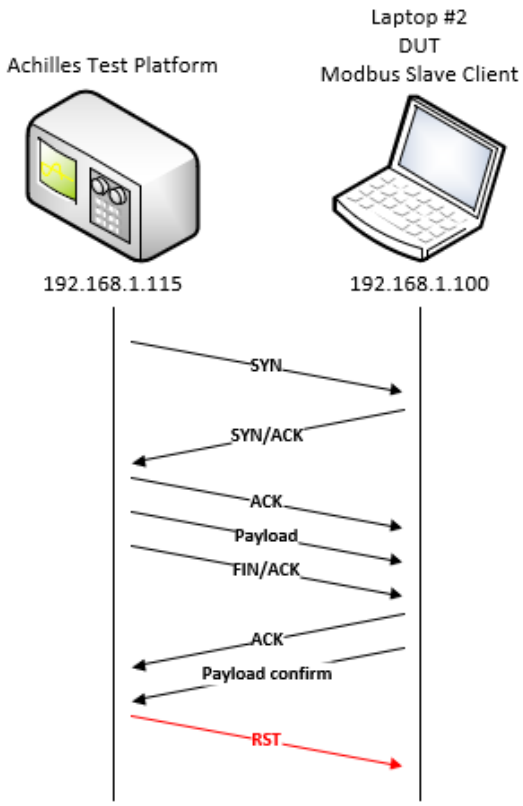


Figure 6.9 Schematic communication of the attack

This shows that with the right hardware and software a high-risk cyber-attack of sniffing & replaying network traffic can be easily performed. Whereby a parameter is changed in the RTU, which in operation scenario could have resulted into the opening of a circuit breaker or another type of action causing malfunctioning of the electrical power grid.

For a real case scenario an adversary will be able to spoof his IP and MAC addresses and inject the packet at the time of an established communication between the SCADA and RTU. Because the connection is already established, a three-way handshake does not need to be performed by the adversary.

6.3 Measures

There are several cyber security measures which can be implemented against the sniffing & replay attack or the manipulation of network traffic, these measures range from proactive, interactive to reactive. Hereby proactive measures are preventive and can be implemented to reduce or resolve the vulnerability of the system. An interactive measure in the form of network monitoring could be implemented to detect unauthorised network traffic. However, with the detection of unauthorised network traffic, a switching action causing outage could have happened already. Prevention is better than cure and hence an algorithm for interactivity is the last resort if preventive measures fail. Thereafter comes inevitably the third category: reactive measures which touches on action plan to execute at the time of detection of a cyber-attack. That is an interesting topic but will not be touched on in this thesis.

6.3.1 Proactive measures

There are already several proactive measures mentioned in chapter 4.2. These measures strengthen the cyber security of the network. Looking more specifically into the sniffing & replay attack, several more measures were found. The problem with the implementation of these measures is that they are not particularly designed for an OT system. Furthermore, utilities are holding back on implementing them. Since these solutions require processing power which utilities are generally not keen on giving out since they cannot afford lack of reliability, possibly introduced by those additional processes. Reliability is number one priority.

Examples of specific proactive measures worth mentioning are described in the following.
1. Using end-to-end encryption will prevent the adversary from being able to read the sniffed packets anywhere in the communication link. Encryption also prevents an adversary to resend the packet since most modern encryption protocols implement a counter. When the packet is resent, the counter does not match, wherefore the destination device is not able to decrypt the packet, so it will be ignored.

2. There is also a method for the authentication of data available and ready for implementation. This authentication protocol is IEC62351, which uses digital signatures to ensure only authenticated devices have access. A third party device will not be authorised to change a parameter and hence a sniffing & replay attack is prevented.

However, the implementation of both proactive measures requires process data from the communication devices. Which need to perform extra calculation for encryption and decryption or authentication.

6.3.2 Algorithm design

Monitoring of the data streams in a network is never a bad idea. Besides keeping an eye on unauthorised traffic, possible optimisation and improvements can be done from network analyses. Monitoring network traffic will however not prevent a cyber-attack from happening, since the cyber-attack needs to be ongoing for the monitoring equipment to detect. However, detection of an intrusion in a segment of the network can prevent further consequences if the utility acts adequately. If the detected threat needs to be prevented the IDS could be merged with a firewall to become an IPS, wherefor detected threats will be blocked. However due to the high potential of false positives this would mean that lots of valid commands would be retained. This could therefore cause reliability issues due to malfunctioning of the communication. So, a solid IDS system could serve as a last resort for detection when the proactive and preventive measures fail.

6.3.2.1 Existing IDS

Utilities have communication philosophies, whereby RTUs do not directly communicate with each other on the process level, meaning on the application protocol level. Communication is always done through the central SCADA, also mentioned in chapter 2.1.2. The adversary can make use of other TCP/IP protocols to search around in the network but will not be able to change process components. Therefore, implementing the IDS after the FEPs on the mirror port of main switch, as shown in Figure 6.10 would be sufficient to monitor all process traffic from and to the RTU of each power substation. If an adversary breaches one substation and tries to communicate with an RTU of another substation the communication has to go through the central SCADA as well as the IDS and will therefore be detected and reported. These systems support a wide variety of open and proprietary application protocols.

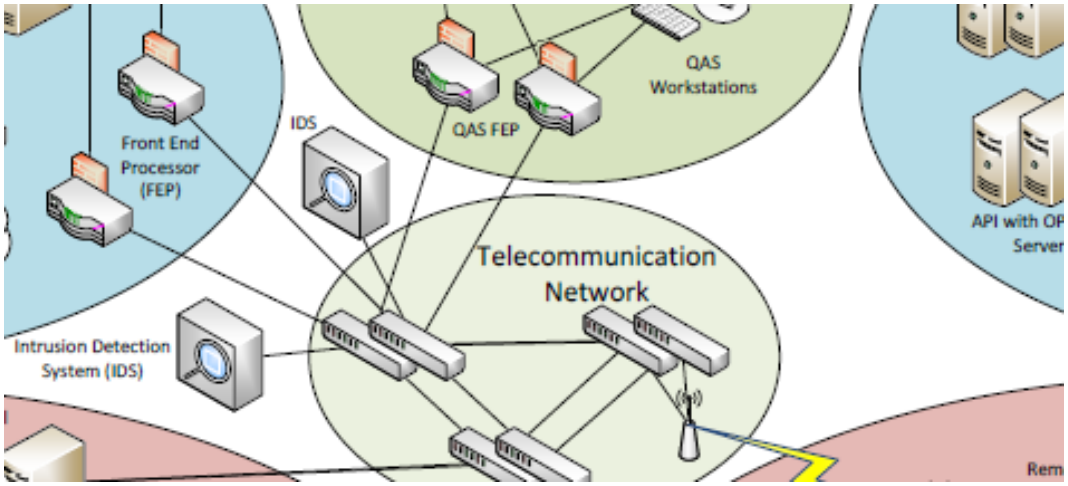


Figure 6.10 Placement IDS on mirror port of main network switch

There are several IDS vendors [55, 56, 57] available which offer IDS particularly for ICS infrastructures. These IDS use Deep Packet Inspection (DPI). DPI operates between the network up to the application layer of the OSI model. Therefore, looking further then the IP addressing, DPI focusses on application protocol process data, the payload of a packet and compares the payload with a set of known signatures. As well as all the other signatures of malware and unauthorised packets. Therefore, the IDS will be able to detect abnormal data changes in process data as well as communication attempts from the malicious device to further infect the network.

However, if the adversary is able to make valid looking packets which perform correct actions, this would go undetected since the IDS is not triggered by any signature and the packet looks like a valid event. However, it's an adversary which disconnects circuit breakers for the reason of causing outage. The adversary is able to manipulate operation, performing valid but illogical looking switching actions. This abnormal switching is represented in the process data.

6.3.2.2 Interactivity

An enhanced, or more solid IDS can be obtained by implementing interactivity to it. To configure such an interactive system the assumption should be that the adversary is able to breach and manipulate all security related to communication. Hence, that an adversary will be able to spoof the IP and MAC address of his malicious device so the source of the packets looks like it has been sent from the SCADA, all while keeping his device undetected. The adversary will be able to inject the packets into the network traffic without performing the three-way handshake of his own once the actual SCADA and RTU connection is established. Under these assumptions monitoring on logical protocol level, layer one to four of the OSI model including MAC, IP and TCP is not effective. Since, if the adversary fails to send correct logical protocol communication, the protocol will drop the packets since they do not make sense. Monitoring should be on the higher process level of monitoring and controlling the electrical power grid, this process data is wrapped in the network packets and comes down to the data send with the application protocols in layer five to seven.

6.3.2.3 Additional algorithm

In this paragraph the design of the proposed additional algorithm is explained and an example is given. In order to determine abnormal and potential harmful process data from normal process data, an additional algorithm should compare the interactive real time data with a set of certified normal process data as presented in Figure 6.11. The process data contain control commands, signalling and alarms which have certain trends and frequency.

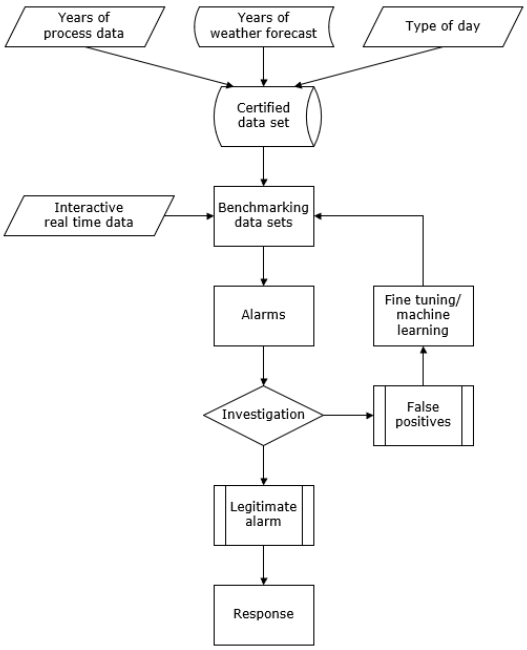


Figure 6.11 Additional Intrusion Detection System configuration methodology

To obtain a set of normal certified process data, sample data must be collected. Sample data of the process data as well as a set of e.g. weather forecast and type of day data, since those could affect the process. The process data contains historical communication as well as calculations performed by software application in the SCADA network. These applications determine the state of the electrical power grid as well as logical procedures to be taken to maintain proper functioning of the electrical power grid. When a utility uses sample data of multiple years, certain normal activities and procedures with a corresponding frequency can be determined.

Implementing weather forecast data into the equation provides forecast for load and generation. However, the influence of weather is different over the world, for Europe implementing weather forecasting is essential with the variety of seasons and weather types. For South East Asia however, there are only two seasons, dry and raining season whereby the weather does not influence the load and generation forecast much. The type of day data e.g. weekday, weekend day and public holiday is essential to determine peak demand and therefore corresponding switching procedures. With the input of these datasets the classes for the certified data set are dynamic, changing with the type of weather and day to compare the interactive real time data with the forecasted switching procedures.

An example switching procedure is for instance, to disconnect a connected bay: according to guidelines, firstly the circuit breaker open, thereafter the switches to open position to provide a visible disconnection. Lastly the earthing switches close to ground all components. With years of process data, the frequency of such event for each substation will become clear depending on what other conditions occur in the electrical power grid. Therefore, the algorithm must be able to check if the procedure is done according to guidelines, logical procedure as well as logical action to perform.

6.3.2.4 Certified data handling

After collection of the sample data, certified sets of process data have to be assembled. The classification of the certified data sets into classes is essential for the algorithm which will be used to compare the interactive real time data with the benchmark. Firstly, the classification should define all types of procedures and events into classes. These classes consist of correct sequences of process data used for procedures and events, such classes could be:

- Connecting and disconnecting of a bay.
- Switching over a bay from Rail A to Rail B.
- Change of tap changer in OLTC for transformers or generators.
- Correct order of alarms from field devices, the alarm levels are distinguished into multiple levels for instance the temperature of oil.
- Many smaller sub-procedures and sub-alarms which are send and received by the system.

The algorithm which can be used is a multiclass classification algorithm. This multiclass classification algorithm compares the interactive real time data with the certified data classes. Whereby frequency of procedure and state of the electrical power grid with previous procedures could be considered. If the network traffic falls in a known class of the classified data set. The type of action is recognised as authorised.

There are several types of algorithms which can tackle a multiclass classification. [58, 59] The one vs. all would be the simplest approach. In eq. 6.1 is a multiclass classification formula of one vs all shown. Basically, the interactive process data will be compared against all certified classes. The formula compares the real time data (x), with class i for every created class represented by $i \in 1, \dots, N$. To seek the arguments of the maxima meaning the class where the interactive real time data matches with a created class.

$$f(x) = \arg \max_{i \in 1,\dots,N} p_i(x) \tag{6.1}$$

Whenever the interactive process data does not fit into a certified class, the system will provide an alarm. This alarm could be either correct and indicate unauthorised switching procedures from a malicious device or operator, which should be investigated. However, IDS are highly sensitive and known for producing lots of false positives. Each false positive also needs to be investigated which requires a lot of resources and is time consuming.

Therefore, fine tuning is important to properly configure the IDS. Fine tuning could be done manually by creating new classes for uncommon special procedures. Another option for fine tuning could be using a machine learning algorithm whereby the algorithm will develop understanding of the normal processes and events within the network through input provided by the software application. Whereby the algorithm can predict the next procedures for operation and therefore the expected network traffic.

6.3.2.5 Validation

The validation of an algorithm is crucial and part of the process for determining the degree to which the model is an accurate representation for real world implementation. Implementation is covered in the next paragraph. For this case a methodology for the creation of an additional algorithm used for intrusion detection is presented. This presentation is still a train of thought which for real world implementation requires evaluation of internal and external factors.

The additional algorithm looks at the process data of the network traffic to control the power grid. There are several application protocols available, these application protocols have their own functionalities and applications. The creation of an algorithm is dependent on the application protocol used. After an actual algorithm is programmed and implemented to monitor a certain application protocol, all alarms have to be investigated. These will create false positives wherefor the algorithm needs to be fine-tuned.

The Modbus TPC/IP protocol which is used for the simulation, is considered to apply for validation. Modbus TPC/IP has several functions. These functions can be determined from the process data as seen in Figure 6.7, wherefor a model of the normal network traffic can be created. However, there is no use case for the creation of an algorithm based on the simulated process data. Since, as earlier stated each utility has their own configurations and implementations. The process data need to be sampled for a long period of time to determine patterns of normal network traffic. It is of course possible to let the simulation run for some time and change a parameter occasionally but that would be based on nothing and would not contribute to any real-world scenario.

Because of the above mentioned, the additional algorithm methodology will be validated in another way, using the following case: configuration change for the electrical power grid by switching over a bay to the other busbar. The substation configuration is as shown in Figure 2.2 whereby there is a double busbar system for each bay to connect to. For the switching over of the bay firstly the two busbars need to be connected, this is done using a couple bay. Thereafter the switches can connect to the to be connected busbar. Thereafter the switches for the other busbar can disconnect, using this method the power flows will not be disrupted. These procedures are performed by the operators with the assistance of the SCADA system. Each procedure requires input for verification of a safe switching procedure. Safety is also built into the devices by logical functions. All these procedures and input data are sent through an application protocol which sends a certain function and parameter for each procedure. This is just one of the many procedures performed in operation. By capturing the network traffic certain trends and frequencies can be assigned to the procedure wherefor it is classified. Then using the algorithm, the real time interactive data will be compared against the certified classes.

Continuing with this case, an adversary is considered to be able to load malware into the field devices which eliminates the logical protection. And thereafter proceeds to send a closing command to the switches to connect to the other busbar while the couple bay is disconnected. With the given input, this procedure is not according to guidelines and procedures and does not seem like a logical switching action and therefore will not fit in any certified class. An alarm will be created to alarm the utility about the event of an incorrect procedure.

6.3.2.6 Implementation

In order to implement such a complex and data absorbing algorithm is a lot of work, wherefor programming is required. Which is also depending on the application protocols used and on the infrastructure configuration of a utility. The result however would be a check on process level, if the procedures are done according to guidelines. As well as to check whether these procedures are logical actions in the state of the electrical power grid and logical related to historical process data, specifically configured for the electrical power grid of the utility. This additionally to the already functioning IDS which monitors on all the cyber security signatures of malware and unauthorised packets.

It is obvious that a lot of effort is required to implement an interactive detection algorithm measure, particularly in a complex process. Step by step implementation is very well feasible however and should certainly be considered in a complex system, in order to keep the overview in all stages from design throughout validation.

As a nuance to this, it can be kept in mind, that not the complete utility process requires interactive measures. Also, there must be a balance in cost of effort versus degree of protection (i.e. risk assessment). After all, it also should be considered to restrict the application of this algorithm to key elements in a utility process, while leaving other elements protected by preventive measures only.

For instance, in an electrical power grid a generator is a key element in contrary to a local transformer. Switching off the local transformer by an adversary action results in a local power outage with discomfort and mainly financial damage. On the other hand, it should be prevented at any time that a key generator is switched off by an adversary action during peak power demand hours, when full capacity of that generator is required.

In the latter case, inappropriate switching off could lead to a cascade of overloading of other generators feeding the grid, triggering overload protections at generators and resulting in a wide national power outage.

7 CONCLUSION AND RECOMMENDATIONS

The primary objective of this research is to conclude on how to detect a high-risk cyber-attack intrusion. This research is performed using several research methods, including desk research into the energy sector, SCADA/EMS/DMS applications, historical cyber-attacks, attack vectors and measures. As well as several interviews with experts in the field about cyber and physical security. And lastly an experiment using simulation for verification and validation purposes. These research methods have answered the sub-questions, after which the main research question could be answered.

The communication between SCADA and RTU is configured so that the SCADA can only initiate the application protocol communication with the RTU. Therefore, all process data goes through the central SCADA. By implementing an IDS placed on the main switch after the front end processors as shown in Figure 6.10, all application protocol process data can be monitored. Existing IDSs use DPI to evaluate between layer 4 to 7 of the OSI model to inspect packets. DPI compares the payload with signatures, while these signatures are known threats which are programmed in the IDS. In order to keep the IDS effective for new found threats, new signatures must be created and the IDS must be updated. If an adversary manages to connect to the OT network while keeping his malicious device undetected and is sophistically enough to inject valid application protocol packets, these packets will not be detected by the IDS since they do not trigger any signature while performing switching actions.

An additional intrusion detection algorithm is proposed. The methodology of this algorithm is to determine abnormal network traffic from normal network traffic, by comparing interactive real time data with certified data sets, the benchmark. The certified data set is created by sample data from preferably more than one year of process data, regional weather forecast data and the type of day. With these data input dynamic classes can be created, while these classes consist of switching procedures or events in the electrical power grid. The comparison of interactive real time data with the certified classes is done using a multiclass classification algorithm, which basically compares the interactive real time data with each of the certified classes. The algorithm should be able to predict the next switching procedure or event in the electrical power grid, which will determine the expected network traffic. If the network traffic falls in a known class of the classified data set, the type of action is recognised as authorised.

The proposed additional intrusion detection algorithm requires a lot of work to implement and thereafter to properly configure. Besides the loads of work for the implementation of an intrusion detection algorithm, an intrusion detection algorithm is not the best solution against a sniffing & replay or high-risk cyber-attack. The intrusion already happened, with the possible consequences of an outage or malfunction to the system. The implementation of proactive measures however would be more effective, since these are preventive. Preventive measures such as encryption or authentication will secure the network communication. Therefore, a third party's intervention of a malicious device would not be possible, and a sniffing & replay attack could not be performed with successful results.

The algorithm used for IDS should be used as a last resort, when the proactive measures fail. When intrusion is detected, further spread can be prevented if acted adequately to the alarms provided by the IDS. Reactive measures are not discussed in this thesis but are essential as well. This shows that just one category of measures is insufficient, the combination of measures is essential for a cyber resilience system. There must be a balance in costs of effort versus degree of protection (i.e. risk assessment). It can be considered to apply this algorithm to the key elements only.

This research focused only on cyber-security, while during this research it showed how wide the spectrum of cyber security really is. Cyber security is an increasing threat due to digitalisation, but just a portion of the whole security aspect of industrial control systems which facilitate our society.

7.1 Follow-up research

Since cyber-security touches such a big spectrum there are a lot of different interesting and relevant research topics to delve into.

As a follow up research for this research the development of an IDS using the comparing method presented in Figure 6.11 would be interesting. However, this needs to be performed at a utility whereby the researcher is authorised to access process data, which is sensitive information: to see if a model using a comparison of historical data against interactive real time data would be possible.

Another follow up research would be into the implementation of encryption or authentication for the communication within the OT network. Looking into the device's vendors offer, as well as encryption protocols which could be implemented. Therefor to determine the investment needed for faster and better equipment which is able to host encrypted communication.

Personally, I was fascinated by the data diode when I discovered its existence and implementation. However, the question is if the data diode is sustainable of future IT/OT infrastructures. Due to the increasing demand of bidirectional data streams of information from and to the corporate network, as mentioned a few times. Research into the implementation and sustainability of a data diode for industrial control system would be interesting.

Another research performed at a utility would be a risk assessment on their infrastructure to determine vulnerabilities. Thereafter a report with recommendations for cyber security improvements can be created.

Physical security for power substation is a topic which has not been touched on. However, research into the currently implemented physical security and possible improvements for physical security would be interesting. Securing power substation, protecting against unauthorised access would contribute to a more secure electrical power grid operation.

Another topic which is briefly mentioned but not discussed is social engineering. Lot of cyber-attacks start of by social engineering, tricking employees into downloading malicious files or extracting login credentials. Research into the human aspect of cyber security would be interesting.

Lastly research into an action plan for when a cyber-attack occurs in an industrial control system. Therefor the operators would be ready for a cyber-attack and know how to react.

7.2 Recommendations

Back in the days utilities built their system around reliability. In order to keep up with customer demand, utilities now have to switch to digitalized systems whereby cyber security plays an increasingly important role. When implementing cyber security measures, it is important to implement a variety of measures hence proactive, interactive and reactive, since only the combination of these will result in a cyber resilience system.

Implementation of the additional detection algorithm is advised to be done step by step from design throughout validation.

Education of employees on the role they play in prevention from cyber-attack is essential since most cyber-attack cases start off with some form of social engineering. Evaluate remote access entry points and reduce them as much as possible, because the combined failure of these two could have a catastrophic impact.

Each utility has its own cyber-security specialist which creates, manages, monitors and implements new solutions to the network. Beside their own experience and testing, an audit from an independent company on the infrastructure will provide a second opinion on the utility's infrastructure. The audit should consist of penetration and robustness testing to hunt down vulnerabilities.

The aspect of physical security is beyond this thesis but plays a big role in security as well. Why would an adversary once he gained access to the power substation, as stated in chapter 6.1 only plug a malicious device between a connection? Once physically inside it is very easy for an adversary to cause mayhem, damage can be done by directly controlling the IEDs or use of the local HMI. Or by using the mechanical switches in the field, opening the oil drain for transformers. As well as changing the cabling in the panels used for monitoring and controlling of the field components.

Therefore, it is important for a utility to be defence in depth, the optimum must be found in costs versus the relevant level of protection against intrusion of a facility regarding all types of adversary actions.

REFERENCES

[1] "www.dnvgl.com," DNV GL, 2019. [Online]. Available: https://www.dnvgl.com/about/index.html. [Accessed 5 February 2019].

[2] "Supervisory Control and Data Acquisition (SCADA) Lecture 1: Introduction," 30 March 2015. [Online]. Available: https://nptel.ac.in/courses/108106022/8. [Accessed 26 February 2019].

[3] "Figure 1.2," 2019. [Online]. Available: https://www.mbcontrol.com/scada-energy-management-solution/.

[4] "Figure 1.3," May 21, 2014. [Online]. Available: https://medium.com/eklektikos-delectus/managing-peak-tea-23ed0ce37176.

[5] D. GL, "Energy Transition Outlook 2018," DNV GL, Høvik, 2016.

[6] "Critical Infrastructe Sectors," Department of Homeland Security, [Online]. Available: https://www.dhs.gov/cisa/critical-infrastructure-sectors. [Accessed 26 March 2019].

[7] "Lecture 4: Applications of SCADA," 30 March 2015. [Online]. Available: https://nptel.ac.in/courses/108106022/12. [Accessed 26 February 2019].

[8] Technical Working Group 1, "National Electric Sector Cybersecurity Organization Resource (NESCOR)," Electric Power Research Institute (EPRI), September 2013.

[9] "Venezuela power cuts: Blackouts continue as protests loom," BBC News, 9 March 2019. [Online]. Available: https://www.bbc.com/news/world-latin-america-47504722. [Accessed 10 March 2019].

[10] "SCADA and Central Applications An Introduction," [Online]. Available: https://www.kth.se/social/files/545950f7f27654434dcd3e53/Lecture+9+-+SCADA+Systems.pdf. [Accessed 25 February 2019].

[11] "Lecture 2: SCADA Hardware," 30 March 2015. [Online]. Available: https://nptel.ac.in/courses/108106022/9. [Accessed 26 February 2019].

[12] "Lecture 3: Software and Protocols," 30 March 2015. [Online]. Available: https://nptel.ac.in/courses/108106022/10. [Accessed 26 February 2019].

[13] Y. Liu, "Generic Substation Event Monitoring Based On IEC 61850 And IEEE 1588 Standards," The University of Adelaide, Adelaide, 2015.

[14] "Difference Between TCP/IP and OSI Model," TechDifferences, 25 March 2016. [Online]. Available: https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html. [Accessed 24 February 2019].

[15] "What Is Combined Non-Conventional Instrument Transformer," Maxwell Technologies, 20 February 2017. [Online]. Available: https://www.maxwell.com/blog/combined-non-conventional-instrument-transformer. [Accessed 27 February 2019].

[16] "Communication Network," [Online]. Available: http://www.uky.edu/WDST/PDFs/[23]%20Communications%20network.pdf. [Accessed 27 February 2019].

[17] G. Johnson, "The OSI Model, Part 2," Applied Motion Products A Moons' Company, 28 October 2015. [Online]. Available: https://www.applied-motion.com/news/2015/10/osi-model-part-2. [Accessed 6 May 2019].

[18] D. v. Slyke, "SCADA The Heart of an Energy Management System," ATCO Electric, Edmonton, 2015.

[19] "Reviews for Advanced Distribution Management Systems," Gartner, 2019. [Online]. Available: https://www.gartner.com/reviews/market/advanced-distribution-management-systems. [Accessed 18 April 2019].

[20] "SCADA SYSTEM," Schneider Electric, 2019. [Online]. Available: https://www.schneider-electric.com/en/product-subcategory/6150-scada-system/. [Accessed 20 February 2019].

[21] "What is HMI and SCADA?," GE, 2019. [Online]. Available: https://www.ge.com/digital/applications/hmi-scada. [Accessed 20 February 2019].

[22] "Spectrum Power SCADA and Energy Management Systems," Siemens, 2019. [Online]. Available: https://w3.usa.siemens.com/smartgrid/us/en/transmission-grid/products/energy-management-and-scada-system-platforms/pages/energy-management-scada-system-platforms.aspx. [Accessed 20 February 2019].

[23] "Electrical Utility Solutions," ABB, 2019. [Online]. Available: https://new.abb.com/substation-automation/applications/electrical-utility-solutions. [Accessed 20 February 2019].

[24] "OSI," SCADA, 2019. [Online]. Available: https://www.osii.com/solutions/products/scada.asp.

[Accessed 20 February 2019].

[25] "EMS Lecture 1: Introduction," 30 March 2015. [Online]. Available: https://nptel.ac.in/courses/108106022/1. [Accessed 26 February 2019].

[26] "EMS Lecture 2: Working of EMS," 30 March 2015. [Online]. Available: https://nptel.ac.in/courses/108106022/2. [Accessed 26 February 2019].

[27] "Load Frequency Control in Power Systems," Electrical Engineering Tutorials, [Online]. Available: http://electricalengineeringtutorials.com/load-frequency-control-in-power-systems/. [Accessed 4 March 2019].

[28] C. K. &. E. D. Shelly Hagerman, "ADMS: The core of the utility of the future," West Nonroe Partners, Chicago, US, 2018.

[29] N. R. E. Laboratory, "Insight into Advanced Distribution Management Systems," U.S. Depertment of Energy , Washington, 2015.

[30] "CSS Cyber Defense Project Hotspot Analysis: Stuxnet," Center for Security Studies, Zurich, 2017.

[31] SANS & E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, Washington, march 18, 2016.

[32] "https://us.norton.com," Norton, [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html. [Accessed 11 March 2019].

[33] "Cyber Kill Chain Applied to ICS," INCIBER-CERT, 27 October 2016. [Online]. Available: https://www.incibe-cert.es/en/blog/cyber-kill-chain-applied-ics. [Accessed 11 March 2019].

[34] M. S. Center, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," Idaho National University, Idaho, 2017.

[35] "Attack vectors in cybersecurity: All you need to know to expel them out from your digital evironments," gbadvisors, 2 May 2018. [Online]. Available: https://www.gb-advisors.com/attack-vectors-in-cybersecurity/. [Accessed 19 March 2019].

[36] "Threat Hunting: Common Attack Vectors and Delivery Channels," Sage Data Security, 12 March 2018. [Online]. Available: https://www.sagedatasecurity.com/blog/threat-hunting-common-attack-vectors-and-delivery-channels. [Accessed 19 March 2019].

[37] E. Hjelmvik, "SCADA Network Forensics with IEC-104," NetreseC, 30 August 2012. [Online]. Available: https://www.netresec.com/?page=Blog&month=2012-08&post=SCADA-Network-Forensics-with-IEC-104. [Accessed 22 March 2019].

[38] L. A. Maglares, "Intrusion Detection in SCADA Systems using Machine Learning Techniques," University of Huddersfield, Huddersfield, 2018.

[39] J. D. M.-P. &. M. D. Stojanovic, "Analysis of SCADA System Vulnerabilities to DDoS Attacks," Researchgate, 2013.

[40] "What is a Zero-Day Exploit?," FireEye, [Online]. Available: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html. [Accessed 22 March 2019].

[41] S. Cooper, "What is a Remote Access Trojan or RAT? (with examples)," Comparitech, 31 December 2018. [Online]. Available: https://www.comparitech.com/net-admin/remote-access-trojan-rat/. [Accessed 22 March 2019].

[42] "Cyber Security Series: Active, Proactive or Reactive? Assessing Your Cyber Security Posture," Capco, Brussels, 2018.

[43] "PAN-OS Administrator's Guide," Palo Alto Networks, Inc, Santa Carla, 2019.

[44] "What is a Firewall?," Forcepoint, [Online]. Available: https://www.forcepoint.com/cyber-edu/firewall. [Accessed 22 March 2019].

[45] M. Kassner, "Why firewalls are not recommended for securing SCADA systems," TechRepublic, 28 November 2016. [Online]. Available: https://www.techrepublic.com/article/why-firewalls-are-not-recommended-for-securing-scada-systems/. [Accessed 23 March 2019].

[46] Dan Crum, "What Is Data Diode Technology & How Does It Work," OWL Cyber Defense, 25 March 2018. [Online]. Available: https://www.owlcyberdefense.com/blog/2018/6/25/what-is-data-diode-technology. [Accessed 26 March 2019].

[47] "Configurating Port Security," Cisco, 13 February 2018. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html. [Accessed 23 March 2019].

[48] "Configuring Dynamic ARP Inspection," Cisco, [Online]. Available:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_52_se/configuration/guide/3750scg/swdynarp.html. [Accessed 21 March 2019].

[49] J. Petters, "IDS vs. IPS: What is the Difference?," [Online]. Available: https://www.varonis.com/blog/ids-vs-ips/. [Accessed 22 March 2019].

[50] "Achilles Test Platform," 2014. [Online]. Available: https://www.ge.com/digital/sites/default/files/download_assets/achilles_test_platform.pdf. [Accessed 2019 April 15].

[51] "ASE2000 RTU Test Set," ASE a Kalkitech Company, 2019. [Online]. Available: https://www.ase-systems.com/ase2000-version-2/. [Accessed 15 April 2019].

[52] "USB Convertors," TP-Link, 2019. [Online]. Available: https://www.tp-link.com/us/home-networking/usb-converter/tl-ue300/. [Accessed 15 April 2019].

[53] "Wireshark," Wireshark, 2019. [Online]. Available: https://www.wireshark.org/. [Accessed 15 April 2019].

[54] "Modbus Tools," Modbus Tools, 2019. [Online]. Available: https://www.modbustools.com/download.html. [Accessed 15 April 2019].

[55] "SILENTDEFENSE VERSION 3.13 Going Toward Active Cyber Security," Forescout, 2019. [Online]. Available: https://www.secmatters.com/silentdefense-version3. [Accessed 2 May 2019].

[56] "SCADAguardian Advanced Real-time ICS Cyber Security and Operational Visibility," NOZOMI Networks, 2019. [Online]. Available: https://www.nozominetworks.com/products/scadaguardian-advanced/. [Accessed 3 May 2019].

[57] "iSID – Industrial Threat Detection Threat and vulnerability detection with system-wide visibility for ICS/SCADA OT networks," Radiflow, 2019. [Online]. Available: https://radiflow.com/products/isid-industrial-threat-detection/. [Accessed 3 May 2019].

[58] M. Aly, "Survey on Multiclass Classification Methods," November 2005. [Online]. Available: https://www.cs.utah.edu/~piyush/teaching/aly05multiclass.pdf. [Accessed 7 May 2019].

[59] R. Rifkin, "Multiclass Classification," 25 February 2008. [Online]. Available: http://www.mit.edu/~9.520/spring09/Classes/multiclass.pdf. [Accessed 07 May 2019].

DNV·GL

Appendix A
Project Execution Plan

Project Execution Plan

Cyber Security for Power System Operators

Author: Casper van der Sluis
Student number: 15049558
University: The Hague University of Applied Sciences
Education: Electrical Engineering
University supervisors: 1st Ben Kuiper
2nd Paul Witte
Company: DNV GL Singapore PTE. LTD.
Company supervisor: Gary Chee Kiong Ang

Date: 26 - February – 2019

1.0	Final	Casper van der Sluis	26-02-2019
0.2	For approval	Casper van der Sluis	21-02-2019
0.1	First draft	Casper van der Sluis	04-02-2019
Revision	**Description**	**Name**	**Date**

Table of Contents

1 BACKGROUND INFORMATION

DNV GL is a global quality assurance and risk management company. Driven by the purpose of safeguarding life, property and the environment, DNV GL enables organisation to advance the safety and sustainability of their business. They provide classification, technical assurance, digital solutions and independent expert advisory services to the maritime, oil & gas, power and renewables industries. As well as certification, supply chain and data management services to customers across a wide range of industries. Operating for over 150 years, with 12500 employees located in more than 300 offices across 100 countries.

DNV GL Energy represents over 20% of the turnover in DNV GL and is still growing. Under DNV GL Energy is the region Advisory Asia Pacific which include countries such as Australia, China, Singapore, India, Japan, Korea and Thailand. Clean Technology Centre (CTC) Singapore is the head office for Advisory Asia Pacific and seen as the hub to the Asia Pacific countries. DNV GL Energy Singapore is divided in two departments, Energy Advisory and Renewables Advisory. Under Energy Advisory is the department Intelligent Network and Communication (INC) which is led by Gary Chee Kiong Ang, my company supervisor. Intelligent Network and Communication is active amongst Protocol Competence Testing, Power System Operation, Cyber Security, IEC 61850 Substation Automation, SCADA/EMS/DMS Digital Transformation and System & Component Level.

The graduation project with the associated thesis will take place in the Clean Technology Centre in DNV GL Singapore, within the Intelligent Network and Communication department.

The graduation project period will be 17 weeks, starting the 4th of February and finish the 31st of May. During this period a thesis will be created about the detection of incident/intrusion in the SCADA system of a Power System Operator. Due to the digitalisation of the control system of the power grid, aspects of cyber security must come play a part. This research shall focus on the detection of incident/intrusions in the SCADA network and will result in a broad overview of possible cyber-attack scenarios. As well as an algorithmic measurement to detect given high risk cyber-attack scenario. Power System Operators can implement these algorithms to create a better protected SCADA system and therefore a more reliable power grid.

The stake holders are DNV GL Singapore PTE. LTD. and The Hague University of Applied Sciences. DNV GL is both the client and the contractor, they will have a consulting role. The Hague University of Applied Sciences will also have a consulting role and will mark the final result.

The technical details will be discussed with DNV GL, as well as the project boundaries. The result will be presented at The Hague University of Applied Sciences in the form of a pitch. When the graduation project proposal will be accepted, the graduation project can be executed.

2 GENERAL INFORMATION

Cyber security for power system operators, focussing on detection of intrusions/incidents in a SCADA system.

Modern Supervisory Control And Data Acquisition (SCADA) systems are essential for monitoring and managing power systems. The power system operators control their SCADA systems from a central point, the control centre and use it as an Energy Management System (EMS) or Distribution Management System (DMS) to manage the energy flows within their network. These systems were designed for reliability, not security.

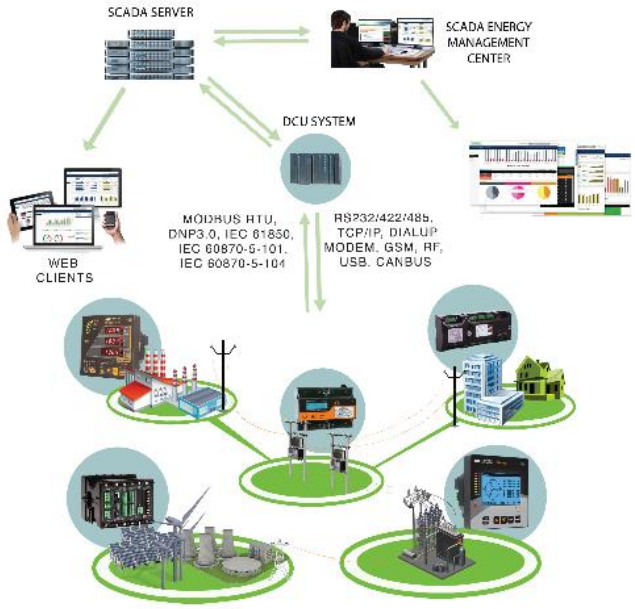


Figure 2.1 SCADA/DMS system overview [1]

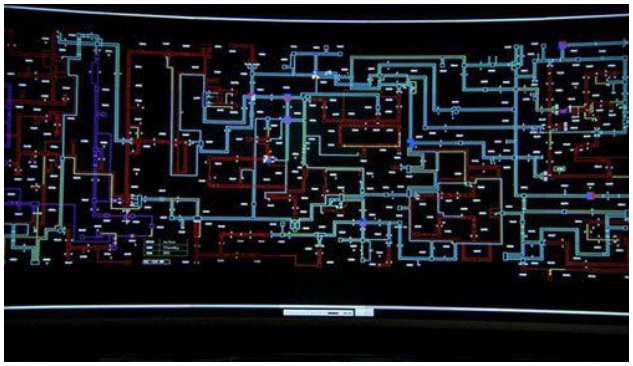


Figure 2.2 Control centre console overview [2]

This research shall focus on the detection of intrusions/incidents within the SCADA network of a power system operator. Creating an algorithm (flowchart diagram) for a high risk cyber-attacks scenario, therefore the algorithm should be able to detect given cyber-attack scenario with the provided variables by the system.

Different SCADA systems of different Power System Operators have different configurations and different functionalities. These functionalities vary from basic to advanced. The standard functionalities are EMS and DMS. These functionalities or software applications are advancing, for instance some vendors offer ADMS which stands for Advanced DMS. This ADMS integrates an Outage Management System (OMS) in the Distribution Management System. The OMS include functionalities for a better determination of the outage location by its Geographic Information System (GIS) and Automatic Meter Reading (AMR) making it easier for the operator to respond correctly.

So looking at the SCADA infrastructure and the software, the aim is to create an algorithm which is able to detect given high risk cyber-attack scenario. From this algorithm, other projects for software development can be explored.

3 PROJECT RESULT

This chapter will focus on the desired project result. This will be done on the bases of requirements stated in the document "Project Description V2"

3.1 Problem theorem

With the digitalisation of the power grid the management and monitoring of the power grid improved strongly. With the control centre in place, the power system operators can now make switching actions from a central point. Instead of calling each other from their local power substation and both having to make a physical switching action. This is convenient however, since everything is controlled from a central point and through a computer operated system. This technologic advancement made the power grid more vulnerable for cyber-attacks.

3.2 Project goal

The project goal is formulated using SMART method. SMART stands for Specific, Measurable, Achievable, Realistic and Time-bound. This will create a proper guideline.

- S Creating an algorithm for a high-risk cyber-attack scenario. The algorithm should be able to detect an incident/intrusion.
- M Verification of algorithm using simulated process data.
- A Algorithm should be able to detect given the incident/intrusion.
- R Extensive knowledge of the INC team is available as well as applied norms and information.
- T Project time is 17 weeks.

3.3 Project result description

The final result of this project will be an algorithm which is able to detect given high risk cyber-attack scenario. The algorithm will be created looking at variables in simulated process data and should later on be verified using simulated process data provided by DNV GL. Actual power system operators process data cannot be acquired due to it being highly sensitive information. The type of cyber-attack will be determined once the overview tree of possible cyber-attack scenarios and corresponding risk assessment has been completed.

First of all, there will be research done on the configuration of a SCADA system. Including types of functionalities power system operators use in their system. As well as used communication protocols within the system. This will give the intern a better understanding of what a SCADA system all comprises. From there the intern should be able to create an in-depth overview of SCADA/EMS/DMS systems.

Research on types of cyber-attack scenarios, also looking at cyber-attack cases such as Ukraine 2015 [3] should increase the understanding of cyber-attacks procedure. With further research into attack vectors and already deployed controls for cyber security by power system operators, the intern should be able to create an inventory list of attack vectors and already deployed controls for cyber security by power system operators.

A high-risk cyber-attack scenario will be chosen once an overview of cyber-attack scenarios has been created. All cyber-attack scenarios will be evaluated with a risk factor.

The chosen high-risk cyber-attack will be researched. From there an algorithm which is able to detect given high risk cyber-attack scenario will be created.

3.4 Program of requirements

In order to realise the project final result a program of requirements has been created. This will give support during the project. All requirements must be met and should be described and verified in the thesis.

General
All documentation including the thesis will be written in English, therefore the thesis should also include a Dutch summary according to Afstudeerhandleiding Elektrotechniek [4].

Several standards from different regions have to be taken into account: ISO27001, IEC62443, NIST SP 800, NERC CIP.

SCADA overview
The SCADA overview should give a clear overview of the general infrastructure of a SCADA system as well as the different types of communication protocols which can be used (EU/US standards). These different communication protocols should be explained and categorized properly.

Inventory list of attack vectors & already deployed controls for cyber security
An inventory list of attack vectors and already deployed controls for cyber security is crucial. It will provide boundaries and a direction for the types of cyber-attack scenario which will be researched.

Overview tree of possible cyber-attack scenarios
With the achieved knowledge so far different types of cyber-attack scenarios can be thought of, these will be ranked an assigned with a risk assessment. The risk factor will be assigned according to NESCOR's Electric Sector Failure Scenarios and Impact Analyses [5] – High Level Ranking Method. The two criteria which will be factored in are "impact, considering all types of impacts" and "cost to the adversary, considering the overall difficulty and cost to the threat agent to carry out the failure scenario." The overall ranking is then calculated as impact divided by the cost to the adversary. The two criteria used for this method correspond to the composite values of "impacts result" and "effects on likelihood and opportunity result". Assigning a score of 0,1,3 of 9 to represent the impact of the failure scenarios, as it ranges from minor to significant. Assigning a score of 0.1,1,3 or 9 to represent the cost and difficulty to the threat agent to carry out the failure scenarios is low to high.

High risk cyber-attack algorithm
The algorithm should be created using Microsoft Visio. The algorithm should be able to detect given cyber-attack scenario. Simulated process data is used to create the algorithm. Looking at the regular pattern process data an abnormal pattern, possible intrusion could be detected with the provided variables of the SCADA system.

Validation of algorithm
The validation of the algorithm should be done using simulated process data. Since the project does not include actual programming of the algorithm the validation is by means of variable comparison.

Thesis
The Thesis and all other documentation should be written in English, except from the Dutch summary which is required. Other requirements are mentioned below, partly coming from appendix 1 of Afstudeerhandleiding Elektrotechniek [4].

- The thesis should be a professional report, using guidelines of Rapport over rapporteren [6].
- When the thesis is written in English there should be a Dutch summary.
- The thesis should roughly be between 40 and 60 pages, excluding the appendixes.
- The thesis should include a competence accountability repot.

The first draft of the table of contents for the thesis is added as appendix i.

Delivery
All above mentioned topics should be documented in the thesis. As well as the project execution plan and following rapports. The thesis will be delivered upon completion of the gradation project. Digital at Onstage before the end of 31st of May. As well as 3x a hard copy at the faculty office by an authorised person before the 3rd of April at 12:00 AM, all dates and times are GMT+1.

4 PROJECT ACTIVITIES

This chapter will describe the project progress. For the whole duration of the graduation: every other week the intern will create a report on the progress to send the university supervisor for accountability. The project activities are separated in the following phases:

4.1 Phase 0: Start graduation route

This phase is not during the project itself but beforehand in order to actually getting a graduation project. Since the graduation project is abroad several preparation tasks include:

- Search for company.
- Formulating graduation project.
- Pitch moment at The Hague University of Applied Sciences.
- Fine tuning graduation project for approval.
- Arranging flight tickets, housing, visa.
- First draft project execution plan.

4.2 Phase 1: Orientation (3 weeks)

In the orientation phase the intern will be introduced to the company. Besides, in this phase the project scope should become clear, tasks include:

- Determining the project boundaries & activities.
- Creating a planning.
- Literature research.
- Standards and norms research.
- Schedule weekly appointment with company supervisor.
- Draft accountability report template for every other week.
- Completion project execution plan.

4.3 Phase 2: Research & Development (10 weeks)

In the research & development phase the main work will be fulfilled. In the following order de tasks will include:

- Research SCADA system and functionalities.
- Research on past cyber-attacks e.g. Ukraine 2015.
- Research on attack vectors & already deployed controls for cyber security.
- Orientating on cyber-attack scenarios.
- Creating an overview tree of possible incidents and the corresponding risk assessment.
- Researching a high-risk cyber-attack scenario.
- Designing algorithm for high risk cyber-attack scenario which can detect such intrusion.
- Verifying algorithm using simulated process data.
- Draft thesis.

4.4 Phase 3: Completion (4 weeks)

The completion phase concerns the delivery of the project.

- Final touches.
- Process review.
- Completion thesis.
- Business assessment.
- Delivery thesis Onstage.
- Delivery thesis x3 hardcopy.

4.5 Phase 4: Final assessment

As earlier stated The Hague University of Applied Sciences will mark the final result.

- Poster presentation.
- Graduation session.

5 PROJECT BOUNDARIES AND CONDITIONS

This chapter focuses on the boundaries and conditions of the project. The boundaries are determined together with the company supervisor, Gary Chee Kiong Ang. In order to make the project feasible and challenging.

5.1 Scope

For a clear scope the boundaries and exclusions will also be described below.

5.1.1 Boundaries

A big part of this research shall focus on the understanding of the SCADA configuration. As well as a general view of cyber security in operational technology. The end result being an algorithm which should be able to detect given cyber-attack scenario. This algorithm does not include programming of any code. The algorithm will be constructed using Microsoft Visio.

5.1.2 Conditions

The following conditions have to be met in order for the project to succeed.

- The project time of 17 weeks must suffice.
- The simulated process data is sufficient.
- Supervisor must be available for questions.
- The given input documentation should be relevant and correct.

6 INTERMEDIATE RESULTS

To reach the project result, several intermediate results have to be accomplished. The intermediate result will be reviewed against the project results, planning and activities. Below are the intermediate results mentioned:

- Completion of project execution plan.
- Overview of SCADA system.
- Inventory list of attack vectors & already deployed controls of cyber security.
- Cyber-attack scenario tree with risk assessment.
- Algorithm for high risk cyber-attack scenario.
- Validation rapport of algorithm.
- Completion of thesis.

7 QUALITY

To manage the quality of the project, and its results to meet the required specifications. Several actions will be undertaken during the graduation project. Below is described how the quality of the graduation project will be maintained:

- Feedback on project execution plan by company supervisor and by university supervisor.
- Feedback on intermediate results by company supervisor and/or INC team.
- Accountability report every other week to check progress.
- Results should be strictly conform program of requirements.
- Technical consult by company supervisor and INC team.
- Any deviations or exceptions should be explained in the thesis.

8 PROJECT ORGANISATION

Graduate intern

Name:	Casper van der Sluis	
Address:	Hof van Azuur 44	21 Telok Blangah Drive #10-03
Postcode:	2614TB Delft, The Netherlands	109258 Singapore
E-mail:	caspervdsluis@live.nl	casper.van.sluis@dnvgl.com
Phone number:	+31 (0)6 22259475	+65 98867673

Company supervisor

Name:	Gary Chee Kiong Ang
Company:	DNV GL Singapore PTE. LTD.
Address:	16 Science Park Drive DNV GL Clean Technology Centre
Postcode:	118227 Singapore
E-mail:	gary.chee.kiong.ang@dnvgl.com
Phone number:	+65 97864559

1st University supervisor

Name:	Ben Kuiper
Company:	The Hague University of Applied Sciences
Address:	Rotterdamseweg 137
Postcode:	2628 AL Delft, The Netherlands
E-mail:	b.kuiper@hhs.nl
Phone number:	+31 (0)15 2606322

2nd University supervisor

Name:	Paul Witte
Company:	The Hague University of Applied Sciences
Address:	Rotterdamseweg 137
Postcode:	2628 AL Delft, The Netherlands
E-mail:	p.m.witte@hhs.nl
Phone number:	+31 (0)15 2606307

9 SCHEDULE

The schedule is created using Microsoft Project Professional, please see Appendix ii.

10 COSTS & BENEFITS

10.1 Costs

The costs for this graduation project from DNV GL are divided in the following:

- Intern allowance of 1200 Singapore Dollar which equals to 772 Euro at time of signing.
- Costs for the guidance of the company supervisor.
- Costs for visa application and administration.
- Costs for the use of facilities of DNV GL.

10.2 Benefits

The greatest earnings of this project lies in the gathering of knowledge about this topic. This is beneficial for both the intern to raise his knowledge level, as for DNV GL who can use the obtained information for future projects.

11 RISKS

During the project, several risks can occur. To be able to deal with these risks during the project they have already been thought out. The risks analysis will be done conform Project management 7th edition of Roel Grit [7]. Leaving some irrelevant topics out, leaving the maximal score at 270.

Table 11.1 Risk analysis

Risk	Value	Factor	Weighting	Total
Time factor:				
1. Processing time project	0-3 months 3-6 months 6+ months	0 1 3	4	4
2. Is the definitive deadline set	No Flexible Yes	0 2 4	4	16
3. Available time to realise the project	Many Enough Insufficient	0 1 3	4	4
Complexity:				
4. Number of functional areas involved	1 2 3+	0 1 3	4	0
5. Is the project an adjustment or a new project	Small changes Big changes New project	0 2 3	5	15
6. To what extend will existing responsibilities have to change	Not Minimal Average Highly	0 1 2 3	5	0
7. Are other project depended on this project	No Yes, enough time Yes, no time	0 1 3	5	0
8. Are subproject depending on coordination between them	No Slightly Highly	1 2 3	3	6
Project group:				
9. Which type of employees are working on the project	Mostly intern Limited intern Mostly extern	0 1 3	4	0
10. What is the geographical distribution of the project	1 place 1-3 place 3+ place	0 1 2	2	2
Project management:				
11. Has the project manager knowledge about the project topic	A lot Enough Insufficient	0 2 4	3	6
12. Has the project manager knowledge about project management	A lot Enough Insufficient	0 2 4	3	6
13. How much experience does the project manager have with such project	A lot Enough Little	0 1 3	3	9
14. How experienced are the consultant with such project	A lot Enough Insufficient	0 1 3	5	0
15. Is it likely that the composition of the project group will change during the project	Little Average High	0 2 5	5	0
Clarity of the project:				

16. Are problem definition and final goal clear	Yes Slightly No	0 1 5	5	0
17. Is the research area accurately defined	Yes Slightly No	0 2 5	5	0
18. Are the project boundaries clear	Yes Most of them No	0 1 5	5	0
			Total	68

Risk percentage = $\frac{Total}{Maximal\ score} * 100\% = \frac{68}{270} * 100\% = 25{,}2\%$. (10.1)

The rule of the thumb stated that if the risk percentage is above 50%, the project should not be executed in this way. The risk percentage is under the limit and therefore has a good chance of success.

Other separate risk topics which should be evaluated are stated below:

Time
Problems may arise when there seem to be not enough time for a topic. To make sure topics are completed within a given timeframe a planning is created. The research shall strictly stick to the schedule. The planning should take some extra time into account.

Illness
Since the intern is in a different environment abroad, there is a high risk of getting sick. Could be from the heat and humidity outside, the aircon inside or unknown/spicy foods. The risk should be limited by adding a buffer, some extra time to the planning.

Width research
Since the topic cyber security is very broad, there is a risk the intern gets stranded at a certain topic for a intermediate result. It should be evaluated how relevant the depth of each topic is for the end result. Otherwise the intern could lose sight on the end result.

Any inexperience
Since the topic cyber security is totally new for the intern. It could be possible that the intern gets flooded with information and not be able to see the wood for the trees. The risk is covered by the experienced consultants from DNV GL which can be asked for advice anytime.

Insufficient motivation
Insufficient motivation would mean that the intern fails the graduation project. The consequences for failing the graduation project are known and are too high. Therefore, the risk for insufficient motivation is low.

12 COMPETENCES

During the course of my Dual Electrical Engineering education all competences have been met at their maximum level. For the graduation project 5 out of the 8 competences have to be met at their maximum level. These competences with their corresponding maximum level are:

Competence	Level
• Analysing	3
• Designing	3
• Realising	3
• Managing	2
• Researching	2

Each task is assigned to a competence, therefor some competences are completed by several tasks.

Analysing
The SCADA system configuration as well as EMS/DMS applications in order to get an understanding of the configuration of a SCADA system. Analysing the historical cyber-attack scenarios.

Designing
An overview tree of cyber-attack scenarios with risk assessment to get an overview of different types of cyber-attack scenarios. Thereafter designing an algorithm for a high-risk cyber-attack scenario which should be able to detect given incident/intrusion.

Realising
All the intermediate results and the final thesis. That those products will meet their requirements and are representative documents.

Managing
The entire course of the graduation project.

Researching
The appropriate standards and norms for cyber security, communication protocols, network configurations. Researching the attack vectors and already deployed controls for cyber security. Researching the types of cyber-attacks scenarios, going more in depth about a high-risk cyber-attack scenario. Once the algorithm is created researching its validation by verifying its purpose with simulated process data.

REFERENCES

[1] "Figure 2.1," 2019. [Online]. Available: https://www.mbcontrol.com/scada-energy-management-solution/.

[2] "Figure 2.2," May 21, 2014. [Online]. Available: https://medium.com/eklektikos-delectus/managing-peak-tea-23ed0ce37176.

[3] SANS & E-ISAC , "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, Washington, march 18, 2016.

[4] "Afstudeerhandleiding Elektrotechniek," The Hague University of Applied Sciences, Delft, 2018-2019.

[5] Technical Working Group 1, "National Electric Sector Cybersecurity Organization Resource (NESCOR)," Electric Power Research Institute (EPRI), September 2013.

[6] H. Hoogland, I. Brand and R. Dik, Rapport over rapporteren, Groningen: Noordhoff Uitgevers B.V., 2010.

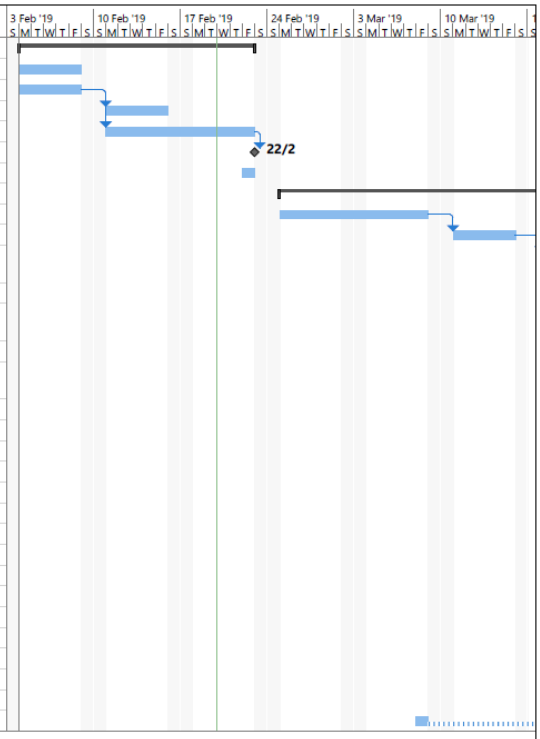
[7] R. Grit, Projectmanagement, Groningen: Noordhoff Uitgevers B.V., 2015.

APPENDIX i
Draft Thesis Table of Contents

Table of Contents

APPENDIX ii
Schedule

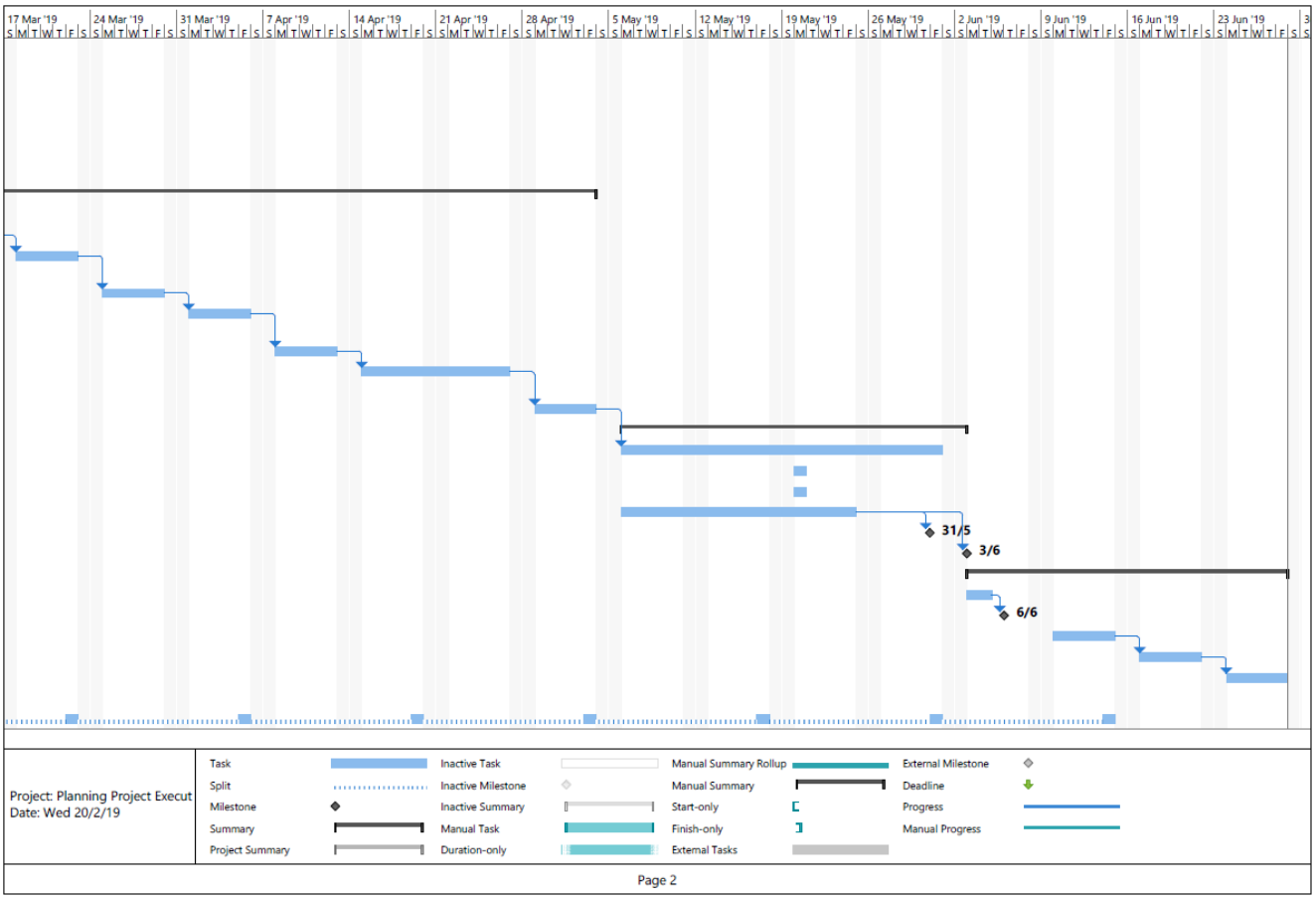
ID	Task Mode	Task Name	Duration	Start	Finish
1		**Orientation Phase**	**15 days**	**Mon 4/2/19**	**Fri 22/2/19**
2		General orientation	5 days	Mon 4/2/19	Fri 8/2/19
3		Literature research	5 days	Mon 4/2/19	Fri 8/2/19
4		Determing project boundaries & activities	5 days	Mon 11/2/19	Fri 15/2/19
5		Project Excecution Plan	10 days	Mon 11/2/19	Fri 22/2/19
6		Completion Project Excepcution Plan	0 days	Fri 22/2/19	Fri 22/2/19
7		Draft template accountability report	1 day	Fri 22/2/19	Fri 22/2/19
8		**Research & Development Phase**	**50 days**	**Mon 25/2/19**	**Fri 3/5/19**
9		Research SCADA system and functionalities	10 days	Mon 25/2/19	Fri 8/3/19
10		Research on past cyber-attacks e.g. Ukraine 2015	5 days	Mon 11/3/19	Fri 15/3/19
11		Research on attack vectors & already deployed controls for cyber security	5 days	Mon 18/3/19	Fri 22/3/19
12		Orientating on cyber-attack scenarios	5 days	Mon 25/3/19	Fri 29/3/19
13		Creating an overview tree of possible incidents and the corresponding risk assessment	5 days	Mon 1/4/19	Fri 5/4/19
14		Researching a high risk cyber-attack scenario	5 days	Mon 8/4/19	Fri 12/4/19
15		Designing flowchart algorithm for high risk cyber-attack scenario	10 days	Mon 15/4/19	Fri 26/4/19
16		Verifying algorithm using simulated process data	5 days	Mon 29/4/19	Fri 3/5/19
17		**Completion Phase**	**20 days**	**Mon 6/5/19**	**Mon 3/6/19**
18		Final Touches	20 days	Mon 6/5/19	Fri 31/5/19
19		Process review	1 day	Mon 20/5/19	Mon 20/5/19
20		Business assessment	1 day	Mon 20/5/19	Mon 20/5/19
21		Completion thesis	15 days	Mon 6/5/19	Fri 24/5/19
22		Deadline Thesis Onstage	0 days	Fri 31/5/19	Fri 31/5/19
23		Deadline Thesis 3x hardcopy	0 days	Mon 3/6/19	Mon 3/6/19
24		**Final assessment phase**	**20 days**	**Mon 3/6/19**	**Fri 28/6/19**
25		Create Poster	2 days	Mon 3/6/19	Tue 4/6/19
26		Poster presentation	0 days	Thu 6/6/19	Thu 6/6/19
27		Create Powerpoint	5 days	Mon 10/6/19	Fri 14/6/19
28		Graduation session preparation	5 days	Mon 17/6/19	Fri 21/6/19
29		Graduation session to be defined	5 days	Mon 24/6/19	Fri 28/6/19
30					
31		Accountability report every other week	8 days	Fri 8/3/19	Fri 14/6/19



Project: Planning Project Execut
Date: Wed 20/2/19

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

Page 1


17 Mar '19
24 Mar '19
31 Mar '19
7 Apr '19
14 Apr '19
21 Apr '19
28 Apr '19
5 May '19
12 May '19
19 May '19
26 May '19
2 Jun '19
9 Jun '19
16 Jun '19
23 Jun '19
31/5
3/6
6/6
Project: Planning Project Execut
Date: Wed 20/2/19
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress
Page 2

APPENDIX B
Competence Accountability

This appendix creates the connection between the completed work and the competences which belong to the Electrical Engineering profile. The project goal which is formulated using the SMART method in chapter 3.2 of the Project Execution Plan is realized and also it is demonstrated that I satisfy the correct level for each competence.

Analysing
The competence analysing is about identifying the research question, choices for solution strategies and mapping of requirements, goals and conditions. The competence analysing has come forward in the beginning of this research. Whereby the essence of this research is based on concern for our society and economy through the increasing threat of cyber-attacks. Therefore, formulating the main and sub research questions around the detection of an intrusion.
Analysing applied to:

- The configuration of an electrical power grid control system and to get an understanding of the functionalities.
- Historical cyber-attacks on industrial control systems to get an understanding of methods adversaries use and how a cyber-attack unfolds.
- Vulnerabilities in the form of attack vectors as well as measures to mitigate these vulnerabilities.
- The results of the simulation to determine possible solutions against the high-risk cyber-attack.
- The current state of intrusion detection systems their functioning and shortcoming.

Designing
The competence designing is about the realisation of a design, this can be about a device, process or method.
The competence designing has come forward in the creation of:

- Several overviews and methods, accordingly to the examined results.
- Several figures are created to visualise and present the information such:
    - Detailed electrical power grid control system.
    - Overview tree of cyber-attack scenarios.
    - Additional detection algorithm methodology.

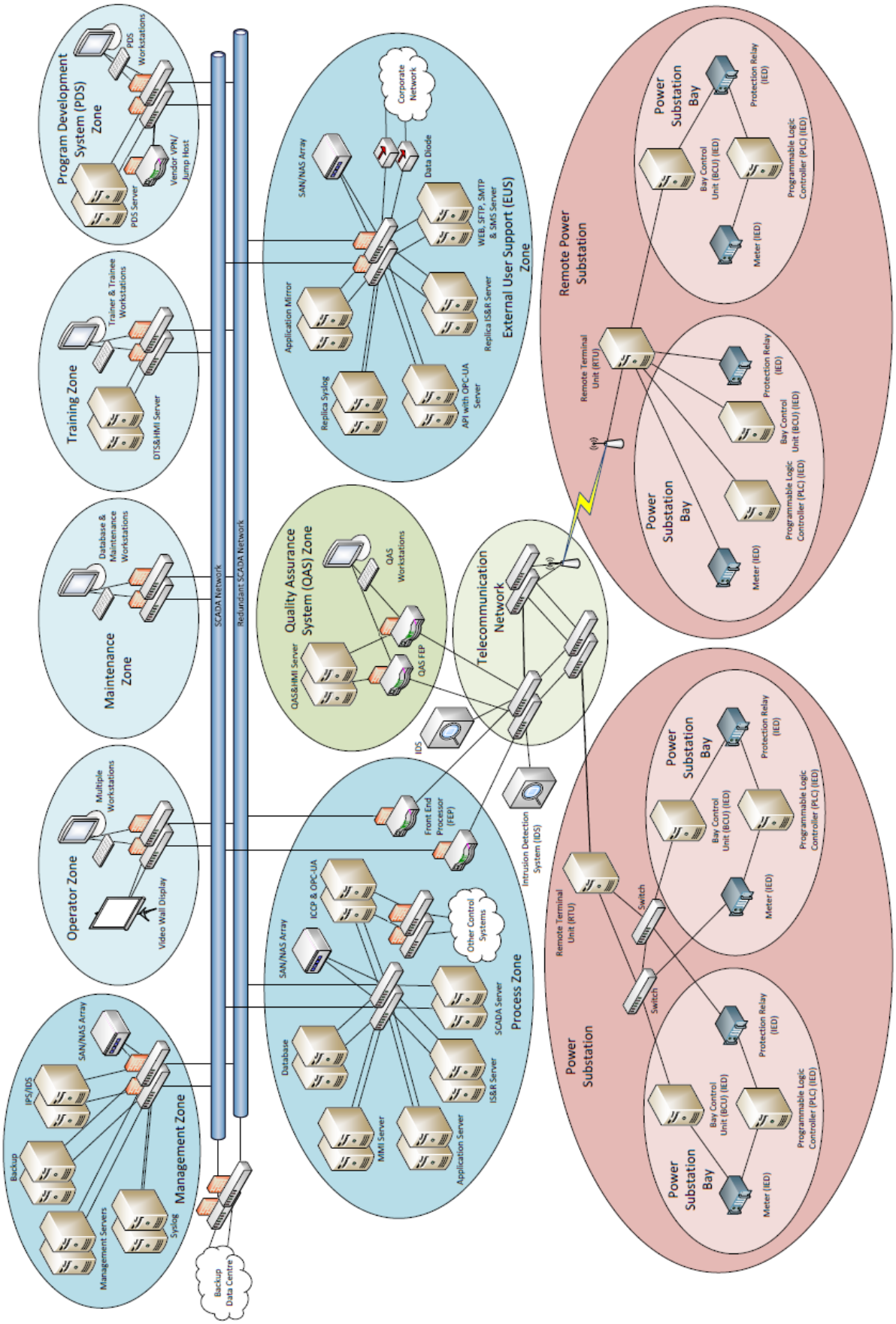
The designs are evaluated and improved throughout the research thanks to newly acquired knowledge.

Realising
The competence realising is about delivering a product, service or implementation of a process or method which complies with the requirements. Realising has come forward for the simulation, by rightly configuring the available hardware and software. This provided insight in the direction for the additional detection algorithm. Realising also came forward in the realisation of all the intermediate results as well as the final thesis. Those products meet the requirements and are representative documents.

Managing
The competence managing is about direction, guidance and initiatives towards the graduation project. The competence managing occurred during the entire course of the graduation project. And even before the start of the graduation project, several international calls happened to determine the research topic as well as making sure of the paperwork. The creation of the project execution plan and schedule has been managed by providing an accountability report every other week to my university supervisor. Communicating and working in a multi-cultural international environment, taking into account of everyone's principles and time.

Researching
The competence researching is about the critical investigative attitude while using existing methods or technics to require and asses information. The competence researching occurred during the whole course of the graduation project. By researching and answering the sub questions via in depth researching and evaluation of documentation, configuration and simulation, the answer for the main research question became clear. Whereby the conclusion is that, the combination of several cyber security measures is essential for a cyber resilience system.

APPENDIX C
Detailed electrical power grid control system overview



APPENDIX D
Achilles Test Report

achilles®
Test Report

Test Overview

Test summary: Ran 1 session and 1 test case with 1 subtest.
Test platform: Achilles Test Platform r3 Version 3.18.20170116233452
Report generated: 2019-04-26 at 03:58:06

Test Summary

All tests completed without anomalies. The following tests ran: Packet Capture Replay (over TCP)

Session 1

Session time: 2019-04-19 at 08:46:49
Testing mode: Robustness
Test summary: Ran 1 test case with 1 subtest.
Device name: None
Device notes: None

Environment

Field	Network 1	Network 2
Achilles IP	192.168.1.115/24	None
Achilles MAC	00:03:1D:10:ED:16	None
DUT IP	192.168.1.100	None
DUT MAC	52:54:00:AE:94:C1	None
VCS IP	192.168.1.150	None
VCS MAC	50:3E:AA:31:B5:45	None

Discovery

Open TCP Ports

Port	Service	Source
2404	iec-104	scan

Open UDP Ports

None configured

Multicast IP Addresses

None configured

Packet Capture Replay (over TCP)

Description: Packet Capture Replay (over TCP) sends TCP data from a packet capture to the DUT. The TCP data can be damaged as it is sent. The test case examines the DUT's ability to maintain both view and control while dealing with the damaged data. This test case is affected by the Maximum Non-Storm Rate parameter specified in Test Suite Settings.

Test notes: None

Testing mode: Robustness

Start time: 2019-04-19 at 08:46:56

End time: 2019-04-19 at 08:47:01

Version: Achilles Test Platform r3 Version 3.18.20170116233452

Anomaly Summary

Test name	T
Packet Capture Replay (over TCP)	

Configuration

Parameter	Value
Packet Capture	1026 bytes (17 packets from 192.168.1.150:54267 to 192.168.1.100:502, from file 'C:\Users\CASVAN\OneDrive - DNV GL\DNV GL Singapore\Project\Simulation\Wireshark captures\S&R attack.pcap')
Percent Damage	0.000
Repeat Packet Capture	1
Skip Initial Repetitions	0
First TCP Data Packet	6
Last TCP Data Packet	6
Destination TCP Port for Replay	Destination port from selected stream
Source TCP Port for Replay	Automatic
Random Seed	Automatic: 14647665
Wait Time for Responses (s)	0.000
Delay Between Packets (s)	0.000
Payload Processing Functions	
Global Packet Capture	Never

Global Target Device	DUT #1
Power Cycle DUT on Test Failure	Disabled
Stabilization Period (s)	5
Recovery Period (s)	15
Power Cycle Duration (s)	5.000
Maximum Non-Storm Rate (% of Link)	1.0000

Link Modes

Port 1: 1000 Mbps - Full Duplex
Port 2: 1000 Mbps - Full Duplex

Event Log

Time (s)	Source	Message
00.001	Test Information	Packet Capture Replay (over TCP): Started
00.273	Test Information	Post-test started
05.276	Test Information	Packet Capture Replay (over TCP): Completed