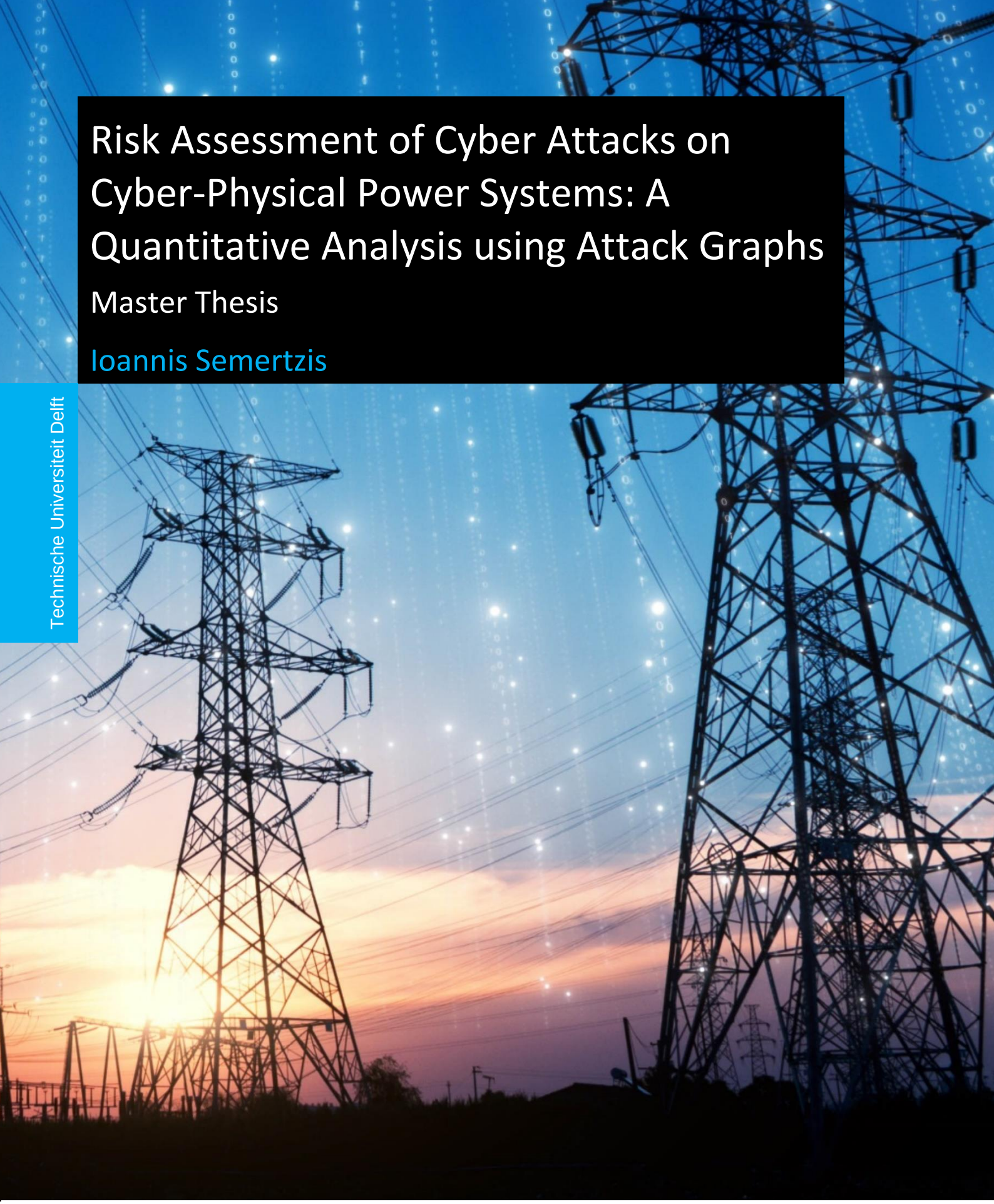
Risk Assessment of Cyber Attacks on Cyber-Physical Power Systems: A Quantitative Analysis using Attack Graphs

Master Thesis

Ioannis Semertzis

Technische Universiteit Delft



TU Delft Delft University of Technology

Challenge the future

Risk Assessment of Cyber Attacks on Cyber-Physical Power Systems: A Quantitative Analysis using Attack Graphs

By

Ioannis Semertzis

in partial fulfilment of the requirements for the degree of

Master of Science
in Electrical Power Engineering

at the Delft University of Technology,
to be defended publicly on Friday October 22nd at 09:00 AM.

Supervisor:	Dr. Alexandru Ştefanov	
Thesis committee:	Prof.dr.ir. Peter Palensky	TU Delft
	Dr.ir. Alexandru Ştefanov	TU Delft
	Ir. Frank Fransen	TNO
	Dr.ir. Jianning Dong	TU Delft
PhD Supervisor:	Ir. Vetrivel Subramanian Rajkumar	

TU Delft

IEPG Intelligent Electrical Power Grids

CRPG Cyber Resilient Power Grids

Abstract

Power grids rely on Operational Technology (OT) networks, for real-time monitoring and control. These traditionally segregated systems are now being integrated with general-purpose Information and Communication Technologies (ICTs). The coupling of the physical power system and its communications infrastructure forms a complex, interdependent structure referred to as a Cyber-Physical System (CPS). As cyber attacks on critical infrastructures become more frequent, power systems are especially vulnerable, as their OT systems were not designed with cyber security considerations. Hence, identifying and quantifying the risk of cyber attacks on power grids is of utmost importance.

In this dissertation, a method for quantitative risk assessment is proposed. The impact of cyber attacks is examined on a holistic model of a cyber-physical power system and their likelihood is assessed through attack graphs. Firstly, the physical power system is modelled to analyze the impact of cyber attacks on power system operation. The dynamic model of the IEEE 39-bus is used to validate the proposed risk assessment method. Various protection schemes are implemented and coordinated to analyze how cyber attacks can lead to cascading failures and a blackout. The communication networks of digital substations are modelled and integrated with the power system model. They emulate the communication network traffic between the control center and digital substations. The physical and cyber system models are integrated via co-simulation.

Secondly, attack graphs for digital substations are designed and used for cyber attack analysis. The attack graph model is based on the topology of a digital substation, specified by industry and academia. A novel method is proposed for defining the probability distributions of the time-to-compromise for each attack step, which is used in the attack simulations to extract the global time-to-compromise of the targeted asset.

Furthermore, an impact assessment method is proposed, which correlates the impact on both layers of the cyber-physical system. Key performance indicators for the power system operation as well as the operation of its communication system are defined and implemented. The overall risk of a specific cyber attack scenario is assessed based on the impact indices, likelihood of the cyber attack to commence, and a proposed metric regarding power system restoration. The proposed methods are validated by examining various cyber attack scenarios on the developed cyber-physical system model. The examined scenarios are based on real-world cyber attacks. Additionally, a study regarding the effect of different attack sequences is conducted. The impact is assessed on both layers of the cyber-physical power system by running dynamic simulations.

On overall, the CPS simulation results show the effectiveness of the proposed methods to assess risks and identify the most critical systems per cyber attack scenario. The proposed methods correlate the vulnerability assessment of the modelled security infrastructure with the corresponding impact on the cyber-physical system. The risk assessment is validated by a comprehensive analysis of selected study cases, examining the cascading failure chains of the power system. These studies show the importance of examining various attack scenarios in order to identify the weak points and bottlenecks in the integrated cyber-physical power system.

.

Acknowledgements

At this point, I would like to take the opportunity to thank the many people that I had the luck to have by my side throughout this Master Thesis project and have given me their valuable feedback, advice, motivation, and support at every step of the way.

First and foremost, I would like to express my sincere gratitude to my Master Thesis Supervisor Asst. Prof. Dr. Alexandru Ştefanov, under the guidance of whom, this thesis project was carried out. I would like to thank him for his continuous support, invaluable feedback and guidance during this study. He provided me with the motivation to strive for excellence and this Master Thesis is a result of this effort.

I am extremely grateful to my PhD. Supervisor, Vetrivel Subramanian Rajkumar for his guidance and support over the course of this thesis. Thank you for standing by me. Additionally, I would like to thank the members of the Cyber Resilient Power Grids research group, especially Alfan Presekal and Yigu Liu, for their help.

Next, I would like to thank my Company Supervisor Ir. Frank Fransen, Senior Scientist at the TNO Cyber Security and Robustness Department. His valuable support during both my internship at TNO and during this study, helped me gain a better understanding of the complex domain of cyber security. Additionally, I would like to thank Prof. Dr. Peter Palensky for his valuable feedback and Asst. Prof. Dr. Jianning Dong who agreed to be part of my committee.

I would like to thank all the people who were by my side and provided me with wonderful memories and experiences. My partner Angelina, for her patience and support during the duration of my studies. My friends Ifigeneia, Giorgos, Kostas, Fanis, Sila, Entela, Danai, and Kyriakos for their support and for offering me a break from my work.

Finally, I would also like to give my highest gratitude to my family for their love and support throughout these two challenging years.

Ioannis Semertzis
Delft, October 2021

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AC	Alternating Current
AVR	Automatic Voltage Regulator
BN	Bayesian Network
CPS	Cyber-physical system
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DC	Direct Current
DSL	Domain-Specific Language
DSO	Distribution System Operator
EMS	Energy Management System
FCFS	First-Come-First-Serve
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
GUI	Graphical User Interface
HMI	Human Machine Interface
ICS	Industrial Control System
ICT	Information and Communication Technology
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
KPI	Key Performance Indicator
LAN	Local Area Network
MAL	Meta-Attack Language
MitM	Man-in-the-Middle
MTTD	Mean-Time to Detect
MTTR	Mean-Time-to-Restore
MU	Merging Unit
NVD	National Vulnerability Database
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technologies
PLC	Programmable Logical Controller
QoS	Quality of Service
ROCOF	Rate-of-change-of-Frequency
RTDS	Real-Time Digital Simulator
RTT	Round Trip Time
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented Systems
SV	Sampled Values

TCP/IP	Transmission Control Protocol/Internet Protocol
TNO	Netherlands Organization for Applied Scientific Research
TSO	Transmission System Operator
TTC	Time-to-Compromise
UFLS	Under Frequency Load Shedding
UVLS	Under Voltage Load Shedding

1. Introduction

1.1. Power Grid Digitalization

The electrical power grid is a critical infrastructure for the modern society. The energy system is experiencing an unprecedented transformation through the renunciation of fossil fuels, market liberalization, and growing environmental awareness. This transition is being led by three drivers: *decarbonization, decentralization* and *digitalization* [1]. Electrical energy production is moving away from carbon-intensive fossil fuels to renewable energy sources, as humanity experiences the grave consequences of climate change. To ensure that the power grid operates in a reliable, safe, and efficient way in this increasingly complex environment, digitally enabled solutions have to be implemented to form the smart grid.

Power grid Operational Technologies (OT) enable real-time monitoring and control of the physical system. These OT systems collect measurement and operational system data from the field such as from substation bays and station control systems. The data are subsequently forwarded to the control center. The real-time data are crucial for the uninterrupted and safe operation of the power system. Additionally, they are processed by the Energy Management System (EMS) for system operation, maintenance, planning, and grid development. Typical OT networks consist of devices and components like bay control units, protection relays, Remote Terminal Units (RTUs), station control systems, communication servers, real-time databases, Supervisory Control and Data Acquisition (SCADA) systems, and EMS [1]. A variety of communication protocols are used for power grid communication and automation applications. Most of these protocols are the Transmission Control Protocol/Internet Protocol (TCP/IP), e.g., IEC 61850, IEC 60870-5-104, Modbus/TCP, DNP 3.0, and Ethernet [1], [2].Transmission System Operators (TSOs) and Distribution System Operators (DSOs) use the aforementioned protocols and Information and Communication Technology (ICT) networks for non-operational functions like integrated electricity market, finances, human resources as well as asset and resource management. Figure 1.1 depicts the smart grid, formed by the interconnection of the physical power grid, ICTs, and application services.

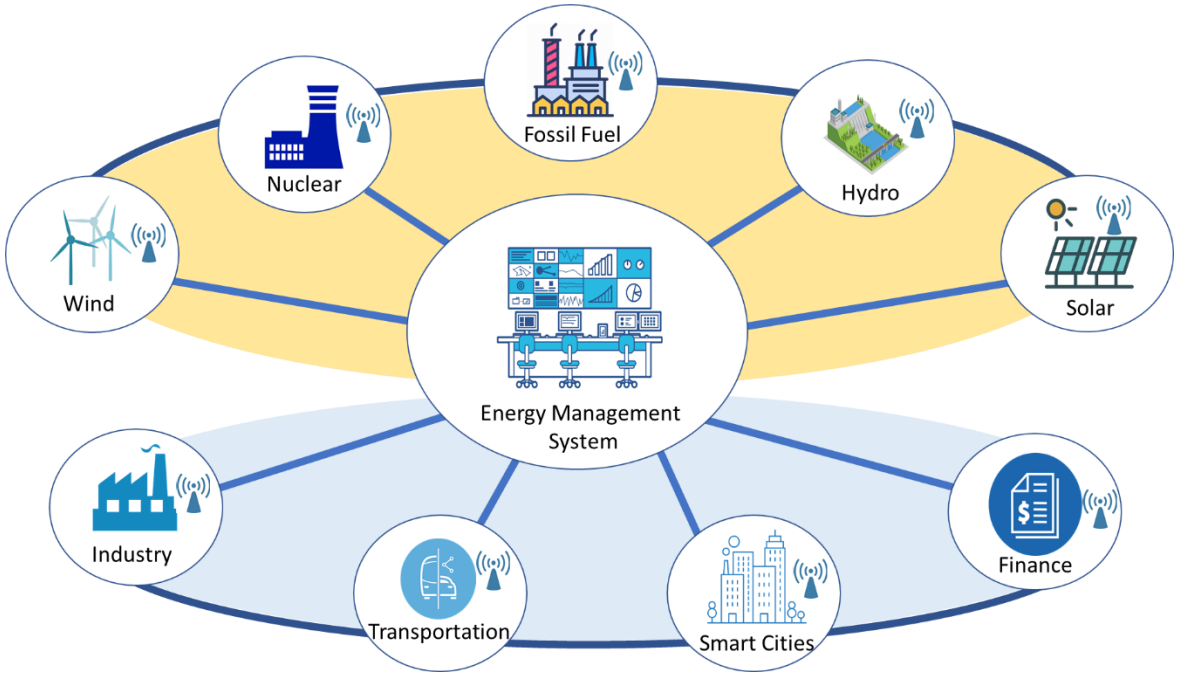


Figure 1.1. The smart grid.

The ICT and OT systems are interconnected and tightly coupled, although segmented as OT networks need to be air-gapped for cyber security reasons. The two communication layers, i.e., ICT and OT

enable the monitoring, control, and data analysis capabilities of the physical power grid. The coupling of these networks with the physical power grid forms an interdependent and complex Cyber-Physical System (CPS). These networks comprising of connected grid edge devices, sensors, ICT-OT and smart applications form the basis of smart grids [1].

In the past, OT systems were confined to select locations such as power plants or substations and were detached from external networks. As a result, the main focus of securing these systems was to strengthen their physical security, as it was the only way for an intruder to gain access. Nowadays, as described above, the utilization of modern networking systems has led to the increasing interdependence between the OT and the ICT environments, making the physical layer of a power grid accessible to cyber threats [1], [3].

1.2. Cyber Security Challenges

In any CPS, *cyber security* is an important and pressing issue for the current and future energy systems. As stated in [1], "*Cyber security is the ensemble of best practices, processes and technologies designed to protect the ICT and OT infrastructures, devices, applications and data from unauthorized access and damage while preserving the confidentiality, integrity and availability of information and services".* Cyber intrusions can cause disruptions in the OT system, which may lead to major power system disturbances; power system controls can be impeded, leading to cascading failures. As a result, catastrophic incidents like blackouts can occur with dire consequences, both operational and societal.

Any CPS is susceptible to cyber attacks, as the OT environment has limited cyber security considerations. Usually, OT security controls inherit the same vulnerabilities like the ones used in the ICT systems. But, the most important issue is that traditional cyber attack mitigation strategies are difficult to be applied to these systems, as their functionality is completely different from ICT networks. OT components and systems are designed to function nearly uninterrupted, for long time periods. Hence, any disruption to any such equipment can affect the normal operation of the physical power system. As a result, a software patch or an update is more difficult to be performed on such devices and system. In contrast to the ICT systems, where high performance is desired, OT system focus on achieving continuity of operations, through high availability and integrity of data [4].

In spite of OT network segmentation, a sophisticated and advanced cyber attacker can gain access to critical OT systems through its interconnection with the ICT systems. Security controls, such as firewalls are vulnerable and their misconfiguration is common. Insider attacks or attacks that originate from trusted sources, can also bypass the most common security practices and mechanisms. Adversaries can also gain access to OT infrastructure via remote access capabilities of OT vendors that utilize the ICT systems through the internet for their tasks, i.e., software updates, technical support etc. [1]. The devices in the OT network can be infected with malware such as viruses, worms, and Trojan horses. This could lead to the disruption of their normal operation, cause damages to the OT infrastructure, and corrupt real-time databases. Furthermore, this could enable cyber attackers to jeopardize the operation of the power grid, by maliciously disconnecting circuit breakers, substations, or even entire power plants. They can also spoof the control settings and fabricate the control setpoints sent to critical equipment, such as transformers and generators. Thereby, cyber attacks can cause equipment damage due to abnormal voltages, excessive torques and lead to the loss of load. Multiple generator and line contingencies, occurring simultaneously could also initiate cascading failures in the power grid, causing a blackout. Such catastrophic events in large, interconnected power systems have severe socioeconomic consequences and are the main topic of research, which this thesis aims to partially address.

1.3. Cyber Attacks on Critical Infrastructures and Power Grids

Major cyber intrusions and attacks have confirmed the importance of cyber security for power grids. The impact of a targeted cyber attack against the control system of an electrical generator was demonstrated by the US Department of Energy's Idaho National Laboratory in March 2007. The 'Aurora' project showed how cyber attacks can physically damage generators [5]. In 2010, Stuxnet was reported as a sophisticated malware that exploited certain vulnerabilities to infect industrial

control systems, spread at high infectious rates, and impacted physical facilities. The main targets were the centrifuges used in nuclear plants for uranium enrichment. Stuxnet targeted the computers that were connected to specific Programmable Logic Controllers (PLC), which were used to monitor and control the physical process of uranium enrichment in centrifuges. However, the infected PLCs were also tricked into reporting to the control center that all processes were normal. Additionally, it used other subsystems of the local network, such as computers and printers, in order to propagate through the entire system, while deleting any traces of its presence [6]. Stuxnet was later modified and infected other industrial control systems worldwide. Such malware can be adapted to target various power plants or control centers directly affecting the security of power grid operation.

The two major incidents relevant to this thesis are the cyber attacks on the power grid in Ukraine in 2015 and 2016. The first occurred on December 23rd 2015. A Ukrainian DSO, reported service outages to customers, occurred due to a targeted cyber attack on the DSO's SCADA systems. Seven 110 kV and twenty-three 35 kV substations were disconnected for three hours. Later, it was found out that three such companies were attacked, resulting in several outages that caused nearly 225,000 customers to lose power across the country. The adversaries intruded into the ICT and OT systems of the three DSOs and shut down power. This operation was performed by using phishing emails, BlackEnergy3 malware, credential theft, network and host discovery, malicious firmware and OT hijack. Furthermore, they modified schedules for uninterruptible power supplies, opened circuit breakers, and used KillDisk for wiping of workstations, servers, and remote terminal units [1], [7], [8]. The cyber attack in 2015 in Ukraine was the first publicly acknowledged cyber incident to directly result in a power outage. In Figure 1.2, the Industrial Control Systems (ICS) Kill Chain mapping chart is presented, based on the analysis conducted in [7].

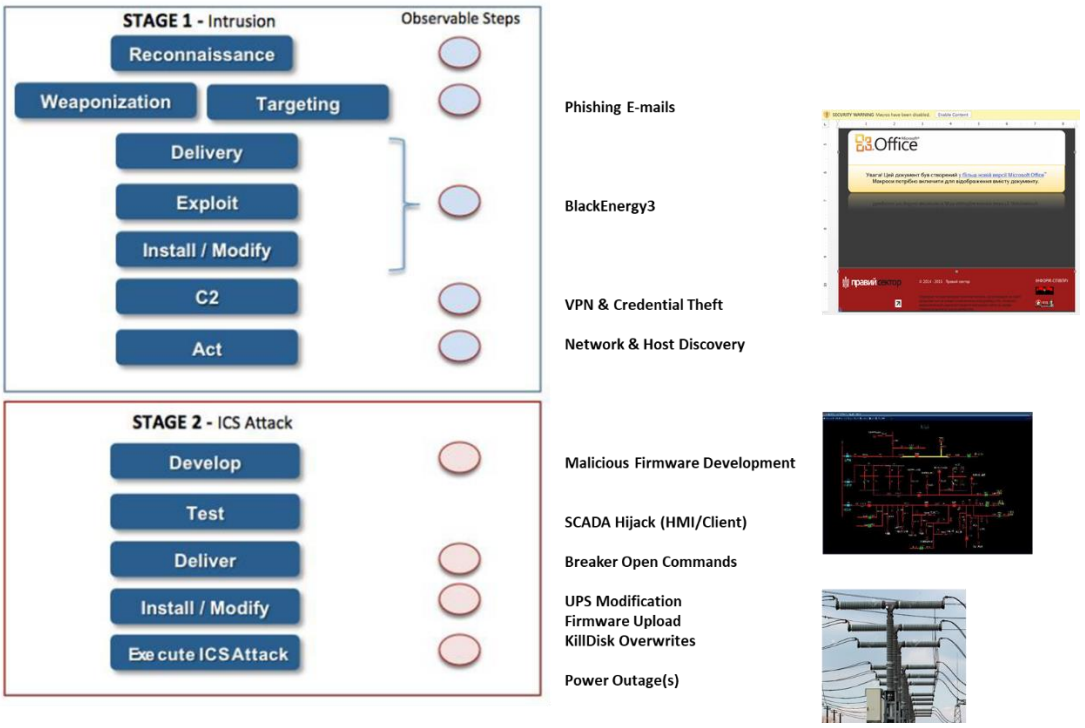


Figure 1.2. Ukraine cyber attack kill chain. Adapted from [7].

The second major attack on power systems in Ukraine, named Industroyer, took place the following year. The cyber attack affected the SCADA system at the transmission level targeting a single 330kV substation. The major difference between the attack occurred in 2015 and this one, is that the latter was fully automated. The attackers infiltrated the substation by exploiting a vulnerability in a specific device. The malware aimed at the industrial hardware of the substation, namely the circuit breakers and protection relays. At a pre-defined moment, the payload of the malware took control over the circuit breakers and protection relays commanding them to open the circuit breaker switches. Additional attacks, initiated at the same time, targeted specific systems and files to prevent recovery

[9]. The attack resulted in a power outage in the distribution network where the total unsupplied load was 200MW [10].

In December 2017, a petrochemical facility in the Middle East initiated a safety system shutdown as the result of a malware attack. The malware, which was named TRITON, was the first to directly interact with the Safety Instrumented Systems (SIS), also known as *industrial safety systems*. SIS are designed to be the last line of automated defense for industrial facilities. Their primary goal is to prevent equipment failures and catastrophic incidents, like explosions or fires. The adversaries penetrated from the ICT network into the OT, through systems that were accessible to both environments [11] [12].

As seen by the incidents above, cyber attacks targeting critical infrastructures such as power grids are a cause for serious concern. Adversaries can exploit the interdependency of the OT and ICT systems, human errors as well as intrusion tools and malware that are available online. The cyber attacks in Ukraine clearly highlighted that power systems are vulnerable to cyber attacks, with alarming consequences. Several reports, either from governmental agencies or independent organizations, have made clear that cyber security for critical infrastructures is of utmost importance. The Canadian Center for Cyber Security in its national threat assessment for 2020, highlighted the increasing number of attacks on ICS in the electricity sector across the globe [13]. The report states that one of the most serious threats for the nation is to be attacked by state-sponsored actors, who are currently developing additional cyber capabilities to disrupt its electricity supply. Additionally, a report by the *Institut français des relations internationales* pinpoints the energy sector as a prime target for cyber attackers [14]. In Figure 1.3 , the timeline of major attacks on the ICS is shown, during the last decade.

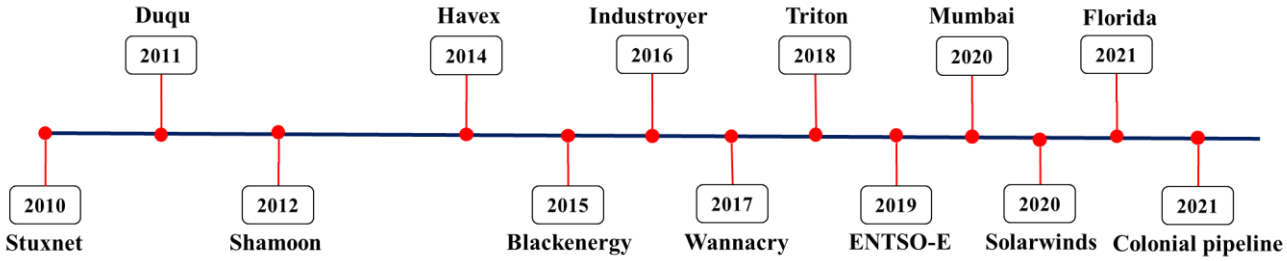


Figure 1.3. Timeline of major cyber attacks on ICS.

1.4. Cyber Security Analysis and Digital Twins

Securing the CPS cannot be achieved by securing individual components of the system. The interdependency between the various vulnerabilities can be used by adversaries, as a part of a cyber intrusion operation. A single stage of an operation could be relatively harmless for the grid or the communications network operation individually, but the combined effects of multiple stages could lead to catastrophic events. As a result, the overall risk assessment of cyber attacks must take into account the vulnerabilities of the examined system as well as their effects on the CPS. The operators of the CPS need to maintain awareness of the situation at all times and to be able to address potential issues. Although timely detection of cyber attacks can speed up the response process, analysis tools for potential threats and risk assessment are extremely important. Hence, the CPS should be examined on its whole, by taking into account the complex interconnectivity of its layers.

The increasing need for digitalization in the modern power grids requires the usage of new technologies that could help the operators and engineers to design, control, and monitor this crucial infrastructure more effectively. These technologies should support the interoperability between different systems and professionals, as the system in question can be regarded as a “system of systems”. A technology that could enable this transition to a digital environment, which also support high levels of automated actions, is the digital twin. Digital twin most commonly refers to a virtual representation of a real-world system, product, process, or another enterprise asset throughout its lifetime [15]. A digital twin model could represent industrial components, power systems or other

critical infrastructures, up to business models, which utilize data analytics to determine present and future behaviors.

Digital twins are an evolution of traditional simulations, as they integrate real-time data. This means that the digital twin is an exact digital replica of the real system, which is fed with the data obtained from its real-world counterpart. It is a powerful tool that can be used throughout the life cycle of an asset (from the design phase to examining preventive maintenance procedures). Simulations are at the core of the digital twin concept. Depending on the use case, digital twins could be used from simple monitoring to managing a fully autonomous system.

This master thesis aims to address this issue, by proposing a method for CPS modelling which can represent the complexity of such infrastructure. This model seeks to be an accurate representation of its real-world counterpart, comprehensively representing each layer and their interconnection. This forms the basis of this thesis project.

1.5. Master Thesis Outline

Chapter 2: State-of-the-art

The state-of-the-art is presented, for various topics such as CPS modelling, risk assessment of cyber attacks on power systems, and attack graphs. The scientific gaps are also identified. The scope of the project and the main research questions are presented. The most important contributions are highlighted, along with a short biography of the author of this thesis.

Chapter 3: Cyber-physical system modelling

The physics-based model for the physical power grid is presented and analyzed. The implementation of the control and protection schemes for the physical power system is presented. Additionally, a method to model the communication network is defined, as well as its topology. Finally, the chapter presents the implementation method for the aforementioned systems along with examined scenarios used for validation.

Chapter 4: Attack graph generation and risk assessment method

In this chapter, the method for developing the attack graph is presented. The assets of the security layer of the modelled ICT/OT infrastructure of the substation are defined. Additionally, the risk assessment equations are presented, both for the physical and the cyber layer.

Chapter 5: Simulation results and discussion

The simulation results for several scenarios are presented and discussed in detail. In this way, it is proven that the designed risk assessment framework is able to identify the impact on the CPS, while important conclusions are drawn regarding the overall risk of cyber attacks on the power grid. Finally, the most important lessons learned from the simulation results are summarized at the end of the chapter.

Chapter 6: Conclusions and recommendations

The conclusions obtained through this study are summarized in this chapter. The research questions of the project are answered, with references to the corresponding chapters that contain more analytical information related to each research question. The challenges of this project are also presented. Finally, the most important topics to be further studied are highlighted and briefly explained, to serve as a guide for the continuation of this project.

2. State-Of-The-Art

2.1. Literature Review

Cyber-physical power systems are large, interconnected networks and their operation is defined by the interdependency of their individual systems. One major drawback of the CPS is that it is vulnerable to cyber attacks, due to flaws in its security design [16]. Critical infrastructures, such as the electrical power grid, are crucial for nation-states and any maliciously induced malfunction could lead to catastrophic damages. In this chapter the reviewed studies in the areas of CPS modelling, impact analysis of cyber attacks and risk assessment are presented and discussed.

2.1.1. Modelling methods for cyber-physical power systems

A literature survey presented in [16], broadly categorized the methods of modelling a CPS into three main categories; *interconnection*, *interaction*, and *interdependent modelling.* Interconnection modelling methods examine the behavior of each layer of the CPS separately, based on their operating principles and an interface is built to correlate their behavior based on signal conversion.

Interaction modelling methods seek to model the effect that each layer has to the others. A way to model this interaction can be achieved through graph theory. The physical power system, consisting of generators, loads, circuit breakers, transformers, transmission lines, and various other components, is connected with the cyber components through communication networks. The studies assume that each physical component is integrated with its cyber counterpart. The latter transmits the associated information to the control center and receive commands, by using routers and switches.

The interdependent modelling is focused on describing the interface relationship between the cyber and physical devices, which changes over time. In this method, the CPS is divided into a three-layer structure, namely the physical, the cyber, and the interface layer. Two types of interdependencies are specified; the one-to-one and the one-to-multiple. In one-to-one, each physical node is monitored and controlled by a single cyber node, while the distributed cyber nodes send the information to the control center. In the one-to-multiple approach, each physical node is monitored by more than one cyber node.

In [17], a method of modelling and simulating the SCADA system of an integrated CPS is proposed. On one hand, the physical system is modelled through static and dynamic modelling of its components. The modelled grid was divided into substations, creating areas of control within a system. Each bus of the physical grid has a substation bay, where the sampling of the continuous-time electrical parameters can be performed. On the other hand, the cyber system is modelled in order to incorporate the SCADA functionalities for real-time communication between the OT environment and the power system. The capabilities of the ICT network include the gathering of measurements and breaker status, WAN communication, and remote control of breakers and Intelligent Electronic Devices (IED) from the OT environment. The ICT devices were modelled using queuing theory and the main focus of this study was to model the communication time delays of the SCADA system.

Complex network theory is used to model CPS, as it is presented in [18]. The authors represented the CPS topology using graph theory and defined a series of indexes for the topological representation of the power network, such as geodesic distance, network connectivity, and geodesic strength. By using a severity index based on loss of load, a risk assessment method is also proposed in order to measure the cascading failures after a disturbance. Another research, presented in [19], focused on the optimization of the communication routing to enhance power system security. The method that is proposed assigns the most reliable communication lines to the most important information of the power system. This optimization method is dynamic, re-scheduling the communication routings considering the cyber-physical interdependence.

2.1.2. Impact of cyber attacks on power grids

In [20], the impact of cyber events is examined in a modelled CPS testbed, which composed of four layers; power system, sensors, control, communication, and application. The power system layer and the associated controls are modelled using Real-Time Digital Simulator (RTDS). Hardware equipment is integrated into the testbed to simulate the sensor layer. A network simulator is used to model the communication layer and is designed based on real-world counterparts. The network simulation handles the data transfer between the control center and substations in real-time. The application layer contains power engineering applications that are used for the analysis of the results as well as to perform various control operations. The Institute of Electrical and Electronics Engineers (IEEE) 14-bus benchmark system was utilized to analyze the dynamic behavior of the system. The type of attacks examined were Denial-of-Service (DoS) and Man-in-the-Middle (MitM). Additionally, induced communication failures were simulated to study the effects on the power grid. Finally, the authors highlighted the importance of a real-time, end-to-end comprehensive system model for analyzing the impact of cyber attacks on the power grid dynamics.

In [21], the impact of cyber attacks on the automation and protection system of a power grid is assessed. By targeting the data frames of Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV) protocols of IEC 61850, the attackers are capable of launching a spoofing attack on the IEDs. The results indicate that cascading failures can be caused by MitM attacks on the protection and control systems of the power system.

The impact of cyber attacks on the reliability of power systems is examined in [22], emphasizing on the cyber security of the SCADA system. In this study, the authors extended a Time-To-Compromise (TTC) model, in order to estimate the time intervals for successfully intruding cyber components of control systems. To test this model, the authors conducted Monte Carlo simulations where breakers in the substations are randomly tripped, simulating false commands that are sent to compromised cyber components. To determine the possible attack paths, two Bayesian Networks (BN) models are used to define all possible attack steps in the network. The first network is designed to find the attack steps in the Local Area Network (LAN) of the control center and to estimate the probabilities of vulnerabilities exploitation. That could enable the attacker to gain the root privileges of control components. The second attack graph model is created to calculate the probability of successful attacks on the communication links between the control center and substations. Furthermore, the Common Vulnerability Scoring System (CVSS) is utilized for scoring the vulnerabilities and their relative severity in the networks. In this particular study, the scores were assigned randomly. Different levels of expertise were assigned to the cyber-intruders, and they were applied in the TTC equations.

Finally, in [23] the authors proposed an approach of CPS modelling, based on the Markov model. The goal of this approach is to model the interactions between the various layers of the complex system. Random contingencies and variations of operating conditions are used as inputs in a Monte Carlo simulation, to quantify the impact on the modelled CPS. The main finding of this paper is that the impact on the physical system does not always correlate with the severity of cyber attacks.

2.1.3. Attack graphs

An attack graph represents the behavior of attackers in a specified network. It provides a way to visualize the different attack paths, which the attackers may use to reach their targets, by exploiting various vulnerabilities present in the targeted system. They are extremely important tools as the behavior of an attacker can be visualized. Researchers have utilized attack graphs to examine the possible attack paths, by examining the interdependency of the identified vulnerabilities [17], [22].

The main advantage of an attack graph is that the generated attack paths from the examined scenarios can be used to identify the potential weak points of the examined system. Network designers and security experts can be aided as prevention strategies can be applied to these specific assets, thus improving the overall security of the system. Attack graphs are also being used in risk analysis studies, and can be an extremely valuable tool for applications like intrusion detection, security defense, vulnerability assessment, etc. When applied to a CPS, a holistic view of the security infrastructure can be provided, helping the operators identify the potential risks.

Attack graphs have different connection models, i.e., serial, parallel and series-parallel complex models [16], as shown in Figure 2.1. The attack path of an attack graph is identified as the series of all attack steps that an attacker would take to compromise the selected target. An attack path is formulated by examining all the possible attack steps from an entry point to the end target, and taking into account the weights associated with each edge of the graph. Attack graphs can be used to identify these different attack paths, as well as to determine the dominant ones. These attack paths are determined by a probabilistic analysis, which considers the weights of the connecting edges between the attack steps. These weights can be probabilities of compromise or other metrics, such as the expected TTC.

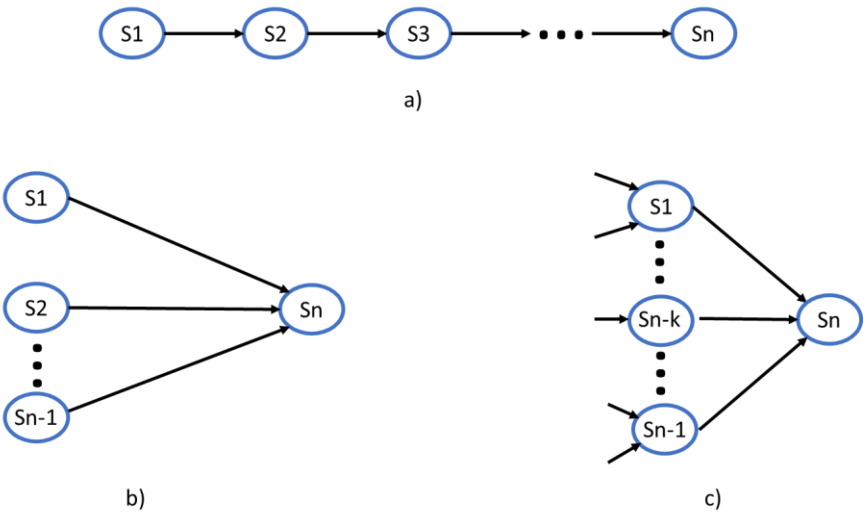


Figure 2.1. a) Serial, b) parallel and c) complex attack graph connection models.

The complexity of the ICT/OT domain of the digital substations of a modern power system means that many attack graph generators, that are developed exclusively for ICT, cannot be used for modelling an OT infrastructure.

In [24], the authors reviewed the existing schemes in attack graph modelling for CPS. Different tools for generating attack graphs can be used. In [25], the authors introduced a probabilistic threat modelling approach for automatic attack graph generation based on network modelling. This model automatically generates probability distributions over TTC for each asset of the system. In [26], the proposed modelling considers the physical network topology, the supported short-range communication protocols, and the industrial communication architecture. The main issue in this research, is that the applied framework needs to be expanded. Finally, in [27] a technique is introduced to explore the cyber security defense strategies based on contingency rankings in power systems. The study also proposed a technique that evaluates the most critical cyber security mechanisms to protect the power grid.

2.1.4. Risk assessment of cyber attacks on power grids

Cyber security for critical infrastructures, such as power grids, is based on risk assessment. The identification of cyber-related risks and critical assets is vital in the security analysis of such incidents. Researchers proposed various frameworks and methodologies for risk assessment. In [28] and [29], the authors proposed a method for identifying the most vulnerable parts of a power system. The proposed scheme first identifies its most critical substations. Traditional N-1 contingency analysis for power grids is combined with analytical hierarchical process. The business model includes the missions of the particular network and establish a relationship between each node of the network, while a risk model assesses the vulnerabilities. The authors used questionnaires to assess the importance of each of the business mission components and to create the vulnerability index. By overlaying these data, namely substation vulnerability index and the substations relative weights for

grid stability, the associated risk index could be formulated. After the critical substations of the network are identified, an analysis is performed on the devices and connections that are present inside a substation. The main inputs for this analysis are the substation layout, the system configuration, as well as costs and security vulnerabilities, which were also assessed through questionnaires. It is important to highlight that the costs considered were the cost of power loss, cost of recovery and cost of a cascade. By constructing the attack graph of the substation's network, the attack paths, vulnerability indices and the associated risk index for the substation's equipment can be defined. The output of this framework is the risk index where the vulnerability indices, as well as the impact severity for each substation, is assessed.

In [30], the authors suggested a method of implementing the interdependency of the vulnerabilities in the risk assessment for a CPS. Two indices, namely the successful-attack-probability index and the attack-impact index, were created based on the vulnerability dependency graph. This graph is a net, in which the nodes are vulnerabilities and the edges represent one-way dependencies between vulnerabilities. The successful-attack probability is not only determined by the characteristics of the examined node, but also by the probability of its source vulnerability. The attack-impact index is calculated by taking into account both the qualitative impact on the physical and the cyber layer of the infrastructure. Factors as economic losses, casualties, environmental damage and repair costs were considered.

These implications on the physical infrastructure were also studied by the authors in [31]. The proposed method involves probabilistic models for the attack planning and execution phases. The examined attacks are split into the preparation and execution stage. The first stage is related to information gathering, where the attacker is assumed able to acquire all the necessary information to launch an attack on the system. In the execution stage the attackers can access the substations, and by disabling their communications, to cause physical damage to the power grid. To study the effects on the physical system, the authors performed a power flow analysis on the examined system. Their main focus was the number of loads that could not be satisfied, as a result of the intrusion. In this study, a hybrid attack model was simulated, combining the Markov model and the probabilistic learning-attacker, dynamic-defender model. The probability of a successful attack is calculated by dividing the number of days that the attacker can open breakers, divided by the number of days in the simulation. The overall risk is calculated by multiplying the probability of a successful attack with the percentage of power that is lost.

2.2. Research Gaps

The complete CPS infrastructure must be modelled to address the challenges imposed on the modern power grids by the increasing need for digitalization. Threats such as cyber attacks must be studied in a comprehensive model, that includes both the physical and cyber layers of the infrastructure. To evaluate the effects of such an incident on the power grid, detailed dynamic models of the physical infrastructure and its communication network are needed. Most of the reviewed studies simulated the effects of cyber attacks on power grids using steady-state models. To capture the cascading failures and to perform a detailed analysis, dynamic models with implemented protection schemes are needed.

An additional research gap identified is that in many cases the authors based their analysis on randomly created events. In the reviewed literature, the impact of cyber attacks on power systems is based on a probabilistic approach. Randomly generated events, such as the opening of circuit breakers and disconnection of generating units, are used to imitate cyber attacks on power grids. On one hand, this analysis can be used to determine the worst-case scenarios and show the effects of cyber attacks on power systems. However, these events cannot capture the effort required by the attacker to compromise these systems and initiate the cyber attack. Furthermore, various assumptions and simplifications are typically used that greatly neglect the complexity of such integrated cyber-physical systems, e.g., not taking into account the likelihood of an intrusion to commence or not examining how an attacker can compromise the targeted systems.

Another gap that was identified in the reviewed studies is the lack of a dynamic CPS models for power grids, that use attack graphs or vulnerability analysis to examine the success rate and the impact of

various attack scenarios. Previous studies focused mostly on the completion of a holistic model for CPS. The use of attack graphs is crucial to this end, as the topology of its communication system, its vulnerabilities and the importance of each asset can be defined. Additionally, important metrics such as the probability of compromise and TTC can be extracted from this analysis and used to calculate the overall risks.

Some studies also performed risk analysis by utilizing hypothetical and, in some cases extravagant scoring. Assessing metrics such as casualties and environmental damage are extremely important in a general risk assessment for critical infrastructures but it is no longer a risk assessment related to cyber security, especially if these metrics are combined with the likelihood of a cyber attack. Regarding the risk assessment for cyber attacks, studies considered the TTC needed by the attacker to perform the attack. An identified gap is that the reviewed studies did not consider the time needed for the system to be restored. This can be crucial for risk assessment, as the restoration time is an important metric to evaluate the reliability of the system.

Finally, most of the reviewed research did not examine the time-varying nature of a CPS. The impact on the physical infrastructure as well as the likelihood of such attacks are some of the aspects needed for a comprehensive risk assessment. On one hand, the identification of critical systems or components of the CPS is vital for conducting the risk assessment. On the other, the time-varying nature of the CPS means that these critical assets can vary, depending on the operating conditions, planned and unplanned maintenance procedures, time, etc.

2.3. Affected Parties

The aforementioned gaps affect both academia and industry. As the threat and potential impact of cyber attacks is expected to increase, CPS modelling is crucial as it provides a testbed for impact analysis and testing mitigation strategies. Industrial entities such as TSOs and DSOs are also affected by the lack of a complete framework for cyber security analysis on the power grid. On one hand, security specialists of such entities are mostly focused on the ICT network, as the majority of the incidents take place there. On the other hand, the catastrophic consequences of an attack that successfully jeopardize the operation of the grid, are too severe to be neglected.

Additionally, engineers and system operators are unable to perform actions that could effectively protect the power system from such threats, as shown in the Ukraine incident. New technologies such as digital twins are expected to increase the collaboration between professionals, as this digital representation of the actual system can be used for the monitoring of the real-world system, planning of mitigation strategies as well as for the testing of these strategies in the digital counterpart of the actual system. This thesis project seeks to partially address this complex issue, by proposing a method for modelling a holistic CPS, as well as defining a method for quantitative risk assessment.

2.4. Project Scope & Research Questions

Based on the problem definition, state-of-the-art of the CPS and cyber security analysis for power systems, as well as on the identified gaps in the reviewed literature, the scope of the work has been defined and is explored through the study of four research questions.

The first goal of this project constitutes the study of *how to create a complete CPS model of a power grid*. To create a unified CPS system, both the physical and cyber layers of the power grid must be modelled and simulated using co-simulation methods. The integrated CPS can be used for studying the cascading failure chains that can occur on the physical power system subject to a cyber attack, as well as the effects on its communication infrastructure. The second goal is to develop *a method for quantitative risk assessment of cyber attacks using attack graphs*. The attack graph will enable us to perform vulnerability assessment on the cyber layer of the CPS, based on known vulnerabilities, as well as to represent cyber attacks that could enable a threat actor to compromise selected targets. An important metric that can be extracted from this analysis is the TTC. Additionally, by simulating these cyber attacks on the physical layer of the CPS, the Key Performance Indicators (KPI) for the power grid operation are calculated. Additionally, a metric to evaluate the restoration effort required for the power system to be restored is proposed.

Four research questions have been formulated to address these goals:

1. *How to model a cyber-physical system, to be able to*
    - *simulate the dynamic response of the physical power system?*
    - *analyze cascading failures caused by cyber attacks on power system communications?*
2. *How to model the attack graph of a digital substation, and how it can be used for vulnerability analysis?*
3. *How to assess the impact on the cyber-physical system operation, for a given cyber attack scenario?*
4. *How to calculate the risk of a cyber attack scenario, based on the security analysis and the associated impact on the cyber-physical system?*

2.5. Thesis Contributions

The contributions of this project, compared to the available literature, are summarized, to highlight the importance of this study:

- A method to model a complete, integrated CPS, by modelling both the physical power system and its communication network. The power grids' sub-systems and functions, such as control and protection mechanisms are implemented. For the communication system, the substation level OT infrastructure is modelled as well as its connection to the control center. The modelled CPS can simulate the operation of its real-world counterpart.
- The substation OT infrastructure is modelled for cyber security studies, by utilizing attack graphs. The interdependencies of the system are analyzed, and associated vulnerabilities of the cyber-physical system are used to generate the attack paths and associated metrics, i.e., TTC. A method to identify the probability distributions of the TTC for each attack step is proposed.
- A quantitative risk assessment methodology for the complete CPS is devised. The impact of cyber attacks on CPS is determined by examining the effects of an attack scenario on both of its CPS layers. The likelihood of a successful attack is determined by the TTC metric, which is defined by the security analysis.

2.6. Author's Background

The author of this report is pursuing his Master's degree in Electrical Power Engineering at the Delft University of Technology. In his previous studies, he obtained the Diploma in Electrical & Computer Engineering at the Democritus University of Thrace, in Greece. He is specialized in Energy systems, emphasizing in Smart Grids. Additionally, the author worked on the power generation industry in Greece. During his studies at TU Delft, he developed a keen interest in the study of cyber security for power grids. He further researched cyber security in a three-month internship in Netherlands Organization for Applied Scientific Research (TNO), where he was able to propose a framework for cyber security analysis for critical infrastructures, utilizing digital twins and attack graphs. For the completion of this thesis project, the author collaborated with the Cyber Resilient Power Grids research group at Delft University of Technology.

3. Cyber-Physical System Modelling

The physical layer comprises of the power grid and its associated control and protection systems. Power grids are complex systems, covering massive areas, and spanning hundreds of kilometers. On top of this physical infrastructure resides the cyber layer, which is responsible for handling the flow of data. This layer is crucial to achieving the desired observability and control. An overview of each system, along with their characteristics of their interconnection will be presented. In the following sections, these two layers will be presented. Their functions will be explained, along with a way to model them. Finally, the implementation method that is followed in this thesis project will also be presented.

3.1. Power System Modelling

Electrical power systems vary in size and structural components. However, some common characteristics can be defined in all these systems [32]:

- Three-phase Alternating Current (AC) systems are by far the most common way to transmit power from generation to demand. Generation and transmission systems are mostly comprised of three-phase equipment. These systems are operating at a constant voltage. Direct Current (DC) systems are also developed, especially during the last decade as they can be used to transmit power over longer distances than AC systems [32].
- Loads can be categorized as industrial, commercial and residential. They are distributed equally among the phases so that they can form a balanced three-phase system.
- Synchronous machines are used for electricity generation. Primary sources of energy are converted to mechanical energy, with the use of prime movers, and later converted to electrical energy by synchronous generators. Other ways of energy production use different technologies, like asynchronous machines on wind turbines.
- Significant distances have to be covered for the produced energy to reach consumers. This requires the transmission grid and its associated sub-systems to operate in different voltage levels.

The transmission system interconnects all major generating stations with the main loads in a system, and it forms the backbone of an integrated power system. Usually, it is a nationwide grid and by interconnections with other national grids, vast networks are created. Such an example is the synchronous grid of continental Europe, which can be seen in Figure 3.1. This vast grid is operating under steady frequency and supplies over 400 million customers. A properly designed and operated power system should follow the following requirements:

- Must be able to meet the constantly changing load demand for active and reactive power, as electricity cannot be stored in sufficient quantities,
- Supply energy at minimum cost and with minimum ecological impact, and
- Meet certain standards, that determine the quality of supplied power, namely constant frequency, constant voltage and an acceptable level of reliability.

In this project, a transmission grid is modelled to act as the physical layer of CPS. In the following sections, the method to solve the power flow for such networks is presented, along with an overview of their subsystems.

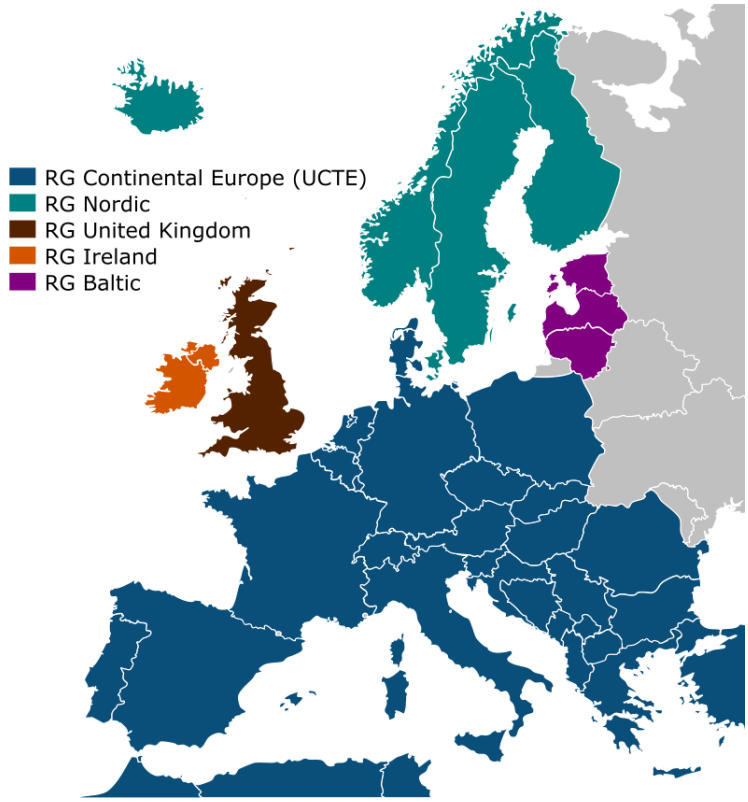


Figure 3.1. Map of European transmission system operators. Adapted from [33].

3.1.1. Mathematical formulation

Graph theory can be used to describe the electrical power grid. A simple way to visualize the power grid is by considering a selection of nodes, which represent substations and connecting edges, representing power lines such as overhead lines and underground cables [34]. By using this representation, the generating power can be supplied to the system and divided over the connected lines. Transformers are installed in the substations to convert between different voltage levels. Substations consist of many ingoing and outgoing power carriers that are connected to busbars by circuit breakers, disconnectors, and instrument transformers. Each substation has control of a specific area, and the operational status of the grid is monitored through its OT and ICT equipment. The substations are represented using the node-breaker model, which includes circuit breakers, protection relays, and measurement transformers. Such a representation can be seen in Figure 3.2, where an examined power grid is shown using graph theory.

Power grids need to be monitored and controlled constantly. To model this characteristic, it is necessary to implement state and control variables in the power system modelling. These variables are defined for each substation, to enable the observability and controllability of the system. Measurements of active power, reactive power, voltages and currents, along with control variables such as active power and voltage setpoints, breaker status etc., need to be constantly monitored by the implemented protection equipment and the grid operators.

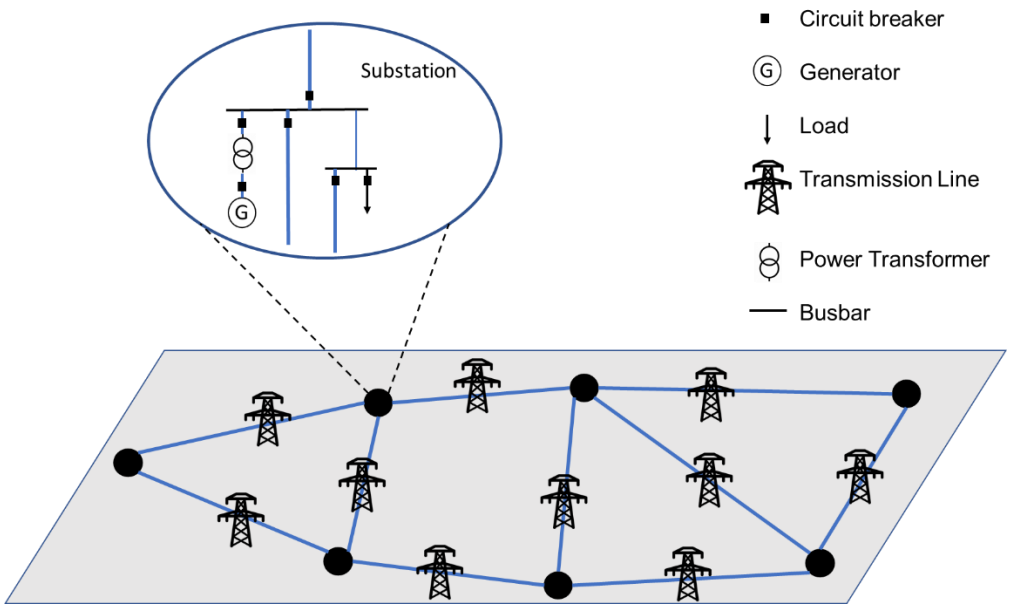


Figure 3.2. Depiction of the power grid, using graph theory.

The method for modelling the physical power system and its connection with the cyber layer is based on [17]. Sampling points are defined, which are the same throughout all layers and components of the model. At a sampling point s, the time of writing/reading values to/from ICT devices is defined as $t_s = t_{s-1} + \Delta t$, where t_s is the sampling time and Δt is the sampling interval that is defined by the user.

The operation of the examined power system is simulated either by power flow or by time-domain simulations. Power flow is an iterative procedure used to determine the flows of power in the network. To perform the power flow calculation a) the nodal power injections, b) the bus voltage magnitude and phase angles, and c) the topology of the system is needed. Power flow simulation defines the following quantities for every node i in a network:

1. Active power: P_i,
2. Reactive power: Q_i,
3. Voltage phasor amplitude: U_i
4. Voltage phasor angle: δ_i

To solve the power flow, the set of non-linear equations for each sampling point s is formulated as:

$$h\left(X_S^{(s)}\right) = 0 \tag{3.1}$$

where the state variables vector and the vector of control variables are:

$$X_S = \left[\theta^{PV+PQ}, U^{PQ}, Q_G^{PV+EQ}, P_G^{EQ}\right]^T \tag{3.2}$$

$$X_C = \left[P_G^{PV}, U^{PV}, n_T, n_B\right]^T \tag{3.3}$$

Equation 3.2 includes the voltage angles for all PV and PQ buses, voltage magnitudes for PQ buses, generated reactive power at PV buses and the slack bus EQ, as well as the active power at the slack bus. Equation 3.3 includes the setpoints for generated active powers and voltage magnitudes at the PV buses, as well as circuit breaker status indicators n_B and transformer tap positions n_T. In the examined model no shunt devices are modelled. To solve the power flow, the method that is applied is the Newton-Raphson algorithm [35]. The static data of the power grid model is specified as the initial control variables $X_C^{(0)}$. The initial results of the state variables $X_S^{(0)}$ are calculated by solving the

power flow and they are written in the ICT/OT devices. If the control variables at the current point s are different from the previous ones, a new power flow calculation is conducted to find $X_S^{(s)}$. Time-domain simulations are characterized by a set of differential-algebraic equations, such as [17]:

$$\begin{cases} \dot{x} = f\left(x, y, \mu^{(s)}\right) \\ 0 = g\left(x, y, \mu^{(s)}\right) \end{cases} \tag{3.4}$$

where f and g are the differential and algebraic equations, respectively. The vectors of these equations are (a) the dynamic state variables x, e.g., rotor angles, angular speeds etc., (b) the algebraic state variables y, such as voltage magnitudes, phasor angles, stator currents etc., and (c) the parameters μ, such as generator set points P_G^{PV} and U^{PV}, active and reactive power consumption, circuit breaker status indicators, transformers tap positions etc. The vectors of state and control variables in the time domain simulations are given by:

$$X_S = [x, y]^T \tag{3.5}$$

$$X_C = \left[\mu^{(s)}\right]^T = \left[P_G^{PV}, U^{PV}, n_T, n_B, P_C^{PQ}, Q_C^{PQ}\right]^T \tag{3.6}$$

Time-domain simulations computations begin by solving the differential-algebraic equations, from which the state variables can be obtained. To perform time-domain simulations, the power flow equations are used to generate the initial conditions of the system, at $t = t_0$ for a specified set of parameters μ_0 as given by:

$$\begin{cases} 0 = f(x, y, \mu_0) \\ 0 = g(x, y, \mu_0) \end{cases} \tag{3.7}$$

At $t_{n+1} = t_n + \Delta t$, where $n + 1$ is the new state, and n is the current state respectively, the dynamic state variables are given by the following equation:

$$x_{n+1} = x_n + \int t_n * t_{n-1} * f(x, \tau) d\tau \tag{3.8}$$

The trapezoidal rule can be applied to Equation 3.8:

$$x_{n+1} = x_n + \frac{\Delta t}{2} * [f(x_n, t_n) + f(x_{n+1}, t_{n+1})] \tag{3.9}$$

This process is repeated at each time step of the simulation until the simulation is finished. The interaction between the physical and the cyber layer of the CPS proceeds as follows. At each sampling point, the parameters vector is read from the cyber layer, at t_s. Any change detected from a previous reading, means that the operator has sent control signals which are incorporated in the simulation. The new values of the state variables are reported to the cyber layer only when a change occurs. Additionally, any change occurring in the physical layer that is a result of physical events updates the state variables vector in the cyber layer. The corresponding state variables $X_S^{(s)}$ are calculated using Equation 3.4 and the possible results are summarized below:

$$X_S^{(s)} = \begin{cases} [x, y]^T, & \mu^{(s)} \neq \mu^{(s-1)} \\ [x, y]^T, & \mu^{(s)} = \mu^{(s-1)}, \quad X_S^{(s)} \neq X_S^{(s-1)} \\ X_S^{(s-1)}, & \mu^{(s)} = \mu^{(s-1)} \end{cases} \tag{3.10}$$

As long as $X_S^{(s)} \neq X_S^{(s-1)}$, the measurements and status data from the state variables are transmitted through the cyber layer. The updated state variables are reported and the sampling point is advanced.

3.1.2. Overview of control systems

Electrical power systems are one of the most complex system ever designed, constructed and operated by humanity. For the requirements presented above to be satisfied, control actions should be implemented, to successfully transfer electrical power to consumers, taking into consideration the operational margins. Following certain approximations presented in [34], the active and reactive power equations can be rewritten in the following form:

$$P = Re(S) = \frac{|V_i||V_j|}{X}\sin(\delta_i - \delta_j) = \frac{|V_i||V_j|}{X}(\delta_i - \delta_j) \tag{3.11}$$

$$Q = Im(S) = \frac{|V_i||V_j|}{X}\cos(\delta_i - \delta_j) - \frac{|V_j|^2}{X} = \frac{|V_j|}{X}(|V_i| - |V_j|) \tag{3.12}$$

As it is shown in the equations above, during the steady-state operation of the power grid, the active power and reactive power control are approximately independent of each other. Additionally, as it can be seen in the equations above the voltage depends on the reactive power and the active power depends on the sine of load angle. This fact is crucial for the control of the power system, as the systems that will be presented, are used to control the active and reactive power output of the generating units, to control the power grid. In the following paragraphs, the control schemes that were considered for this project will be presented.

The active power in traditional power grids, and as a result the frequency of the system, is controlled by dedicated control units that change the outputs of generating units. The frequency of the system should remain nearly constant, for the operation of the power system to be considered satisfactory. A difference between the active power that is generated and the one consumed change the kinetic energy of the generators, which alters the system frequency. To restore the active power balance, speed governors are used. This control system is used for *primary control* of the frequency. This control scheme dictates that the speed governor of each power generating unit of the power grid, such as a synchronous machine, provides the primary speed control function. The basic principle of the speed governor control system of a generating unit is depicted in Figure 3.3.

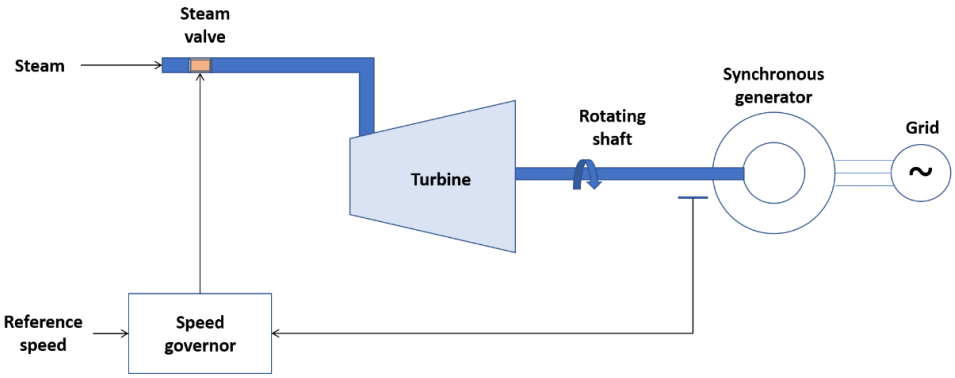


Figure 3.3. Diagram of the primary speed control, for a steam generator. Adapted from [30].

The frequency can be regarded as a global variable of the system. In an interconnected system, the frequency has the same value everywhere, independent of the location. The same principle cannot be applied to voltage, as its amplitude depends on the busbar location. As a result, voltages on the system can only be controlled locally. A system that can be used to control the voltage is the Automatic Voltage Regulator (AVR), which forms the basis of the generator reactive power control. Its operation is depicted in the diagram shown in Figure 3.4. AVRs are used to control the voltage of the synchronous machine and to ensure that every change in the terminal voltage of a generator will be corrected by the excitation system.

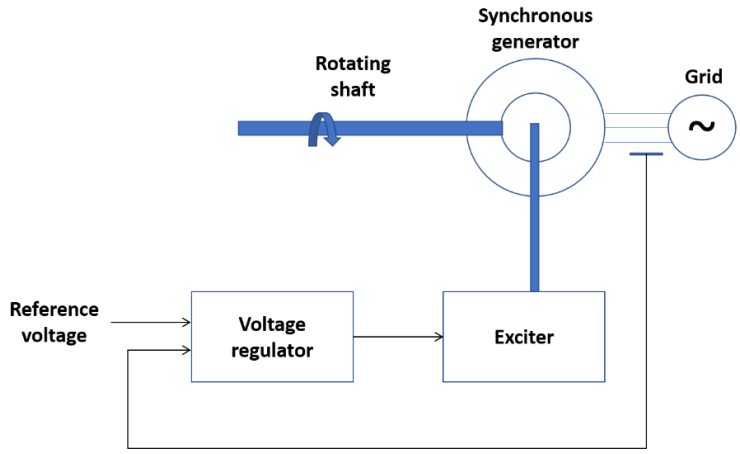


Figure 3.4. Diagram of the AVR. Adapted from [30].

Finally, another category of a system that is implemented for voltage control is the tap-changing transformer. Tap-changing mechanisms are used to adjust the ratio of the transformer windings. This control scheme is used to change the voltage level at the high-voltage terminals of the transformer, providing a way to control the terminal voltage at the transformer position.

The control systems are in charge of correcting the operation of the power system after any disturbance and fault while keeping its functionality at the predefined margins of operation. Their setpoints can be adjusted by operators, or they can be a subject of malicious attacks. The setpoints and their state of operation can be monitored through the ICT layer, as described in Section 3.1.1.

3.2. Power System Protection

Faults will always occur on a power system, no matter how well it is designed, and pose a significant danger both for the reliability as well as for the security requirements [36]. As such, their prompt and reliable operation are of great importance for the design and operation of the power system. The objective of the protection devices is to keep the power system stable by isolating its faulted areas while securing the normal operation for the rest of the system. Protection devices are installed throughout power systems, and their design and configuration are determined by the corresponding protection scheme. Protection schemes are based on multipurpose IEDs. A single IED can support functions that previously were supported by multiple conventional devices, thus reducing the needed number of devices and the needed interconnections between them [37]. These devices have protection functions, are capable of communicating with control centers, can perform control actions as well as log data from system events. Protection systems are usually comprised of the following components:

- Measurement transformers, such as current and voltage transformers. These transformers are used to step down the high voltages and currents of the electrical power system to levels that are convenient for the relays to operate with.
- Protection relays, programmed with specific thresholds and operating time, within the required fault-clearing time. Multiple protection functions can be implemented in a single device [21].
- Circuit breakers, that open/close based on the signal from the protection relay.
- Communication channels for remote monitoring of the measured values, and remote tripping of equipment.

A power system is operating with a variety of implemented protection schemes in order to satisfy the aforementioned requirements of the operation. Each protection scheme safeguards a defined area, which is known as a protection zone. This area can range from a single component of the grid, like a generator, transformer or motor, to a whole substation. These protection schemes require a level of coordination, to satisfy the selectivity of the protection equipment.

In this thesis project, the protection schemes that were implemented are summarized in Table 1. The author's main contribution was mainly in the design of the Rate of Change of Frequency (ROCOF), over/under frequency, distance, and overload protection schemes, as is highlighted in bold in Table 1. To choose appropriate security margins, operating conditions, and operating times, both academic and industrial literature sources were used, as will be explained in the following sections.

Table 1. Overview of the implemented protection schemes.

Protection Scheme	Applied on
Over/Under Frequency	Generators
Over/Under Voltage	Generators
Rate of Change of Frequency (ROCOF)	Generators
Over-flux	Generators
Pole-slip (out of step)	Generators
Under Frequency Load Shedding	Loads
Under Voltage Load Shedding	Loads
Distance	Lines
Overload	Lines

3.2.1. Frequency protection for generators

The frequency protection scheme is applied to the generating units in this thesis. As the system needs to have a stable frequency, the main functionality of this protection is to disconnect generating units, if they violate the specified limits. Synchronous generators are designed to operate at a nominal frequency and any deviation could cause damage to these machines.

Table 2. Frequency range requirements for European countries. Adapted from [38].

Frequency (Hz)	Minimum Time Delay				
	Denmark	Germany	Ireland	Scotland	UK
52.0 - 53.0	3 min	0	0	0	0
51.5 - 52.0	30 min	0	60 min	Continuous Operation	Continuous Operation
51.0 - 51.5	30 min	Continuous Operation	60 min	Continuous Operation	Continuous Operation
50.5 - 51.0	30 min	Continuous Operation	60 min	Continuous Operation	Continuous Operation
49.5 - 50.5	Continuous Operation	Continuous Operation	Continuous Operation	Continuous Operation	Continuous Operation
47.5 - 49.5	30 min	Continuous Operation	60 min	Continuous Operation	Continuous Operation
47.0 - 47.5	3 min	0	20 sec	20 sec	20 sec
< 47.0	0	0	20 sec	20 sec	20 sec

The frequency range for transmission grid operators are different and they are varying, depending on each country. In Table 2**,** a study presented in [38] investigated the frequency range requirements for different European countries, based on their grid codes. The frequency protection settings were selected based on the IEEE guide for AC generation protection [39]. The specified time settings were set based on the 60 Hz applications. The over/under frequency setting for the generating units of the modelled system are presented in Table 3.

Table 3. Over/under frequency protection settings.

Over frequency Threshold (Hz)	Time Setting (s)
> 61.8	5
> 61.0	100
> 60.6	600
Under frequency Threshold (Hz)	
< 58.4	90
< 57.7	30
< 57.1	0.167 (10 cycles)

3.2.2. Rate of change of frequency protection

In general, ROCOF protection examines the frequency of voltage, and it is comparing it over time to derive an estimate of its change. It is based on the basic principle of power grids, which mandates a match between load and generation. If the system becomes unbalanced, either by excess generation or shortfall, the frequency will deviate from its nominal operating value. For a synchronous generator, the per unit formulation for ROCOF is given below [40]:

$$ROCOF = \frac{df(t)}{dt} = \frac{\frac{\Delta P(t)}{S_{B-i}}}{2H_i} \mathrm{f}_0 \tag{3.13}$$

where $\Delta P(t)$ is the change of the active power in MW, f_0 is the nominal frequency of the system, H_i is the inertia constant of the generator in seconds, and S_{B-i} is the nominal apparent power of the generator in MVA. The subscript i denotes the i-th generator among n generators in the system. Similar to the frequency protection discussed above, each country has different specifications for ROCOF protection. Based on the study of their grid codes, a summary of the applied ROCOF settings is depicted in Table 4. As it can be seen, ROCOF protection varies depending on the properties of the grid that is applied. In this project, the settings that are selected for ROCOF protection are shown in Table 5.

Table 4. ROCOF requirements of various European countries. Adapted from [41].

Country	ROCOF limit [Hz/s]	Time setting (s)
Denmark	2.0	0.2
Germany	2.0	0.5
Ireland	1.0	0.5
Netherlands	2.0	0.5
Italy	2.5	0.1
UK	1.0	0.5

Table 5. Selected ROCOF protection settings.

ROCOF Threshold (Hz/s)	Time Setting (s)
> 2.0	0.5
< -2.0	0.5

3.2.3. Distance and overload protection for transmission lines

The main operating principles of the protection systems for transmission lines are speed and selectivity. The circuit breakers are required to operate in a timely manner, in case of a fault or an overload. Otherwise, the excessive current could damage the transmission line resulting in the loss of equipment. Additionally, the implemented protection schemes should be designed in such a way that only the faulted part of the power system is disconnected, thus securing the safe operation of the rest of the grid.

In transmission lines, a common practice is to implement distance protection as the primary protection of the line, while overload protection acts as secondary protection. Distance protection is based on the concept of zonal protection, which is defined by the protected line length, as well as the length of its neighboring lines. Distance relays are placed on both ends of a transmission line. The operation of the distance relays is based on the voltage and currents measurements of the line. If the measured impedance of the line violates specific thresholds, a disturbance or fault is detected. In this thesis project, three Zones are defined; Zone 1 is set to 85% of the protected line length, Zone 2 at 100% of the line length plus 60% of the shortest neighboring line. Zone 3 is set at 100% of the length of the two aforementioned lines plus 20% of the next shortest line's length. In Table 6 the equations for the zonal impedances and the associated time settings are provided.

Table 6. Implemented settings for distance protection.

Zone	Zonal Impedance (Ohms)	Time Setting (s)
1	$Z_1 = 0.85 * Z_{minA-B}$	0
2	$Z_2 = Z_{maxA-B} + 0.6 * Z_{minB-C}$	0.6
3	$Z_3 = Z_{maxA-B} + Z_{minB-C} + 0.2 * Z_{minC-D}$	0.8

For the overload protection of transmission lines, a definite time characteristic was adapted based on [42], [43]. To calculate the exact parameters of an overload relay, a thermal analysis of the transmission lines is required, which is beyond the scope of this work. As a result, based on the information obtained through the reviewed literature, thresholds and time settings were applied. The implemented settings are shown in Table 7. The time characteristic for the overload protection is modelled as a stepped definite time.

Table 7. Implemented settings for overload protection.

Current threshold (p.u.)	Time Setting (s)
> 1.3	300
> 1.5	180
> 2.0	60
> 2.2	30

3.2.4. Settings of existing protection schemes and coordination

To successfully implement the modelled protection schemes, presented in the sections above, their coordination with the existing schemes, shown in Table 1, is studied. The implemented schemes are based on the work presented in [21], and their selected settings are summarized in Table 8 and

Table 9. These protection schemes are applied to a) generators and b) loads. For generators, the additional schemes include over/under voltage, over-flux and out of step protection. For the loads, the applied protection schemes are the Under Frequency Load Shedding (UFLS) and Under Voltage Load Shedding (UVLS).

Table 8. Protection schemes for generators.

Voltage protection threshold (p.u.)	Time Setting (s)
> 1.5	0.083 (5 cycles)
> 1.1	10
< 0.9	15
< 0.8	2
Over-flux protection threshold (p.u.)	**Time Setting (s)**
> 1.1	60
> 1.2	3
Pole slip angle change by (degrees)	**Time Setting (s)**
360	0.005

Table 9. Load shedding schemes.

Under frequency load shedding		
Threshold (Hz)	Time Setting (s)	Load Shed (%)
< 59.1	5	5.3
< 58.9	2.5	5.9
< 58.7	1	6.5
< 58.5	0.1	6.7
Under voltage load shedding		
Threshold (p.u.)	Time Setting (s)	Load Shed (%)
< 0.8	30	5

The coordination of the implemented protection schemes for the synchronous generators, is shown in Table 10. The protection schemes are sorted based on their time settings. As it can be seen, for generators the out of step protection is the one that has the smallest time setting to protect the generators from asynchronous operation. In the case of transmission lines, overload protection is mainly a backup protection which will trip in the case of a maloperation of the distance relays.

Table 10. Protection coordination for generators.

Type of protection	Pick-up value	Units	Time setting (s)
Out of step	-	-	0.005
Overvoltage	> 1.5	p.u.	0.083
Under frequency	< 57.1	Hz	0.17
ROCOF	2	Hz/s	0.5
Undervoltage	< 0.8	p.u.	2
Overflux	> 1.2	p.u.	3
Over frequency	> 61.8	Hz	5

3.3. Communication Network Modelling

The cyber layer of the CPS can be imagined as residing on top of the physical power system layer. The cyber system can be divided into two sub-layers, namely the digital substation's LAN and the overall WAN. The first layer represents the ICT/OT infrastructure of a digital substation. This layer oversees the monitoring of the state of the power grid, and each substation which has an area of control. The protection equipment installed in each substation monitors the state of the system and issues protective actions based on their functionality. The operational data from each individual substation is then transmitted to the centralized control center, via the WAN. This enables the operators of the control center to have a complete picture of the operating state of the system, and if required to perform corrective actions by issuing commands to multiple substations.

3.3.1. Modelling the local area network of a digital substation

Digital substations are in charge of monitoring and control their specified areas of the power grid. Physical electrical devices such as measurement transformers are used to monitor the system, by continually measuring the voltage and the current parameters. The interface of these transformers is connected to the IEDs and other logical units, through a device called Merging Unit (MU). MU is defined in IEC 61850-9-1 as an interface unit that accepts current transformer or voltage transformer measurements and as inputs and produces multiple time-synchronized digital outputs, providing data communication through logical interfaces [44]. MUs are used to directly connect electrical devices such as measurement transformers, sensors, and circuit breakers to the targeted devices, thus eliminating the need for hardwiring while increasing digitalization. Their main function is to acquire the analogue measured values and to convert them to digital signals. These values are transmitted using the IEC 61850 standard to an Ethernet LAN, where the IEDs are connected to. MUs can also support input/output functions, like receive trip and open/close signals as well as transmitting measurement values [44].

An important aspect of the digital substation is time synchronization. A method for achieving time synchronization is by using Global Positioning System (GPS) or equivalent time synchronization sources. These time sources provide all measurements and data packets with specific timestamps. These timestamps are crucial for the functionality of the communication network, and the synchronization must be very accurate, as the power system needs to be controlled and monitored in a timely manner.

An example of a digital substation's LAN network can be presented in Figure 3.5. The design is based on the technical reference, provided by ABB [44]. A digital substation uses Ethernet-based technology for communication in the LAN. This technology is suitable as it offers high data rates (from 10 Mbps to 10 Gbps) and is suitable mainly for LAN applications as the coverage rate is up to some hundred meters [45]. The substation's MUs are connected to an Ethernet switch, which is in charge of scheduling the traffic. The operational information from the metering devices is then given to the substation's protection and control unit and are also transmitted to the control center. The centralized protection and control unit contains various monitoring and control applications, such as IEDs, engineering workstation, and the Human-Machine Interface (HMI) of the substation. The communication getaway is in charge of connecting the individual substation to the WAN, which is used for communication with the control center. Control commands can be received from both the control center and the centralized unit of the substation OT. Finally, all these systems are synchronized using a certain method, like a GPS clock.

To model the LAN of a digital substation, graph theory can be used. The aforementioned architecture can be represented as a graph $G = (V, E)$, where V are the vertices of the system and E the edges connecting them. A representation of the aforementioned graph is presented in Figure 3.6. The MUs of a substation act as the coupling point between the physical and the cyber layer. Communication is bidirectional; data packets containing information about the power grid operation are transmitted from the MUs and are received by the substation's control unit as well as the control center, while control commands are issued from the latter. Commands are executed based on First-Come-First-Serve (FCFS) scheduling logic, and the selection is based on the time of arrival of each packet.

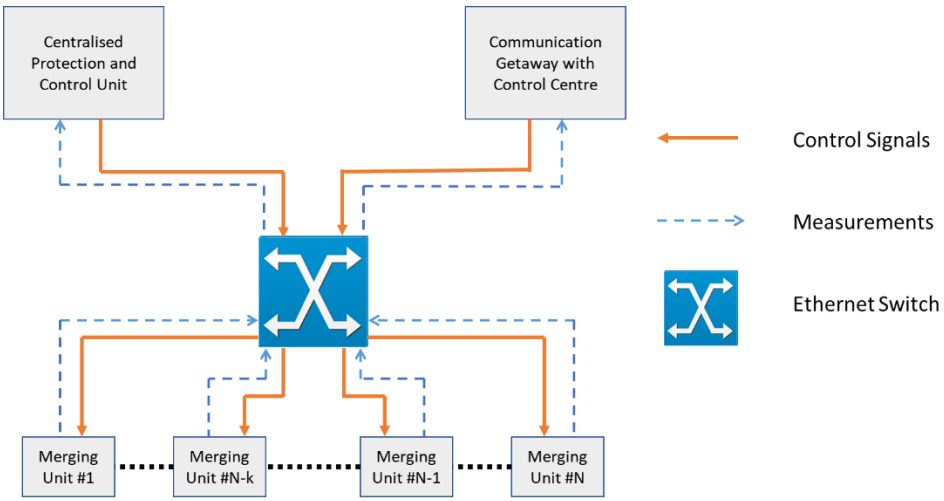


Figure 3.5. Centralized architecture for digital substation's LAN.

Each MU monitors specific areas of the substation, and the monitored state and control variables are updated, only when a change occurs. Each measurement received from the physical system has a unique identification ID, a specific name that is associated with its function and topological position, the actual measurement and a unique timestamp, based on the clock of the system.

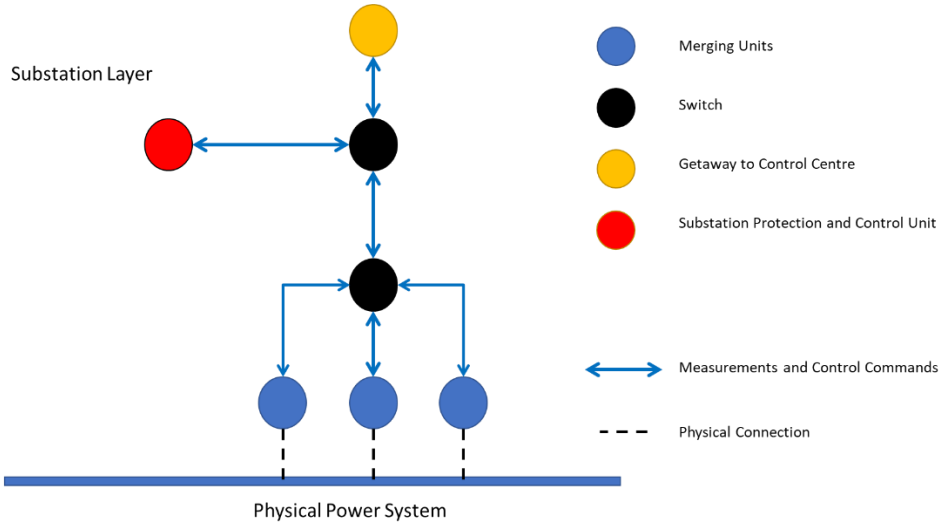


Figure 3.6. Substation's LAN representation, using graph theory.

The data received by the physical power grid, due to the physical connection of MUs with the electrical equipment, are considered to be real-time information of the power system. When the state and control data are updated, the value of the variable is changed, and the new timestamp is provided. These packets are then transmitted from each MU to the substation switches. The time that an updated value is received by the receiving node is calculated by taking into account the individual time delays of the edges connecting the transmitting and receiving nodes. This is described by the following equation:

$$t_{S\to R}^{delay} = \sum_{i=0}^{e_{shortest\ path}(S,R)} t_i^{delay} \tag{3.14}$$

where $t_{S\to R}^{delay}$ is the total time delay for a packet to be transmitted from the sending node S to the receiving node R via the shortest path, $e_{shortest\ path}(S,R)$ are the edges of the shortest path between the two nodes, and t_i^{delay} is the transfer time delay of the path's edges. These delays should satisfy strict requirements for the substation's communication network, and they also depend on the technology used for connecting these systems. Each node on the modelled system also has a processing time, to either forward the information or to act. By calculating the sum of the path transfer delay plus the overall processing time for the specific application, the total delay $t_{p,i}^{delay}$ of the specified process can be identified. The total delay should be less than the accepted latency tolerance $t_{\xi(i)}$ that is allowed for the specific operation i [17]. The processing time is different to each application and the required latency is also based on the type of application [45].

$$t_{S\to R}^{delay} + \sum_{i=0}^{N} t_i^{process} = t_{p,i}^{delay} \tag{3.15}$$

$$t_{p(i)}^{delay} \le t_{\xi(i)} \tag{3.16}$$

Additionally, an important consideration is the throughput in bytes per second of the individual edges. In the examined system, each MU is connected to an ethernet switch, which is responsible for transmitting the data to the other nodes. A typical example is that an edge connecting the switch node and the control unit node has to be modelled in such a way that all the available data from the MUs can reach the desired node. To satisfy these constraints, each edge of the network has a static pre-defined max data rate λ_i^{max}, based on the applied technology, i.e., fiber optic, ethernet cable etc. This is given by:

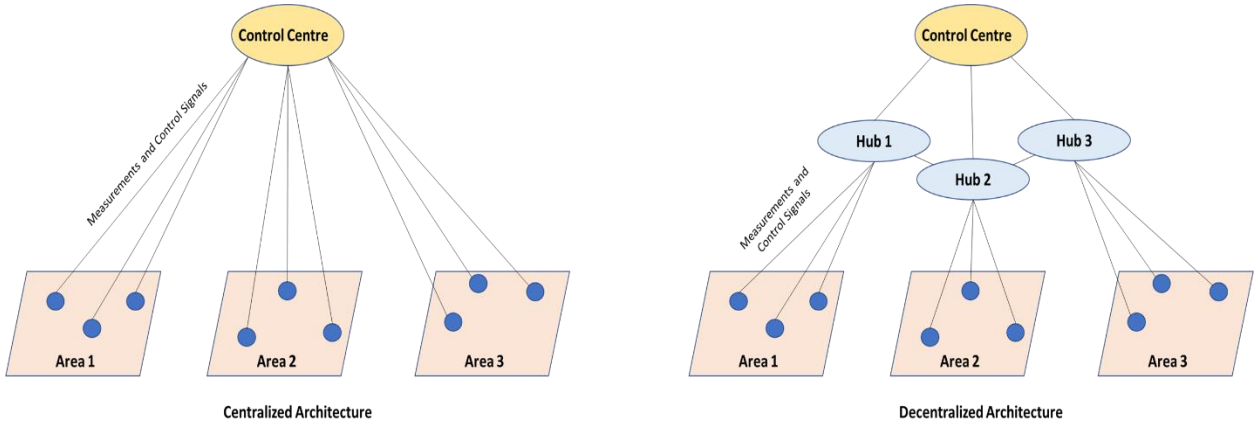
$$\lambda_\iota[t] \le \lambda_i^{max} \tag{3.17}$$

The data rate λ_ι through a specific edge should always satisfy the constraint shown in Equation 3.17 to avoid packet loss. This enables us to study the effects of specific scenarios such as DDoS attacks,

as the overflow of data could cause significant delays in the system, affecting the controllability and observability of the examined system.

3.3.2. Modelling the wide area network

The WAN of the CPS is used for connecting the individual digital substations with the control center of the transmission grid. As these substations are distributed in a huge area, this network can span for hundreds of kilometers. To model this network there are two communication architectures that can be implemented; a centralized and a decentralized one [46]. These architectures are shown in Figure 3.7.



a) b)

Figure 3.7. WAN architecture for a) centralized and b) decentralized approach.

A centralized architecture can be imagined as a star graph. The control center acts as the internal node, and each substation is a leaf. This architecture is simple, as each substation is directly connected to the control center. But as this network is vast individual connections between each substation and the control center will increase the cost of the overall infrastructure.

In a decentralized architecture, a layer of communication nodes is added which act as data routing hubs. These hubs can also be digital substations, and be used to connect various substations in a specified area with the control center. Additionally, as suggested in [46] these hubs could reduce the overall latency for the transmission of measurements and control commands, which is crucial for specific applications such as transient stability and small signal stability. In this work, we model the WAN based on the decentralized architecture. The power system is divided into three areas of control, with a substation in each area acting as a data routing hub. Additionally, in this work we consider a scenario in which these particular hubs are targeted by malicious actors, and the impact of such an attack is also assessed.

3.4. Cyber-Physical System Implementation and Validation

In this work, the CPS for the IEEE 39 bus system is modelled. The physical layer is modelled using the power system analysis software application, i.e., DlgSILENT PowerFactory. PowerFactory is a software solution for analyzing generation, transmission, distribution and industrial systems. It is fully Windows compatible and combines reliable and flexible system modelling capabilities with state-of-the-art control algorithms. The physical layer will include the aforementioned system along with its protection mechanisms. The goal for the physical layer of the CPS is to be a close representation of a real-world power system.

The cyber layer of the system is modelled in Mininet, a network emulator which can be used to create networks of virtual hosts, switches, controllers, and links. Mininet is a Linux network software, and it supports flexible custom routing and software-defined networking. The communication between these two simulators is achieved by using the Open Platform Communications Unified Architecture (OPC UA). This protocol is mainly used for industrial automation and in this work is used to enable the

communication between the two layers of the CPS. It is based on client-server communication and its focus is on communication with industrial equipment and systems for data collection and control. Additionally, it supports cross-platform communication.

The proposed tools are implemented to construct the CPS testbed shown in Figure 3.8. The CPS model presented above is used to simulate cyber attack scenarios. Selected nodes on the communication network emulator are altered by the user, through manual entries or by code, and the effects on the system stability can be observed in the power system model. This whole system is simulated in real-time.

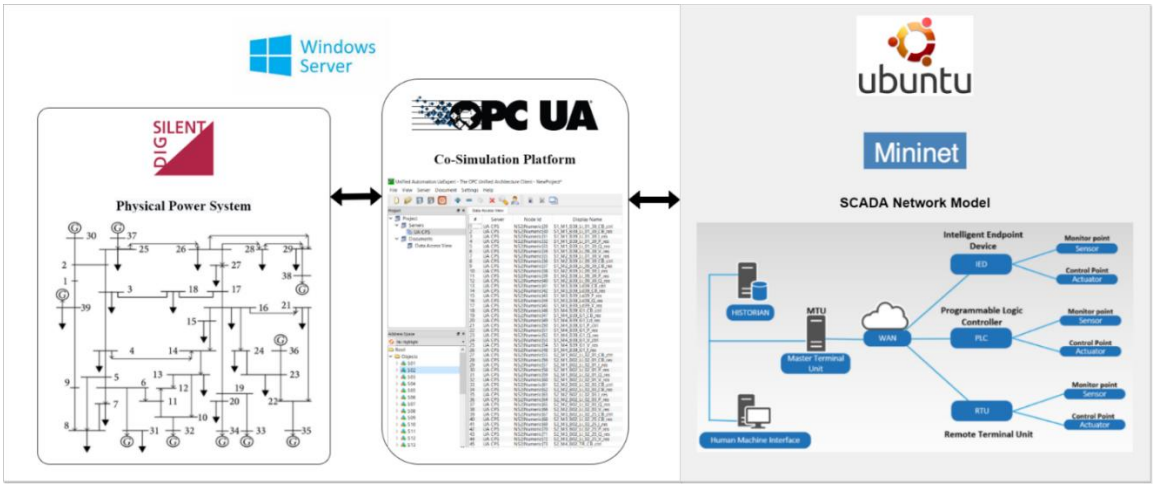


Figure 3.8. Tools used to model the CPS and their interconnection.

3.4.1. Power system implementation and validation

The physical power system that is modelled in this project is the 39 bus New England system. It is a simplified model of the high voltage transmission system in the northeast of the U.S.A. The power system consists of 10 generators, 19 loads, 34 lines and 12 transformers. The nominal frequency of the system is 60 Hz and the main voltage level is 345 kV. Generator buses operate at 16.5 kV, while specific buses operate at voltage levels such as 138 kV and 230 kV. The model of the power system is based on the data provided by [47], and the operating conditions and parameters are given in Appendix A.

The modelled system incorporates the static and dynamic models needed for time-domain simulations. The power system is divided into 27 substations, which can be seen in Figure 3.9. These substations control their specified areas, and the various protection and control mechanisms are implemented in this model. The specified substations can include generating units, loads, and transformers or they can only be covering a single bus of the system and the connected overhead lines. Furthermore, the grid is split into three control areas which they specify the WAN topology. Each area has a hub substation, which is connected with the control center.

Finally, the control mechanisms of the power system are implemented in the model by using the PowerFactory modules from associated libraries. The loads are voltage-dependent, while the generators are controlled through AVRs and primary frequency controllers (governors). This model of the power system can be used for time-domain simulations and this benchmark model is mainly used for stability studies on power systems. The main contributions as part of thesis are the implementation of the protection schemes, presented in Section 3.2.

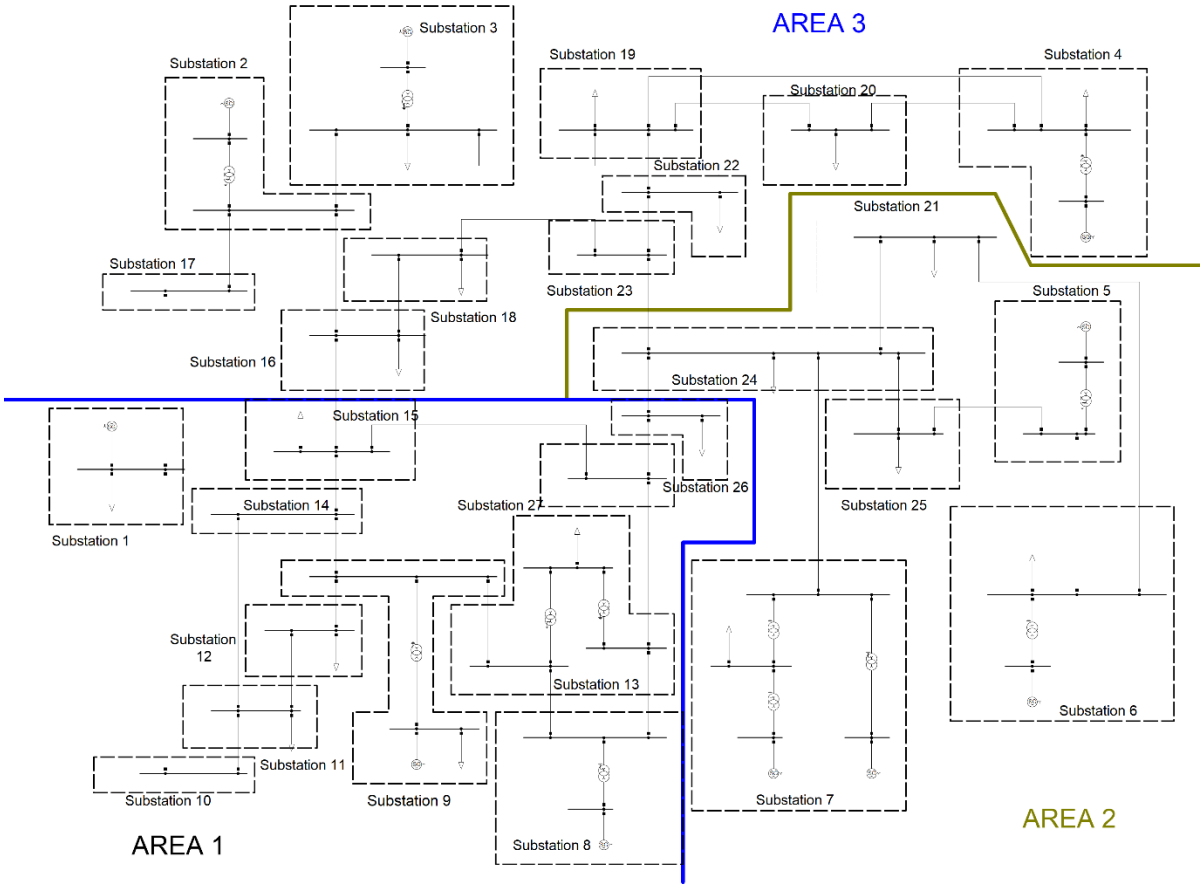


Figure 3.9. The 39-bus system along with its specified substations and areas.

To validate the modelled power system, certain scenarios were examined to show the potential cascading failures that can occur in the power system as a result of a cyber attack scenario. These scenarios tested the operation of the applied protection schemes, and also provided us with results regarding the impact of potential cyber attacks on the physical infrastructure.

In the presented scenario, the circuit breakers of two substations are maliciously opened, disconnecting them from the power system. This scenario is formed based on the investigation by Federal Energy Regulatory Commission, stating that in the U.S.A. Thirty critical substations that malicious actors could target to cause a blackout were identified [48]. The selection of the substations is based on their criticality based on their topology and the results of an N-1 contingency analysis. The attack locations are depicted in Figure 3.10. The power system is divided into three areas of control. The dynamic simulation has a run time of 30 seconds, with the integration time step being 10 milliseconds. In Table 11, the detailed results of the cascading failure sequence are presented. The results of the dynamic simulations, shown in Figure 3.11.

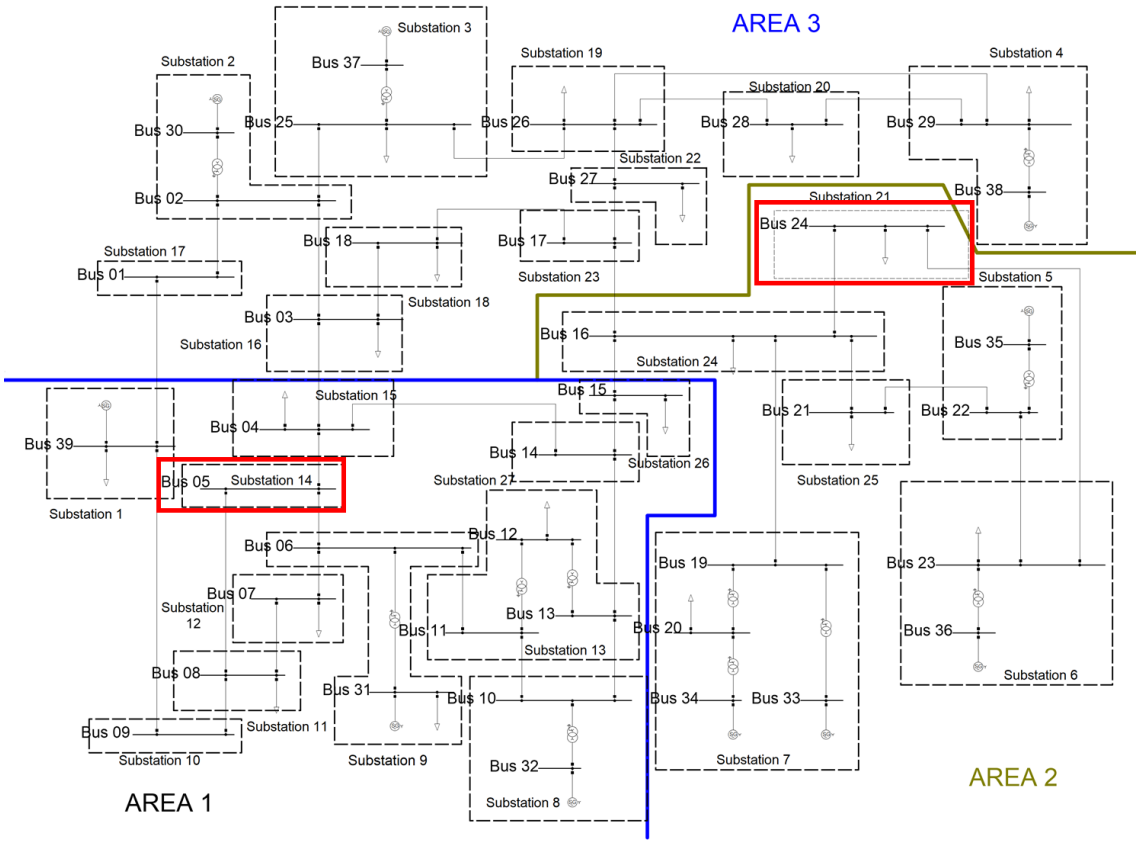


Figure 3.10. Targeted substations in the cyber attack scenario.

The first attack is initiated at 5 seconds by opening the three circuit breakers of substation 14, with one second time interval between the actions. As a result, the lines at the neighboring substations are overloaded. Due to the increase in current magnitude and the decrease of voltage, the measured impedance drops below the threshold set for distance protection relays. This is shown in Figure 3.11 a). Due to the tripping of multiple lines, line 01-02 is severely overloaded as it is shown in Figure 3.11 b). The excessive current causes the distance protection to trip. The frequency of generators connected in buses 31 and 32, namely generators 2 and 3, starts to increase. Due to the islanding occurring in Area 1, the load supplied by the generators drops significantly, causing their speed to increase as their control systems cannot decrease their speed in time. This causes the ROCOF protection to open the circuit breakers as the threshold of 2 Hz/s is violated. This event is shown in Figure 3.11 c).

The attack on the second substation occurs at 11 seconds, and again the two circuit breakers of the system are targeted. The results are similar to the first attack, as distance relays trip the line circuit breakers from the neighboring substations, causing the generators that operate in this area to disconnect or to form islands of operation. This can be depicted in Figure 3.11 d), where the generators 6 and 7 are disconnected due to ROCOF violation. The UFLS of the remaining loads across the system activates, limiting the active power demand as it is shown in Figure 3.11 e). As the modelled loads are voltage-dependent, as described in [47], their total active power is increasing due to the increase of the voltage. But as a result, the majority of the generators operating in Area 3 trip due to ROCOF protection. On the other hand, the load shedding that is applied to Load 39, presented in Figure 3.11 f), is successful as the power balance is restored and the load can still be supplied by the interconnection.

The simulation ends with most of the loads in Area 2 and Area 3 left unsupplied, except for three islands of operations. Due to the load shedding actions, three generators are still operational as they supply a certain number of loads. The total loss of load at the end of the simulation is approximately 64% of the total load, ending in a partial blackout. The state of the grid after the attack can be seen in Figure 3.12, where red lines indicate disconnected equipment. The cascading failures seen in this

scenario highlight how cyber attacks can have a severe impact on the physical power system. Additionally, as seen in real-world cascading failures like the ones observed in the U.S.A - Canada 2003 blackout and in Turkey in 2015, distance relays can confuse heavy loading situations for uncleared faults, as the impedance enters the third zone of protection [49] [50].

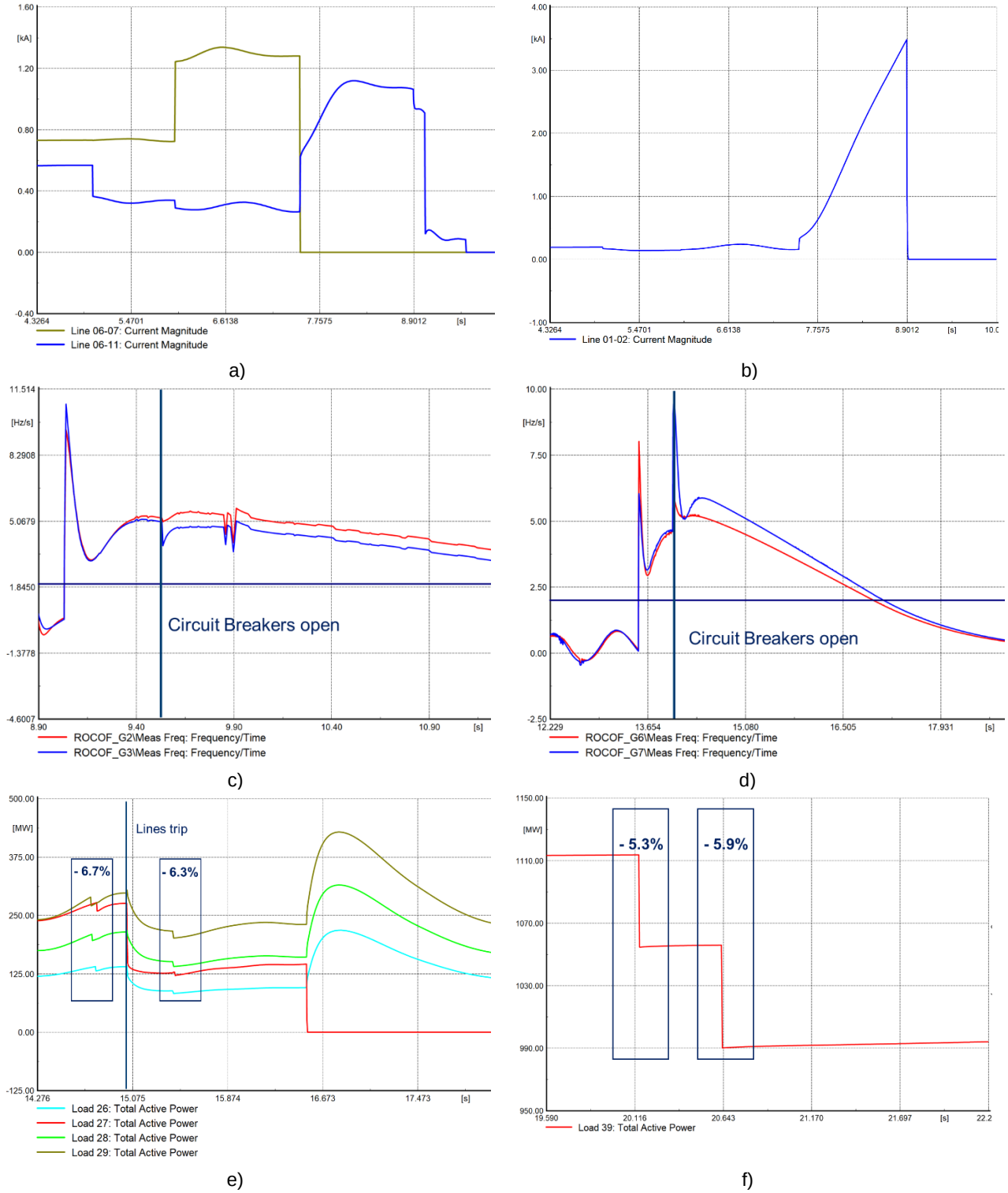


Figure 3.11. Operation of a) -b) distance, c) - d) ROCOF and e) - f) UFLS protection schemes, for the examined scenario.

Table 11. Sequence of events for the cyber attack scenario.

Time (seconds)	Event
0	Start of simulation.
5 - 7	**Cyber attack on substation 14. Lines 05-06, 04-05, and 05-08 maliciously disconnected.**
7.514 - 9.031	Multiple lines in the vicinity of the attack location tripped by distance protection, i.e., lines 06-07,13-14. Distance relay 01-02 is tripped. Generators G2 and G3 form an island of operation.
9.532	Generators G2 and G3 trip due to ROCOF protection.
10.467	Line 08-09 trips on distance protection. Area 1 is unsupplied.
11 - 12	**Cyber attack on substation 21. Lines 16-24 and 23-24 maliciously disconnected.**
13.516	Distance relay trips line 21-22.
14.017	Generators G6 and G7 disconnect due to ROCOF.
14.624 - 16.537	Lines 02-03, 16-19. 17-27, 25-26, and 26-27 trip due to distance protection. G5 disconnects due to ROCOF. Load shedding to all loads (6.7 and 6.5%).
17.039 - 20.643	Generators G8 and G9 disconnect due to ROCOF. Additional load shedding to Load 39 (5.3 and 5.9%).
30	End of simulation. Cyber attack results in islanding. Three islands remain with external grid, G4 and G10 supplying Loads 20, 25 and 39. Total loss of load amounts to nearly 4000 MW.

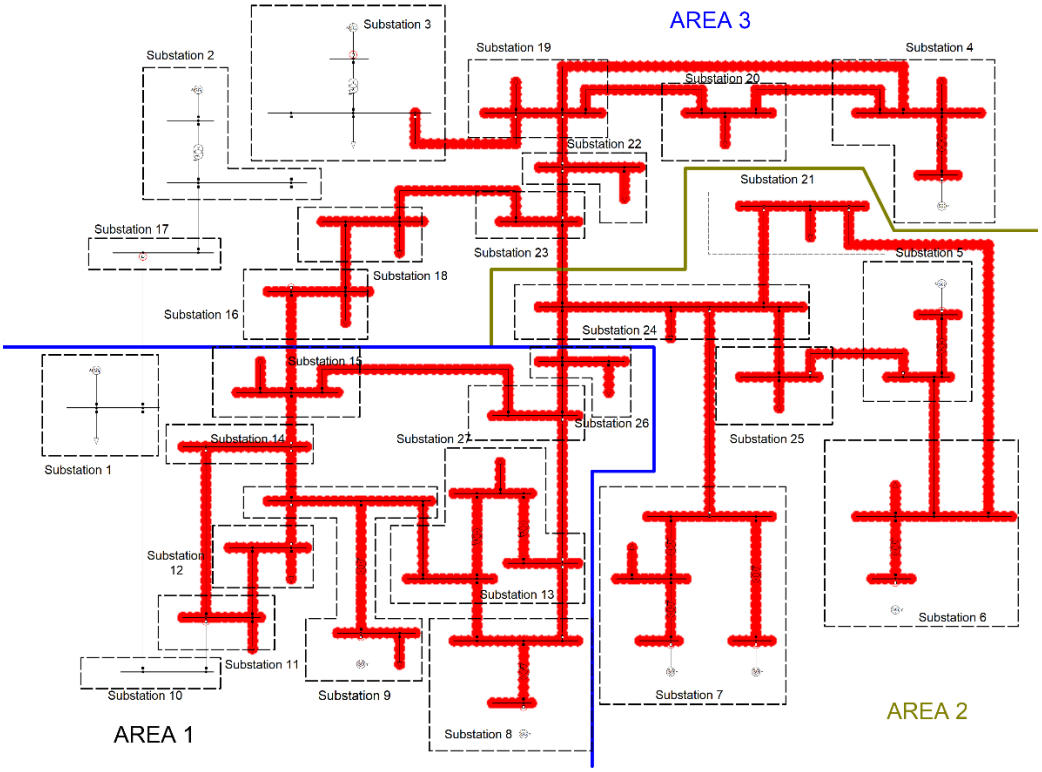


Figure 3.12. State of the grid in the aftermath of the cyber attack scenario.

3.4.2. Communication system implementation and validation

In this project, Mininet is used to create the communication network of the digital substations. Mininet has two primary advantages; it enables the creation of networks of any size and can emulate real-world TCP traffic. It also supports software-defined networking and OpenFlow [51]. Mininet is running on Linux operating systems.

In this project, a network of 27 digital substations was created using Python. These digital substations were designed, based on the requirements of their defined counterparts in the physical system. They vary in size, but their topology is based on Figure 3.6. Each substation has specific MUs, and they are connected to either lines, transformers or generators. Each MU monitors and controls specific equipment, which have unique IDs. The MUs are modelled as hosts in the network, and they connect to an ethernet switch, which can be used to monitor the traffic in a substation.

The centralized monitor and control unit of the substation is modelled as a host. The control unit can change the control parameters of the CPS, by sending commands to the ID which corresponds to the particular variable. A control command can be issued by either the local control unit or the control center and has the following format: **S[Substation number]_MU[Number of MU]_[ID of the control variable] + [New Value]**.

As an example, to open the circuit breaker on substation 19, the implemented command would be **S19_MU1_635+1**. Commands which are generated locally in a substation can be directly implemented by specifying the MU number and ID. These commands are implemented by using the local interface in Mininet, which is modelled using Python scripts. The main contribution of the author was to replicate the implemented code for 24 substations.

The MUs has to be mapped with a list of extracted variables from PowerFactory. Each MU is coded manually, as the list of variables were different for each substation. To validate that our simulated network can emulate real TCP/IP traffic, the following method is used:

- When the network is initiated, the traffic should be zero, as the co-simulation between the physical and cyber layers is not active.

- A ping command is sent to the database of the modelled substation, which should generate 2 packets per second; the sending packet and the confirmation packet, as the handshake rule is applied.
- Finally, by running the co-simulation the number of packets per second in the database of the modelled substation is expected to be $\mathrm{MUs} * 2$, which depends on the number of MUs in the modelled substation.

Using Wireshark, the traffic through the ethernet switch of the substation is monitored, as shown in Figure 3.13.

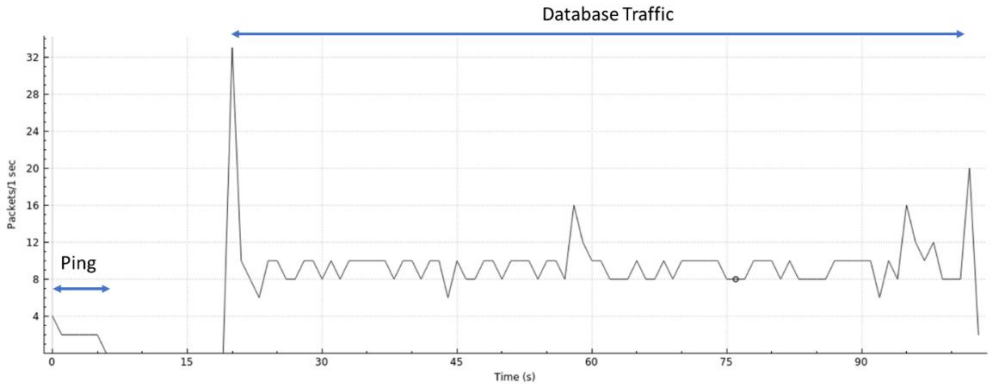


Figure 3.13. Captured TCP/IP traffic in Wireshark, while testing the connection of substation 19.

The examined substation is 19, which has five MUs. A ping command is issued and the results agree with the validation method above. When the ping commands are stopped the traffic returns to zero. Finally, a co-simulation is performed, by running a time-domain simulation in PowerFactory and monitoring the grid measurements through the emulated communication system. The traffic flow results shows that each second the number of packets is ten, which is in agreement with the validation method.

4. Attack Graph and Risk Assessment Method

As presented in Chapter 1, the rise of cyber attacks on critical infrastructures poses a dire threat to the operation of the energy system. Although the frequency of these events is low, the potential impact may be catastrophic. Hence, it is crucial to investigate the risk of such events on the power system. To conduct this analysis, attack graphs are used to specify the likelihood of an attack to commence, while the dynamic model of the CPS is used to assess the potential impact on the examined system. In the following sections, the attack graph model is presented along with the methodology for assessing the risk.

4.1. Attack Graph of a Digital Substation

4.1.1. Specification of the assets

The increasingly dynamic nature of modern power systems, along with the advanced requirements for resiliency and reliability are addressed by the concept of Central Protection and Control (CPC) for the next generation of substations. With the advanced integration of control systems with the network protection devices, system robustness and reliability can be maintained, while each substation can act more intelligently [44].

The integration of ICT with the OT systems in a digital substation provides a) real-time monitoring and control, b) management of critical activities, and c) improved security against unauthorized access. In a digital substation, most hard-wired copper connections are replaced by optical fiber cables, while electronic devices from different vendors can be integrated, through the IEC 61850 standard. This results in a more versatile and efficient system, with lower construction and maintenance costs.

To model the ICT/OT infrastructure of a digital substation, the assets present need to be identified, along with their interconnections. An important consideration is that power systems are comprised of a conglomeration of devices and systems, many of which were installed decades ago. This is related to the fact that the installed OT systems in real-world digital substations are designed to operate for an extended time, unlike their ICT counterparts. Additionally, the equipment and software applications in each substation can vary significantly. Thus, a general attack graph for digital substations can only be created based on the proposed topology defined by standards or vendors, taking into account that this model needs to be adjusted for each individual case, in order to properly address the level of cyber security. The adapted general topology for the modelled digital substations is given in Figure 4.1. This is based on the technical reference provided in [52].

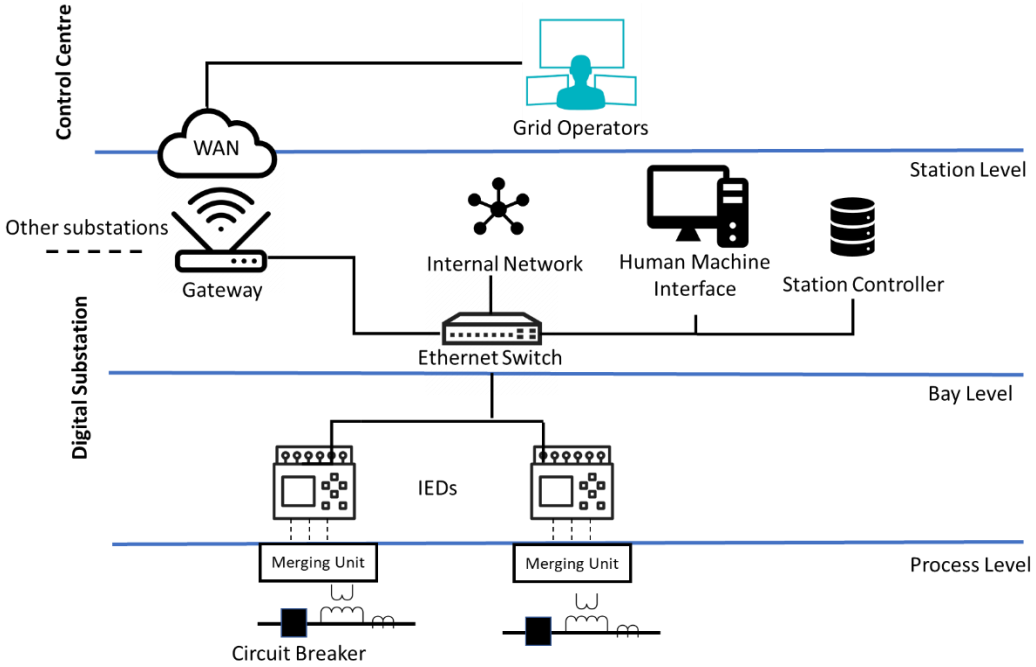


Figure 4.1. Topology and assets of the digital substation.

In this simplified model, the assets that are specified are related to the control and monitoring operations. The modelled assets are as follows:

- *Control Center:* It encompasses all remote applications monitoring, supervision and control of the power system. In this study this asset is considered secure, and will not be a target of attacks.
- *WAN*: It represents the communication network that connects individual substations with the centralized control center. This asset acts as an initial access point for attackers.
- *Gateway*: It is the communication interface between an individual substation and the control center. It is used for the communication of measurements and indications from the digital substation to control center and of commands from the latter for remote control.
- *Station Controller*: This asset represents the station control unit, where the measurements from the substation are collected and processed.
- *Human Machine Interface (HMI)*: It represents the operator console, from which the operators of a digital substation can issue commands and monitor the system, though its Graphical User Interface (GUI).
- *Internal Network*: It represents the extended LAN of the digital substation, and is considered as an entry point for the attackers. This may include operational equipment like printers, servers etc., additional utilities of the substation, as well as any other asset which is not related with the operation of the digital substation.
- *IED*: They are used for several applications like power system protection and monitoring, etc. Attackers can compromise these devices, causing the controlled equipment and breakers to disconnect or otherwise be affected.
- *Circuit Breakers/ Protection Settings*: They represent the physical processes of the power system and are considered potential targets.

The specified substations can act as communication hubs which are used for routing the measurement and command data packets from connected digital substations to the control center

and vice-versa [46]. The attackers are assumed of being able to discover substations that can be targeted by traversing through the gateway of these hubs.

To create the aforementioned attack graph, we utilize the Meta-Attack Language (MAL) framework for domain-specific languages (DSL). This framework defines which information about a developed system is required, and specifies the generic attack logic. MAL is a meta language, which means that a set of techniques is provided to create any DSL. In the following section, the techniques of MAL are presented, which are utilized in this work to create the DSL for digital substations.

4.1.2. Meta-attack language framework

MAL was designed by KTH Stockholm [53] in order to define domain-specific attack graphs, which not only model the traditional ICT assets but also different types of networks, such as the OT environment of a digital substation. It is a framework for creating DSL languages, enabling the creation of a threat model, specified by the user. Additionally, it provides a software compatible file after compiling, that enables the visualization of the aforementioned model.

A threat model is defined by objects and the links between them. An object is defined by character X. The assets are partitioned into a set of classes such as:

$$X = \{X_1, \dots X_n\} \tag{4.1}$$

and each class has several attack steps $A(X_i)$. An attack step can be written as $X.A$, which stands for attack step A of an object in class X. The relationships between two assets are represented as links. A link λ is a binary tuple of objects, where each of these objects are taken from a class, as shown below

$$\lambda = (x_i, x_j) \tag{4.2}$$

Links can be partitioned to a set of associations, $\Lambda = \{\Lambda_1, \dots, \Lambda_n\}$ which are used to relate classes to each other, so that

$$x_i, x_k \in X_m,\ x_j, x_l \in X_n |\ \lambda_1 = (x_i, x_j) \in \Lambda \wedge \lambda_2 = (x_k, x_l) \in \Lambda \tag{4.3}$$

Classes play roles in associations which can be written as $\Psi(X_i, \Lambda)$. Attack steps can be connected to each other with directed edges $e \in E$, where the directed edge is denoted by e while a set of directed edges is denoted by E. This connection between attack steps implies that the first step leads to the second.

$$e = \left(X_i.A_k, X_j.A_l\right) |\ X_j = \Psi(X_i, \Lambda) \tag{4.4}$$

To each attack step a probability distribution is associated specifying the expected time it would take the attacker to perform the step. This gives the local TTC of each attack step, $\varphi(A) = P(T_{loc}(A) = t)$. After specifying the modelled assets and their associations, we can compute the global time to compromise of various attack steps. By examining the TTC value we can assess the level of security for various points in the modelled infrastructure in terms of attack resilience. For computing the global time, assumptions have to be made for the expected local time to compromise of the individual attack steps, but also regarding the order in which the attacker will attempt various available attack steps.

For instance, an attacker with poor planning capabilities could be modelled by a random walk, while an all-knowing expert attacker could be modelled to always follow the shortest path to every attack step. In this study, we will only consider attackers that select the shortest path to reach their target, as it is considered wiser for the defender to prepare for a highly rational attack rather than the opposite. The global TTC for an individual target can be calculated based on the shortest time to reach any parent plus the local time increment of the attack step. This also depends on the logical connection between the assets as they can be connected by an OR logic or an AND logic. If a set of parent assets $\left\{\mathrm{A}_{\mathrm{parent}_1}, \dots, \mathrm{A}_{\mathrm{parent}_n}\right\}$ are connected with an OR logic to the child asset A_{child}, then the attacker will reach the child asset based on the minimum time of its parents. This is given in the following equation:

$$T_{glob}(A_{child}) = \min\left(\left\{\mathrm{T_{glob}}\left(\mathrm{A_{parent_1}}, \dots, \mathrm{A_{parent_n}}\right)\right\}\right) + \mathrm{T_{loc}}(A_{child}) \quad (4.5)$$

On the other hand, for AND attack steps the MIN function is replaced with MAX and the global time is calculated as below

$$T_{glob}(A_{child}) = \max\left(\left\{\mathrm{T_{glob}}\left(\mathrm{A_{parent_1}}, \dots, \mathrm{A_{parent_n}}\right)\right\}\right) + \mathrm{T_{loc}}(A_{child}) \quad (4.6)$$

This means, that an attacker needs to perform all individual attack steps, in order to successfully reach the targeted asset. Finally, in this work, the global time for different targets of an attack scenario is calculated as

$$T_{glob}(scenario) = \max\left(\left\{\mathrm{T_{glob}}(\mathrm{target_1}, \dots, target_n)\right\}\right) \quad (4.7)$$

as we consider that the feasibility of a specified scenario is determined by the time that the attackers need to achieve all their goals.

To visualize the attack paths as well as to extract the time to compromise results, securiCAD software is used [54]. securiCAD is a software developed by the foreseeti Inc. with the aim of performing attack simulations on ICT infrastructures. After creating the model using MAL, we are able to generate a graphical interface of our infrastructure, simulate attacks, and generate attack paths.

4.1.3. Attack graph implementation

In this work, a DSL is developed, based on the MAL framework. This language, named *Substation-Lang*, is used to describe the assets, associations and attack steps for the domain of digital substations and their interconnection through the WAN. The generated attack graph is based on the topology shown in Figure 4.1. The list of assets is summarized in Table 12, along with a short description. The attack graph model considers mostly the equipment related to the monitoring and protection of a digital substation, while the assets are given in an abstract form. This means that although an asset could include multiple sub-systems, in this work they are represented as a single device or system for simplicity. Additionally, assets and security controls such as firewalls, authentication servers, timing servers, etc. are also excluded, due to the added complexity. A model of a digital substation, based on the IEC 61850 standard is proposed in [55]. This model, named SCL-Lang details several assets and their associations. Hence, it is also studied and partially implemented in the *Substation-Lang* model.

Table 12. List of modelled assets for Substation-Lang.

Category	Asset Name	Description
Physical Impact	CircuitBreakers	Circuit breakers of transmission lines
	LoadControl	Circuit breakers of loads
	Generators	Represents the power plants that are connected to the modelled substations
Communication	ControlCentre	Is used to establish the connection between a digital substation and the Control Center
	WAN	Describes the overall WAN of the system
	HubSubstation	Represents the gateways of specified substations, acting as communication hubs
	Gateway	Represents the gateway router, that connects the digital substation with the overall WAN
	SubNetwork	A specific portion of the overall LAN network of a digital substation
Station	Controller	The control station of the digital substation, used for data collection of all connected devices

	OperatorConsole	The HMI of the digital substation, where the operators can monitor and manually control the protection and control devices through the GUI of the installed software
Product	IED	Device used for automation, control, and protection applications
	EthernetSwitch	I/O device between the StationController and the IEDs/Power System assets

The attack types related to each modelled asset are given in Table 13. Additionally, a description is provided for each attack step. The modelled attack types were based on the MITRE ATT&CK for ICS tactics [56]. The complete code of the developed language is provided in Appendix D.

Table 13. List of modelled attack types.

Asset	Attack Type	Description
HubSubstation	connect	Gain unauthorized access to the substations connected to the hub substation
	denialOfService	Launch a DoS attack on the gateway router of the hub substation
	discover	Discover the other hubs present in the communication network
Gateway	denialOfService	Launch a DoS attack on the gateway router
	lanAccess	Gain unauthorized access to the LAN of the digital substation
	wanAccess	Gain unauthorized access to the communication network
Controller	automatedCollection	Obtain information regarding the topology of the system
	manInMiddle	Take control and send unauthorized commands to relays and other control functions
OperatorConsole	commandLineInterface	Compromise the station and issue control commands through its GUI. Represents the HMI interface of the digital substation
IED	modifyParameter	Send control commands to the IED, by compromising the station controller or operator console
	denialOfService	Launch a DoS attack on the IED
	firmwareCompromise	Access the IED and through its firmware are able to compromise
EthernetSwitch	lateralMovement	Access the connected systems to the ethernet switch
	transferCommand	Transfer commands, which originated from controller or the operator console
	discoverIED	Discover the connected IEDs by compromising the switch
	discoverGateway	Discover the gateway of the digital substation
	lanConnect	Connect to the LAN of the digital substation
CircuitBreakers	open	Inject malicious control commands to open the transmission line breakers
LoadControl	disconnect	Inject malicious commands, disconnecting the loads of the substation
Generators	issueControlCommands	Issue unauthorized commands on the control units of the generator
	tripCircuitBreaker	Open the circuit breakers of generator

The generated topology is then implemented in the securiCAD software [54], wherein the entire attack graph can be visualized, as shown in Figure 4.2. The entry point of the attacker is assumed to be already compromised. The targeted assets are highlighted with a star. The topology shown in the figure is generated through a *.mal executable file, and the icons used are obtained either from securiCAD software (attacker icons) or based on the icons file of SCL-Lang, which is publicly available on GitHub [57].

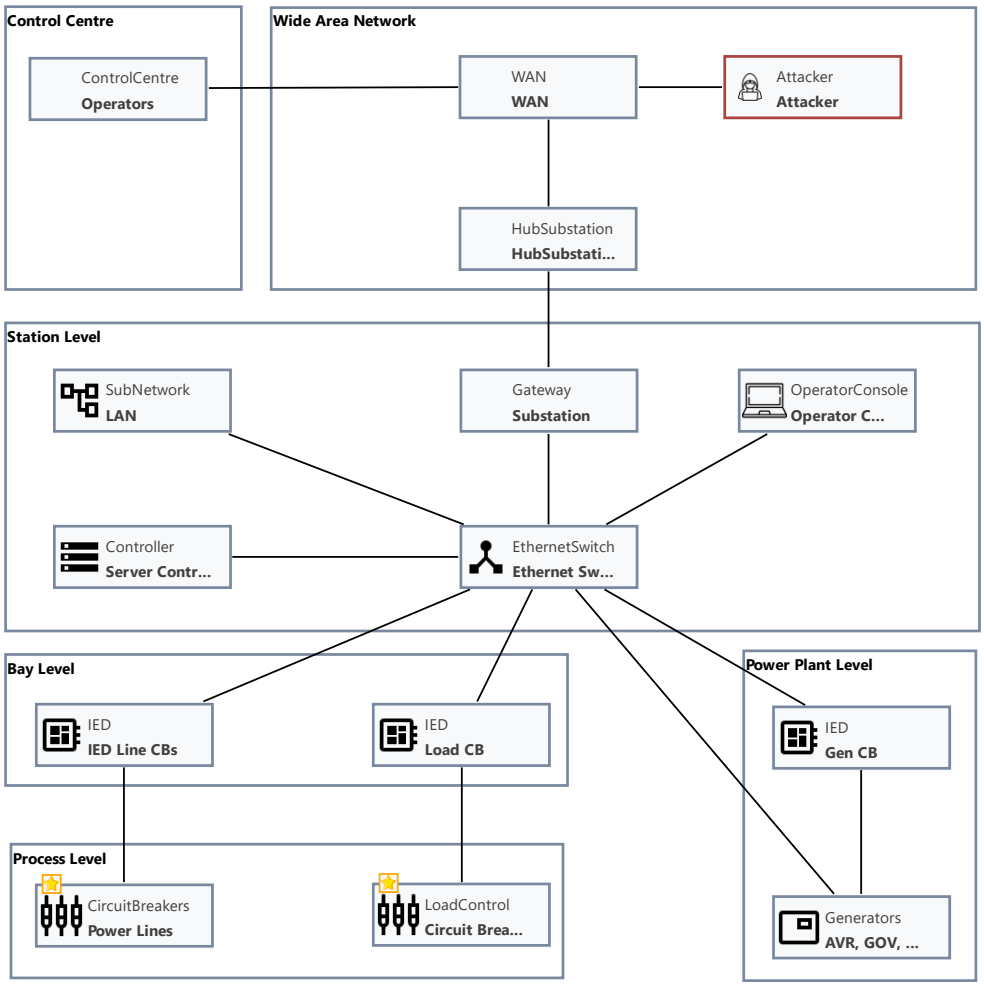


Figure 4.2. Attack graph model in securiCAD.

4.2. Calculation of Time-to-Compromise

4.2.1. Specification of vulnerabilities in the examined assets

Based on the created attack graph, each asset has an associated set of attack steps. These attack steps represent the different ways that an attacker could compromise that particular asset. For a given asset, the associated vulnerabilities that will enable the attacker to successfully compromise this step need to be a) identified, and b) divided based on their compromise type.

We categorize the known vulnerabilities for each asset based on the compromise type. To identify the vulnerabilities of an asset, the National Vulnerability Database (NVD) was used [58]. In this online database, one can search for the Common Vulnerabilities and Exposures (CVE) list of a specific asset. A way to perform this search is given in Figure 4.3, where the known vulnerabilities for the Siemens SIPROTEC IED are generated. The results of this search are the ID of the vulnerability, a short summary of how the attacker can use the vulnerability to impact the operation of the asset, as well as the associated CVSS rating. Although many studies considered the CVSS score in their vulnerability assessment, in our work we will consider all CVEs, regardless of their rating. The main

reason for that is that although the CVSS scores provide a good indication for the potential severity of a vulnerability, they were originally designed for computer network systems, meaning that the scoring criteria can be different for ICS cyber security [59].

Search Parameters:

- Results Type: Overview
- Keyword (text search): SIPROTEC
- Search Type: Search All
- CPE Name Search: false

There are **13** matching records.
Displaying matches **1** through **13**.

Vuln ID	Summary	CVSS Severity
CVE-2019-19279	A vulnerability has been identified in SIPROTEC 4 and SIPROTEC Compact relays equipped with EN100 Ethernet communication modules (All versions). Specially crafted packets sent to port 50000/UDP of the EN100 Ethernet communication modules could cause a Denial-of-Service of the affected device. A manual reboot is required to recover the service of the device. At the time of advisory publication no public exploitation of this security vulnerability was known to Siemens. **Published:** March 10, 2020; 4:15:18 PM -0400	*V3.1:* 7.5 HIGH *V2.0:* 7.8 HIGH
CVE-2019-10938	A vulnerability has been identified in SIPROTEC 5 devices with CPU variants CP200 (All versions < V7.59), SIPROTEC 5 devices with CPU variants CP300 and CP100 (All versions < V8.01), Siemens Power Meters Series 9410 (All versions < V2.2.1), Siemens Power Meters Series 9810 (All versions). An unauthenticated attacker with network access to the device could potentially insert arbitrary code which is executed before firmware verification in the device. At the time of advisory publication no public exploitation of this security vulnerability was known. **Published:** August 02, 2019; 10:15:14 AM -0400	*V3.1:* 9.8 CRITICAL *V2.0:* 7.5 HIGH
CVE-2019-10931	A vulnerability has been identified in All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90), SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90), SIPROTEC 5 device types 7SS85 and 7KE85 (All versions < V8.01), SIPROTEC 5 device types with CPU variants CP200 and the respective Ethernet communication modules (All versions < V7.59), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions < V7.59). Specially crafted packets sent to port 443/TCP could cause a Denial of Service condition. **Published:** July 11, 2019; 6:15:11 PM -0400	*V3.0:* 7.5 HIGH *V2.0:* 5.0 MEDIUM

Figure 4.3. Search results for vulnerabilities of Siemens SIPROTEC family products, using NVD.

To calculate the TTC distributions, we examine the vulnerabilities identified in products/equipment/software from major vendors, that are commissioned in power system substations. In Table 14, an example is given, showing how the identified vulnerabilities can be categorized based on the specified attack step. The vulnerabilities for an example IED asset of the attack graph are examined, considering it is a Siemens SIPROTEC relay [23].

In this example, based on its description, the vulnerabilities are grouped together. For instance, vulnerability 2019-19279 is identified on SIPROTEC 4 and SIPROTEC Compact relays equipped with specific ethernet communication modules. Attackers could cause a DoS on the affected device, by sending specially crafted packets to a specific port of the device. On the other hand, vulnerability 2019-10938 is identified in SIPROTEC 5 devices, with specific Central Processing unit (CPU) variants. Unauthorized attackers with network access to the targeted device, could insert arbitrary code, which is executed before firmware verification of the device. This vulnerability is grouped in the Firmware Compromise.

The grouping of the identified vulnerabilities can be extended, as depending on the number of specified attack steps, each category can include only selected vulnerabilities. An abstract model of the device, could include many vulnerabilities per compromise type, while a more detailed model, will include only selected ones.

In this work, known vulnerabilities for other major vendors like ABB, Schneider Electric, CISCO etc. were considered, as their products are widely used. Additionally, we made the assumption that all identified vulnerabilities can still be exploited, thus not including a patch in the device which could fix a number of them.

Table 14. Categorization of vulnerabilities per attack step, for the asset IED.

Attack Step	CVEs
Firmware Compromise	2019-10938 2019-10930 2018-4839 2016-7114 2016-4785
Denial of Service	2019-19279 2019-10931

	2018-16563
	2018-11451
	2016-7113
	2016-7112
	2015-5374

4.2.2. McQueen method for determining the time-to-compromise

To assess the global TTC of a specified scenario, it is important to specify the individual local TTC for each modelled attack step. The method used in this work, is adapted from the one proposed by McQueen et al. in the study "Time-to-Compromise Model for Cyber Risk Reduction Estimation" [60]. In this study, a novel approach for calculating the TTC of individual components was proposed, considering the nature of the vulnerabilities in the system and the attacker skill level. TTC is modelled as a random process, which is composed of three attacker subprocesses:

- **Process 1** is for the case where at least one vulnerability is known for a component that would achieve privilege level access, and the attacker has at least one exploit readily available that can be used against one of the known vulnerabilities.
- **Process 2** examines the case where at least one vulnerability is known for a component that would enable the attacker to achieve privilege level access, but the attacker does not have a readily available exploit that can be successfully used against it.
- **Process 3** describes the identification of zero-day vulnerabilities and exploits.

Each of the three processes above have different failure probability distributions. Processes 1 and 2 are mutually exclusive while Process 3 is intertwined with the other two. The probability of Process 1 is calculated by using search theory and is given by

$$P_1 = 1 - \exp\left(-\frac{V*M}{K}\right) \tag{4.8}$$

where P_1 is the probability that the attacker has an exploit readily available that will compromise the component, V is the number of vulnerabilities associated with a specific attack step of a component, m is the number of exploits readily available to the attacker, and K is the total number of vulnerabilities. In this study, the value of K is 7000 is used, which is an assumption presented in [22].

The value of M is a function of the attacker's skill level. In the aforementioned studies, the number of readily available exploits is considered as a function of the attacker's skill level. These constants are assumed based on exploits identified through websites like Metasploit [60]. The values of M are set as 100, 250 and 360 for beginner, intermediate, and expert level attackers, respectively [22]. These values indicate the different attack levels, and can be adjusted to accurately model the available exploits based on the examined system. Based on [60] the mean time for a successful attack on Process 1 is assumed to be $\mathrm{t}_1 = 1\ day$.

Processes 1 and 2 are mutually exclusive, i.e., when $V > 0$ the probability that the attacker is in Process 2 is the complement of the probability for Process 1. Thereby

$$P_2 = \exp\left(-\frac{V*M}{k}\right) = 1 - P_1 \tag{4.9}$$

where P_2 is the probability that the attacker does not have an exploit readily available that can be used to compromise the target. In Process 2, the attackers need to develop their own exploit in order to successfully take advantage of a known vulnerability. Based on [60] the average time needed for each try is assumed to be $5.8\ days$. The mean time of Process 2 is then calculated as shown below

$$t_2 = 5.8 * ET \tag{4.10}$$

where t_2 is the mean time of Process 2 and ET is the expected number of tries that the attackers will perform in order to develop an exploit. The expected number of tries is given by the following equation

$$ET = \frac{AM}{V} * \left(1 + \sum_{tries=2}^{V-AM+1} \left[tries * \prod_{i=2}^{tries} \left(\frac{NM-i+2}{V-i+1}\right)\right]\right) \quad (4.11)$$

where AM is the average number of vulnerabilities for which an exploit can be found or created by the attacker given their skill level, NM is the number of vulnerabilities that this skill level of attacker will not be able to use, and V is the number of vulnerabilities on the component of interest. The fraction of the known vulnerabilities that the attackers can target is given by $AM = int(f_C * V)$, and f_C is determined by the skill level of the attackers. In the reviewed study, f_C is a numerical value, ranging from 1.0 for expert level attackers to 0.15 for novice level attackers.

Finally, Process 3 hypothesizes that the rate of new vulnerabilities becomes constant over time, and the attacker level is implemented as proposed in [61]. To calculate this, we need a probability variable u that indicates that process 2 is unsuccessful, i.e.,

$$u = (1 - k)^V \quad (4.12)$$

where k is the skill level of the attacker. In [60], the skill level is given in the discrete domain, as for each skill category, a constant value is assigned i.e., 1 for expert level attackers. The mean time for Process 3 is then calculated as shown below

$$t_3 = \left(\left(\frac{1}{k}\right) - 0.5\right) * 30.42 + 5.8 \quad (4.13)$$

where the value 30.42 is assumed to be the mean time between vulnerabilities, measured in days. This value can be changed based on expert input. The overall TTC for a component is then given by the following equation:

$$TTC = t_1 * P_1 + t_2 * P_2 * (1 - u) + t_3 * u * P_2 \quad (4.14)$$

4.2.3. Calculating time-to-compromise in the continuous domain

In this work, the discrete method described in section 4.2.2 is modified to calculate the TTC in the continuous domain. In [60], four discrete categories of adversary skill levels are defined, and numerical values were assigned to them. The main drawback of this method is that it considers a single value for the level of attacker, which is highlighted by the authors in [62]. But an expert level attacker could be in the range of a single professional to a nation-backed group of experts, with many resources. For this reason, the skill level of the attackers must not be defined as a single discrete value, but as a probability distribution.

The main assumption for this modification is that although a power system could be targeted by malicious actors, their efficiency could vary depending on their level. Some groups are identified as extremely capable based on their previous attacks on ICS infrastructures, as presented in MITRE ATT&CK for ICS groups description [56]. However, these groups only represent a fraction of the overall spectrum of cyber actors, and an organization could consider these groups as the worst-case scenario and not the most common threat.

The proposed mathematical changes are mostly related to the mapping of the skill levels of the attackers, and the parameters that are affected by this numerical value. We consider that the skill level of an attacker is defined by a normal distribution, based on their characterization. The parameters of the distributions for the assumed skill levels of attackers are given in Table 15. Although in this work we consider this specification for attackers, a single distribution could also be used to describe the entire spectrum of potential attackers.

Table 15. Normal distribution parameters for different level of attackers.

Level of attacker	mean $\boldsymbol{\mu}$	variance $\boldsymbol{\sigma^2}$
Expert	0.85	0.04
Intermediate	0.5	0.07
Beginner	0.2	0.05

The first change in this method is that the skill level k receives a value based on the probability distribution described above. Additionally, the number of available exploits for the attackers is given by

$$m = M * k \tag{4.15}$$

where m is the fraction of available exploits that an attacker has, based on their skill level. In this approach, M describes the number of total available exploits that an attacker could utilize. For instance, if there are in total 200 known exploits that an attacker could use, an attacker with a skill level of 0.5, would be able to use only 100 of them.

Another change that is made is that the fraction of vulnerabilities that an attacker can target is again defined by the skill level of the attacker i.e., $AM = k * V$. This is related with the second process described in section 4.2.2.

On one hand, these mathematical additions do not change the overall method, as the method can still be used in the discrete domain. On the other, based on the defined probability distribution for the attackers this method can be used in the continuous domain.

4.2.4. Probability distribution of time-to-compromise for an attack step

The method for calculating the TTC proposed in the sections above, is used for determining the expected TTC for an attack step, in the specified asset. In this work, we will use this method to extract the probability distribution of the TTC for an individual attack step of a considered component. To conduct this analysis, we will use the algorithm shown in Figure 4.4. The number of vulnerabilities V for the examined attack step of a component, the level of attackers and the number of samples are given as inputs. The level of attackers is assumed to follow their category-defined probability distribution. By performing a Monte-Carlo simulation we calculate the TTC for each sample. The extracted values are then used to create the histogram showing the TTC distribution, for each attacker type.

For each sample, a single value of k is considered. This value is determined by the defined distribution and is randomly generated. Based on the equations proposed in Sections 4.2.2 and 4.2.3, the TTC is calculated for each particular case. The generated histogram portrays the TTC for S samples, given a pre-defined level of attacker i.e., expert, intermediate or beginner. In Figure 4.5 such an example is given for a component with three identified vulnerabilities ($V = 3$), for 10000 samples. As it can be seen in Figure 4.5 a) and b), expert and intermediate level attackers can successfully compromise this particular component in a relatively small time period, with their average time ranging from 4.5 to 8 days, respectively. On the contrary, a beginner level attacker would need an extended amount of time to successfully compromise the system, and depending on their overall skill level, this could range anywhere from 50 to 300 days. This is shown in Figure 4.5 c).

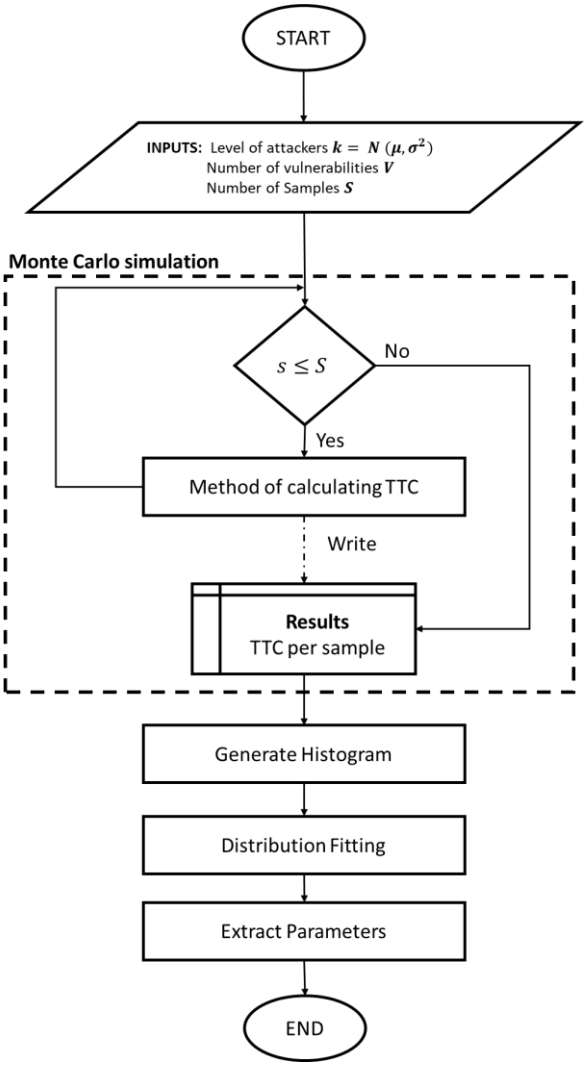


Figure 4.4. Proposed algorithm to calculate the TTC distribution for an attack step of a component.

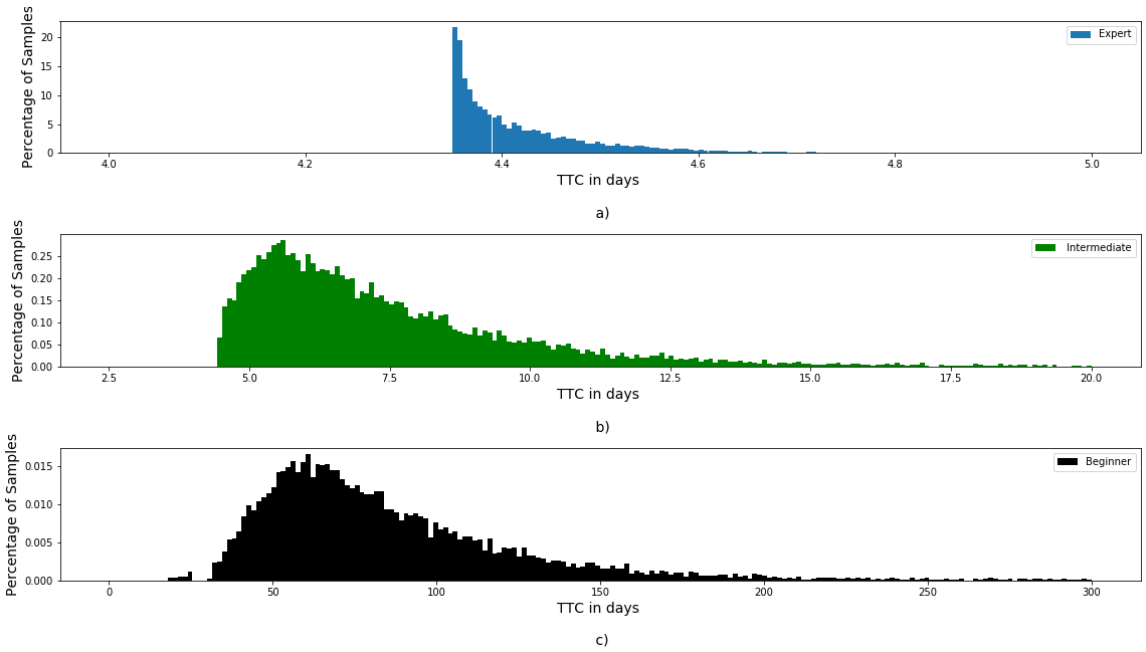


Figure 4.5. Generated histograms, for a) expert b) intermediate and c) beginner level attackers.

To extract the key parameters of each TTC distribution, a fitting process is performed. In Figure 4.6, various distributions are tested for accurate fitting of the generated histogram of an expert level attacker. As can be seen in this example, Gamma and exponential distributions parameters can be used to describe the TTC distribution in this case. Depending on the generated histogram different distributions can be used, based on how accurately they fit.

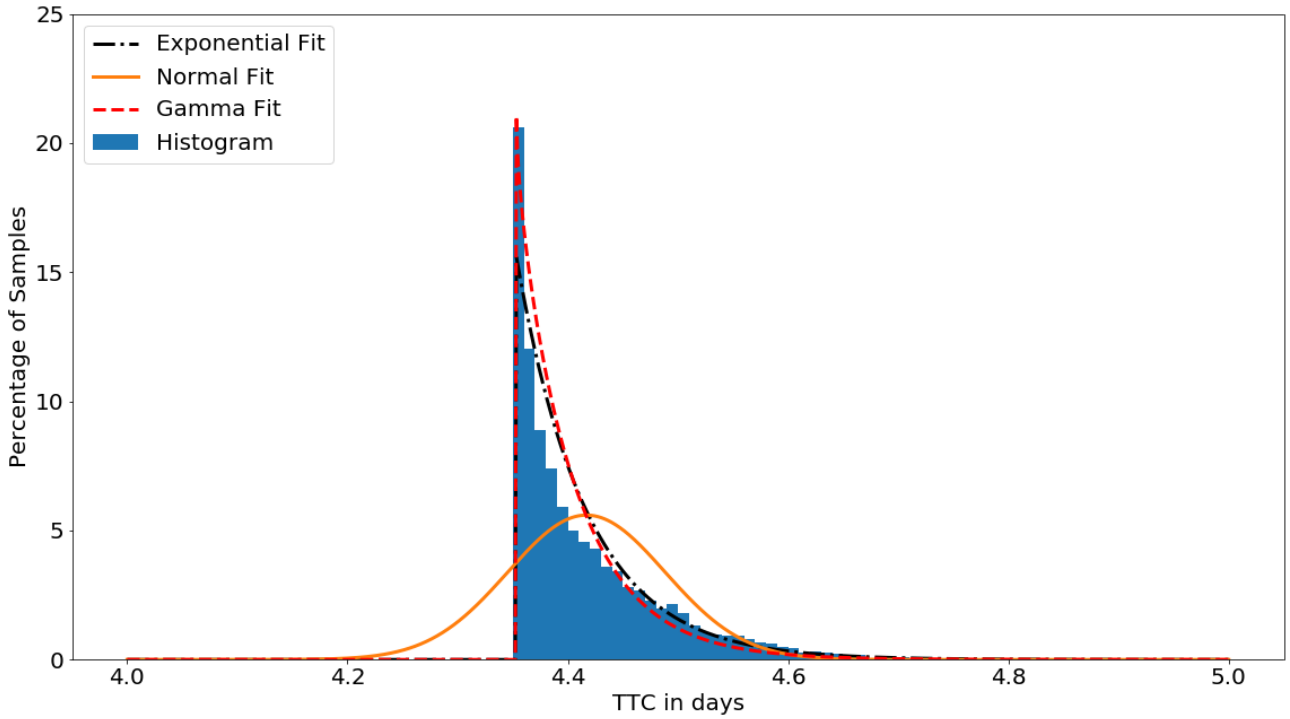


Figure 4.6. Fitting of various distributions on the TTC histogram of expert level attackers.

The parameters of the fitted distributions are then act as inputs in the attack graph model. For each attack step there will be a unique TTC distribution, depending on the number of identified vulnerabilities. In this work, we consider only expert level attackers to highlight the worst-case scenario. The extracted probability distributions for the specified attack steps and for their assets, are given in Appendix C.

4.2.5. Calculation of overall time-to-compromise

The generated TTC probability distributions, defined based on the analysis performed in the previous section, are subsequently inputs into the modelled attack graph. These distributions are either defined using the MAL syntax or by manually inserting them in the securiCAD model. Thus, we can define the average TTC for an attacker to reach their target.

In this work, the attacker is considered as advanced, meaning that the overall TTC is calculated based on Dijkstra's Single-Source shortest path algorithm [54]. The attack simulations are performed using the Monte-Carlo method. For each sample, the attacker starts from a specified entry point. In every iteration, the attackers need a certain time to accomplish each attack step. As the attack steps are determined by a given probability distribution for the TTC, repeated attempts will give slightly different outcomes. This means that the attackers succeed in successfully compromising the targeted assets in a range of different time periods, which are defined based on the probability distributions of the asset and all parent assets.

Additionally, by considering the TTC as a probability distribution and not a single numerical value, all possible attack paths can be generated. This can be used to identify all the weaknesses present in the modelled infrastructure. On the other hand, if a component of the system is deemed extremely vulnerable i.e., many unpatched vulnerabilities are identified which can be exploited by the attackers, then this attack path will be the dominant one.

By generating the results for every sample of the attack simulation, we can extract the average time that the attackers need to successfully reach the targeted asset. The final result of the attack simulation is a Cumulative Distribution Function (CDF), which gives the distribution of the individual TTC per sample. By extracting these results, the average TTC can be calculated. An example of the generated histogram showing the TTC distribution, based on the results of the analysis from securiCAD is given in Figure 4.7. The figure shows that for the considered case, the average time that attackers need to successfully compromise the selected target is 39 days. Furthermore, other parameters such as the variance of the histogram, are also depicted.

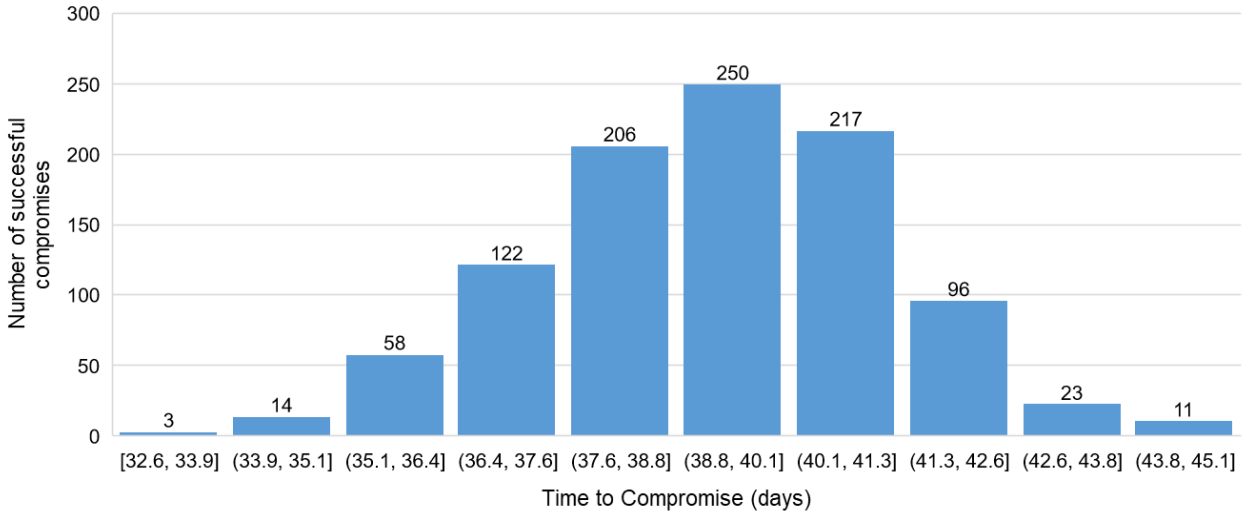


Figure 4.7. Histogram of successful compromises per days, for 1000 samples.

In this work, we only specify the local TTC of the attackers based on the method proposed in Sections 4.2.2 and 4.2.3. Additional considerations that could be implemented into future studies are the inclusion of the initial access discovery, weaponization, testing and delivery times based on the ICS Kill Chain [63]. A more detailed model of a digital substation could identify all possible paths that an attacker can take, but also increase the complexity of the studied system.

4.3. Risk Assessment Method

To quantify the risk of a cyber attack scenario on the CPS, a general risk equation method is proposed. This method combines the probabilistic analysis performed in the attack graph, with a quantitative impact analysis from the dynamic model of the CPS. The equation proposed in this work is formulated as follows

$$Risk(j) = Likelihood(j) * \left(I_{ph}(j) + I_{comm}(j)\right) * F_{Rest}(j) \tag{4.16}$$

where $Risk(j)$ is the calculated risk for a scenario j, $Likelihood(j)$ describes the likelihood of success for the examined scenario, I_{ph} is the quantitative impact assessment of the cyber attack scenario on the physical power system, I_{comm} is the impact assessment on the modelled communication network of the CPS and F_{Rest} is a proposed factor regarding the restoration efforts required. In the following sections, each index of this general risk equation will be analyzed.

4.3.1. Likelihood of a cyber attack scenario

The main assumption regarding the likelihood of an attack scenario is that risk is directly related to the time that an attacker needs to compromise the selected target [54], [60]. Additionally, the Mean-Time to Detect (MTTD) is defined, which is a common KPI defined by cyber security experts [64]. In this research, we assume that the MTTD is defined by the security experts of the CPS, and has a constant value that can be used for the likelihood assessment. The formulation of likelihood is defined as follows

$$Likelihood(j) = \frac{MTTD}{TTC_{avg}(j) + MTTD} \tag{4.17}$$

where $TTC_{avg}(j)$ is the average TTC defined by the security assessment of the attack graph, and $MTTD$ is a constant representing the detection capabilities of the attackers. The result of this function is in the range of [0,1]. If $TTC_{avg}(j) \ll MTTD$, the likelihood is close to 1, while if an asset is well protected and cannot be compromised by an attacker, then

$$\lim_{TTC_{avg} \to \infty} \frac{MTTD}{TTC_{avg}(j) + MTTD} = 0 \tag{4.18}$$

Defining a method to calculate the MTTD is beyond the scope of this work, and it is assumed to be 14 days.

4.3.2. Power system impact assessment

As the examined power system has a variety of control and protection schemes as presented in Chapter 3, the impact caused by a cyber attack scenario can be studied. To assess the impact, we examine the state of the grid before the attack, and its state after reaching an equilibrium post the attack. The main assumption for this type of analysis is that no remedial actions, other than the ones performed by the implemented automation and protection systems are considered. The proposed physical impact equation, is given by

$$I_{ph}(j) = w_L * I_{Load} + w_f * I_{Freq} + w_c * I_{comp} + w_V * I_{Volt} \tag{4.19}$$

where w_L, w_f, w_C, and w_V are weighting factors while the functions I_{Load}, I_{Freq}, I_{Volt} and I_{comp} examine the impact based on the loss of load, frequency and voltage deviations, and the affected components of the power system, respectively. The loss of load and the voltage deviation indices are given by the following equations

$$I_{Load\,(j)} = \sum_{i=1}^{N_{Loads}} \frac{\Delta P_{Load,i}(j)}{P_{initial,i}\,(j)} \tag{4.20}$$

$$I_{Volt\,(j)} = \frac{1}{N_{buses}} \sum_{i=1}^{N_{buses}} \frac{|\Delta V_i(j)|}{\Delta V_{allowed}} \tag{4.21}$$

where $\Delta P_{load,i}$ is the difference between the initial $P_{initial,i}$ and the final active power of each load, ΔV_i is the difference between the initial and final voltage magnitude in p.u. and $\Delta V_{allowed}$ is the permissible voltage deviation. For the loss of load index, the range is $[0, N_{Loads}]$ while for the voltage deviation index the range is between $[0, \frac{1}{\Delta V_{allowed}}]$, where the permissible voltage deviation is considered to be $\pm 5\%$. The aforementioned equations are based on the ones proposed in [17]. The proposed index regarding the disconnected components of the power system is given by

$$I_{comp}(j) = \frac{1}{N_{branch}} \left(\sum_{i=1}^{N_{Lines}} d_{Lines},i\,(j) + \sum_{i=1}^{N_{Trafo}} d_{Trafo},i\,(j) \right) \tag{4.22}$$

where d_{Lines},i and d_{Trafo},i are binary indicators, which show the energizing status of the lines and transformers respectively. They become 1 if the components are disconnected at the end of the simulation, while N_{branch} is that number of total branch components in the system.

Finally, an additional aspect that is considered in this study is the potential fragmentation of the main grid into smaller islanded areas, as a result of cascading failures. An algorithm is developed to identify the islands of operation, based on the operating frequency of the generators at the end of the simulations. The fragmented areas are then examined individually, to determine the frequency deviation. This method can also be applied in the case of normal operation as the "island" of operation, in this case, is considered to be the entire examined power system.

ALGORITHM: Define the level of fragmentation of the power system

Inputs:

$f_{gen} = \left[f_{gen,i} \mid i = 1,2,...,N_{gen} \right]$: Measured Frequency

ε : Measurement Error

Outputs:

N_{subnet} : Number of detected areas of operation

n_{subnet} : Number of generators per area, with $n_{subnet} \in N_{gen}$

f_{subnet} : Operating frequency of area of operation

1. **Set** $N_{subnet} = 0, n_{subnet} = \varnothing, f_{subnet} = \varnothing$
2. **For** $\forall f_{gen,i}$ **do**
3. $N_{subnet} = N_{subnet} + 1$
4. $n_{subnet} \leftarrow n_{subnet}(N_{subnet}) = 1$
5. $f_{subnet} \leftarrow f_{subnet}(N_{subnet}) = f_{gen,i}$
6. **For** $\left(\forall f_{gen,j} \mid j \neq i \right)$ **do**
7. **If** $\left| f_{gen,i} - f_{gen,j} \right| \leq \varepsilon$ **do**
8. $n_{subnet}(N_{subnet}) = n_{subnet} + 1$
9. Delete $f_{gen,j}$ element
10. **End If**
11. **End For**
12. **End For**
13. **Return** $N_{subnet}, n_{subnet}, f_{subnet}$

To calculate the frequency deviation in the formed islands of operation, the following equation is proposed

$$I_{Freq}(j) = \frac{1}{N_{Generators}} \sum_{i=1}^{N_{Subnet}} \frac{\left| \Delta f_{subnet,i}(j) \right|}{\Delta f_{allowed}} * n_{subnet,i} \tag{4.23}$$

where $\Delta f_{subnet,i}$ is the per unit frequency deviation of an island of operation, $\Delta f_{allowed}$ is the permissible frequency deviation and $n_{subnet,i}$ is the number of generators that belong to the specified island. The output of this metric has a range of $[0, \frac{1}{\Delta f_{allowed}}]$, where the permissible frequency deviation is considered to be $\pm 1\%$. The specified impact metrics can fully assess the impact of a cyber attack scenario on the physical power system, by capturing the effects of the potential cascading failures on the grid operation.

4.3.3. Communication system impact assessment

To assess the potential impact of cyber attacks on the communication network of the CPS, we examine the effect of cyber attacks on the network traffic. The metrics presented in literature are mostly focused on aspects affecting the Quality of Service (QoS). These metrics examine the average

delays, packets loss, jitter, etc. [65]. In this thesis, we examine the transmission delays of commands from the control center to the edge devices of the digital substations. The proposed equation is formulated as below

$$I_{cyb}(j) = I_{Delay}(j) \tag{4.24}$$

where I_{Delay} measures the average Round-Trip Time (RTT) between the control center and the edge devices. To assess the impact of the delay on digital substations, the following equation is proposed:

$$I_{Delay}(j) = \sum_{i=1}^{N_{substations}} \max\left(0, log\left(\frac{RTT_{avg,i}(j)}{t_{margin}}\right)\right) \tag{4.25}$$

where $RTT_{avg,i}$ is the average RTT measured using TCP ping test in the examined network, and t_{margin} is the minimum acceptable latency that is required for WAN control and monitoring procedures. The value that is defined in this work is 100 milliseconds, as it is minimum requirement for WAN monitoring procedures, namely for wide-area power oscillation monitoring and dynamic state estimation [45]. When the delay is lower than the margin value, the term $log\left(\frac{RTT_{avg,i}(j)}{t_{margin}}\right) < 0$. On the other hand, if a DoS attack is launched, the increased delay will be captured by this equation, which is able to capture both the volume and the intensity of the attack. Additional metrics such as jitter, packet lengths, etc., examining other aspects of the communication systems can also be studied, but are outside the scope of this work. Hence, in this work we limit our focus to delay variations, caused by an attack on the communications system.

4.3.4. Restoration factor

An important consideration regarding any event or failure in the power system is the restoration procedure and time. The impact of an outage or a large-scale blackout is usually assessed based on the time that it took for the system operators to restore the system to an operating state. An indicator that is used to this end is the Mean Time to Restore (MTTR). Additionally, due to the frequent occurrence of faults and component failures, organizations like IEEE issued standards such as Power Systems Reliability (3006 series) [66].

The main issue is that the MTTR metric is difficult to be directly applied in the case of cyber attacks. Although the aforementioned studies provide data collected from decades of documentation and analysis of faults and equipment failures, cyber attacks are difficult to be analyzed using these metrics, as their occurrences are rarer, while their impact can vary significantly. For this reason, instead of using a metric regarding the timing of restoration, we propose a factor which will be incorporated in the risk analysis to indicate the effort required to restore the examined system. This factor considers the disconnection of the generating units of the system, their capacity, and their type. Reconnecting or restarting the generating units of a system is usually a time-consuming task, and coupled with the gradual restoration of loads, comprises most of the restoration time.

The proposed factor is given by the following equation

$$F_{Rest}(j) = exp\left(\left(\sum_{i=1}^{N_{gen}} \frac{a_i(j) * P_{nominal,i}}{P_{total}}\right) * T\right) \tag{4.26}$$

where $P_{nominal,i}$ is the nominal capacity of the i_{th} generator, P_{total} is the total capacity of the examined network, a_i is the binary status of the circuit breaker of the generator (1 if the generator is disconnected) and T is the restoration index which is based on the type of the generator. The restoration index is calculated as follows

$$T = \max_{0 \le i \le N_{gen}} (T, a_i(j) * T_i) \tag{4.27}$$

where T_i are the individual restoration indices of each generator, depending on their categorization. Initially, the restoration index T is set to 0, and based on the type of the disconnected generators, the maximum restoration index is calculated. This is based on the fact that the restoration procedures for each disconnected generating unit will commence in parallel, meaning that the overall restoration indicator will have the maximum value. In this work, we will consider the indices, as presented in Table 16.

In the examined IEEE 39-bus system, there are three types of generating units; a hydro plant, coal/nuclear power plants and the external grid. The lowest restore index is assigned to the hydro plant, as these types of power plants usually can have black start capabilities and small times to be restored [67]. For the coal/nuclear power plants, a slightly larger indicator is assumed taken into account that these units have a significant time interval to be restored as well as being largely dependent on external power sources [67], [68]. Finally, for the external grid connection we chose the largest indicator, given the fact that this unit has the highest nominal capacity. In the normal operation or when all generating units are connected to the grid, after an attack simulation, $F_{Rest}(j) = \exp(0) = 1$. If a number of generators are disconnected, then the restoration index is determined by the fraction of lost capacity compared to the total capacity of the system, times the maximum indicator.

Table 16. Restoration indicators per generator type

Generator Type	Restoration indicator T_i
Hydro	0.5
Coal/ Nuclear	0.8
External Grid	1.0

5. Results and Discussion

In this chapter, a variety of scenarios are examined to illustrate the possible ways that an attacker can affect the operation of the CPS. The impact on its operation is assessed by performing online simulations using the models presented in Chapter 3. To assess the likelihood, attack simulations are conducted in the attack graph of the digital substations. From the examined scenarios, the most critical substations, given a specified operating state of the power system, are identified.

5.1. Simulation Setup

To assess the risk for the cyber attack scenarios, we utilize the CPS model and the attack graph of the digital substations, that were developed in this thesis. The likelihood of a cyber attack is calculated using the attack graph model while the impact on the CPS is assessed by using real-time simulations performed using DlgSILENT PowerFactory and Mininet. The overall design of the CPS is given in Figure 5.1, where the interaction between the physical and cyber layers is portrayed.

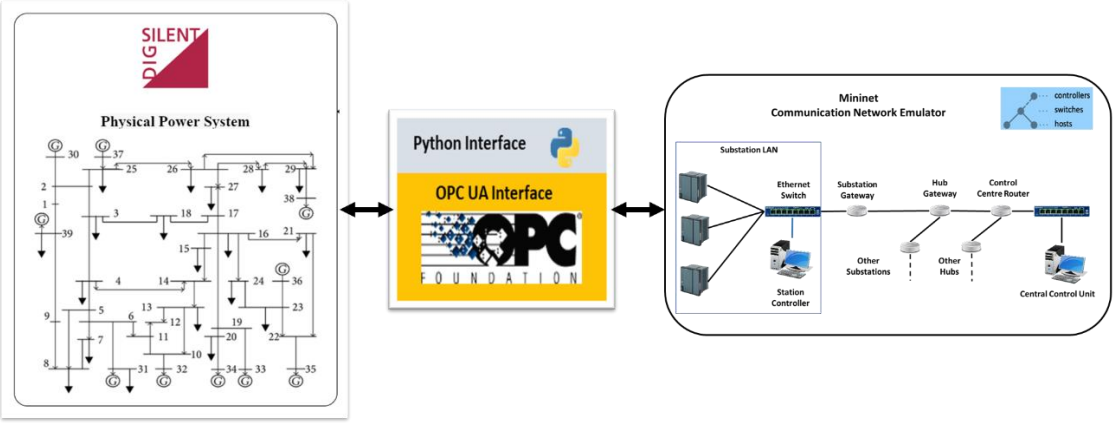


Figure 5.1. Simulation setup for CPS.

The control and protection functions are implemented in the dynamic model of IEEE-39 bus system. To examine the impact of an attack scenario in the overall grid, we employ RMS simulations. The events are created either on PowerFactory software, or by issuing control commands from Mininet. The Python API implementation in PowerFactory is used to analyze the effects on the system and extract the results to be used in the risk assessment method.

An assumption made is that particular substations in the grid can be regarded as communication hubs. This network design is adapted based on the decentralized communication architecture proposed in [46]. In Figure 5.2 the hub substations considered in this study are presented. The selection of the hub substations was random, and it was implemented using Mininet, as shown in Figure 5.1. The topology of the cyber layer is comprised of hosts, such as the MUs and the control stations, while switches and routers are used for data and command communication.

The assets that comprise the attack graph of each substation were randomly selected, and in this work, we will consider only different vendors for IEDs. An additional consideration is regarding the station controller, which is considered either patched or unpatched. A patched station controller is assumed to have an infinite TTC for the *manInMiddle* attack step, which means that the attackers need to compromise either the IEDs or the operator console to perform the specific attacks. In Table 17 the specified assets for each substation are given. The vulnerabilities for each product were specified based on [58].

Table 17. Specified assets per digital substation.

Substation ID	IED Vendor	Patched Controller
9, 12, 14	Siemens	✔
4, 11, 16, 23, 25	Siemens	
1, 18, 24	Schneider Electric	✔
6, 7, 10, 15, 19, 20	Schneider Electric	
2, 13, 21, 22, 26	ABB	
3, 5, 8, 17, 27	ABB	✔

Finally, the developed methods examine the risk of cyber attacks given a specified operating condition for the examined system, as shown in Figure 5.3. Depending on the operating state of the system, the impact of certain scenarios in each substation can vary significantly, based on the load distribution, the loading of transmission lines etc. This is an important consideration, as the impact of a cyber attack depends on the operating conditions of the system.

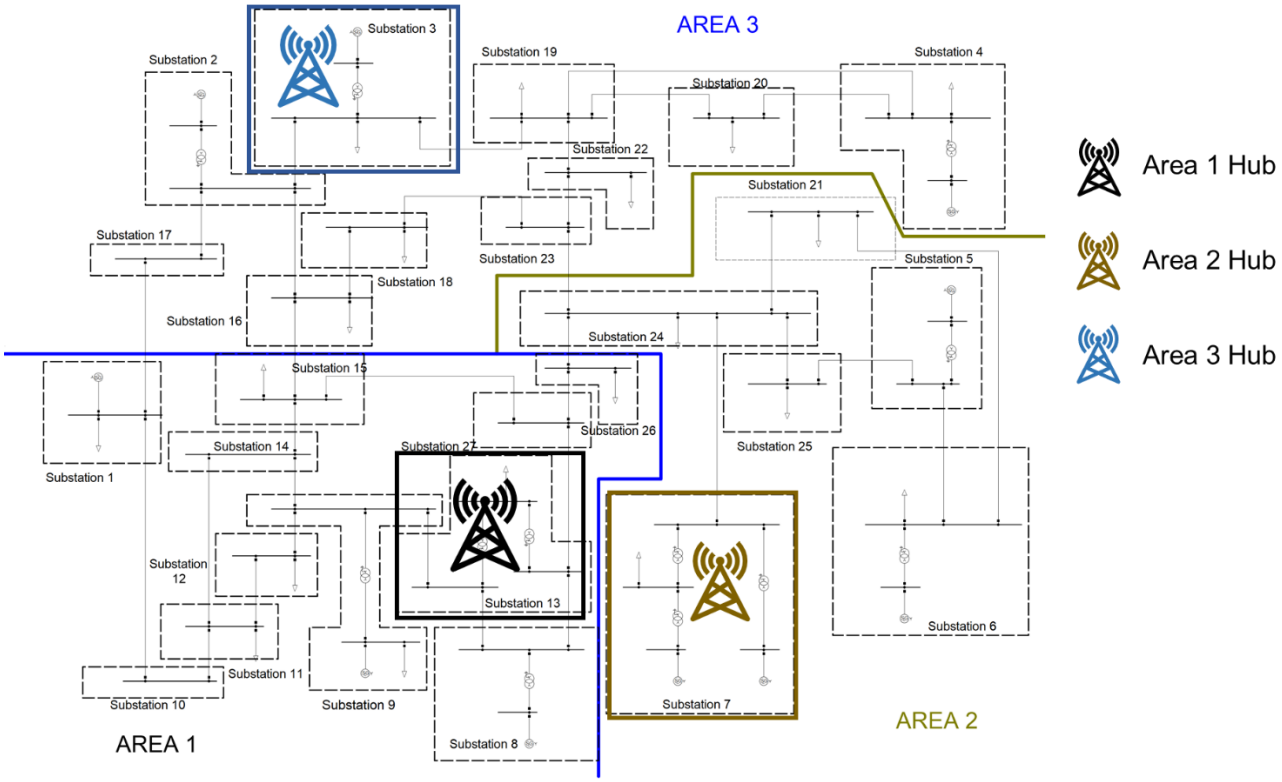


Figure 5.2. Specified hub substations for the IEEE-39 bus system.

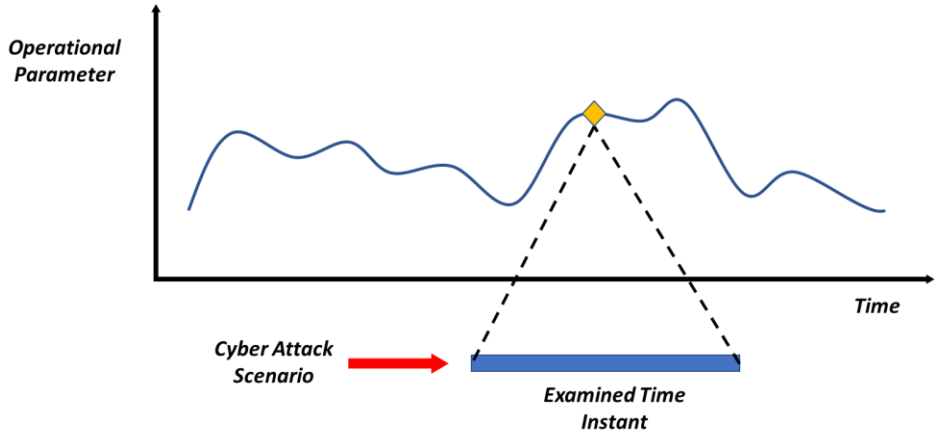


Figure 5.3. Examined time instance.

5.2. Scenario 1: Maliciously Injected Control Commands on Digital Substations

In the first scenario the attackers seek to jeopardize the operation of the power system, by targeting different assets of a digital substation. These assets are the circuit breakers of the transmission lines connected to a digital substation, the connected loads and the generators. In this scenario the following assumptions are made:

1. All the line circuit breakers of a substation, are assumed to be controlled by a single IED. Similarly, the total load of a substation can be disconnected by opening a single breaker.
2. The protection and control settings of the generating units can be targeted through the IEDs and the local controllers of a digital substation. Additional assets that could be included in the attack graph, to represent a power plant were out of the scope of this thesis, due to added complexity.
3. The impact on the communication system is assumed to be negligible, as the commands issued are not affecting the network traffic. Additionally, the substations are considered to have additional generating units such as batteries or Uninterruptible Power Supply (UPS) systems, which can support the communication network and the devices in the substation even in a case of an outage.

As it is specified in the previous chapter, no remedial actions will be taken from the grid operators. In this scenario, three variations are considered:

- Coordinated opening of all line breakers,
- Individual load disconnection, by opening the circuit breaker of the targeted substation,
- Disconnection of individual power plants, by opening the circuit breakers of the targeted substation.

5.2.1. Coordinated opening of all line breakers

In the first variation of the examined scenario, the attackers issue trip commands to the circuit breakers of the connected transmission lines in a digital substation. The lines are disconnected simultaneously, disconnecting the targeted substation from the main grid. The reasoning of the attackers is that to maximize the impact of their attack, they cause a N-k contingency. This scenario was inspired by the Industroyer attack that took place on Ukraine in 2016. For each digital substation, the equipment vendors are assigned randomly. The results from the likelihood analysis for each substation are summarized in Table 18.

Table 18. Likelihood assessment using the calculated TTC.

Substations	Entry Point	Target	$TTC_{avg}(days)$	Likelihood
9, 12, 14	WAN	CircuitBreakers	26	0.35
4, 11, 16, 23, 25			16	0.47
1, 18, 24			20	0.41
6, 7, 10, 15, 19, 20			15	0.48
2, 13, 21, 22, 26			16	0.47
3, 5, 8, 17, 27			39	0.26

The entry point in this scenario is considered to be the WAN. The TTC is calculated based on the shortest path algorithm, assuming that the attacker will choose the most effective way to reach the target. The time that is needed to develop additional tools for their attack phase is omitted. The generated attack paths for this scenario are given in Figure 5.4. As it can be seen, in the case of an unpatched controller, the attackers are able to compromise the control server and issue trip commands. In the case of a patched controller, the attackers can perform the attack by compromising either the IED or the operator console to open the circuit breakers through the GUI.

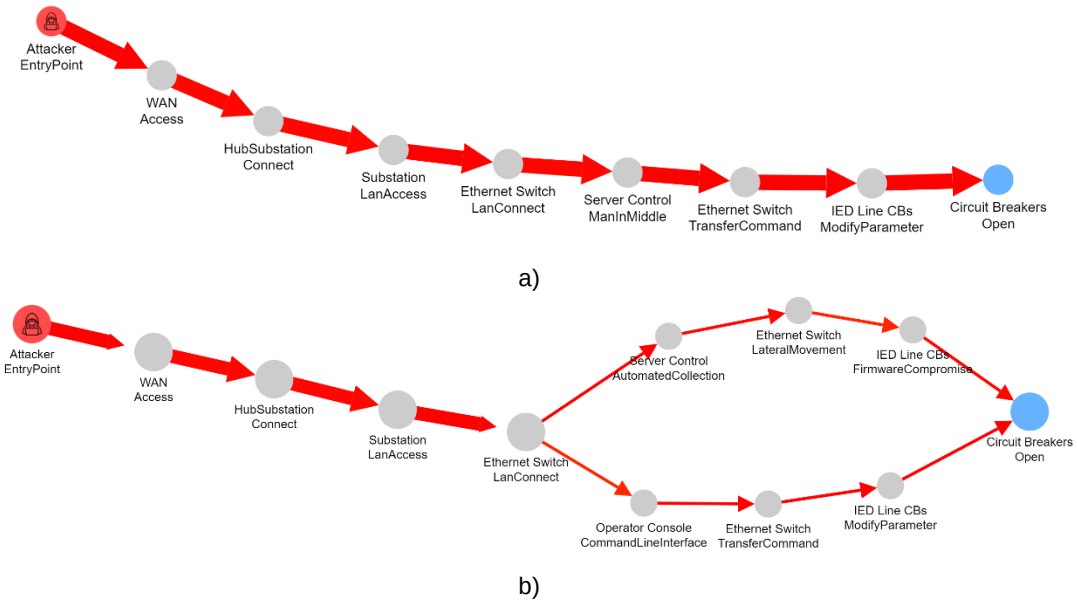


Figure 5.4. Generated attack paths for scenario 1.1 a) unpatched and b) patched controller.

The operation of the system is assumed to be steady at the time of the attack, which occurs at 5 seconds. The simulation run time varies, depending the substation attacked. The main reason for this is that due to the cascading failures that can occur, the set of non-linear equations cannot be solved after a certain time, causing the simulation either to progress extremely slowly or to crash. This behavior is mostly observed in cases where the grid is severely affected, thus the impact can be assessed within the selected time t_{sim}. The risk assessment results of scenario 1.1 are presented in Table 19.

Table 19. Risk assessment for cyber attacks on the line circuit breakers.

Substation	$t_{sim}[s]$	I_{Freq}	I_{Volt}	I_{Load}	I_{comp}	I_{ph}	I_{cyb}	F_{Rest}	Likelihood	Risk
1	60	0.29	0.2	0.28	0	0.62	0	1	0.41	0.25
2	**60**	**90.35**	**18.95**	**18.16**	**0.93**	**91.64**	**0**	**1.39**	**0.47**	**59.87**
3	60	10.09	1.19	1.84	0.04	8.5	0	1.03	0.26	2.28
4	60	11.25	1.41	3.8	0.02	11.06	0	1.05	0.47	5.46
5	60	11.16	1.3	3.19	0.04	10.5	0	1.04	0.26	2.84
6	60	10.08	1.18	1.86	0.04	8.51	0	1.03	0.48	4.21
7	60	11.1	0.3	2.69	0.02	8.76	0	1.03	0.48	4.33
8	60	11.17	1.18	3.21	0.07	10.62	0	1.04	0.26	2.87
9	25	60.11	13.13	11.72	0.67	61.65	0	1.23	0.35	26.54
10	60	0.18	0.58	0.06	0.02	0.94	0	1	0.48	0.45
11	60	1.17	0.73	1.19	0.02	2.71	0	1	0.47	1.27
12	**25**	**90.06**	**19.97**	**18.25**	**1**	**93.25**	**0**	**1.39**	**0.35**	**45.37**
13	60	11.14	2.77	4	0.13	13.64	0	1.04	0.47	6.67
14	29	20.86	5.2	5.8	0.33	24.69	0	1.07	0.35	9.25
15	60	1.12	0.74	1.23	0.04	2.96	0	1	0.48	1.42
16	60	0.81	0.6	1.06	0.04	2.5	0	1	0.47	1.18
17	60	0.16	0.55	0.02	0.04	1.09	0	1	0.26	0.28
18	60	0.24	0.59	1.07	0	1.79	0	1	0.41	0.73
19	60	10.63	2.24	3.12	0.11	11.75	0	1.05	0.48	5.92
20	60	0.41	0.58	1.04	0.02	2.04	0	1	0.48	0.98
21	60	21.02	2.85	4.92	0.11	19.37	0	1.07	0.47	9.74
22	60	0.57	0.63	1.13	0	2.04	0	1	0.47	0.96
23	60	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
24	60	30.83	3.96	6.41	0.22	27.95	0	1.1	0.41	12.61
25	60	21.16	2.99	5.09	0.11	19.75	0	1.07	0.47	9.93
26	60	0.63	0.67	1.18	0.02	2.38	0	1	0.47	1.12
27	29	90.23	19.97	18.23	1	93.32	0	1.39	0.26	33.73

The impact assessment results of the coordinated attacks are presented in Figure 5.5. In the x-axis the ID of each modelled substation is given while on the y-axis the $I_{ph} * F_{Rest}$ for each scenario is portrayed. From the simulation results it is found that an attack on substations 2, 9, 12, and 27, could initiate cascading failures in the system, resulting in a partial or complete blackout. In Figure 5.6, the associated risks are calculated based on the equation presented in the previous chapter (Equation 4.16). As it can be seen, by considering the vulnerability assessment from the attack graph, we are able to identify the most vulnerable substations for a given attack scenario. Although an attack on substations 9 and 27 could pose a significant threat to the CPS operation, the likelihood of such an attack to occur is low. On the other hand, substations 2 and 12 are identified as critical, as a potential attack could result in major outages with a higher likelihood for the attackers to compromise the system.

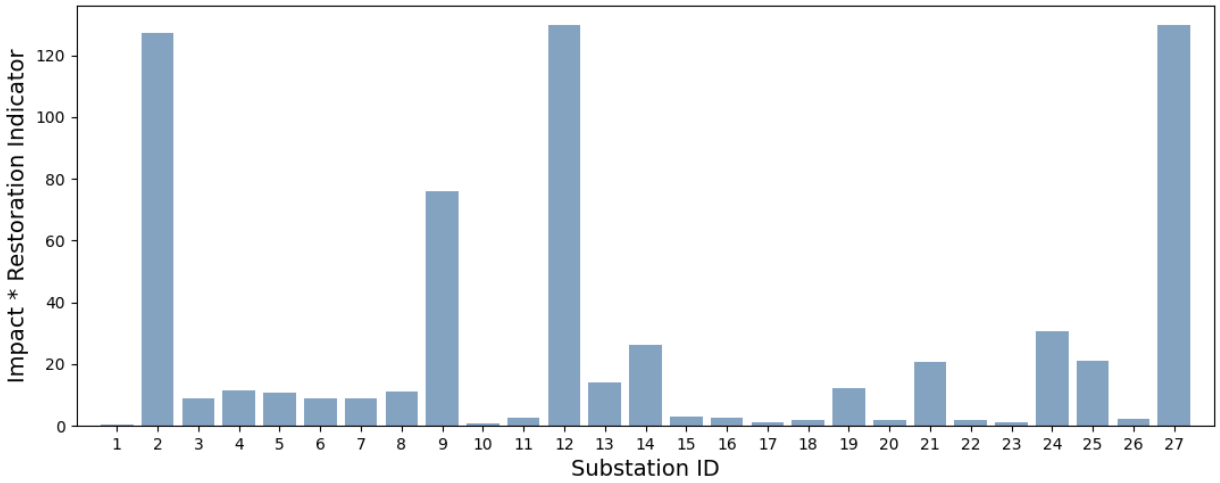


Figure 5.5. Impact assessment of opening all line breakers, per substation.

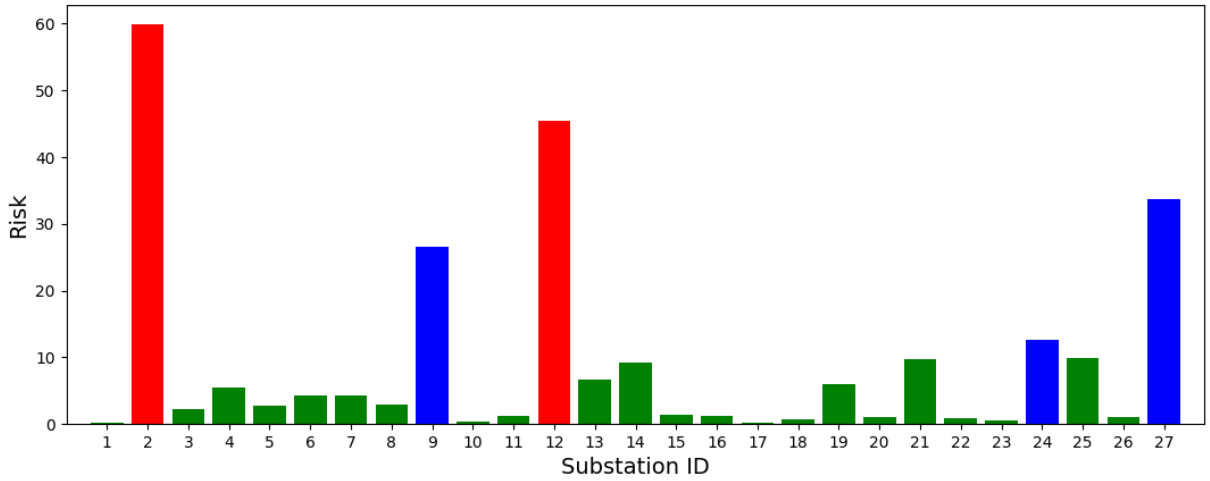


Figure 5.6. Risk assessment of opening all line breakers, per substation.

As an example, we will examine the cascading failures in two substations, one with a relatively medium impact such as substation 24 and one with a high impact such as substation 27. Their sequence of events is given in Table 20 and Table 21 respectively. Additionally, the de-energized components can be seen in Figure 5.7 and Figure 5.8, for each case respectively.

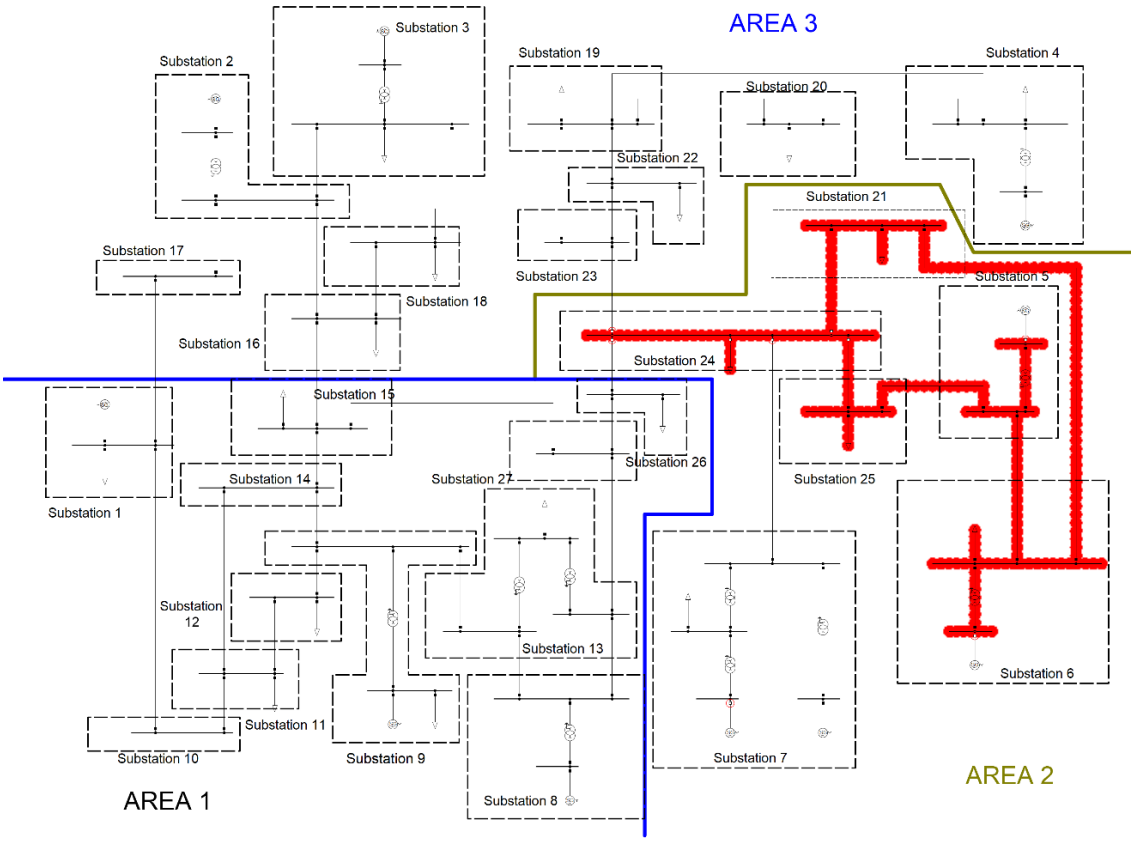


Figure 5.7. De-energized part of the grid, for cyber attack on substation 24.

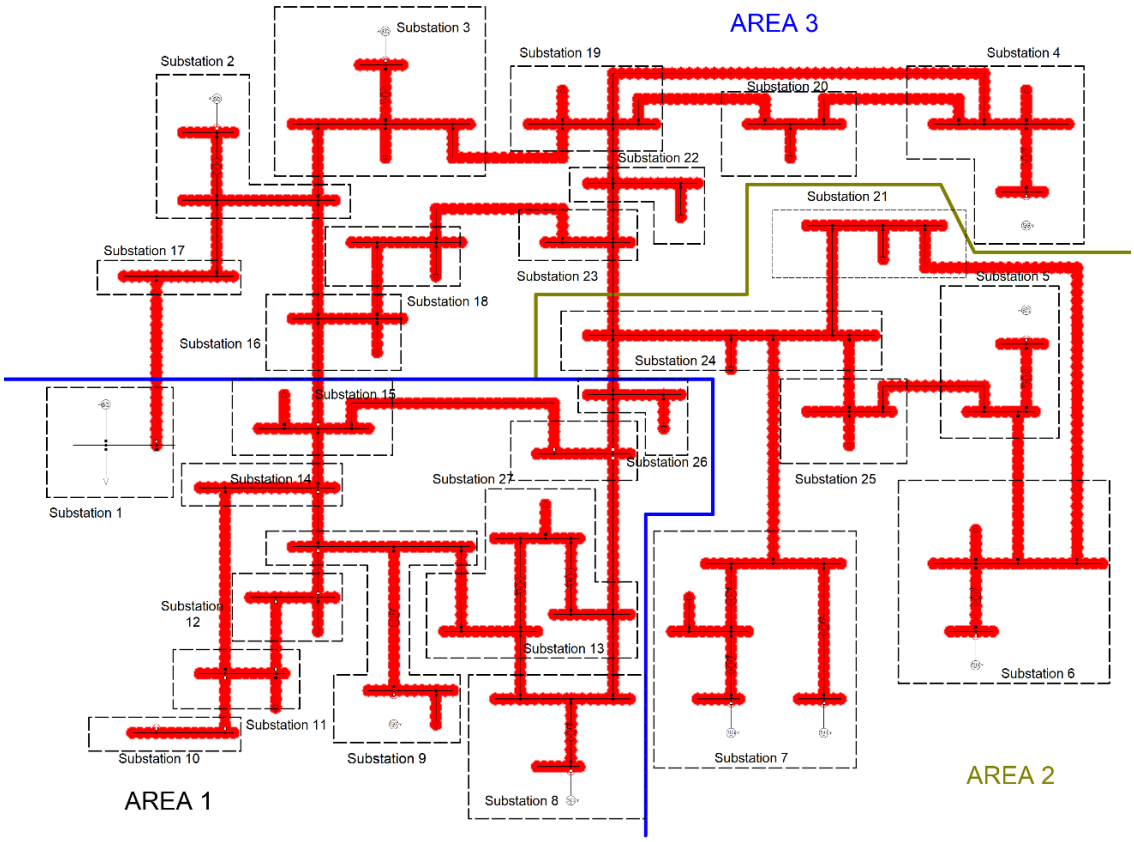
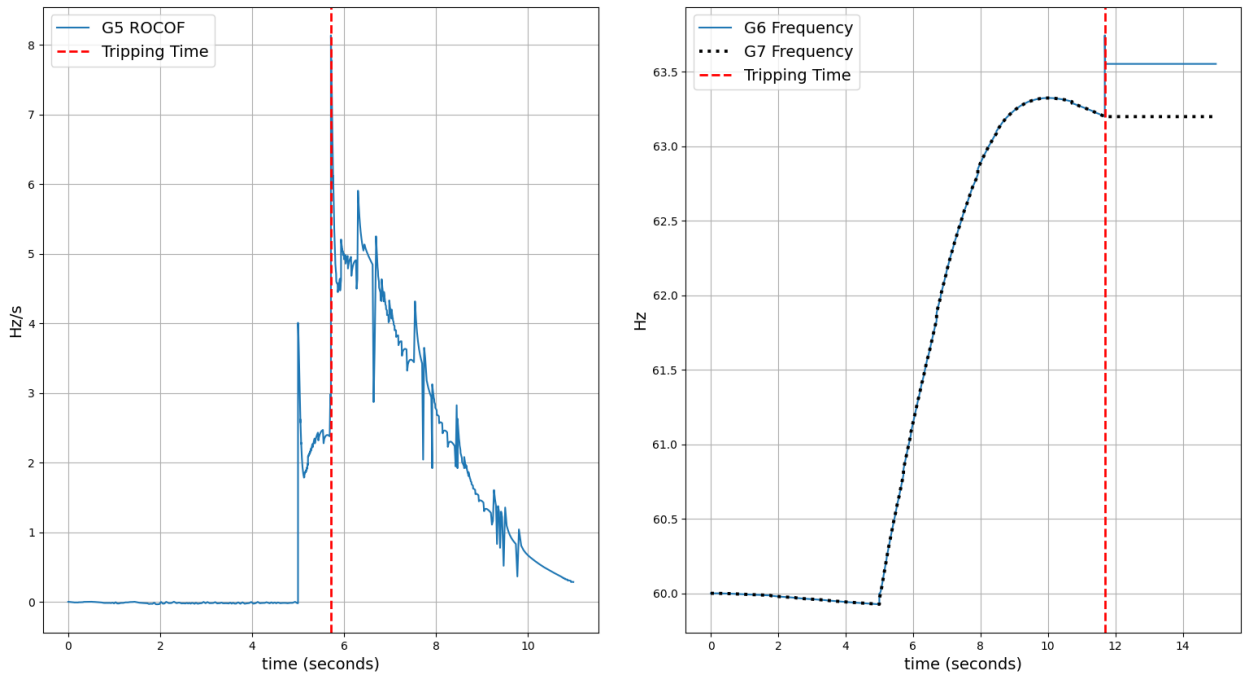


Figure 5.8. De-energized part of the grid, for cyber attack on substation 27.

In the case of an attack on Substation 24, the entire Area 2 is disconnected from the main grid as a result of the attack. Two islands of operation are formed; a) one comprising of generators G4 and G5 supplying Load 20, and b) one consisting of generators G6 and G7 supplying Loads 21, 23 and 24. In the first island, due to the mismatch between generation and consumption, the frequency of generator G5 rises with a high rate, thus tripping the ROCOF protection. This can be seen in Figure 5.9 a), where the trip event is highlighted with the red line. On the second island, as the load demand is limited, the frequency of generators G6 and G7 rises significantly, thus leading to their disconnection by the over frequency protection. This can be seen in Figure 5.9 b). Finally, the rest of the system is stabilized, through the activation of the under-frequency load shedding protection, which decreases the loads by 5.9 and 5.3%.

Table 20. Sequence of events for cyber attack on Substation 24.

Time (seconds)	Event
0	Start of simulation.
5	**Cyber attack on the substation 24. Trip commands are issued simultaneously on all line breakers, disconnecting the substation from the system.**
5.716	Generator G5 trips due to ROCOF protection.
11.687-11.697	Generators G6 and G7 trip due to the over frequency protection. G6 and G7 formed an island of operation, where the load demand was limited. Thus, their frequency increased tripping their over frequency protection.
13.076 – 14.438	The UFLS of all the remaining loads activates, decreasing the loads by 5.9 and 5.3%.



a) b)

Figure 5.9. Attack on substation 24 a) G5 ROCOF and b) G6 and G7 frequency.

In the case of substation 27, the trip commands issued cause the disconnection of Area 1 from Area 2. The increased currents through the interconnection between Areas 1 and 3, cause the tripping of the distance relays in other substations, as seen in Figure 5.10 a). As more lines are disconnected,

generators G2 and G3 are islanded by the majority of loads and as a result their frequency is increased, activating their ROCOF protection, as shown in Figure 5.10 b). As Area 1 is disconnected, the UFLS protection decrease gradually the active power of all loads of the system, as shown in Figure 5.10 c). This causes the frequency of the interconnected system to increase, and after nearly 10 seconds the remaining generators are disconnected due to over-frequency protection, which is shown in Figure 5.10 d).

Table 21. Sequence of events for cyber attack on Substation 27.

Time (seconds)	Event
0	Start of simulation.
5	**Cyber attack on the substation 27. Trip commands are issued simultaneously on all line breakers, disconnecting the substation from the system.**
6.568 - 8.587	Multiple lines in the vicinity of the first attack location are tripped by distance protection, i.e., lines 05-06, 06-07, 07-08.
8.587	Generators G2 and G3 are disconnected by ROCOF protection.
12.722 - 15.587	Load shedding on all system's loads. Loads are gradually decreased by 6.7, 6.5, 5.9 and 5.3%.
16.445 - 18.132	The remaining lines in Area 1 are disconnected, due to distance protection.
25.045 - 25.146	The increased system frequency, causes all generators of the system to disconnect, leaving only the external grid operating.

By examining the results of the risk assessment, the main findings were the following:

- In the case of substation 24, three generators trip but the overall system is stabilized due to the load shedding, and the impact is limited. On the other hand, in the case of substation 27, the cascading failures initiated by the cyber attack, result in a blackout. Apart from the external grid and Load 39, the rest of the system is lost.
- Substation 2 is identified as the most vulnerable and critical asset of the power system. This is expected, as substation 2 has an unpatched controller and as a result, the likelihood of a successful attack is increased. On the other hand, substations 12 and 27 can still be considered critical as their potential impact is very high.

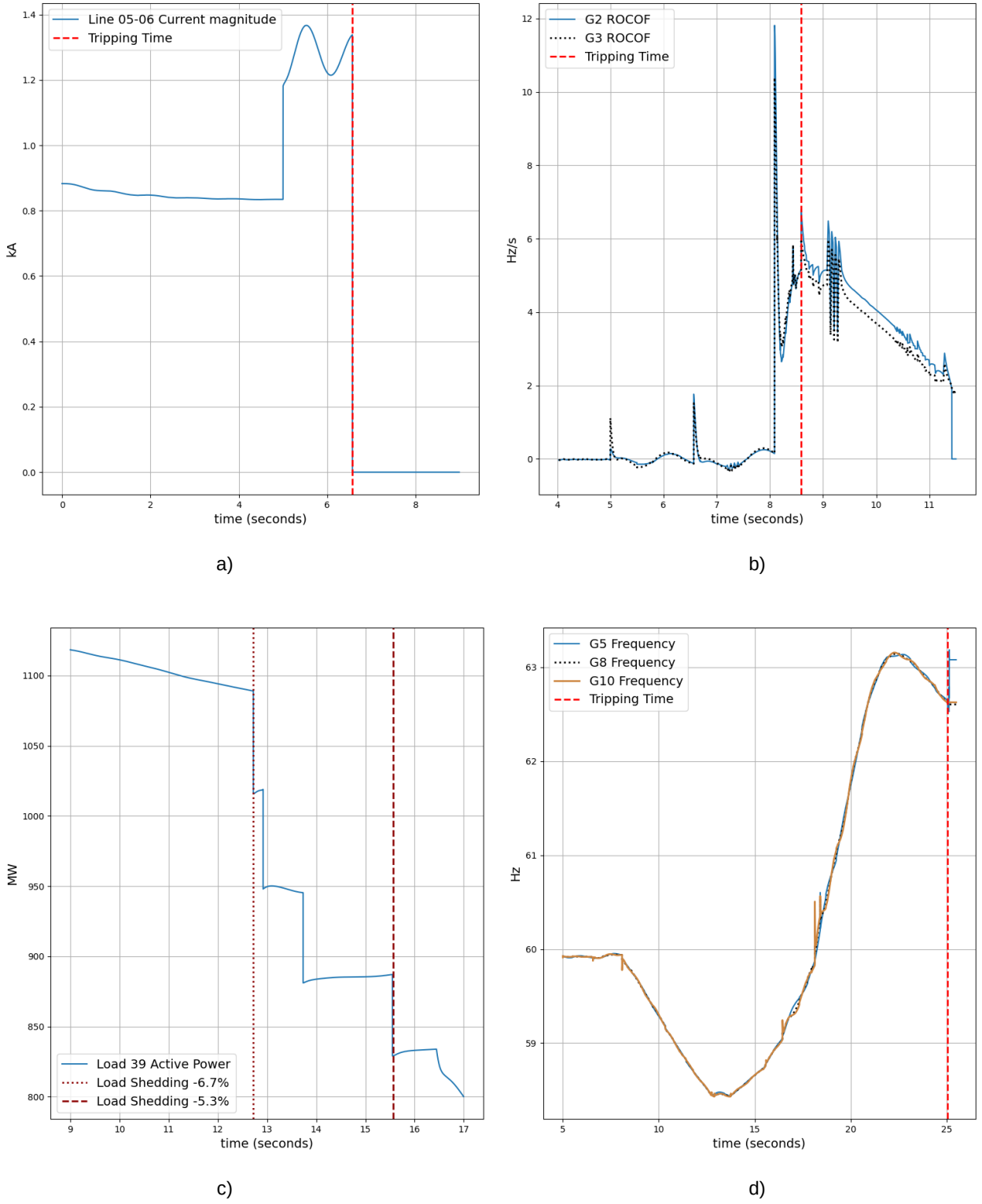


Figure 5.10. Attack on Substation 27 a) distance protection tripping, b) G2 and G3 ROCOF protection and c) load shedding, and d) over frequency protection.

5.2.2. Disconnection of loads and generating units

In this scenario variation, the attackers target a) the individual loads that are controlled by the targeted substation and b) the individual generating units connected to the substations. In the examined model there are 20 loads distributed in various substations, while substations 1 to 9 are controlling the various power plants of the system. In Table 22 the results of the risk analysis for individual attacks on the load of each substation are presented.

Table 22. Risk assessment of cyber attacks on the loads of substations.

Substation	t_{sim} [s]	I_{Freq}	I_{Volt}	I_{Load}	I_{comp}	I_{ph}	I_{cyb}	F_{Rest}	Likelihood	Risk
1	**18**	**100**	**20.49**	**19**	**1**	**99.49**	**0**	**2.72**	**0.41**	**110.95**
3	60	0.45	0.07	1.07	0	1.36	0	1	0.26	0.35
4	60	0.64	0.05	1.05	0	1.42	0	1	0.47	0.67
6	60	21.34	2.42	5.2	0.11	19.38	0	1.07	0.48	9.95
7	60	21.02	2.3	3.74	0.09	17.41	0	1.07	0.48	8.94
9	60	0.17	0.02	1.01	0	1.12	0	1	0.35	0.39
11	60	1.17	0.27	1.23	0	2.08	0	1	0.47	0.98
12	60	0.4	0.14	1.12	0	1.46	0	1	0.35	0.51
13	60	0.22	0.09	1.06	0	1.27	0	1	0.47	0.60
15	60	1.11	0.27	1.24	0	2.07	0	1	0.48	0.99
16	60	0.73	0.1	1.1	0	1.56	0	1	0.47	0.73
18	60	0.24	0.07	1.08	0	1.27	0	1	0.41	0.52
19	60	0.2	0.05	1.06	0	1.21	0	1	0.48	0.58
20	60	0.4	0.05	1.05	0	1.3	0	1	0.48	0.62
21	60	0.75	0.05	1.05	0	1.47	0	1	0.47	0.69
22	60	0.57	0.13	1.13	0	1.55	0	1	0.47	0.73
24	60	0.74	0.1	1.1	0	1.57	0	1	0.41	0.64
25	60	0.56	0.11	1.11	0	1.5	0	1	0.47	0.71
26	60	0.63	0.19	1.18	0	1.68	0	1	0.47	0.79

On one hand, based on the results portrayed in the table above, it can be seen that most cases of load disconnection result in minor impact on the operation of the power grid. Disconnecting the load of either substations 6 or 7 results in the eventual disconnection of two generating units, but the overall system remains intact. For nearly all other cases, the impact is negligible.

In contrast, the disconnection of the load in substation 1 results in a blackout, with a risk index of over 100. As the entire grid is disconnected, the restoration effort required will be maximum according to the proposed factor. The reason for this blackout is that the load connected to substation 1 accounts for 22% of the total load of the system. This can be regarded as a special case, as substation 1 is connected both to the external grid and the largest load of the system. As a result, by disconnecting its load, the overall frequency of the system is increased. This is shown in Figure 5.11 where the frequency of generators G1 (external grid), G2 and G3 are given. The attack time, the tripping time, as well as the threshold value of 61.8 Hz are highlighted.

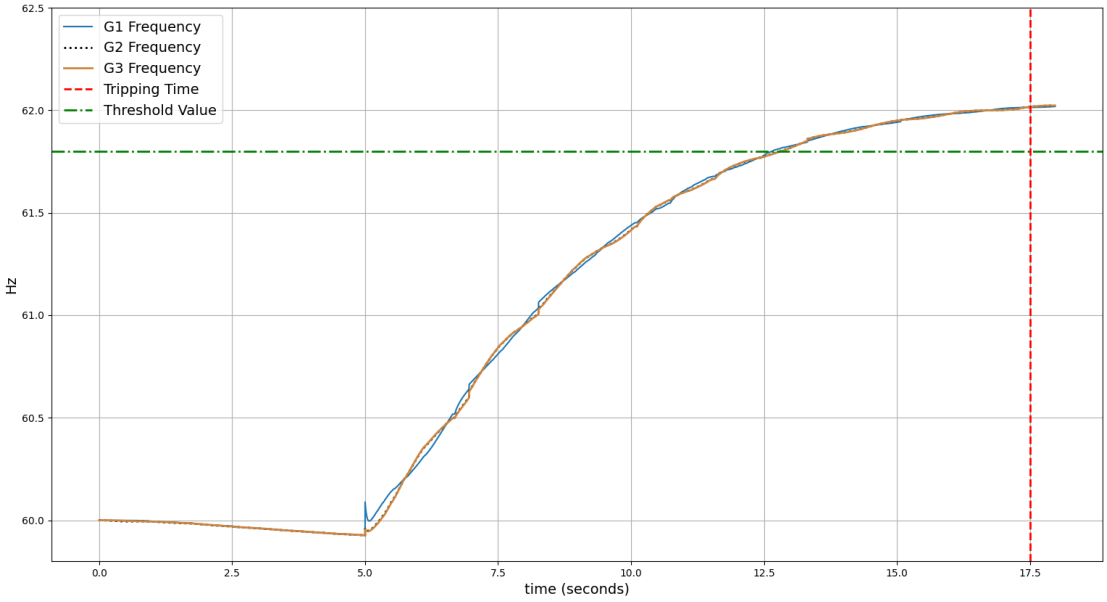


Figure 5.11. Over frequency protection, for cyber attack on substation 1.

Similarly, in the second case the attackers inject false control commands to the breakers of the generators. Each substation is connected to a generating unit by a single circuit breaker. The risk assessment is shown in Table 23, while the sequence of events for the case of disconnection of the external grid is shown in Table 24. Overall, it can be seen that by disconnecting individual generators, the attackers will not be able to severely affect the system. In most cases, only the targeted substation is affected and as it can be seen by the individual indices for loss of load and for the voltage deviation (I_{Load}, I_{Volt}), the impact is limited. An exception is the attack on substation 1, where the disconnection of the external grid results in a blackout.

Table 23. Risk assessment of disconnection of each generating unit.

Generator	t_{sim} [s]	I_{Freq}	I_{Volt}	I_{Load}	I_{comp}	I_{ph}	I_{cyb}	F_{Rest}	Likelihood	Risk
1	**11**	**100**	**20.49**	**19**	**1**	**99.49**	**0**	**2.72**	**0.35**	**94.71**
2	60	10.72	0.1	2.57	0	8.03	0	1.03	0.41	3.39
3	60	11.17	0.18	3.21	0.02	9.18	0	1.04	0.26	2.48
4	60	11.17	0.29	3.12	0.02	9.21	0	1.04	0.47	4.50
5	60	10.46	0.2	2.02	0.02	7.67	0	1.03	0.47	3.71
6	60	11.14	0.26	3.16	0.02	9.21	0	1.04	0.26	2.49
7	60	11.36	0.31	3.1	0.02	9.3	0	1.03	0.47	4.50
8	60	11.41	0.32	3.1	0.02	9.34	0	1.03	0.26	2.50
9	27	11.8	0.4	4.32	0.02	10.84	0	1.05	0.47	5.35
10	60	10.07	0.07	1.01	0.02	6.33	0	1.03	0.45	2.93

In the examined operating condition, the external grid mainly supplies load 39, which is connected to the substation. As the external grid is disconnected, the frequency of the system is decreased because of the difference between the remaining generating power and the load demand. The remaining generators provide more power to the grid to cope with the reduced generation, thus increasing the loading of the transmission lines. The distance protection of line 21-22 is tripped, as the overloading of the lines is identified as a fault by the relay.

The UFLS protection is activated in all connected loads in order to stabilize the frequency of the system. Nevertheless, the frequency of the system continues to decrease, causing generators G2, G3, G4, G5 and G9 to be disconnected due to their under-frequency relays as shown in Figure 5.12. Finally, the remaining generators are unable to supply the load demand and as a result they are disconnected by increased ROCOF or under frequency protection.

Table 24. Sequence of events for disconnection of external grid.

Time (seconds)	Event
0	Start of simulation.
5	**Cyber attack on the substation 1. External grid is disconnected by opening the circuit breaker.**
7.821	Line 21-22 trips due to distance protection, due to extensive overcurrent.
8.021 - 8.695	Load shedding on all the loads. Loads are gradually decreased by 6.7, and 6.5%.
9.341	Line 23-24 trips due to distance protection, due to extensive overcurrent.
9.508	Generators G2, G3, G4, G5 and G9 disconnect due to under frequency protection.
9.689 - 10.711	Additional load shedding. Generators G6, G7, G8 are disconnected due to ROCOF protection. Generator G10 disconnects due to under frequency protection. Entirety of the power system is de-energized.

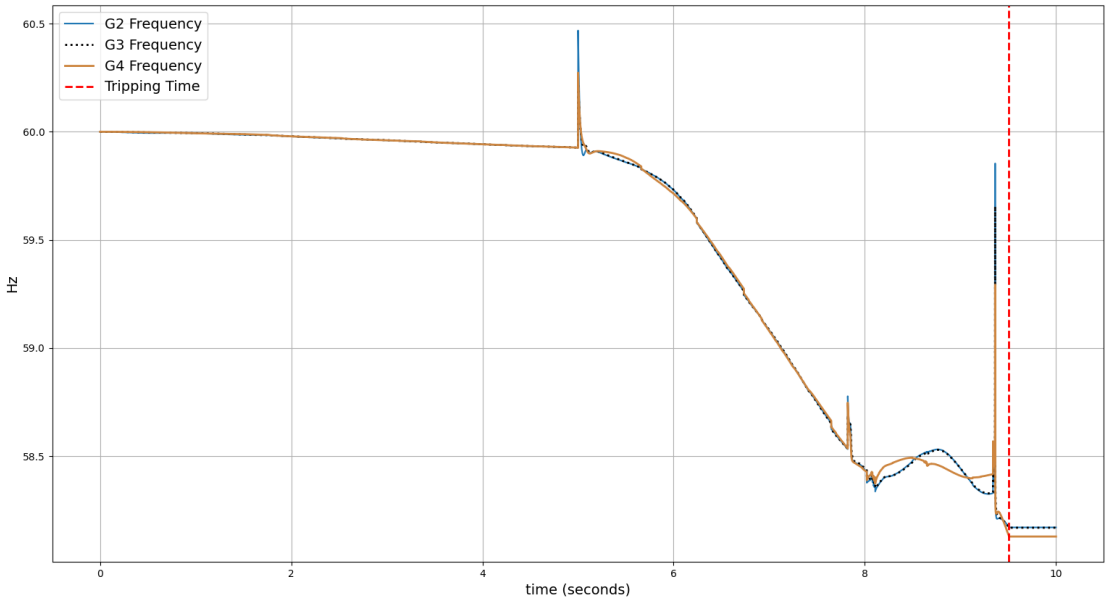


Figure 5.12. Under frequency protection for cyber attack on external grid.

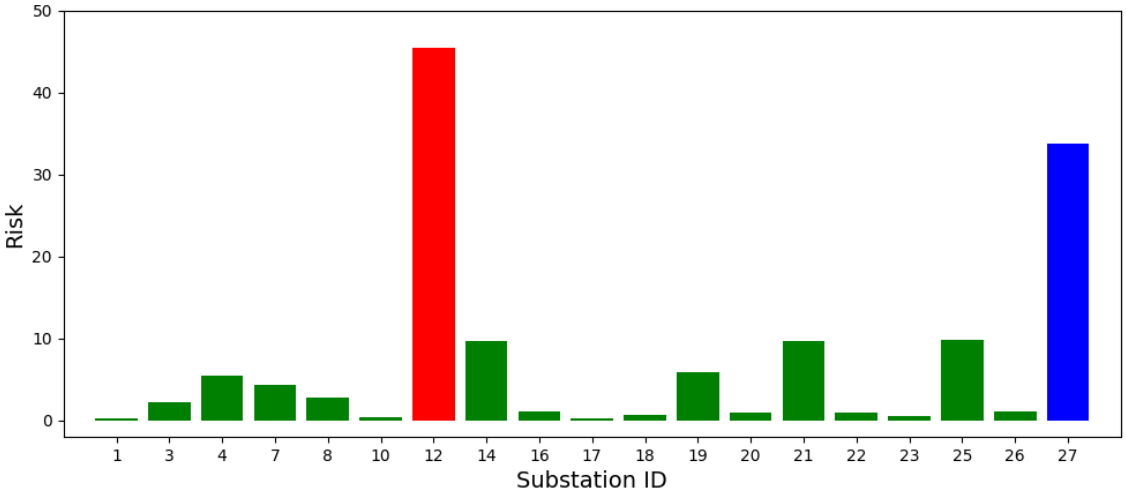
As it can be seen from the results presented above, the disconnection of most of the loads and generators results in a minor risk for the operation of the system. On the other hand, an attack on critical assets such as the external grid, or the disconnection of the largest load of the system, could result in a blackout. From this analysis, substation 1 is identified as a critical asset because of the importance of the connected external grid and critical load.

5.3. Scenario 2: Coordinated Opening of Line Breakers, under Different Switching Sequences

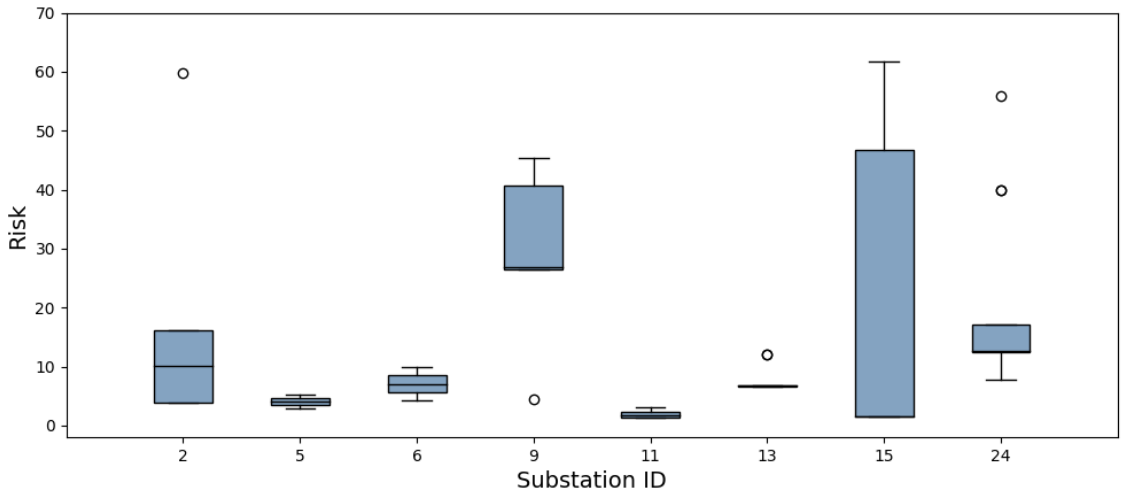
As each substation has a number of transmission lines connecting it to the rest of the power grid, we perform a sensitivity analysis considering different cyber attack switching sequences. Based on the size of the substations the possible switching scenarios are the factorial of the number of circuit breakers present in the substation i.e., $N_{scenarios} = N_{breakers}!$. For example, substation 14 has two connections, with substations 1 and 2 respectively, thus two possible sequences of attack (CB1-CB2, CB2-CB1). On the other hand, substation 24 has a total of 5 connected transmission lines, thus $5! = 120$ possible combinations of different opening sequences. We consider that each sequence of attack on the substations have the same probability of occurrence. The time interval between each breaker opening is chosen to be 2 seconds.

By performing this analysis, the different variations of the impact can be examined. By utilizing the Python API of PowerFactory to automate the simulations, all possible combinations were studied. The results of the risk assessment for all cases are presented in detail in Appendix C. The analysis showed the following:

- By attacking certain substations, the impact on the operation of the power system is the same, regardless of the switching sequence. For instance, substation 12 is still identified as a critical substation, as all examined cases resulted in a high impact. The risk scores for these substations are given in Figure 5.13 a). As it can be seen, these results are the same as with Scenario 1.1.
- On the contrary, the impact of a cyber attack on eight substations can vary significantly depending the opening sequence, as shown in the box plot in Figure 5.13 b). In the box plots for each substation, the interquartile range of the can be seen with the blue box. The spread of the risk scores can be seen by the whiskers, while the outliers for some cases are represented in circles.



a)



b)

Figure 5.13. Risk assessment for different opening sequences a) substations with no variations and b) substations with variations.

Outliers can be seen in substations 2, 9, 13 and 24. These are cases, where the assessed risks are numerically distant from the rest of the data. For substation 2 it is shown that from six different variations only one will result in a severe impact. Additionally, substations 15 and 24 are identified as potential critical targets, as certain switching sequences result in a blackout. Substation 15 is the most critical of these two, as more cases could result in major impact.

For substation 24 there are 120 different sequences of switching attacks. The ID of each breaker of this substation is shown in Figure 5.14. In Table 25, a set of results for the risk assessment are given for this substation. From 120 attack sequences, 117 have a relatively small impact, resulting in a lower risk while three cases resulted in major outages. This can be also seen in the box plot above, as these three cases are shown as outliers.

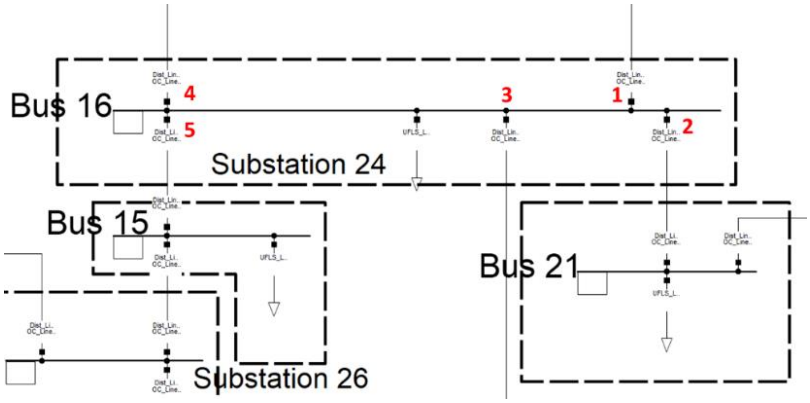


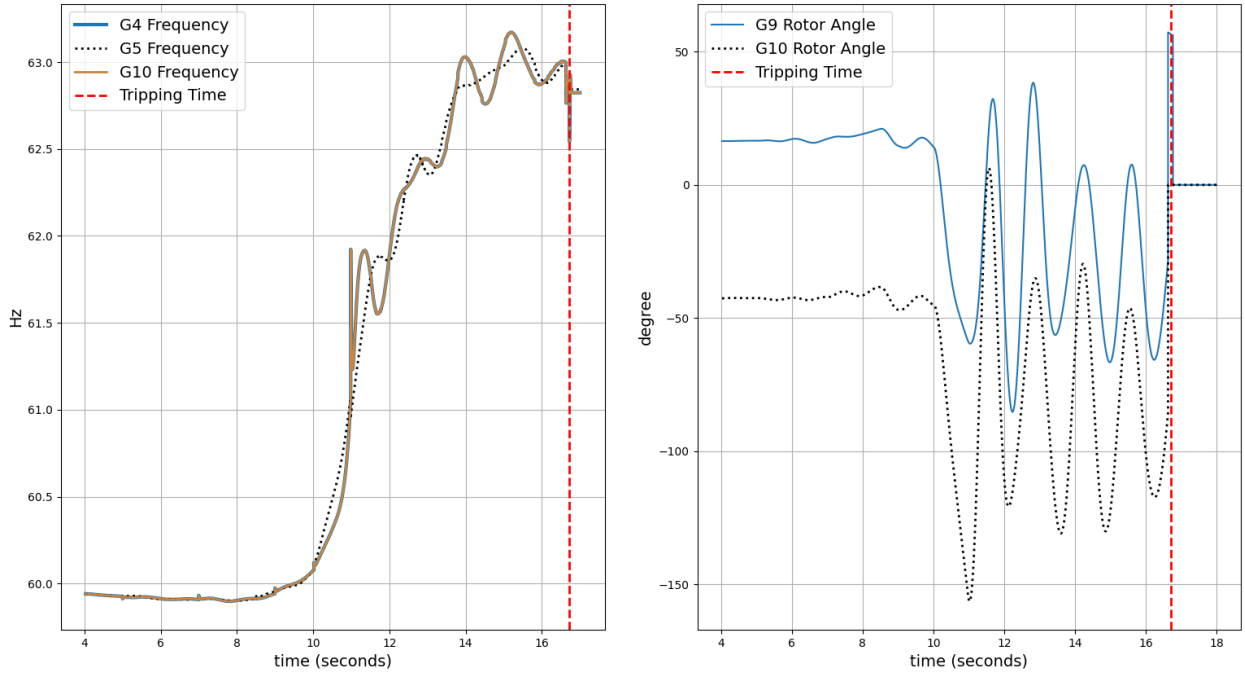
Figure 5.14. ID of each circuit breaker in substation 24.

Table 25. Risk assessment results for substation 24.

#	Sequence	I_{Freq}	I_{Volt}	I_{Load}	I_{comp}	I_{ph}	I_{cyb}	F_{Rest}	$Likelihood$	$Risk$
1	4,3,5,1,2	60.52	11.22	12.42	0.67	60.64	0	2.25	0.41	55.94
2	4,3,2,1,5	70.53	15.38	15.37	0.89	74.93	0	1.3	0.41	39.94
3	4,3,2,5,1	70.53	15.38	15.37	0.89	74.93	0	1.3	0.41	39.94
4	2,5,1,4,3	40.56	6	7.36	0.26	36.25	0	1.15	0.41	17.10
…	…	...	...	...	...	...	...	...	...	…
119	2,4,3,5,1	20.9	1.37	4.45	0.13	17.58	0	1.07	0.41	7.71
120	3,4,2,5,1	21.34	1.31	4.41	0.13	17.69	0	1.06	0.41	7.69

Although each case is assumed to have the same probability of occurrence, the attackers need to identify the most effective way to target this particular substation. An additional observation is that even though the first sequence has a lower impact index compared to sequence two and three (I_{ph}), it has a higher overall risk. The reason is due to the inclusion of the restoration factor. In the first case, the external grid is also disconnected which accounts for nearly 58% of the total installed capacity of the examined power system. As a result, the restoration effort required for this particular case is assessed to be significantly higher.

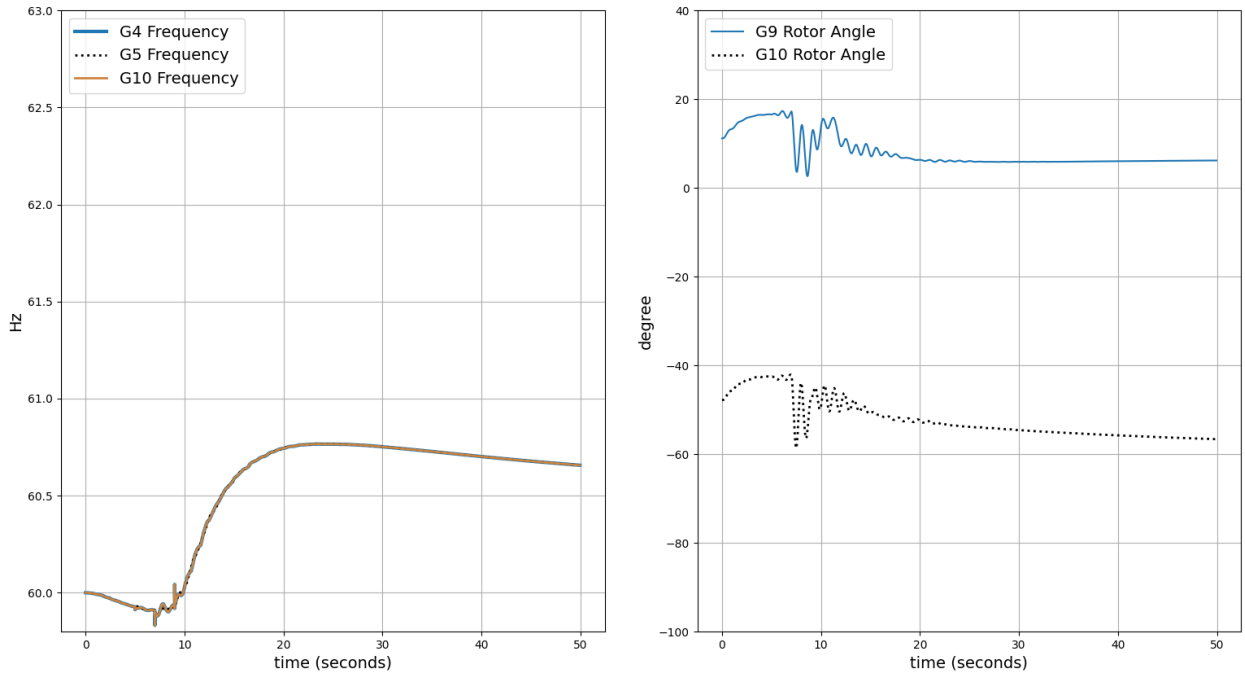
Additionally, an attack on substation 15 can result to two extreme cases; a very low impact and a major one. For the major impact attack, after the opening of the first two breakers the distance relays of the nearby lines are tripped, due to the increase of the current magnitude. This occurs as the power flow in the network is re-distributed in order to supply the remaining connected loads. As the other breakers open, the system becomes unstable as the grid is split into two areas of operation. The grid becomes fragmented into different operating islands, with different frequencies. The frequency on areas 2 and 3 are shown in Figure 5.15 a). Additionally, the generators become unstable, as shown in the oscillations of their rotor angles in Figure 5.15 b). The various generating units are disconnected by their frequency protection at 16.722 seconds, resulting in a blackout.



a) b)

Figure 5.15. Major impact on substation 15 a) frequency and b) rotor angles.

On the contrary, for certain opening sequences the impact is limited. As it can be seen in Figure 5.16 a) and Figure 5.16 b), the frequency of the system is quickly stabilized as well as the generators. The main difference is that in the examined sequence, the protection relays of the nearby lines did not trip, thus no cascading failures occurred.



a) b)

Figure 5.16. Minor impact on substation 15 a) frequency and b) rotor angles.

Overall, from this analysis it is shown that the attack sequence is an extremely important factor from the perspective of an attacker. Based on this assessment potential targets can be identified; although substations 15 and 24 were characterized as medium/low impact targets in scenario 1, it is shown

that a cyber attack could still result in a major outage. Thus, it is also required for grid operators to study and assess such scenarios.

5.4. Scenario 3: Distributed Denial-of-Service Attack on Substation Gateway

In this scenario, the attackers launch a DDoS attack on the gateway router of the digital substation. The goal of the attackers is to affect the monitoring and control capabilities of the system operators in the control center. By flooding the communication network, the transmission time of legitimate TCP packets between the control center and the substations is affected, causing the latency of communication links to increase. In this scenario, we examine the possible effects of such an attack considering two locations; an edge substation and a hub substation. On one hand, by analyzing the results of the dynamic simulations it is found that a DDoS attack on the gateway router has no impact on the operation of the physical power system, as the decentralized protection and control schemes are not affected by the increased communication delays between the control center and the substations. On the other, the monitoring and remote-control capabilities of the system operators are greatly affected, as the measurements and control commands are transmitted with increased delays. As a result, in this scenario we will only present the results regarding the communication network. In Figure 5.17 the topology of the simulated network is given, as well as the attack locations. In Table 26, the average TTC is computed for these two scenarios and the likelihood is assessed.

Table 26. Likelihood assessment for scenario 3.

Attack Scenario	Entry Point	Target	$TTC_{avg}(days)$	Likelihood
3.a	SubNetwork	Gateway	16	0.47
3.b	SubNetwork	HubGateway	22	0.38

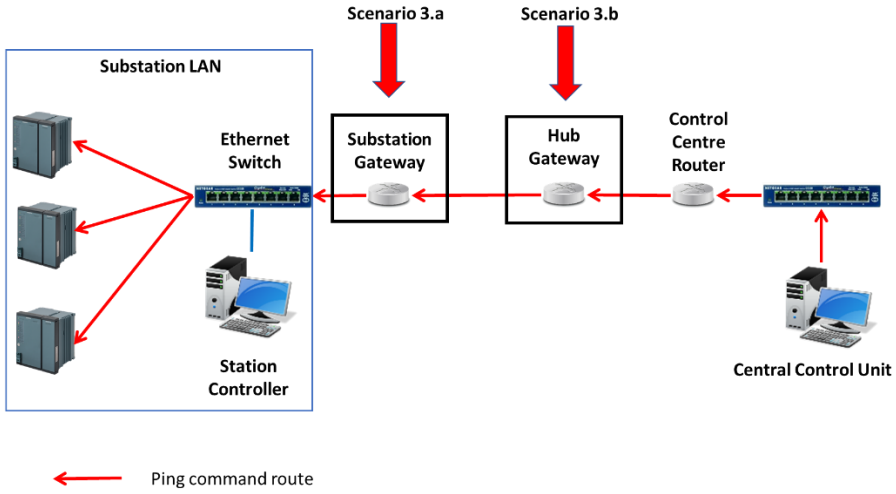


Figure 5.17. Mininet topology and DDoS scenarios.

The power system measurements are collected using the OPC UA interface of PowerFactory. These measurements are then transmitted using TCP/IP protocol, through the software-defined network created in Mininet, emulating the operating traffic. The attacks are launched in Mininet using hping3 tool which is used for penetration testing. This tool supports TCP, UDP, ICMP and RAW-IP protocols, it has a traceroute mode and it can be used to launch a DoS attack. For each attack location, we used different time intervals between the generated traffic for the DoS. To measure the average RTT for each attack scenario and to assess the risk, hping3 is used to ping the edge devices in a digital substation, in this case the MUs, from the central control unit of the control center. The results of the DDoS attack on substation 5 and on the hub substation 7 are given in Table 27 and Table 28, respectively.

Table 27. Risk assessment of DDoS attack on gateway router of substation 5.

DDoS (packets/s)	Affected Substations	$RTT_{avg}[ms]$	I_{cyb}	I_{ph}	F_{Rest}	$Likelihood$	$Risk$
100	5	508	0.705	~0	1	0.47	0.33
200	5	6335	1.8	~0	1	0.47	0.85

Table 28. Risk assessment of DDoS attack on gateway router of hub substation 7.

DDoS (packets/s)	Affected Substations	$RTT_{avg}[ms]$	I_{cyb}	I_{ph}	F_{Rest}	$Likelihood$	$Risk$
200	5	525	4.33	~0	1	0.38	1.65
	6	515					
	7	620					
	21	500					
	24	485					
	25	520					
333	5	5032	10.32	~0	1	0.38	3.92
	6	4980					
	7	5300					
	21	5500					
	24	4850					
	25	5120					

The effect of the DDoS attack can be captured, using Wireshark. In Figure 5.18 a) the traffic on the gateway router of substation 5 is captured, and as can be seen the DDoS attack commences after 60 seconds. The attackers send 200 packets per second, resulting in a significant increase of the network latency. The attack results in an increase of the transmission delays by over 126%, as the average RTT is increased from 50 to 6335 milliseconds. This means that a corrective command from the control center that should be transmitted within 100 milliseconds, would now take 6 seconds to transmit.

In Figure 5.18 b), the DDoS attack commences in the router of the hub substation around 100 seconds, resulting in increased delays with all connected substations. By targeting a hub substation, the communication links of all substations in the attacked area are affected. As the router of the hub substation will have increased bandwidth limits, the maliciously injected packet rate volume must be sufficient to affect the system. The risk of such scenario is low, mostly because of the negligible impact on the physical system operation. Despite this, an attack with 333 packets/second could still severely affect the monitoring and control capabilities of the operators, as commands issued by the control center will be transmitted after 5 seconds.

A DDoS is one of the simplest forms of cyber attack to execute. On March 2019, an electric utility in Kern County, California and Converse County, Wyoming was targeted by a DDoS attack [69]. According to the Department of Energy, the attack did not disrupt electrical delivery, but caused interruptions in electrical system operations. The results presented above align with this real-world attack as the physical power system remained intact.

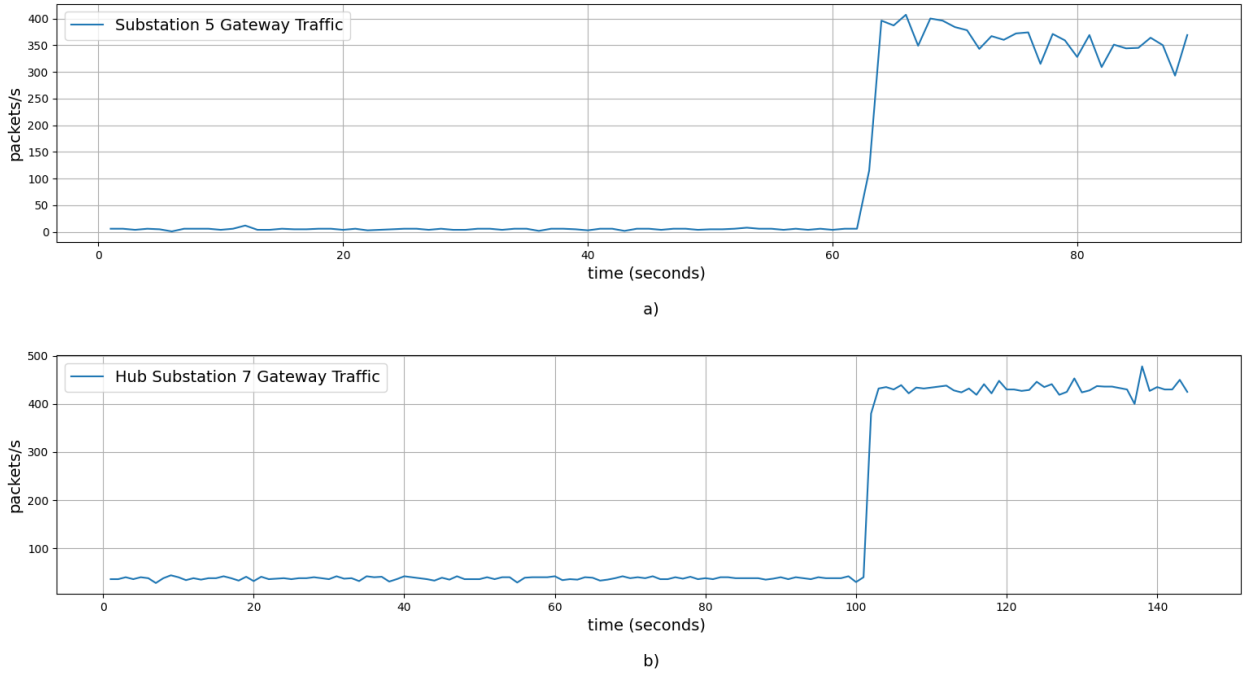


Figure 5.18. Traffic capture at a) gateway of substation 5, and b) gateway of hub substation 7.

5.5. Scenario 4: Coordinated Cyber-Physical Attack targeting two Substations

This scenario examines a coordinated attack on two digital substations. The attackers are assumed to have initial access to the LAN of a single substation, and by discovering its connections with the hub substation, they launch a coordinated attack on multiple substations in the system. They are considered to have excellent knowledge of the targeted grid topology and being capable of launching an attack by targeting the most critical connections of each substation, while at the same time they launch a DDoS attack on the gateway router of the hub substation. By affecting the communication link between the control center and the targeted substations, the system operators will not be able to effectively monitor or control the operation of the power system.

The examined case study was simulated using the CPS designed in this thesis:

- Through Mininet, the AVR voltage setting of generator G6 which is located to substation 5 is set from 1.05 to 1.9 p.u.,
- Using hping3 in Mininet a DDoS attack is initiated on hub substation 7, with 100 packets/second,
- Through Mininet, a trip command is sent to the line breaker connecting substation 7 with the rest of the grid.

The initial access point of the attackers on the network is considered to be the LAN of substation 5. The attackers are able to compromise the operator console, which enables them a) to tamper the control setpoints of voltage on the AVR of generator G6, and b) to access the WAN and compromise the gateway router of substation 7, which is the hub substation for Area 3. By accessing the LAN of substation 7, the attackers are able to perform a) a malicious attack on the IED controlling the circuit breaker of the transmission line of substation 7, and b) a DDoS on the gateway router of substation 7, affecting the communication between the control center and the hub substation.

This attack is not random, and the attack locations are chosen based on the topology of the grid and the criticality of the assets. The targeted circuit breaker disconnects a vital transmission line, which connects two generating units with the rest of the grid.

From the attack graph analysis, all targeted nodes were examined to determine the $TTC_{glob} = \max\{TTC_{S5}, TTC_{DoS}, TTC_{S7}\}$, where TTC_{S5} is the average time for compromising the voltage settings of the generator G6 located in Substation 5, TTC_{DoS} is the average time needed by the attackers to launch a DoS attack on hub substation 7, and TTC_{S7} is the average time needed for opening the circuit breaker of substation 7. Based on this, the average TTC is calculated based on $TTC_{avg} = \max\{29, 22, 30\}$. This means that although the attackers need on average 22 days to successfully launch a DDoS attack, more time is needed for the complete attack to commence. The attack path for this particular scenario is shown in Figure 5.19. The targets are highlighted in blue, while the various paths that the attackers can follow to reach their objectives are indicated by the red arrows.

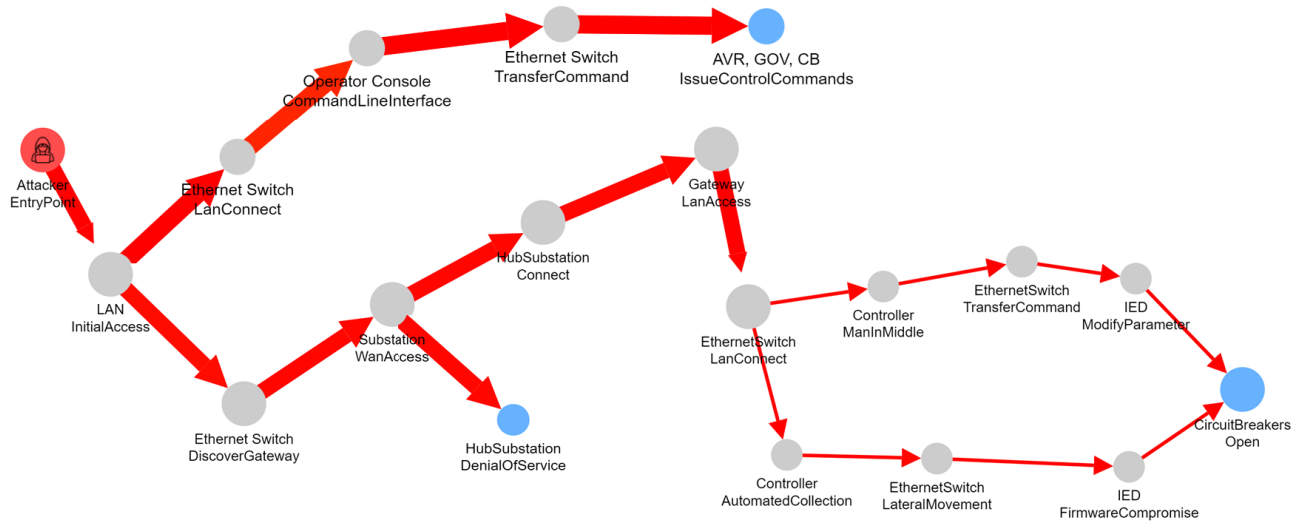


Figure 5.19. Generated attack path for scenario 4.

As previously shown in Scenario 3, by attacking the hub substation the attackers are able to cause significant delays in all connected substations. By measuring the delays in substations 5, 6, 7, 21, 24, and 25 it was found that the average RTT ranges from 230 to 530 milliseconds. The risk assessment results are given in Table 29, while the state of the power system after the attack is shown in Figure 5.20.

Table 29. Risk assessment of scenario 4.

Targeted Substations	TTC_{avg}	I_{Freq}	I_{Volt}	I_{Load}	I_{comp}	I_{ph}	I_{cyb}	F_{Rest}	*Likelihood*	*Risk*
5,7	30	70.44	13.8	14.9	0.76	71.52	3.33	2.35	0.32	**56.28**

After the voltage setting of the AVR of generator G6 is altered, the system remains intact, although the bus voltages and the frequency of the system are affected. This instability, which is initiated after the tampering attack, can be observed in the current magnitudes of the lines near the attack location, portrayed in Figure 5.21 a). As the circuit breaker of the second substation maliciously opens, nearby transmission lines are disconnected due to the distance protection, as the current increases to over 1.5 times the nominal value. The reason is that substation 7 includes two generating units, namely G4 and G5, thus reducing the overall power generation of the system. This imbalance causes the increase of the line currents.

As the line breakers open, the terminal voltage of generator G6 rises. Due to the tampering attack at 5 seconds, the voltage of the generator had already increased by 10%, thus the instability induced by the switching actions activates the over voltage protection, disconnecting the power plant from the main grid. Thus, the majority of Area 2 is de-energized as generator G7 disconnects due to ROCOF protection.

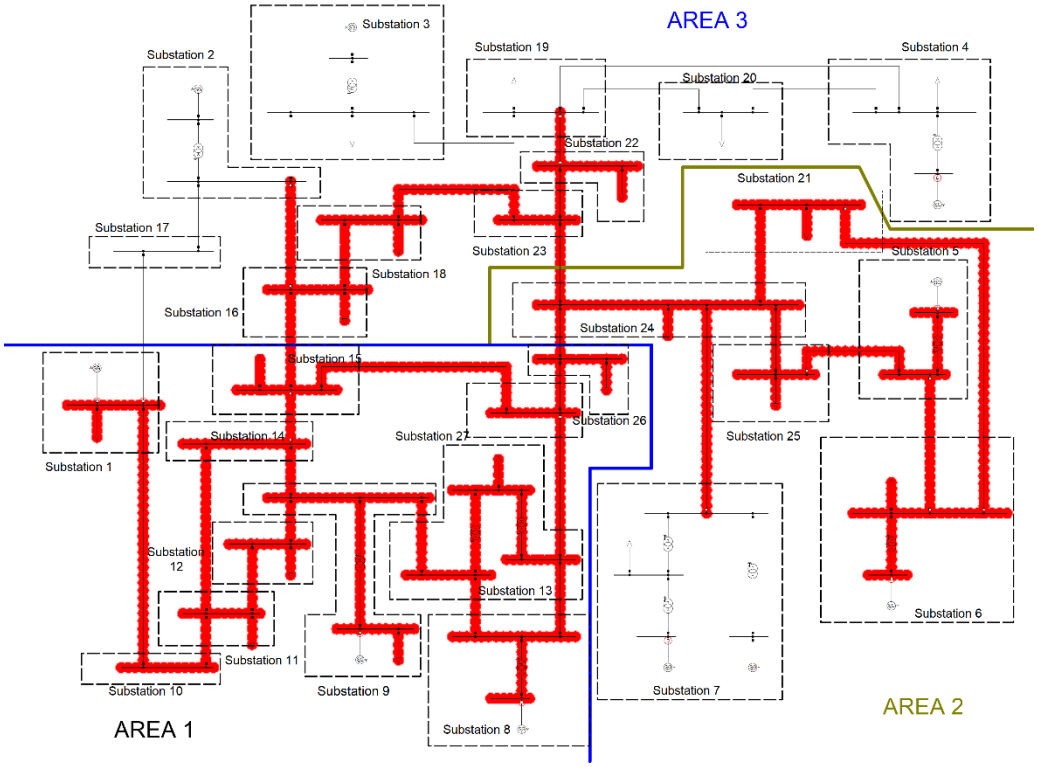


Figure 5.20. De-energized part of the grid, for scenario 4.

The disconnection of four generating units, causes the frequency to drop, thus activating the UFLS protection of the loads. The tripping of multiple lines, as the result of extensive overloading, splits the system into two islands of operation; generators G8, G9 and G10 form an island which supplies the loads of Area 3, while the external grid and generators G2 and G3 form an island in Area 1.

In the first island, generator G9 is disconnected due to ROCOF protection, as can be seen in Figure 5.21 c). Because of that, the frequency of the remaining generators is stabilized, and the loads can be supplied. The frequency of the remaining generators is considered within the safety requirements. In the second island of operation, the mismatch between generation and demand causes the over frequency protection of all three generators to trip, shown in Figure 5.21 d). Overall, this scenario results in a blackout, with an extensive restorative effort required for the system to be restored as many generators are disconnected, including the external grid. The majority of the loads are lost, but Area 3 remains connected, along with the smaller island comprising of generator G4 and Load 20, in Area 2. The sequence of events for this scenario is summarized in Table 30.

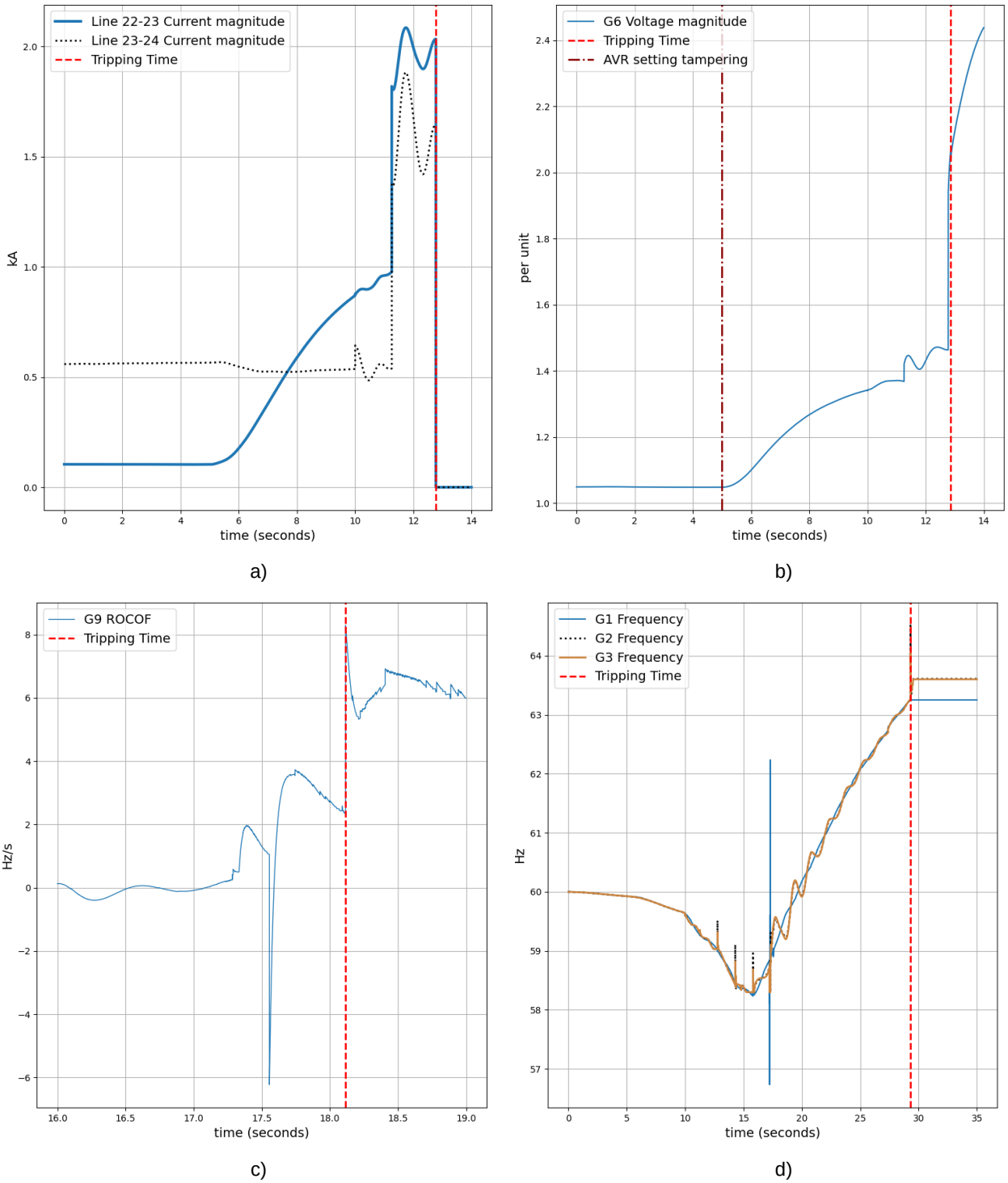


Figure 5.21. Scenario 4 results a) line currents, b) generator G6 voltage, c) G9 ROCOF, and d) frequency of generators.

Table 30. Sequence of events for scenario 4.

Time (seconds)	Event
0	Start of simulation.
5	**Cyber attack on substation 5. The voltage setting of the AVR of generator G6 is tampered is set from 1.05 to 1.9 p.u.**
10	**Cyber attack on substation 7. The line breaker, connecting the substation with the power grid is maliciously opened. A DDoS attack is launched on the gateway of the substation.**
10.5	Generator G5 is tripped due to ROCOF protection. Generator G4 forms an island, supplying Load 20.
11.278 - 12.775	Multiple lines in the vicinity of the attack location are tripped by distance protection, i.e., lines 21-22, 22-23, 23-24.
12.858 - 13.275	Generators G6 and G7 are disconnect, due to overvoltage and ROCOF protection respectively. Area 2 is de-energized.
14.044 - 14.293	Load shedding on all the loads. Active power of loads is decreased by 6.7%.
14.295 - 17.556	Multiple lines are tripped by distance protection, due to prolonged overloading. The active power of the loads is decreased even further by the UFLS protection. The frequency of the connected generating units is increased due to the mismatch of generation and power demand. Two islands of operation are formed.
18.116	Generator G9 is disconnected by the ROCOF protection. This stabilizes generators G8 and G10. The frequency of the second island, comprised of the external grid and generators G2 and G3 continues to increase.
29.308 – 29.549	The external grid and generators G2 and G3 are disconnected, due to over frequency protection. Areas 1 and 2 are de-energized.

This scenario is presented to show a) that the modelled CPS can be used to examine a variety of scenarios specified by the user, ranging from opening a single switch to target many different components of the power system, and b) that the impact on the physical and the cyber system can be combined in a meaningful way.

Regarding the latter, the assessed impact on the cyber system indicates that the efforts of power grid operators to timely perform remedial actions is affected, while the overall restoration effort could also be jeopardized by the attackers. Taking as example the 2015 attack in Ukraine, the ability of the operators to assess the impact were hindered by the telephone DoS attack in the call center of the affected DSOs [8].

5.6. Discussion

From the analysis of the results of all examined scenarios, the following observations are made:

- Depending on the operating state, the digital substations can be categorized based on how critical they are for the operation of the overall system. Certain substations such as substations 2, 12 and 27 are found to be high-impact targets for potential attackers, with scores over 90.
- Under given operating conditions, individual disconnections of loads and generators have a limited impact on the operation of the grid. A special case is an attack on substation 1. By disconnecting either the load or the external grid, the attackers are able to cause a blackout, resulting in a high-risk score.

- The sequence and timing of cyber attacks needs to be considered in any study. From scenarios 1.1 and 2 it is found that depending on the switching sequence, the impact can vary significantly, as seen in the examples of substations 15 and 24. Although these substations were assessed as low impact targets based on the results of scenario 1.1, the study of multiple attack combinations showed that they can be categorized as critical targets.
- A DDoS attack on the communication gateway of a digital substation can be used to hinder the restoration efforts and the potential remedial actions from the grid operators. Such an attack has a limited impact on the system if it is launched on its own, as shown in scenario 3. Additionally, based on the reviewed literature DDoS attacks can be easily detected and mitigated.
- Results from Scenario 4 show that highly skilled and sophisticated attackers can target specific critical substations. Although substations 5 and 7 were categorized as low risk in the case studies of scenario 1, a coordinated cyber attack on these two substations resulted in a blackout.
- The inclusion of the restoration factor in the risk assessment method showed that even if certain attack scenarios resulted in islanding or a blackout, the required restoration efforts can vary significantly. Assessing the exact restoration time is out of the scope of this research.
- To identify the most critical assets and systems, a variety of scenarios must be examined. These scenarios are complementary to each other; to indicate with a high level of precision the most vulnerable systems, different attack patterns, strategies and ways that attackers can target the CPS have to be studied. In this work we examined only selected cases.

In conclusion, the dynamic models of the physical and cyber layers of the combined CPS enable a thorough impact assessment of cyber attacks. On the other hand, the vulnerability assessment and attack simulations on the modelled attack graph can indicate the paths that an attacker can use to compromise the various critical assets.

6. Conclusions and Recommendations

This chapter summarizes and concludes the scientific and technical implications of the research findings of this thesis. The answers to the research questions posed in Chapter 2 are presented along with final concluding remarks. The scientific contributions are presented, and their importance to the overall research topic is highlighted. Finally, the challenges that were faced in this thesis, along with recommendations for future work are also discussed.

6.1. Answers to Research Questions

1. **How to model a cyber-physical system, to be able to**

   - **simulate the dynamic response of the physical power system?**

     By implementing protection schemes and control mechanisms, the dynamic model of a real-world power system is designed. This model can be used for simulating the dynamic response of a system, when it is subjected to cyber attacks.

   - **analyze cascading failures caused by cyber attacks on power system communications?**

     The cyber-to-physical interaction can be studied, by modelling the ICT/OT infrastructure of the power system, as described in Chapter 3. Based on the conducted literature review regarding the LAN topology of a substation as well as the overall WAN topology, the communication network for the CPS is specified. The design is based on the latency requirements for the overall system. Through the communication network, cyber attacks can be simulated and have an impact on the physical power system, as portrayed in the examples presented in Chapter 3. Additionally, the cascading failures can be successfully simulated.

2. **How to model the attack graph of a digital substation, and how it can be used for vulnerability analysis?**

   By using the Substation-Lang DSL, created using the MAL framework, the attack graph of a digital substation and the WAN is created. This research highlighted the applicability of these tools to properly address the complex ICT/OT domain of a critical infrastructure, such as power substations. The proposed modelling method presented in Chapter 4, addresses this issue by examining the importance of defining the assets and the associated attack steps. Furthermore, as the substations of a power system are comprised by a conglomeration of devices and systems, the method proposed by McQueen et. al. [60] is used to identify the individual TTC for the considered attack steps of each modelled asset.

   The aforementioned method is modified to determine the TTC probability distribution of the individual attack steps, based on the known vulnerabilities and the level of the attackers. The discrete method proposed by McQueen is modified to represent attackers in the continuous domain. The probability distributions act as inputs in the generated attack graph and by conducting attack simulations, the average TTC for a specific target is identified. By using this method, we are able to identify the weak points in each topology, and to observe the difference in the generated results. By examining selected assets, the method is verified. This method can be used in a more detailed model of an attack graph to assess the security of the examined system.

3. **How can we assess the impact on the operation of the cyber-physical system, for a given cyber attack scenario?**

   To capture the impact a variety of metrics have to be used, as each one can give an indication regarding the state of the system. KPIs like the loss of load, voltage deviation and the number of lost components are common impact indices that are implemented in this work. The proposed method for identifying the islands of operation and their frequency deviation can assess the potential fragmentation of a power system into smaller islands of operation.

By conducting dynamic simulations, the proposed metrics are able to accurately assess the impact of cyber attacks on the physical power system. These metrics can be used to investigate potential variations of a specific attack scenario, as is shown in the results presented in Chapter 5. Assessing the impact of different switching sequences on each substation, it is found that the effect of cyber attacks is influenced significantly by the order that circuit breakers are opened. As it was examined in the case of substation 15, the impact can vary from a blackout, with an impact index of over 90, to a small-scale outage affecting only the targeted substation, where the impact index is very small.

By utilizing a novel method to assess the impact on the communication network, the effect of cyber attacks such as DDoS can be examined. In this work, we examined how the volume of the DDoS attack can affect the modelled cyber system. By measuring the RTT we can measure the communication delays in our system. An increase on the transmission time for a packet of over 126% was observed with a 200 packet/sec DoS attack scenario. This shows that even though DoS attacks on power systems are not considered a serious threat as it cannot affect the operation of the physical system, if they are used in combination with spoofing or with tampering attacks, it could affect the overall restoration procedure following the attack.

Finally, by introducing a novel method to assess the potential restoration procedures required in the wake of a cyber attack, we can identify the most critical scenarios for the operation of a power system. This metric is introduced, as traditional methods usually employ the MTTR indicator. Although this metric is well established and widely used for reliability studies on the power system, it is found that it cannot properly be used to assess the restoration effort required after a cyber attack incident.

4. **How to calculate the risk of a cyber attack scenario, based on the security analysis and the associated impact on the cyber-physical system?**

   The developed risk assessment method combines the results of the impact assessment, which is conducted using dynamic simulations, with the security assessment results. The likelihood of an attack is determined by examining the average time that the attackers need to perform all associated attack steps to their target. By combining those indices, a single numerical value can describe the level of risk for a studied asset or system. The results showed that to identify the most critical assets of the CPS, various case studies have to be considered.

6.2. Contributions

The contributions of this work are the following:

- A modelling method for CPS, able to simulate the potential cascading failures that can occur in a power system, due to a cyber attack incident. The models of the physical and cyber layers are based on the operating principles of its real-world counterpart.
- A method for modelling the attack graph of a digital substation is proposed. A DSL called Substation-Lang is developed in this work, which can be used for security assessment. Additionally, an algorithm is devised which can calculate the probability distribution of the TTC for the various attack steps, based on the known vulnerabilities present in specified components and systems.
- A novel method is proposed for quantitative risk assessment of cyber attacks on the CPS. This method combines the probabilistic analysis performed in the attack graph, with a quantitative impact analysis from the dynamic model of the CPS. Mathematical models were developed to enable us to assess the impact on the combined CPS, using metrics for both the physical and the cyber system. Finally, a novel method is proposed to assess the likelihood of a cyber attack based on security metrics, while the most important addition to the related research is a method to assess the restoration effort required to restore the power system in the event of a cyber attack.

6.3. Challenges Faced

- **Modelling the CPS**

  The main challenges were about the implementation of the various models used to design the CPS. For the physical power system, the testing and experimentation of the dynamic simulations took an extended period to be finished. Additionally, the modelling of the communication system in Mininet required the manual modelling of assets, as well as the naming conventions.

- **Modelling the attack graph for the security assessment**

  As the security domain of the digital substations is described in an abstract way, by both academia and industry literature, certain assumptions had to be made. Furthermore, related work on the MAL generated DSLs that could be used for the modelling of power systems are still on development state.

- **Automated scenario generation in PowerFactory**

  For certain scenarios, the automated generation of case studies had to be programmed using Python. This procedure required an extensive understanding for leveraging the Python API for scenario manipulation and the analysis of datasets, generated by dynamic simulations. Additionally, certain scenarios required extensive simulation times, such as Scenario 2. As 248 different cases are examined, the simulation time is approximately 12 hours.

6.4. Recommendations on Future Work

In this thesis project, a novel method is proposed to assess the risk of cyber attacks on critical infrastructures such as the power system. As the scope of this research is broad, research can be conducted in the following research topics:

- **Inclusion of Wide Area Monitoring, Protection, and Control Systems (WAMPACS) in the CPS model**

  An important addition to this model could be additional control systems which can be used to wide area monitoring and control. These systems could automatically issue control commands to the control and protection units of the modelled CPS. As WAMPACS are a vital part of the emerging smart grids, the addition of these systems could be used to assess possible methods for impact mitigation and provide opportunities to study more types of cyber attacks, like false data injection attacks. The developed model and risk assessment method could act as a benchmark system for testing the role of WAMPACS to cyber attack mitigation techniques.

- **Addition of more assets in the attack graph model, as well as defences**

  The attack graph model can be expanded, taking into account additional assets in a power substation such as the operation servers, operating system of the engineering workstation, the presence of firewalls etc. Creating a more detailed graph and applying the method proposed in this thesis work to calculate the TTC, could be used to identify additional attack paths and the potential weak points of the security design.

- **Risk assessment method**

  The novel risk assessment method, proposed in this work, needs to be validated by security experts and expanded to capture the potential impact and risk on a CPS. Potential additions can be a) the inclusion of additional metrics to assess the impact on the communication system of the CPS, b) further research on the power grid restoration procedures after a cyber attack, and c) inclusion of metrics regarding the cyber security related impact such as loss of data and information steal. Finally, the repeatability of an examined cyber attack scenario is an important consideration that could be included in a future work. An attack scenario that is repeatable could pose a higher risk for an organization, as its frequency of occurrence is also increased.

Bibliography

[1] B. Tuinema, J. L. Rueda Torres, A. I. Stefanov, F. M. Gonzalez and M. A. M. M. van der Meijden, “Cyber-Physical System Modelling for Assessment and Enhancement of Power Grid Cyber Security, Resilience and Reliability,” in *Probabilistic Reliability Analysis of Power Systems: A Student's Introduction*, Springer, 2020, pp. 237-270.

[2] E. E. Miciolino, G. Bernieri, F. Pascucci and R. Setola, "Communications network analysis in a SCADA system testbed under cyber-attacks," in *2015 23rd Telecommunications Forum Telfor (TELFOR)*, Belgrade, 2015.

[3] M. F. M. Arani, A. Abiri Jahromi, D. Kundur and M. Kassouf, "Modelling and Simulation of the Aurora Attack on Microgrid Point of Common Coupling," in *2019 7th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Montreal, QC, Canada, 2019.

[4] W. A. Conklin, “IT vs. OT Securiy: A Time to Consider a Change in CIA to Include Resilience,” in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, 2016.

[5] J. Bumgarner, "Computers as Weapons of War," *IO Journal,* vol. 2, no. 2, pp. 4 - 8, 2010.

[6] N. Falliere, L. Murchu and E. Chien, "W32. Stuxnet Dossier," 2010. [Online]. Available: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

[7] R. M. Lee, M. J. Assante and T. Conway, "Analysis of the cyber-attack on the Ukrainian power grid," in *E-ISAC white paper*, SANS - Industrial Control Systems, 2016.

[8] D. E. Whitehead, K. Owens, D. Gammel and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, 2017.

[9] R. M. Lee, "CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids," Dragos Inc., 2017.

[10] M. J. Assante, R. M. Lee and T. Conway, "Modular ICS malware," in *E-ISAC white paper*, SANS - Industrial Control Systems, 2017.

[11] A. A. Di Pinto, Y. Dragoni and A. Carcano, "Triton: the first ICS cyber attack on safety instrument systems," *Proc. Black Hat USA,* pp. 1-26, 2018.

[12] M. Giles, "Triton is the world's most murderous malware, and it's spreading," *MIT Technology review,* 5 March 2019.

[13] Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2020," Government of Canada, 2020.

[14] G. Desarnaud, "Cyber Attacks and Energy Infrastructures: Anticipating Risks," Études de l'Ifri, 2017.

[15] M. Dietz, M. Vielberth and G. Pernul, "Integrating Digital Twin Security Simulations in the Security Operations Center," in *15th International Conference on Availability, Reliability and Security*, 2020.

[16] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications," *IEEE Access,* vol. 8, pp. 151019-151064, 2020.

[17] A. Stefanov, C. C. Liu, M. Govindarasu and S. S. Wu, "SCADA modeling for performance and vulnerability assessment of integrated cyber physical systems," *Int Trans Electr Energy Syst,* vol. 25, no. 3, pp. 498-519, 2015.

[18] G. J. Correa-Henao and J. M. Yusta-Loyo, "Representation of electric power systems by complex networks with applications to risk vulnerability assessment," *DYNA,* vol. 192, no. 82, pp. 68-77, 2015.

[19] G. Qinglai, X. Shujun, X. Luo and S. Hongbin, "EMS communication routings' optimization to enhance power system security considering cyber-physical interdependence," *IET Cyber-Phys. Syst., Theory Appl.,* vol. 3, no. 1, pp. 44-53, 2018.

[20] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," *IEEE Transactions on Smart Grid ,* vol. 6, no. 5, pp. 2444-2453, 2015.

[21] V. S. Rajkumar, M. Tealane, A. Stefanov, A. Presekal and P. Palensky, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, Virtual, 2020.

[22] Y. Zhang, L. Wang, Y. Xiang and C. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations," *IEEE Transactions on Smart Grid,* vol. 6, no. 4, pp. 1707-1721, 2015.

[23] Oyewole, P. A., Jayaweera and D., "Power System Security with Cyber-Physical Power System Operation," *IEEE Access,* vol. 8, pp. 179970-179982, 2020.

[24] M. Ibrahim, Q. Al-Hindawi, R. Elhafiz, A. Alsheikh and O. Alquq, "Attack Graph Implementation and Visualization for Cyber Physical Systems," *Processess,* vol. 8, no. 12, 2020.

[25] P. Johnson, A. Vernotte, M. Ekstedt and R. Lagerstrom, "pwnpr3d: An attack-graph-driven probabilistic threat-modelling approach," in *11th International Conference on Availability, Reliability and Security (ARES)*, 2016.

[26] O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, O. Yoshinobu, Y. Tomohiko, Y. Elovici and A. Shabtai, "Extending attack graphs to represent cyber-attacks in communication protocols and modern IT networks," *IEEE Transactions on Dependable and Secure Computing,* 2020.

[27] M. Touhiduzzaman, A. Hahn and A. Srivastava, "ARCADES: analysis of risk form cyberattack against defensive strategies for the power grid," *IET Cyber-Physical Systems: Theory & Applications,* vol. 3, no. 3, pp. 119-128, 2018.

[28] Z. Mohajerani et. al.,, "Cyber-related risk assessment and critical asset identification within the power grid," in *IEEE PES T&D 2010*, New Orleans, LA, 2010.

[29] F. Farzan, M. A. Jafari, D. Wei and Y. Lu, "Cyber-related assessment and critical asset identification in power grids," in *ISGT 2014*, Washington, DC, 2014.

[30] W. Wu, R. Kang and Z. Li, "Risk assessment method for cybersecurity of cyber-physical systems based on interdependency of vulnerabilties," in *2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Singapore, 2015.

[31] C. Chen, V. Mooney and S. Grijalva, "Electricity Grid Cyber-Physical Security Risk Assessment Using Simulations of Attack Stages and Physical Impact," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, Manhattan, KS, USA, 2020.

[32] P. Kundur, Power System Stability and Control, McGraw-Hill, Inc., 1993.

[33] ENTSO-E, "ENTSO-E at a glance," 2015.

[34] P. Schavemaker and L. van der Sluis, Electrical Power System Essentials, Delft, the Netherlands: John Wiley & Sons, Ltd, 2008.

[35] J. Grainger and W. Stevenson, Power System Analysis, McGraw Hill, Inc., 1994.

[36] ALSTOM GRID, "Network Protection & Automation Guide," Alstrom Grid, 2011.

[37] J. M. Gers and E. J. Holmes, Protection of Electricity Distribution Networks, London, United Kingdom: The Institution of Engineering and Technology, 2011.

[38] W. Christiansen and D. T. Johnsen, "Analysis of requirements in selected Grid Codes," Technical University of Denmark (DTU), 2006.

[39] IEEE, "IEEE Guide to AC Generator Protection," *IEEE Std C37.102-2006 (Revision of IEEE Std C37.102-1995),* pp. 1-177, 2006.

[40] E. Rakhshani, D. Gusain, V. Sewdien, J. L. Rueda Torres and V. D. M. M. A. M. M., "A Key Performance Indicator to Assess the Frequency Stability of Wind Generation Dominated Power System," *IEEE Access,* vol. 7, pp. 130957-130969, 2019.

[41] R. Bründlinger, "Grid codes in Europe: Overview on the current requirements in European codes and national interconnection standards," in *NEDO/IEA PVPS Task 14 Workshop (Austrian Institute of Technology - AIT)*, Vienna, Austria, 2019.

[42] A. Kubis and C. Rehtanz, "Response based system protection scheme against line overload cascades," in *12th IET Inf. Conf. Dev. Power Syst. Prot. DPSP*, 2014.

[43] Y. Yang et. al,, "Thermal modelling and real time overload capacity prediction of overhead power lines," in *IEEE Int Sympo Diag. for Elec Mach, Power Electr and Drives*, 2009.

[44] ABB, "Centralized Protection and Control - White Paper," ABB, 2019.

[45] M. Kuzlu, M. Pipattanasomporn and R. S., "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Computer Networks,* no. 67, pp. 74-88, 2014.

[46] Y. Wang, Y. P. and B. A., "Decentralized Communication and Control Systems for Power System Operation," *IEEE Transactions on Smart Grid,* vol. 6, no. 2, pp. 885-893, 2015.

[47] PowerFactory, DIgSILENT, "39 Bus New England System," DIgSILENT GmbH, Gomaringen.

[48] R. Smith, "U.S. Risks National Blackout from small-scale attack," in *Wall Street Journal*, 2014.

[49] U.S. Canada Power System Outage Task Force, "Causes of the August 14th Blackout in the United States and Canada," 2003.

[50] A. M. Abdullah and K. Butler-Purry, "Distance protection zone 3 misoperation during system wide cascading events: The problem and a survey of solutions," *Electr. Power Syst. Res.,* vol. 154, pp. 151-159, 2018.

[51] "Mininet - An Instant Virtual Network on your Laptop," [Online]. Available: http://mininet.org. [Accessed 19 May 2021].

[52] Siemens AG , Power Enginneering Guide - Edition 8.0, Erlangen, Germany, 2017.

[53] P. Johnson, R. Lagerström and M. Ekstedt, "A Meta Language for Threat Modelling and Attack Simulations," in *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security*, New York, NY, USA, 2018.

[54] "securiCAD cyber risk simulation," foreseeti, [Online]. Available: www.foreseeti.com/securicad/. [Accessed 29 July 2021].

[55] E. Ling and M. Ekstedt, "Generating Threat Models and Attack Graphs based on the IEC 61850 System Configuration description Language," in *SAT - CPS 2021*, Virtual Event, USA, 2021.

[56] MITRE, "MITRE ATT&CK for ICS," [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page. [Accessed 29 July 2021].

[57] E. R. Ling, "SCL-Lang," GitHub, [Online]. Available: https://github.com/mal-lang/SCL-Lang. [Accessed 20 September 2021].

[58] National Institute of Standards and Technology, "National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/vuln. [Accessed 21 07 2021].

[59] W. W., L. Chen, L. Han, Z. Zhou, Z. Xia and X. Chen, "Vulnerability Assessment for ICS system based on Zero-day attack graph," in *International Conference on Intelligent Computing, Automation and Systems (ICICAS)*, 2020.

[60] M. McQueen, W. Boyer, M. Flynn and B. G.A., "Time-to-Compromise Model for Cyber Risk Reduction Estimation," in *Quality of Protection Workshop (ESORICS)*, 2005.

[61] D. Leversage and B. E.J, "Estimating a System's Mean Time to Compromise," *IEEE Security & Privacy,* vol. 6, no. 1, pp. 52-60, 2008.

[62] A. Zieger, F. F. and K. Kossakowski, "The β-Time-to-Compromise Metric for Practical Cyber Security Risk Estimation," in *11th International Conference on IT Security Incident Management & IT Forensics (IMF)*, 2018.

[63] M. Assante and R. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, 2015.

[64] S. I. Pérez, S. Moral-Rubio and C. R., "A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity," *Chaos, Solitons and Fractals,* vol. 150, 2021.

[65] H. Li and W. Zhang, "QoS Routing in Smart Grid," in *IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010.

[66] IEEE, Historical Reliability Data for IEEE 3006 Standards: Power Systems REliability, 2012.

[67] G. Patsakis, D. Rajan, I. Aravena, J. Rios and S. Oren, "Optimal Black Start Allocation for Power System Restoration," *IEEE Transactions on Power Systems,* vol. 33, no. 6, pp. 6766-6776, 2018.

[68] W. Sun, C. Liu and S. Liu, "Black start capability assessment in power system restoration," in *IEEE Power and Energy Society General Meeting*, 2011.

[69] K. Fazzini and T. DiChristopher, "An alarmingly simple cyberattack hit electrical systems serving LA and Salt Lake, but power never went down," 2 May 2019. [Online]. Available: https://www.cnbc.com/2019/05/02/ddos-attack-caused-interruptions-in-power-system-operations-doe.html. [Accessed 29 September 2021].

Appendix A: IEEE-39 bus system data

In this section, the data for the IEEE-39 bus system are provided. In the following tables, the load and generation parameters, and the characteristics of the defined areas are given. These results are taken by the technical reference for the 39-bus system, provided by PowerFactory [47].

Loads are voltage-dependent for power flow calculations and time domain simulations. Active and reactive power are given by

$$P = P_{Ldf} * \left(\frac{U}{U_{Ldf}}\right)^{kpu} \quad \text{(A.1)}$$

$$Q = Q_{Ldf} * \left(\frac{U}{U_{Ldf}}\right)^{kqu} \quad \text{(A.2)}$$

where kpu is the constant current behavior for active power and kqu is the constant impedance behavior for reactive power. These constants are set to 1 and 2 respectively.

Table A-1. Load demand.

Load	Bus	Substation	Active Power (MW)	Reactive Power (Mvar)
Load 03	Bus 03	16	322.0	2.4
Load 04	Bus 04	15	500.0	184.0
Load 07	Bus 07	12	233.8	84.0
Load 08	Bus 08	11	522.0	176.0
Load 12	Bus 12	13	7.5	88.0
Load 15	Bus 15	26	320.0	153.0
Load 16	Bus 16	24	329.0	32.3
Load 18	Bus 18	18	158.0	30.0
Load 20	Bus 20	7	628.0	103.0
Load 21	Bus 21	25	274.0	115.0
Load 23	Bus 23	6	247.5	84.6
Load 24	Bus 24	21	308.6	-92.2
Load 25	Bus 25	3	224.0	47.2
Load 26	Bus 26	19	139.0	17.0
Load 27	Bus 27	22	281.0	75.5
Load 28	Bus 28	20	206.0	27.6
Load 29	Bus 29	4	283.5	26.9
Load 31	Bus 31	9	9.2	4.6
Load 39	Bus 39	1	1104.0	250.0

Table A-2. Generator dispatch.

Generator	Bus	Bus Type	Active Power (MW)	Voltage (p.u.)
G1	Bus 39	PV	1000.0	1.0300
G2	Bus 31	Slack	N.A.	0.9820
G3	Bus 32	PV	650.0	0.9831
G4	Bus 33	PV	632.0	0.9972
G5	Bus 34	PV	508.0	1.0123
G6	Bus 35	PV	650.0	1.0493
G7	Bus 36	PV	560.0	1.0635
G8	Bus 37	PV	540.0	1.0278
G9	Bus 38	PV	830.0	1.0265
G10	Bus 30	PV	250.0	1.0475

Table A-3. Characteristics of defined areas.

Area	Generation (MW)	Demand (MW)	Losses (MW)	Capacity (MW)
1	2305.97	2730.89	7.36	9775
2	2350	1821.75	16.88	2465
3	1620	1680.79	18.31	2295

Appendix B: Results for the TTC Probability Distributions

In the following tables, the probability distribution parameters of the considered components are given. The names of the considered vendors and products are given, along with the number of known, non-duplicate vulnerabilities that are used for extracting the TTC. For each specified attack step, the histogram of TTC per sample is generated, as presented in Chapter 4. The parameters of the probability distribution that fits the best in the generated histogram are extracted and is used as an input in the attack graph model.

For the asset gateway, no relevant product could be identified; based on the results provided by NVD selected vulnerabilities are identified.

Table B-1. Selected probability distributions of TTC and parameters.

Asset	Equipment	Attack steps	Number of known vulnerabilities per attack step	Fitted Distribution	Parameters
Ethernet Switch	CISCO 2000/4000/5000 Industrial Switches	Discover Devices	1	**Truncated Normal**	Mean: 9.207 Variance: 1.15
HMI	Siemens SICAM SCC	Command Line Interface	0	**Truncated Normal**	Mean: 28.76 Variance: 1.913
Station Controller	Siemens SICAM PAS	Automated Collection	3	**Gamma**	Shape: 0.6072 Scale: 0.1078 Location: 4.35
		Man in the Middle	4	**Truncated Normal**	Mean: 4.13 Variance: 0.137
Gateway	-	Discover	2	**Truncated Normal**	Mean: 5.31 Variance: 0.274
		Denial of Service	2	**Truncated Normal**	Mean: 5.31 Variance: 0.274
		Connect	1	**Truncated Normal**	Mean: 9.207 Variance: 1.15

Table B-2. Selected probability distributions of TTC and parameters, for IEDs.

Equipment	Attack steps	Number of known vulnerabilities per attack step	Fitted Distribution	Parameters
Siemens SIPROTEC	Denial of Service	8	**Gamma**	Shape: 0.5025 Scale: 1.4875 Location: 3.461
	Firmware Compromise	5	**Truncated Normal**	Mean: 3.97 Variance: 0.148
ABB Relion	Denial of Service	2	**Gamma**	Shape: 0.9405 Scale: 0.2978 Location: 5.012
	Firmware Compromise	0	**Truncated Normal**	Mean: 28.76 Variance: 1.913
Schneider Electric MiCOM	Denial of Service	1	**Truncated Normal**	Mean: 9.2033 Variance: 1.1401
	Firmware Compromise	1	**Truncated Normal**	Mean: 9.2033 Variance: 1.1401

Appendix C: Substation-Lang Code in MAL

The code for Substation-Lang is given below. The code is created using the MAL syntax and describe the DSL that is modelled in this thesis. The code is written in Java. The code is used to create an executable file, which is imported in securiCAD.

Substation_Lang.mal

```
#id: "org.mal-lang.Substation_Lang"
#version: "1.0.0"
// Author: Ioannis Semertzis

include "Substation_impact.mal"
include "Substation_comm.mal"
include "Substation_station.mal"
```

Substation_station.mal

```
category Station {

  asset Controller {

      | automatedCollection [Gamma (0.6072,0.1078)]
      // user info: " Access to a system interface may allow collection and enumeration
of other attached, communicating servers and devices."
          -> ethernetSwitch.lateralMovement

      | manInMiddle [TruncatedNormal (4.1313,0.1368)]
      // user info: "The attacker is able to take control, and send unauthorized
commands to the equipment."
          -> ethernetSwitch.transferCommand

  }

  asset OperatorConsole {
      // user info: "It represents the HMI interface."

      | commandLineInterface [TruncatedNormal (28.76,1.9133)]
          -> ethernetSwitch.transferCommand

  }

}

category Product {

    asset IED {
      | modifyParameter
       // user info: "The parameters are modified by attackers, by compromising the
OperatorConsole or the Control Server."
          -> circuitBreakers.open,
             generators.tripCircuitBreaker,
             loadControl.disconnect

       | denialOfService
       // user info: "The attacker can launch a DoS attack on the IED, and a manual
reboot is required to return it to normal."


       | firmwareCompromise
       // user info: "The attackers access the IEDs and manipulate its firmware to
launch an attack."
          ->  circuitBreakers.open,
              generators.tripCircuitBreaker,
              loadControl.disconnect
  }


```

```
47  asset EthernetSwitch {
48
49      | lateralMovement [TruncatedNormal(4.35,0.001)]
50      // user info: "The attacker has successfully identified the equipment."
51          -> ied.denialOfService,
52             ied.firmwareCompromise
53
54      | transferCommand
55          -> generators.issueControlCommands,
56             ied.modifyParameter
57
58      | discoverIED [TruncatedNormal (9.2077,1.15)]
59      // user info: "The attacker can identify the equipment that is connected to the
switch."
60          ->  ied.denialOfService,
61              ied.firmwareCompromise
62
63      | discoverGateway [TruncatedNormal (9.1, 1.147468)]
64      // user info: "By obtaining information from the LAN, the attacker can target hub
substation gateway."
65          -> gateway.wanAccess,
66             gateway.denialOfService
67
68      | lanConnect
69          -> controller.automatedCollection,
70             controller.manInMiddle,
71             operatorConsole.commandLineInterface
72  }
73 }
74
75 associations {
76  EthernetSwitch [ethernetSwitch] 1 <-- Communication --> 1 [gateway] Gateway
77  Controller [controller] 1 <-- Communication --> 1 [ethernetSwitch] EthernetSwitch
78  OperatorConsole [operatorConsole] 1 <-- Communication --> 1 [ethernetSwitch]
EthernetSwitch
79  EthernetSwitch [ethernetSwitch] 1 <-- Communication --> 0..* [ied] IED
80 }
```

Substation_impact.mal

```
1 category Impact {
2   // user info: "It represents the physical impact on the digital substation."
3   asset CircuitBreakers{
4       | open
5       // user info: "Trip signals are sent to the CBs, disconnecting the transmission
lines of the substation."
6   }
7
8   asset LoadControl {
9       | disconnect
10      // user info: "Loads are disconnected maliciously by attackers."
11  }
12
13  asset Generators {
14      | issueControlCommands
15      // user info: "Control commands are issued to the control units of the generators,
namely AVR and GOV."
16
17      | tripCircuitBreaker
18      // user info: "The attackers disconnect the generating unit from the main grid."
19  }
20 }
21
22 associations {
23  EthernetSwitch [ethernetSwitch] 1 <-- TransmitCommands --> 0..* [generators]
Generators
24  IED [ied] 0..* <-- Controls --> 0..* [circuitBreakers] CircuitBreakers
25  IED [ied] 0..* <-- Controls --> 0..* [loadControl] LoadControl
26  IED [ied] 0..* <-- Controls --> 0..* [generators] Generators
27 }
```

Substation_com.mal

```
category Communication {

  asset ControlCentre {
  // user info: "In this work it is considered secured."
  }

  asset WAN {
  // user info: "Asset WAN describes the general topology of the communication network."
      | access
          ->  hubSubstation.connect,
              hubSubstation.discover,
              hubSubstation.denialOfService
    }

    asset HubSubstation {
         | connect [TruncatedNormal (5.30471, 0.2738)]
      // user info: "By accessing the hub, attackers can find the substations to
attack."
          ->  gateway.lanAccess,
              gateway.denialOfService

      | denialOfService [TruncatedNormal(5.31, 0.273)]
      // user info: "The attacker can perform a DoS attack to the connected hub."

      | discover [TruncatedNormal(9.1, 1.147468)]
      // user info: "Through WAN discover other Hubs."
          -> wan.access
    }

    asset Gateway {

          | denialOfService [TruncatedNormal (5.31, 0.273)]

          | lanAccess [TruncatedNormal (5.30471, 0.2738)]
          // user info: "The attacker can gain access to the LAN network of the
substation."
              -> ethernetSwitch.lanConnect,
                 ethernetSwitch.discoverIED


          | wanAccess [TruncatedNormal (5.31, 0.273)]
      // user info: "The attacker could gain access to the overall WAN, and try to
attack different substations."
               -> hubSubstation.discover,
                  hubSubstation.denialOfService,
                  hubSubstation.connect
      }

      asset SubNetwork {
          | initialAccess
              -> ethernetSwitch.lanConnect,
                 ethernetSwitch.discoverGateway
      }
}

associations {
 ControlCentre [controlCentre] 1 <-- Communication --> 1 [wan] WAN
 WAN [wan] 1 <-- Communication --> 1..* [hubSubstation] HubSubstation
 HubSubstation [hubSubstation] 1 <-- Communication -->  1..* [gateway] Gateway
 SubNetwork [subNetwork] 0..1 <-- Connect --> 1 [ethernetSwitch] EthernetSwitch
}
```

Appendix D: Risk Assessment Results of Scenario 2

The detailed results of the risk assessment for scenario 2 are presented in Table D-1.

Table D-1. Risk assessment results for scenario 2.

Substation	Sequence	I_{Freq}	I_{Volt}	I_{Load}	I_{comp}	I_{ph}	I_{cyb}	F_{Rest}	*Likelihood*	*Risk*
1	1,2	0.3	0.2	0.28	0	0.63	0	1	0.41	0.26
	2,1	0.3	0.2	0.28	0	0.63	0	1	0.41	0.26
2	2,3,1	32.18	4.6	7.46	0.22	30.33	0	1.13	0.47	16.11
	2,1,3	10.67	1.42	0.52	0.09	8.14	0	1.03	0.47	3.94
	3,2,1	32.18	4.6	7.46	0.22	30.33	0	1.13	0.47	16.11
	3,1,2	90.34	18.95	18.16	0.93	91.63	0	1.39	0.47	59.86
	1,2,3	10.7	1.42	0.53	0.09	8.16	0	1.03	0.47	3.95
	1,3,2	10.67	1.42	0.52	0.09	8.14	0	1.03	0.47	3.94
3	2,1	10.09	1.19	1.84	0.04	8.5	0	1.03	0.26	2.28
	1,2	10.09	1.19	1.84	0.04	8.5	0	1.03	0.26	2.28
4	2,1	11.32	1.42	3.86	0.02	11.16	0	1.05	0.47	5.51
	1,2	11.32	1.42	3.86	0.02	11.16	0	1.05	0.47	5.51
5	2,1	21.3	2.43	5.18	0.09	19.13	0	1.07	0.26	5.32
	1,2	11.18	1.3	3.18	0.04	10.51	0	1.04	0.26	2.84
6	2,1	21.29	2.44	5.18	0.11	19.35	0	1.07	0.48	9.94
	1,2	10.08	1.18	1.86	0.04	8.51	0	1.03	0.48	4.21
7	1	11.1	0.3	2.69	0.02	8.76	0	1.03	0.48	4.33
8	1,2	11.19	1.18	3.21	0.07	10.63	0	1.04	0.26	2.87
	2,1	11.19	1.18	3.21	0.07	10.63	0	1.04	0.26	2.87
9	2,3,1	90.1	19.97	18.24	1	93.26	0	1.39	0.35	45.37
	2,1,3	60.39	13.17	12.14	0.67	62.24	0	1.23	0.35	26.79
	3,2,1	90.1	19.97	18.24	1	93.26	0	1.39	0.35	45.37
	3,1,2	60.39	13.17	12.14	0.67	62.24	0	1.23	0.35	26.79
	1,2,3	10.38	2.62	3.04	0.13	12.16	0	1.03	0.35	4.38
	1,3,2	60.47	13.09	11.37	0.67	61.43	0	1.23	0.35	26.45
10	2,1	0.18	0.58	0.06	0.02	0.94	0	1	0.48	0.45
	1,2	0.18	0.58	0.06	0.02	0.94	0	1	0.48	0.45
11	1,2,3	1.86	1.28	2.21	0.07	5.07	0	1	0.47	2.38
	1,3,2	1.19	0.73	1.19	0.02	2.73	0	1	0.47	1.28
	2,1,3	1.84	1.28	2.21	0.07	5.06	0	1	0.47	2.38
	2,3,1	2.71	1.79	2.31	0.11	6.54	0	1	0.47	3.07
	3,1,2	1.19	0.73	1.19	0.02	2.73	0	1	0.47	1.28
	3,2,1	1.19	0.73	1.19	0.02	2.73	0	1	0.47	1.28
12	2,1	90.12	19.97	18.24	1	93.27	0	1.39	0.35	45.38
	1,2	90.31	19.97	18.23	1	93.36	0	1.39	0.35	45.42
13	1,2,4,3	11.21	2.79	3.98	0.13	13.68	0	1.04	0.47	6.69
	1,2,3,4	11.21	2.79	3.98	0.13	13.68	0	1.04	0.47	6.69
	1,4,2,3	11.29	2.79	3.98	0.13	13.71	0	1.04	0.47	6.70
	1,4,3,2	11.29	2.79	3.98	0.13	13.71	0	1.04	0.47	6.70
	1,3,2,4	11.31	2.79	3.98	0.13	13.73	0	1.04	0.47	6.71
	1,3,4,2	11.32	2.79	3.98	0.13	13.73	0	1.04	0.47	6.71
	2,1,4,3	11.21	2.78	3.98	0.13	13.68	0	1.04	0.47	6.69
	2,1,3,4	11.21	2.79	3.98	0.13	13.68	0	1.04	0.47	6.69
	2,4,1,3	11.32	2.79	3.98	0.13	13.73	0	1.04	0.47	6.71
	2,4,3,1	11.32	2.79	3.98	0.13	13.73	0	1.04	0.47	6.71
	2,3,1,4	11.29	2.79	3.98	0.13	13.71	0	1.04	0.47	6.70
	2,3,4,1	11.29	2.79	3.98	0.13	13.72	0	1.04	0.47	6.71
	4,1,2,3	11.32	2.76	4	0.15	13.94	0	1.04	0.47	6.81
	4,1,3,2	11.32	2.77	4	0.15	13.94	0	1.04	0.47	6.81
	4,2,1,3	11.34	2.77	4	0.15	13.96	0	1.04	0.47	6.82
	4,2,3,1	11.34	2.77	4	0.15	13.96	0	1.04	0.47	6.82
	4,3,1,2	21.31	4.24	6.78	0.24	24.07	0	1.07	0.47	12.10

13	4,3,2,1	21.31	4.24	6.78	0.24	24.07	0	1.07	0.47	12.10
	3,1,2,4	11.31	2.79	3.98	0.13	13.73	0	1.04	0.47	6.71
	3,1,4,2	11.32	2.79	3.98	0.13	13.73	0	1.04	0.47	6.71
	3,2,1,4	11.29	2.79	3.98	0.13	13.71	0	1.04	0.47	6.70
	3,2,4,1	11.29	2.79	3.98	0.13	13.72	0	1.04	0.47	6.71
	3,4,1,2	11.23	2.76	4	0.15	13.9	0	1.04	0.47	6.79
	3,4,2,1	11.23	2.76	4	0.15	13.9	0	1.04	0.47	6.79
14	2,1,3	21.65	5.81	6.66	0.35	26.77	0	1.07	0.35	10.03
	2,3,1	21.65	5.81	6.66	0.35	26.77	0	1.07	0.35	10.03
	1,2,3	20.13	5.73	5.68	0.35	24.95	0	1.07	0.35	9.34
	1,3,2	20.13	5.73	5.68	0.35	24.95	0	1.07	0.35	9.34
	3,2,1	21.68	5.28	6.66	0.33	26.04	0	1.07	0.35	9.75
	3,1,2	21.64	5.28	6.59	0.33	25.95	0	1.07	0.35	9.72
15	3,2,1	1.39	0.76	1.25	0.04	3.14	0	1	0.48	1.51
	3,1,2	1.39	0.76	1.25	0.04	3.14	0	1	0.48	1.51
	2,3,1	1.39	0.76	1.25	0.04	3.13	0	1	0.48	1.50
	2,1,3	90.42	19.45	18.12	0.98	92.57	0	1.39	0.48	61.76
	1,3,2	1.39	0.76	1.25	0.04	3.14	0	1	0.48	1.51
	1,2,3	90.42	19.45	18.12	0.98	92.57	0	1.39	0.48	61.76
16	2,3,1	0.82	0.6	1.06	0.04	2.51	0	1	0.47	1.18
	2,1,3	0.83	0.6	1.06	0.04	2.51	0	1	0.47	1.18
	3,2,1	0.82	0.6	1.06	0.04	2.51	0	1	0.47	1.18
	3,1,2	0.82	0.6	1.06	0.04	2.51	0	1	0.47	1.18
	1,2,3	0.83	0.6	1.06	0.04	2.51	0	1	0.47	1.18
	1,3,2	0.82	0.6	1.06	0.04	2.51	0	1	0.47	1.18
17	2,1	0.16	0.55	0.02	0.04	1.09	0	1	0.26	0.28
	1,2	0.16	0.55	0.02	0.04	1.09	0	1	0.26	0.28
18	2,1	0.24	0.59	1.07	0	1.79	0	1	0.41	0.73
	1,2	0.24	0.59	1.07	0	1.79	0	1	0.41	0.73
19	3,2,4,1	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	3,2,1,4	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	3,4,2,1	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	3,4,1,2	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	3,1,2,4	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	3,1,4,2	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	2,3,4,1	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	2,3,1,4	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	2,4,3,1	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	2,4,1,3	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	2,1,3,4	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	2,1,4,3	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	4,3,2,1	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	4,3,1,2	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	4,2,3,1	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	4,2,1,3	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	4,1,3,2	10.62	2.24	3.12	0.11	11.75	0	1.05	0.48	5.92
	4,1,2,3	10.62	2.24	3.12	0.11	11.75	0	1.05	0.48	5.92
	1,3,2,4	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	1,3,4,2	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	1,2,3,4	10.64	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	1,2,4,3	10.63	2.24	3.12	0.11	11.76	0	1.05	0.48	5.93
	1,4,3,2	10.62	2.24	3.12	0.11	11.75	0	1.05	0.48	5.92
	1,4,2,3	10.62	2.24	3.12	0.11	11.75	0	1.05	0.48	5.92
20	2,1	0.41	0.58	1.04	0.02	2.05	0	1	0.48	0.98
	1,2	0.41	0.58	1.04	0.02	2.05	0	1	0.48	0.98
21	1,2	21.01	2.85	4.92	0.11	19.36	0	1.07	0.47	9.74
	2,1	21.04	2.86	4.92	0.11	19.38	0	1.07	0.47	9.75
22	2,1	0.58	0.63	1.13	0	2.05	0	1	0.47	0.96
	1,2	0.58	0.63	1.13	0	2.05	0	1	0.47	0.96

23	3,2,1	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
	3,1,2	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
	2,3,1	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
	2,1,3	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
	1,3,2	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
	1,2,3	0.17	0.58	0.07	0.04	1.16	0	1	0.47	0.55
24	4,3,5,1,2	60.52	11.22	12.42	0.67	60.64	0	2.25	0.41	55.94
	4,3,2,1,5	70.53	15.38	15.37	0.89	74.93	0	1.3	0.41	39.94
	4,3,2,5,1	70.53	15.38	15.37	0.89	74.93	0	1.3	0.41	39.94
	2,5,1,4,3	40.56	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	2,5,4,1,3	40.57	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	2,5,4,3,1	40.57	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	5,2,1,3,4	40.56	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	5,2,1,4,3	40.56	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	5,2,3,4,1	40.56	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	5,2,4,1,3	40.58	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	5,2,4,3,1	40.58	6	7.36	0.26	36.25	0	1.15	0.41	17.09
	2,5,1,3,4	40.56	6	7.36	0.26	36.24	0	1.15	0.41	17.09
	2,5,3,1,4	40.56	6	7.36	0.26	36.24	0	1.15	0.41	17.09
	2,5,3,4,1	40.56	5.99	7.36	0.26	36.24	0	1.15	0.41	17.09
	5,2,3,1,4	40.56	6	7.36	0.26	36.24	0	1.15	0.41	17.09
	1,2,5,4,3	40.44	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	1,5,2,4,3	40.44	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	3,2,5,4,1	40.43	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	3,5,2,4,1	40.43	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	2,1,5,4,3	40.44	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	2,3,5,4,1	40.43	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	5,1,2,4,3	40.44	5.99	7.37	0.26	36.18	0	1.15	0.41	17.06
	5,3,2,4,1	40.43	5.99	7.36	0.26	36.18	0	1.15	0.41	17.06
	1,2,5,3,4	40.42	5.99	7.37	0.26	36.17	0	1.15	0.41	17.05
	1,5,2,3,4	40.43	5.99	7.37	0.26	36.17	0	1.15	0.41	17.05
	3,2,5,1,4	40.42	5.98	7.37	0.26	36.17	0	1.15	0.41	17.05
	3,5,2,1,4	40.42	5.98	7.37	0.26	36.17	0	1.15	0.41	17.05
	2,1,5,3,4	40.43	5.99	7.37	0.26	36.17	0	1.15	0.41	17.05
	2,3,5,1,4	40.42	5.98	7.37	0.26	36.17	0	1.15	0.41	17.05
	5,1,2,3,4	40.42	5.99	7.37	0.26	36.17	0	1.15	0.41	17.05
	5,3,2,1,4	40.41	5.99	7.36	0.26	36.17	0	1.15	0.41	17.05
	1,5,3,2,4	40.36	5.98	7.38	0.26	36.15	0	1.15	0.41	17.04
	3,5,1,2,4	40.35	5.98	7.38	0.26	36.14	0	1.15	0.41	17.04
	5,1,3,2,4	40.35	5.98	7.38	0.26	36.14	0	1.15	0.41	17.04
	5,3,1,2,4	40.34	5.98	7.38	0.26	36.14	0	1.15	0.41	17.04
	4,1,3,2,5	31.84	4.12	7.22	0.22	29.43	0	1.1	0.41	13.27
	4,1,3,5,2	31.84	4.12	7.21	0.22	29.43	0	1.1	0.41	13.27
	4,1,5,3,2	31.81	4.12	7.22	0.22	29.42	0	1.1	0.41	13.27
	4,5,1,3,2	31.81	4.11	7.22	0.22	29.41	0	1.1	0.41	13.26
	1,4,3,5,2	31.79	4.12	7.22	0.22	29.4	0	1.1	0.41	13.26
	3,4,1,5,2	31.78	4.12	7.22	0.22	29.4	0	1.1	0.41	13.26
	1,3,4,2,5	31.77	4.12	7.22	0.22	29.39	0	1.1	0.41	13.25
	1,3,4,5,2	31.77	4.12	7.22	0.22	29.39	0	1.1	0.41	13.25
	3,1,4,2,5	31.76	4.12	7.22	0.22	29.39	0	1.1	0.41	13.25
	3,1,4,5,2	31.77	4.12	7.22	0.22	29.39	0	1.1	0.41	13.25
	1,4,3,2,5	31.73	4.1	7.17	0.22	29.32	0	1.1	0.41	13.22
	3,4,1,2,5	31.78	4.11	7.08	0.22	29.26	0	1.1	0.41	13.20
	4,2,3,1,5	31.68	4.1	7.09	0.22	29.21	0	1.1	0.41	13.17
	1,4,5,3,2	31.04	4	6.84	0.22	28.54	0	1.1	0.41	12.87
	5,4,1,3,2	30.99	4.01	6.43	0.22	28.11	0	1.1	0.41	12.68
	3,4,5,1,2	30.98	4.01	6.43	0.22	28.1	0	1.1	0.41	12.67
	5,4,3,1,2	30.98	4.01	6.43	0.22	28.1	0	1.1	0.41	12.67
	4,2,5,1,3	30.79	3.97	6.39	0.22	27.94	0	1.1	0.41	12.60

	4,2,5,3,1	30.79	3.97	6.39	0.22	27.94	0	1.1	0.41	12.60
	4,5,2,1,3	30.8	3.97	6.39	0.22	27.94	0	1.1	0.41	12.60
	4,5,2,3,1	30.8	3.97	6.39	0.22	27.94	0	1.1	0.41	12.60
	4,1,5,2,3	30.79	3.97	6.39	0.22	27.93	0	1.1	0.41	12.60
	4,5,1,2,3	30.78	3.97	6.39	0.22	27.93	0	1.1	0.41	12.60
	4,2,3,5,1	30.77	3.97	6.39	0.22	27.92	0	1.1	0.41	12.59
	1,4,2,3,5	30.7	3.97	6.4	0.22	27.89	0	1.1	0.41	12.58
	1,4,5,2,3	30.69	3.97	6.39	0.22	27.89	0	1.1	0.41	12.58
	2,4,1,3,5	30.7	3.97	6.4	0.22	27.89	0	1.1	0.41	12.58
	2,4,5,1,3	30.7	3.97	6.39	0.22	27.89	0	1.1	0.41	12.58
	2,4,5,3,1	30.7	3.97	6.39	0.22	27.89	0	1.1	0.41	12.58
	5,4,2,1,3	30.7	3.98	6.39	0.22	27.89	0	1.1	0.41	12.58
	5,4,2,3,1	30.7	3.98	6.39	0.22	27.89	0	1.1	0.41	12.58
	1,4,2,5,3	30.69	3.98	6.39	0.22	27.88	0	1.1	0.41	12.57
	3,4,5,2,1	30.68	3.97	6.39	0.22	27.88	0	1.1	0.41	12.57
	2,4,1,5,3	30.69	3.97	6.39	0.22	27.88	0	1.1	0.41	12.57
	5,4,1,2,3	30.69	3.98	6.39	0.22	27.88	0	1.1	0.41	12.57
	5,4,3,2,1	30.68	3.97	6.39	0.22	27.88	0	1.1	0.41	12.57
	1,3,5,4,2	30.66	3.97	6.39	0.22	27.87	0	1.1	0.41	12.57
	3,1,5,4,2	30.66	3.97	6.39	0.22	27.87	0	1.1	0.41	12.57
	1,5,4,3,2	30.63	3.97	6.39	0.22	27.86	0	1.1	0.41	12.56
	1,2,4,3,5	30.62	3.97	6.4	0.22	27.85	0	1.1	0.41	12.56
	3,5,4,1,2	30.63	3.97	6.4	0.22	27.85	0	1.1	0.41	12.56
	2,1,4,3,5	30.62	3.97	6.4	0.22	27.85	0	1.1	0.41	12.56
	2,3,4,1,5	30.63	3.97	6.4	0.22	27.85	0	1.1	0.41	12.56
	5,1,4,3,2	30.63	3.97	6.39	0.22	27.85	0	1.1	0.41	12.56
	5,3,4,1,2	30.62	3.97	6.4	0.22	27.85	0	1.1	0.41	12.56
	1,5,3,4,2	30.6	3.97	6.4	0.22	27.84	0	1.1	0.41	12.56
	5,1,3,4,2	30.59	3.97	6.4	0.22	27.84	0	1.1	0.41	12.56
24	1,3,2,4,5	30.58	3.97	6.39	0.22	27.83	0	1.1	0.41	12.55
	1,3,2,5,4	30.59	3.97	6.4	0.22	27.83	0	1.1	0.41	12.55
	1,3,5,2,4	30.59	3.97	6.4	0.22	27.83	0	1.1	0.41	12.55
	1,2,3,4,5	30.58	3.96	6.4	0.22	27.83	0	1.1	0.41	12.55
	3,1,2,5,4	30.58	3.97	6.4	0.22	27.83	0	1.1	0.41	12.55
	3,1,5,2,4	30.58	3.97	6.4	0.22	27.83	0	1.1	0.41	12.55
	3,2,1,4,5	30.58	3.96	6.4	0.22	27.83	0	1.1	0.41	12.55
	3,5,1,4,2	30.59	3.97	6.4	0.22	27.83	0	1.1	0.41	12.55
	2,1,3,4,5	30.58	3.96	6.4	0.22	27.83	0	1.1	0.41	12.55
	2,3,1,4,5	30.58	3.96	6.4	0.22	27.83	0	1.1	0.41	12.55
	5,3,1,4,2	30.59	3.97	6.4	0.22	27.83	0	1.1	0.41	12.55
	1,2,4,5,3	30.56	3.96	6.4	0.22	27.82	0	1.1	0.41	12.55
	1,5,4,2,3	30.56	3.96	6.4	0.22	27.82	0	1.1	0.41	12.55
	3,1,2,4,5	30.57	3.97	6.39	0.22	27.82	0	1.1	0.41	12.55
	2,1,4,5,3	30.56	3.96	6.4	0.22	27.82	0	1.1	0.41	12.55
	2,3,4,5,1	30.57	3.96	6.4	0.22	27.82	0	1.1	0.41	12.55
	5,1,4,2,3	30.56	3.96	6.4	0.22	27.82	0	1.1	0.41	12.55
	3,5,4,2,1	30.55	3.96	6.4	0.22	27.81	0	1.1	0.41	12.54
	5,3,4,2,1	30.55	3.96	6.4	0.22	27.81	0	1.1	0.41	12.54
	1,2,3,5,4	30.49	3.96	6.41	0.22	27.78	0	1.1	0.41	12.53
	3,2,1,5,4	30.48	3.95	6.41	0.22	27.78	0	1.1	0.41	12.53
	2,1,3,5,4	30.49	3.95	6.41	0.22	27.78	0	1.1	0.41	12.53
	2,3,1,5,4	30.48	3.95	6.41	0.22	27.78	0	1.1	0.41	12.53
	4,3,1,2,5	22.1	1.55	5.3	0.15	19.42	0	1.07	0.41	8.52
	4,3,1,5,2	22.1	1.55	5.3	0.15	19.41	0	1.07	0.41	8.52
	4,5,3,1,2	22.07	1.55	5.3	0.15	19.4	0	1.07	0.41	8.51
	4,2,1,3,5	22.05	1.51	5.32	0.15	19.38	0	1.06	0.41	8.42
	3,4,2,1,5	22.38	1.45	5.24	0.13	19.18	0	1.06	0.41	8.34
	4,3,5,2,1	21.7	1.39	5.08	0.15	18.84	0	1.07	0.41	8.27
	4,1,2,3,5	20.98	1.9	4.43	0.2	18.78	0	1.06	0.41	8.16

24	4,1,2,5,3	20.98	1.9	4.43	0.2	18.78	0	1.06	0.41	8.16
	4,5,3,2,1	21.02	1.4	4.47	0.15	17.91	0	1.07	0.41	7.86
	3,2,4,1,5	20.89	1.39	4.48	0.15	17.84	0	1.07	0.41	7.83
	3,2,4,5,1	20.83	1.39	4.48	0.15	17.81	0	1.07	0.41	7.81
	4,2,1,5,3	21.01	1.37	4.5	0.15	17.89	0	1.06	0.41	7.77
	2,4,3,1,5	20.91	1.37	4.45	0.13	17.58	0	1.07	0.41	7.71
	2,4,3,5,1	20.9	1.37	4.45	0.13	17.58	0	1.07	0.41	7.71
	3,4,2,5,1	21.34	1.31	4.41	0.13	17.69	0	1.06	0.41	7.69
25	1,2	21.18	2.98	5.03	0.11	19.69	0	1.07	0.47	9.90
	2,1	21.01	2.96	4.85	0.11	19.4	0	1.07	0.47	9.76
26	1,2	0.64	0.67	1.18	0.02	2.39	0	1	0.47	1.12
	2,1	0.64	0.67	1.18	0.02	2.39	0	1	0.47	1.12
27	1,2,3	90.18	19.97	18.24	1	93.3	0	1.39	0.26	33.72
	1,3,2	90.18	19.97	18.24	1	93.3	0	1.39	0.26	33.72
	2,1,3	90.23	19.97	18.23	1	93.32	0	1.39	0.26	33.73
	2,3,1	90.23	19.97	18.23	1	93.32	0	1.39	0.26	33.73
	3,1,2	90.18	19.97	18.24	1	93.3	0	1.39	0.26	33.72
	3,2,1	90.18	19.97	18.24	1	93.3	0	1.39	0.26	33.72

These results show all the examined cases of switching sequences, for every substation. In total 248 cases are examined.

Appendix E: Published Conference Paper MSCPES 2021

Critical Components Identification for Cyber-Physical Power Systems Considering Time-Varying Operational States

Yigu Liu, Ioannis Semertzis, Alexandru Stefanov, Peter Palensky
Department of Electrical Sustainable Energy
Delft University of Technology
Delft, the Netherlands
y.liu-18@tudelft.nl

ABSTRACT

The security issues of Cyber-Physical power Systems (CPS) have attracted widespread attention from scholars. Vulnerability assessment emerges as an effective method to identify the critical components and thus increase the system resilience. While efforts have been made to study the vulnerability features of power systems under the occurrence of a single, discrete disturbance or failure at a specific time instant, this paper focuses on identifying the critical components of the cyber-physical system considering time-varying operational states. To investigate the potentially ever-changing CPS vulnerability features, in this paper we construct a database of cascading failure chains using quasi-dynamic simulations to capture the vulnerability relationships among components under time-varying operational states. Then, by adopting sequential mining algorithms, we mine the most frequent cascading failure patterns and identify the critical components based on the data mining results. Simulation studies are conducted on IEEE 39-bus and IEEE RTS-96 systems to evaluate the effectiveness of the proposed method for the identification of critical components at both cyber and physical layers.

KEYWORDS

cyber-physical systems, vulnerability assessment, data mining algorithms.

ACM Reference Format:

Yigu Liu, Ioannis Semertzis, Alexandru Stefanov, Peter Palensky. 2021. Critical Components Identification for Cyber-Physical Power Systems Considering Time-Varying Operational States. In *MCPES'21: 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, May 18, 2021, Virtual Event*, 7 pages. https://doi.org/10.1145/3470481.3472702

1 Introduction

With the rapid development of Information and Communication Technologies (ICTs) and Operational Technologies (OTs), the power grids are now tightly coupled with communication infrastructures in an unprecedented way, which forms a complex, interdependent Cyber-Physical System (CPS). Digitalization is expected to increase power grid sustainability, affordability, and resiliency. However, cyber-related vulnerabilities are inevitably introduced in the cyber-physical system, which can be exploited by adversaries and thus weaken power grid robustness and security of supply. Furthermore, they also exacerbate the breadth and depth of cascade propagation when CPS experiences disturbances, which increase the overall system vulnerability with catastrophic potential consequences.

Vulnerability assessment is typically used to enhance cyber-physical system security by identifying the weak points in the system. The current vulnerability assessment methods for CPS can be broadly grouped into two categories: (i) topology-based methods [1][2], which abstract the CPS into an interdependent network and evaluate the systematic vulnerabilities from a structural perspective, and (ii) operation-based methods [3][4], which consider the CPS operational aspects, e.g., power flow and information communication, in either or both cyber-physical domains. For topology-based methods, Buldyrev et al. [1] adopt percolation theory to prove that a broader degree distribution increases the vulnerability of the interdependent networks to random failures. Complex network theory [2] is also a popular method to construct indices and evaluate the vulnerability of system components, e.g., degree, closeness, and betweenness. However, topology-based methods naturally neglect the heterogeneity of nodes in both cyber and physical layers and focus on the structure of the interdependent network. Consequently, the inherent physical mechanisms, e.g., power flows and routing protocols, at both CPS layers are ignored, which may result in unrealistic conclusions. To this end, Falahati et al. [3] use a linear programming model to maximize the data connection at the cyber layer and adopt a DC optimal power flow model to minimize the load curtailment. Furthermore, Ye et al. [4] define an interaction model to simulate the cascading failures in CPS.

Although efforts have been made on modeling and systematic evaluation of CPS vulnerability, the current literature has an obvious drawback. The existing work only evaluates the CPS at a single time instant. However, we argue that this may not always be the case. Instead of considering CPS disturbances or failures as single-occurrence events, in this research we treat them as a set of sequential discrete events. Disturbances and failures can occur at any time instant during CPS operation over a certain time period. Meanwhile, the operational states, e.g., loads and power flows, are constantly varying in time. Under such assumption, the vulnerability features generated by the existing static methods,

*Both authors contributed equally to this research.

MCPES'21, May 19–21, 2021, Nashville, TN, USA

ACM ISBN 978-1-4503-8608-1/21/05.
https://doi.org/10.1145/3470481.3472702

which aim at a particular time instant may not be applicable to time-varying CPS operational states. To this end, a fundamentally new approach is needed to systematically capture the vulnerability characteristics and identify the most critical CPS components to develop effective and economic mitigation strategies.

To address these issues, in this paper, we propose a novel cascading failure model considering the interaction between cyber and physical layers for every single time instant. Based on quasi-dynamic simulations, we generate a database of cascading failure chains. This contains various operating conditions. We adopt the PrefixSpan sequential mining algorithm [5] to identify the frequent sequential cascading patterns. Vulnerability indices are constructed based on complex network theory to evaluate the importance of components in the cascading failure process and identify the critical components in CPS. The contributions of this paper are summarized as follows:

1) This paper proposes a novel vulnerability assessment method for the identification of critical components in CPS considering the time-varying operational states.

2) This paper investigates CPS modeling from both topological and operational perspectives. From a topological perspective, the cyber topology and structural interdependency between cyber and physical layers are thoroughly investigated. From an operational perspective, we present a detailed modeling process considering the interaction between cyber and physical layers.

3) Based on the constructed CPS model, a database of cascading failure chains is constructed containing systematic vulnerability features. Moreover, we introduce sequential data mining algorithms to identify the frequent cascading failure patterns and design vulnerability metrics to identify the critical cyber-physical system components.

The remainder of this paper is organized as follows. Section II discusses the system vulnerability under time-varying operational states. Section III provides the modeling and simulation process of cascading failures. Section IV presents the identification of critical components. The case study and conclusion are presented in Section V and Section VI, respectively.

2 System Vulnerability Considering Time-varying Operational States

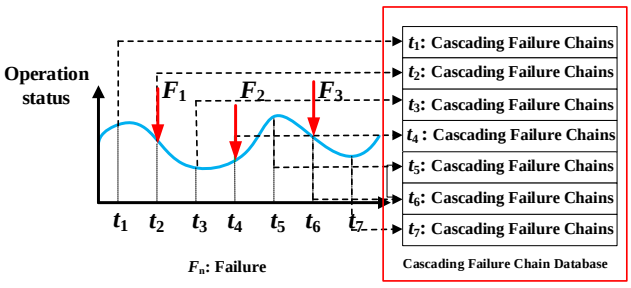


Figure 1: The time-varying operational states of CPS.

In previous discussion, we argue that the current vulnerability assessment methods may not be applicable or even feasible when considering the change of CPS operational status. As shown in Fig. 1, in a real-world scenario, the operational states of CPS are constantly changing, which means the system will react to failures or disturbances differently at various time instants. More concretely, the cyber-physical system may show different cascading failure patterns under time-varying operational states, which will directly change the vulnerability features. In this context, we first model a failure, e.g., line tripping, in CPS to trigger the cascading failures at a specific time instant, e.g., t_2, t_4 or t_6 as represented in Fig. 1. To thoroughly investigate the vulnerability characteristics of CPS at a specific time instant, we consider that any component in the cyber-physical system may fail, and we generate possible cascading failure chains for all components. These cascading failure chains contain the detailed vulnerability features of CPS at the time instant. By combining cascading failure chains of all-time instants, a cascading failure chain database is generated, which captures the intricate relationships among components and reveals the fault propagation mechanism of CPS under different operating conditions. For instance, for a certain time interval $[t_1, t_u]$, suppose the cascading failure chain set includes $\boldsymbol{X}_{CF}(t_1)$ at t_1, $\boldsymbol{X}_{CF}(t_2)$ at t_2 ,..., $\boldsymbol{X}_{CF}(t_u)$ at t_u, then the cascading failure chain database $\boldsymbol{X}_D$ can be presented as:

$$\boldsymbol{X}_D = \left\{ \boldsymbol{X}_{CF}(t_u) \middle| 1 \le u \le U \right\} \tag{1}$$

The definition of $\boldsymbol{X}_{CF}(t_u)$ can be found in Section III, Part C. At last, we intend to employ sequential data mining algorithms to mine the cascading failure database and identify the critical components of CPS. Generally, the sequential data mining algorithms return the patterns that are frequently shown in the database. For cyber-physical systems, if a cascading failure pattern frequently appears in $\boldsymbol{X}_D$, it means that the corresponding components play a critical role in the cascading process. If such critical components are reinforced and cyber secure, the system resilience will be greatly improved.

3 Modeling of CPS and Cascading Failures

In this Section, we investigate CPS modeling from both topological and operational perspective. We model the cascading failures at each time instant to show how CPS will react to disturbances under different operating conditions. Then, by collecting the cascading failure chains at each time instant, a database is generated to further reveal the systematic vulnerability features of the cyber-physical system.

3.1 Topological Modeling of CPS

In this paper, we abstract the CPS into an interdependent network, in which nodes and edges are used to represent the cyber-physical system components and interconnections among them, respectively.

Physical Layer: the generators, substations and loads are considered as physical nodes, while the transmission lines and transformers are considered as physical edges. Consequently, we can directly map a power grid into an undirected and unweighted graph based on its own topology.

Cyber Layer: the Supervisory Control and Data Acquisition (SCADA) system in the control center and station control systems in substations are abstracted into cyber nodes, while their communication links are considered as cyber edges. It is worth mentioning that for the cyber layer we only consider the influence of the cyber layer topology on the physical layer operation. In this research, we do not consider the detailed communication mechanisms, e.g., routing protocols. Typically, the communication networks for power grids are implemented as double-star or mesh networks [6][7] From the perspective of complex network theory, double-star networks are scale-free networks [8]. The control centers are considered hub nodes with higher degrees in the system. If one of these nodes fail, the cyber-physical system will suffer severe consequence. The double star networks are sensitive to intentional cyber-physical attacks, but resilient to random failures. On the other hand, mesh networks, as opposite to double-star networks, show the feature of small-world [9], which indicates that mesh networks have a broader degree distribution and are more vulnerable to random failures. Generally, a broader degree distribution increases the robustness of complex networks. However, when cyber and physical layers are coupled to form an interdependent network, a broader degree distribution increases the vulnerability of the interdependent networks to random failures [1]. Meanwhile, the research of Ye et al. [4] also shows that power grids coupled with double-star communication network have a lower probability of catastrophic failures than with mesh networks. Therefore, in this paper, we adopt the double-star network to model the topology of the cyber system.

Structural Interdependency: in this paper, we consider the interdependence between cyber and physical layers as a "one-to-one" correspondence [1]. The number of nodes in the cyber layer is the same as in the physical layer, and a cyber node is exclusively interconnected with a physical node. Parshani et al. [10] defines the interdependency of networks as intersimilarity from a topology perspective and investigates the robustness of interdependent networks under different intersimilarities. The results show that for scale-free networks, the interdependency should be "degree-to-degree", which means that the node with the highest degree in the cyber layer should be interconnected with the node with the highest degree in the physical layer.

3.2 Operational Modeling of CPS

Failures such as protection maloperation or loss of communications may trigger cascading effects in the cyber-physical system. Furthermore, when power grids are tightly coupled with communication infrastructures, the extent of fault propagation in CPS may be significantly increased considering the complex interdependencies between the cyber and physical layers. For example, one disturbance in one network may simultaneously have an influence within the network and on its interdependent networks. In this subsection, we present the simulation process of generating the cascading failure chains for every time instant used to generate the cascading failure chain database.

When the power system is congested, system operators redispatch generation or even shed load to ensure that the power grid is securely and economically operated. Therefore, an optimal DC power flow model represented by equations (2) – (7) is used to minimize the load shedding when disturbances occur in the cyber-physical system.

$$\min \sum_{y \in D} W_y \left| p_y - P_{dy} \right| \tag{2}$$

$$s.t. \quad \boldsymbol{F} = \boldsymbol{AP} \tag{3}$$

$$\sum_{x=1}^{n} p_x = 0 \tag{4}$$

$$P_{dy} \le p_y \le 0, y \in D \tag{5}$$

$$P_{gx}^{\min} \le p_x \le P_{gx}^{\max}, x \in G \tag{6}$$

$$-F_l^{\max} \le F_l \le F_l^{\max}, L_l \in \boldsymbol{L} \tag{7}$$

where G and D are the set of generators and loads, respectively, W_y is the cost of load shedding, $\boldsymbol{L} = \left\{ L_l \middle| l = 1,2,...,N_l \right\}$ is the set of branches in the power grid and $\boldsymbol{P} = \left[p_1, p_2, ..., p_k, ... \right]^{\mathrm{T}}$ is the vector of power node injections. Equation (3) represents the DC power flow equation. $\boldsymbol{A}$ is the nodal admittance matrix and $\boldsymbol{F} = \left[F_1, F_2, ..., F_l, ... \right]$ is the vector of branch power flows. p_y represents the load of node *y*. P_{dy} represents the rated load at node *y*. p_x represents the output power of generator *x*. $P_{gx}^{\max}$ and $P_{gx}^{\min}$ are the upper and lower limits of the output power of generator *x*, respectively. $F_l^{\max}$ is the transmission capacity of the *l*-th branch.

Ye et al. [4] propose an interaction model and analyses the system performance under both intentional attacks and random failures. Dong et al. [11] propose a probabilistic failure model to simulate the cascading process between cyber and physical layers. Based on these works, an interactive model is used to capture the main features of both cyber and physical layers and give a rough approximation to describe the interdependency between the two layers, which is presented as follows.

Cascading failures in the same layer: we consider that cascading failures in power grids are mainly caused by load redistribution when branches are disconnected and by hidden failures. Due to a hidden failure [12], the outage of branch L_l

may cause the failure of its neighbors with a low probability P_1. When a branch is overloaded due to system load redistribution, we assume that the branch will be disconnected with a probability P_2. We do not consider the mutual influence among cyber nodes, i.e., the failure of a cyber node will only influence the data communication and will not cause a failure of other cyber nodes.

The impact of disturbances in the cyber layer to the physical layer: we consider that the cyber nodes are directly coupled with the physical nodes of power grids. When a cyber node is out of service, the control center loses the remote monitoring and control capabilities of the physical node and all corresponding branches in the substation. Consequently, when these branches are overloaded, they will operate in an insecure state and will be eventually disconnected by system protection after a period of time. On the other hand, a failed cyber node may be on the communication path between the control center and another cyber node. Under such circumstances, we consider that the control center also loses the monitoring and control capabilities of the associated physical nodes.

3.3 Construction of Cascading Failure Chain Database

In this paper, we investigate systematic cyber-physical system vulnerabilities. Therefore, we include various cascading failure scenarios by assuming that each component is possible to fail at every time instant. More specifically, we trip all the branches one by one to collect all possible cascading failure chains at every time instant. Then, by repeating the same process, the cascading failure chains are combined to generate the cascading failure chain database as shown in Fig. 1. The detailed simulation process of one single time instant is presented in Fig. 2. A disconnected branch is removed from the power grid topology. The updated topology is represented by N_{real}. Furthermore, we consider $N_{control}$ to be a subset of N_{real} for which the system operator still has monitoring and control capabilities. The branches connected to the physical nodes affected by the failure of their corresponding cyber nodes are removed from $N_{control}$. We consider that the cyber nodes are vulnerable to cyber attacks and some will fail due to malicious attacks or other contingencies in each iteration. The cyber nodes will be removed with a small probability P_3.

The cascading failure process at time instant t_U starts by disconnecting branch L_l and scanning for cyber and hidden failures. The N_{real} and $N_{control}$ CPS topologies are updated. The DC power flow is first calculated based on the updated N_{real}. If there are overloaded branches, we calculate the optimal DC power flow based on the updated $N_{control}$. The results of the optimal DC power flow give the power injections for the physical nodes in $N_{control}$. The redispatch of generation with minimum load shedding costs is implemented using N_{real}. We calculate load redistribution based on the new power injections and previously available measurements for the physical nodes affected by the failure of their cyber nodes. The overloaded branches are disconnected with their corresponding probabilities. It is worth mentioning that a branch may be disconnected based on local measurements by protection relays and control commands from the control center. When a branch is overloaded, system operators will adjust the generation or initiate load shedding. If the overload is not mitigated, the branch will be tripped by overload protection. Therefore, in our paper, we assume that when a branch is overloaded, it is tripped by local protection with a probability P_2. The process is repeated until there are no further overloaded branches. The cascading failure chain is exported to the database.

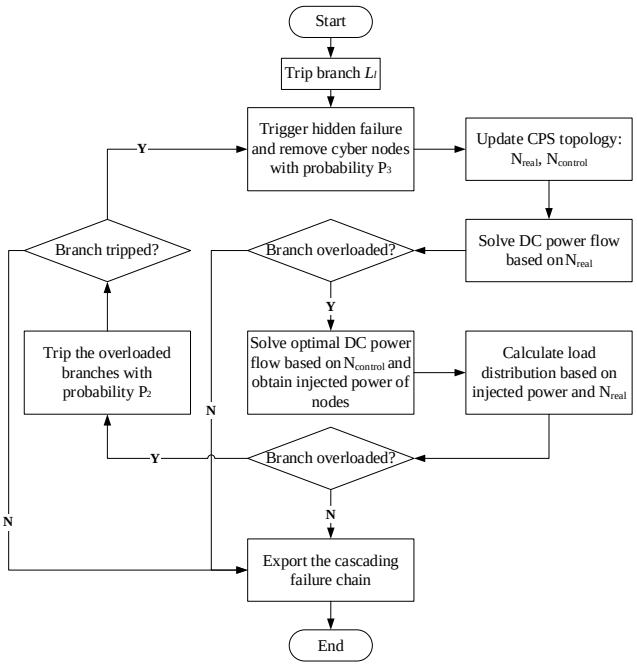


Figure 2: Simulation process of cascading failures.

It is worth mentioning that the simulation process illustrated in Fig. 2 is used to generate the cascading failure chain $\boldsymbol{X}_{CF}^{L_l}(t_u)$ initiated by the disconnection of branch L_l at t_u. To thoroughly capture the vulnerability features of CPS and generate the cascading failure chain $\boldsymbol{X}_{CF}(t_u)$ at t_u, this simulation should be conducted for every branch in $\boldsymbol{L}$. This can be represented by equations (8) and (9).

$$\boldsymbol{X}_{CF}^{L_l}(t_u) = \rho(C_1, C_2, \ldots, C_n), C_k \in \boldsymbol{C} = \boldsymbol{V}_C \cup \boldsymbol{L} \tag{8}$$

$$\boldsymbol{X}_{CF}(t_u) = \left\{ \boldsymbol{X}_{CF}^{L_l}(t_u) \middle| L_l \in \boldsymbol{L} \right\} \tag{9}$$

where $\rho(C_1, C_2, \ldots, C_n) = C_1 \rightarrow C_2 \rightarrow, \ldots, \rightarrow C_n$.

$\boldsymbol{V}_C = \left\{ v_g \middle| g = 0,1,2,...,N_g \right\}$ represents the set of cyber nodes at the cyber layer. The cascading failure chain database $\boldsymbol{X}_D$ can be generated based on equations (1) and (9).

4 Critical Components Identification from a Data Mining Perspective

In this section, we take advantage of the fact that $\boldsymbol{X}_{CF}^{L_l}(t_u)$ can be viewed as a *sequence* for data mining and employ the PrefixSpan sequential data mining algorithm to capture the most frequent cascading failure sequence, i.e., CPS vulnerable sequence. Based on the identified patterns, we propose a vulnerability metric to further quantify the vulnerability of each component in the cyber-physical system.

4.1 Identification of Vulnerable Cascading Failure Sequence

For a cyber-physical system, the cascading failure chain database can be very large, in which some cascading failure patterns may show up repeatedly. We use the frequency of these patterns to quantify the vulnerability of each CPS component. The cascading failure patterns are defined as candidate sequences waiting to be evaluated whether they are vulnerable sequences or not.

Definition 1 (candidate sequence): Based on the definition of $\boldsymbol{X}_{CF}^{L_l}(t_u)$, if there exists $\{C_{j1},C_{j2},\ldots,C_{js}\}\subseteq\{C_1,C_2,\ldots,C_n\}$, a sequence $\alpha=\rho(C_{j1},C_{j2},\ldots,C_{js})$ is called a *subsequence* of a cascading failure chain $\boldsymbol{X}_{CF}^{L_l}(t_u)$, which can be denoted as $\alpha \triangleright \boldsymbol{X}_{CF}^{L_l}(t_u)$.

Normally, the frequency of a candidate sequence indicates the vulnerability of its associated components. To quantify such frequency, the definition of vulnerability degree is defined as follows:

Definition 2 (vulnerability degree): for a candidate sequence $\alpha=\rho(C_{j1},C_{j2},\ldots,C_{js})$, the vulnerability degree is defined as:

$$\boldsymbol{V}_D(\alpha)=\left|\left\{\rho\middle|(\rho\in\boldsymbol{X}_D)\wedge(\alpha\triangleright\rho)\right\}\right| \tag{10}$$

Based on the definitions above, PrefixSpan can be adopted to identify the vulnerable sequence with higher vulnerability degrees. The details of PrefixSpan are reported in [5].

4.2 Vulnerability Metric for Critical Components Identification

Based on the vulnerable sequences identified above, in this part, we propose a vulnerability metric to further quantify the vulnerability of each CPS component. As discussed in Section III, for each cascading failure chain $\boldsymbol{X}_{CF}^{L_l}(t_u)$, the components highly positioned in the chain result in high vulnerabilities. Therefore, we propose a metric named *total sequential vulnerability* to identify the critical components in the cyber-physical system.

Definition 3 (total sequential vulnerability): for a vulnerable sequence $\beta_m=\rho(\ldots,C_i,\ldots)$, the sequential vulnerability $S_{\beta_m}(C_i)$ of component C_i in β_m is defined as

$$S_{\beta_m}(C_i)=N_{\beta_m}-\delta_{\beta_m}(C_i)+1 \tag{11}$$

where N_{β_m} is the number of components in β_m and $\delta_{\beta_m}(C_i)$ is the order of C_i in β_m. Based on equation (11), by combining the sequential vulnerability of component C_i in all M vulnerable sequences containing C_i, the total sequential vulnerability of C_i can be represented as

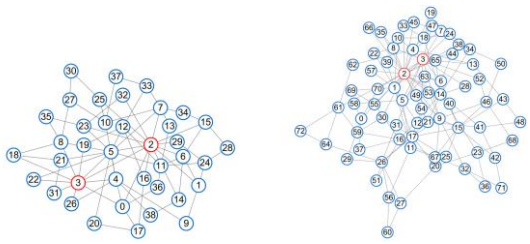
$$S(C_i)=\sum_{m=1}^{M}S_{\beta_m}(C_i) \tag{12}$$

5 Case Study

In this section, we conduct experiments on IEEE 39-bus and IEEE RTS-96 models to evaluate the effectiveness of the proposed method. Their cyber-physical systems and the proposed method are implemented in Python. The probabilities for the simulation of cascading failure chains are set as follows: $P_1=0.05$, $P_2=0.95$, $P_3=0.01$.

5.1 Generation of Cyber Layer

As discussed in Section III, we use a scale-free network to simulate the cyber layer. Based on the Barabási–Albert (BA) model [8], Fig. 3 shows the generated cyber topologies of IEEE 39-bus and IEEE RTS-96 system, respectively.



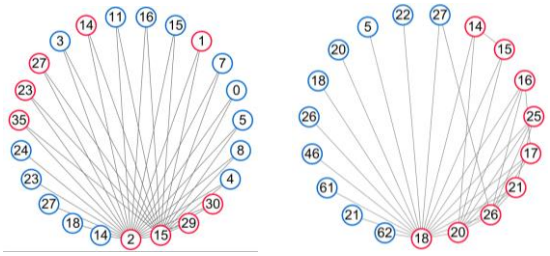
(a) (b)

Fig. 3: Cyber layer topology: (a) IEEE 39-bus system, (b) IEEE RTS-96 bus system.

5.2 Critical Components Identification

The method proposed in Section III is used to generate the vulnerable sequences of IEEE 39-bus and IEEE RTS-96 system. For IEEE RTS-96 system, we use the peak loads of each week for a 52-week load profile to simulate the time-varying operational states of CPS. For IEEE 39-bus system, we change the load proportionally in each simulation over 52 weeks. In the final

database, there are 1901 cascading failure chains for IEEE 39-bus system and 6479 cascading failure chains for IEEE RTS-96 system. Fig. 4 shows all the vulnerable sequences identified for the two test systems. Furthermore, based on equations (11)-(12), the total sequential vulnerabilities are calculated to quantify the vulnerabilities of CPS components in the test systems. Table I and II show the top 5 components in both cyber and physical layers with the highest total sequential vulnerabilities.



(a) (b)

Fig. 4: Vulnerable Sequence Identification: (a) IEEE 39-bus system, (b) IEEE RTS-96 bus system. The cyber nodes are represented with blue, while the power system branches are represented with red.

From the perspective of degree distribution, in Fig. 4(a), the components with the highest degree are branches 2, 15 and 29. This ranking is different from the ranking of total sequential vulnerability. This is because the total sequential vulnerability also considers the position of components in a vulnerable sequence. When a component frequently appears at the start position of a sequence, it means this component has a more significant impact on other components in the system. If the cyber-physical security of such components can be strengthened, then the scale of cascading failures will be reduced and thus the system will be more resilient. It is worth mentioning that although the degree distribution and total sequential vulnerability of power nodes are much higher than the ones of the cyber nodes, they are equally important for cyber-physical systems.

TABLE I. VULNERABLE COMPONENTS OF IEEE39-BUS SYSTEM SORTED BY TOTAL SEQUENTIAL VULNERABILITY

Branches in Physical Layer			**Nodes in Cyber Layer**		
Ranking	***ID of Branches***	$S(C_i)$	***Ranking***	***ID of Nodes***	$S(C_i)$
1	2	50	1	3	5
2	15	24	2	16	4
3	1	5	3	11	3
4	35	4	4	15	3
5	23	4	5	8	3

TABLE II. VULNERABLE COMPONENTS OF IEEE RTS-96 SYSTEM SORTED BY TOTAL SEQUENTIAL VULNERABILITY

Branches in Physical Layer			**Nodes in Cyber Layer**		
Ranking	***ID of Branches***	$S(C_i)$	***Ranking***	***ID of Nodes***	$S(C_i)$
1	18	93	1	27	3
2	20	64	2	5	2
3	16	25	3	18	1
4	26	23	4	21	1
5	17	17	5	20	1

On the other hand, as shown in Table I and II, we can observe that the span of $S(C_i)$ is quite large, which means, taking IEEE 39-bus system as an example, branch 2 is more vulnerable than branch 23, and by extension, other branches ranked behind branch 23 in the system. Such results indicate that for cyber-physical systems, there is a limited number of critical components, which must be reinforced and cyber secure. In our case, Table I and II give the top 5 critical components in both cyber and physical layers of the IEEE 39-bus and IEEE RTS-96 systems.

6 Conclusion and Future Work

This paper focuses on revealing the vulnerability features of cyber-physical systems considering the time-varying operational states. First, we model the cascading failures considering the interaction of cyber and physical layers. By combining cascading failure chains of all-time instants, a cascading failure chain database is generated. This captures the intricate relationships among components and reveals the fault propagation mechanism of CPS under different operating conditions. The PrefixSpan sequential data mining algorithm is adopted to identify the vulnerable sequences. The total sequential vulnerability metric is proposed to quantify the vulnerabilities of CPS components. The simulation results show that there is only a limited number of critical CPS components. The resilience of the cyber-physical system can be greatly improved if these critical components are reinforced and cyber secured. This paper provides a new perspective on CPS vulnerability assessment. As an extension to this paper, one can perform an in-depth study of considering the cyber-related operational mechanisms, e.g., routing protocols and information flows, when modeling the cascading failures between the cyber-physical layers.

REFERENCES

[1] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” in Nature, vol. 464, pp. 1025–1028, Apr. 2010. DOI: https://doi.org/10.1038/nature08932

[2] Amin Abedi, Ludovic Gaudard, Franco Romerio, “Review of major approaches to analyze vulnerability in power system”, in Reliability Engineering & System Safety, vol. 183, pp. 153-172, 2019. DOI: https://doi.org/10.1016/j.ress.2018.11.019

[3] B. Falahati, Y. Fu and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515-1524, Sept. 2012. DOI: 10.1109/TSG.2012.2194520

[4] Y. Cai, Y. Cao, Y. Li, T. Huang and B. Zhou, "Cascading Failure Analysis Considering Interaction Between Power Grids and Communication Networks," in IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 530-538, Jan. 2016. DOI: 10.1109/TSG.2015.2478888.

[5] J. Pei et al., "Mining sequential patterns by pattern-growth: the PrefixSpan approach," in IEEE Transactions on Knowledge and

Data Engineering, vol. 16, no. 11, pp. 1424-1440, Nov. 2004. DOI: 10.1109/TKDE.2004.77.

[6] G. W. Li, W. Y. Ju, X. Z. Duan, and D. Y. Shi, “Transmission characteristics analysis of the electric power dispatching data network,” in Proc. CSEE, vol. 32, no. 22, pp. 141–148, 2012. DOI: 10.13334/j.0258-8013.pcsee.2012.22.020

[7] J. Hu, Z.-H. Li, and X. Z. Duan, “Structural feature analysis of the electric power dispatching data network,” in Proc. CSEE, vol. 29, no. 4, pp. 53–59, 2009. DOI: CNKI:SUN:ZGDC.0.2009-04-010

[8] Albert-László Barabási*, Réka Albert, “Emergence of Scaling in Random Networks,” in Science, vol. 286, no. 5439, pp. 509-512, Oct 1999. DOI: 10.1126/science.286.5439.509

[9] Watts, D., Strogatz, S. “Collective dynamics of ‘small-world’ networks.” in Nature, vol. 393, pp. 440–442, June 1998. DOI: https://doi.org/10.1038/30918

[10] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, “Intersimilarity between coupled networks,” in Europhy. Lett., vol. 92, no. 6, 2010. DOI: 10.1209/0295-5075/92/68002

[11] D. Zhengcheng, F. Yanjun, T. Meng, “Influences of Various Coupled Patterns and Coupling Strength on Power-communication Coupled Networks,” in High Voltage Engineering, vol. 41, no. 10, pp. 3464-3469, Oct. 2015. DOI: 10.13336/j.1003-6520.hve.2015.10.038

[12] F. Yang, A. P. S. Meliopoulos, G. J. Cokkinides and Q. B. Dam, "Effects of Protection System Hidden Failures on Bulk Power System Reliability," in 2006 38th North American Power Symposium, Carbondale, IL, USA, 2006, pp. 517-523. DOI: 10.1109/NAPS.2006.359621