Master's thesis

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

Bjørn Olav Gjørven & Alexander H. Bakken

# Design and Validation of a Novel Architecture for Virtual Smart Grid Cyber Ranges

Master's thesis in Communication Technology and Digital Security
Supervisor: Marie Moe, Martin Gilje Jaatun & Thomas Haugan
July 2020

NTNU
Norwegian University of Science and Technology

CINELDI
Centre for intelligent electricity distribution
- to empower the future Smart Grid

Bjørn Olav Gjørven & Alexander H. Bakken

# Design and Validation of a Novel Architecture for Virtual Smart Grid Cyber Ranges

Master's thesis in Communication Technology and Digital Security
Supervisor: Marie Moe, Martin Gilje Jaatun & Thomas Haugan
July 2020

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

NTNU
Norwegian University of
Science and Technology

# Abstract

Advanced cyber attacks on critical infrastructures are increasing in frequency and sophistication. At the same time, the conventional power grid is being restructured into a smart grid, and adequate cyber security training is in high demand. A smart grid cyber-physical range (SGCR) is probably the best way to provide realistic training scenarios in a controlled environment, whereby conducting advanced cyber-security and incident response training on simulated cyber-physical systems (CPSs) in the smart grid domain. However, there are few SGCRs in the world today, and the field of cyber ranges are currently contained with multiple challenges, such as flexibility, realism, adaptability, etc. In this master's thesis, we aim to cope with some of these challenges by designing a novel virtual SGCR in terms of providing the identified stakeholders with the opportunity to conduct advanced cyber security training. Due to the nature of our study, we apply design science methodology as our principal research method, which includes the problem-solving design cycles and empirical cycles. The cycles are used to solve a specified design problem, and is accompanied with a comprehensive literature study and semi-structured interviews. The literature study provides an in depth knowledge of many relevant topics derived from the design problem, such as the smart grid, critical infrastructures, advanced persistent threats, cyber kill chains, previous cyber attacks, incident response and state-of-the-art cyber ranges. The enrolled participants for the interviews are field experts on cyber ranges, smart grids and incident response. The objective is to acquire the necessary requirements to design and test a final treatment artifact. We test and validate the novel architectural design through partial implementation. The final test results and artifact design, as well as the project limitations and future work are thoroughly discussed. As part of the CINELDI project, we conclude this master's thesis with a novel design for a virtual SGCR, with the capability for incident response and advanced cyber security training. We name the resulting design; *smart grid cyber-security & cyber-physical range for CINELDI* (SG3C).

# Preface & Acknowledgements

This thesis is submitted in fulfillment of the requirements for the five-year integrated master of science (MSc) degree in Information Security and Communication Technology (IIK) at the Norwegian University of Science and Technology (NTNU).

We want to sincerely thank our supervisors, Martin Gilje Jaatun and Thomas Haugan for their excellent guidance and advice. Also, we would like to thank Associate Professor Marie Moe for believing in us and motivating us to embark on the project.

We would like to thank the CINELDI project for providing us with this very interesting master's thesis.

Lastly, a huge thanks to our families and friends for their full support.

# List of Acronyms

**AHK** AutoHotKey.

**AMS** advanced metering system.

**APT** advanced persistent threat.

**BE3** Black Energy 3.

**BI** business intelligence.

**C2** command & control.

**CI** critical infrastructure.

**CIA** confidentiality, integrity and availability.

**CINELDI** Center for Intelligent Electricity Distribution.

**CKC** cyber kill chain.

**CPR** cyber-physical range.

**CPS** cyber-physical system.

**CR** cyber range.

**CRM** control room management.

**DER** distributed energy resources.

**DES** distributed energy storage.

**DG** decentralized energy generation.

**DOS** denial of service.

**DSB** Directorate for Civil Protection.

**DSL** digital subscriber line.

**DSM** demand-side management.

**DSO** distribution system operator.

**EMI** electromagnetic interference.

**ENISA** European Union Agency for Cyber Security.

**ERP** enterprise resource planning.

**EV** electric vehicle.

**GHG** green house gase.

**HMI** human machine interface.

**ICS** industrial control system.

**ICT** information and communication technology.

**IEC** International Electrotechnical Commission.

**IIK** Information Security and Communication Technology.

**IoT** internet of things.

**ISA** International Standard on Auditing.

**ISIM** information security incident management.

**ISO** International Organization for Standardization.

**IT** information technology.

**KQ** knowledge question.

**LotL** living off the land.

**MA** MITRE ATT&CK.

**MES** manufacturing execution systems.

**MVP** minimal viable product.

**NCR** Norwegian Cyber Range.

**NSD** Norwegian Centre for Research Data.

**NTNU** Norwegian University of Science and Technology.

**OFC** optical fiber communication.

**OS** operating system.

**OT** operational technology.

**PLC** programmable logic controller.

**PMU** phasor measurement unit.

**PV** photovoltaic system.

**QoS** quality of service.

**RAT** remote administration tool.

**RES** renewable energy source.

**RMC** range management center.

**RTA** Red Team Automation.

**RTT** round trip time.

**RTU** remote terminal unit.

**SC** satellite communication.

**SCADA** supervisory control and data acquisition.

**SG3C** *smart grid cyber-security & cyber-physical range for CINELDI*.

**SGCR** smart grid cyber-physical range.

**SSI** semi-structured interview.

**TOR** the onion router.

**TSO** transmission system operator.

**VM** virtual machine.

**VPE** virtual participant environment.

**VPN** virtual private network.

**VSE** virtual scenario environment.

**WAN** wide area network.

# Contents

THIS PAGE IS INTENTIONALLY LEFT BLANK

# Chapter 1
# Introduction

Smart grid cyber security has received significant attention from governments and the electric power and utility industry, as the traditional power grid is being restructured into a smart grid [1]. In the traditional power grid, cyber-security defense mechanisms were barely emphasized, or not applied at all [2]. The electrical power grid will no longer solely carry one-way power flow (i.e from the generation plant to consumers), but will be equipped with several intelligent characteristics. These include a bidirectional flow of both electricity and data, enhanced monitoring and fault detection, as well as a comprehensive network of sensors that allow the capability of self-healing, and many other beneficial features [2]. To achieve these intelligent features, the emerging smart grid aims to incorporate advanced information and communication technology (ICT) in order to become a full-fledged cyber-physical system (CPS) [3]. A CPS can be described to be a highly linked, flexible and seamless system that encompass the cooperation between systems, networks and human interactions [4]. The physical term in CPS, comes from the physical process being monitored and controlled by computers and networks through the use of sensor and actuators [5]. Examples include robotics systems, internet of things (IoT), control systems, medical devices and the smart grid [6]. As such, the smart grid is realised by merging the worlds of information technology (IT) and operational technology (OT), which evidently brings new challenges in terms of cyber security [7].

In recent time, there has been a significant increase in industrial control system (ICS) threat activity groups, which are targeting and disrupting critical infrastructures by coordinated cyber attacks, for instance, the Black Energy 3 (BE3) and Crashoverride attacks on the Ukrainian electrical power systems in 2015/2016 [8]. The BE3 attack succeeded to destroy several remote terminal units (RTUs), which are used to control important processes within substations. Moreover, the attack campaign managed to control several Ukrainian distribution system operators (DSOs), and manually, turn off the electrical power for several hours in parts of the network [9, 10]. Barely one year later, in the same country, a modular malware (framework) called, Crashoverride, disrupted power grid operations by leveraging typical industrial protocols, such as

IEC 101, IEC 104 and OPC DA, and was a lot more autonomous as opposed to the BE3 attack [11]. Cyber attacks can potentially create substantial economic impacts by causing blackouts for up to days, or even weeks in some areas [12]. As other countries have been victims to similar cyber attacks, the Norwegian power system should be prepared for handling such incidents in the future [9].

> "Digital security and vulnerabilities in critical infrastructures are a major challenge, both national and international. To address this challenge, it requires an cooperation between research and various disciplines, which also involves businesses and public enterprises that is responsible for the critical infrastructures."
>
> – Minister of Research and Higher Education in Norway, Iselin Nybø [13].

A recent study on Norwegian DSOs in context of incident response is pointing out a gap between IT-staff and ICS-staff in terms of understanding information security, consequently, a cross-functional team is recommended [14]. Furthermore, in light of current APTs and possible cyber intrusions, the industrial detection mechanisms are found to be insufficient, and may not be improved due to various risk perceptions. Additionally, the incident response training within the Norwegian power industry is given low-priority, and evaluation of post-training, as well as minor incidents, are not performed [14]. It is, however, recommended that cyber security training of regular staff should be considered as fundamental in terms of protecting power systems, as this would enhance the defence against coordinated cyber attacks [15]. Unfortunately, it's practically impossible nor advisable to conduct advanced cyber security training on real-world cyber-physical systems, such as the smart grid, as it would lead to unacceptable risks [16, 6]. Accordingly, there is a strong urge to acquire the ability of creating and carry out smart grid cyber-security training scenarios, without causing harm to the real-world systems; this is where a cyber range (CR), or more accurately, a cyber-physical range (CPR) comes into play.

> "An important aspect of cyber security is the response capacity when an incident occurs. However, the largest investments seem to be made in tools and systems to fight cyber-attacks rather than addressing human behavior as a means of improving cyber security technologies and processes. Consequently, there is a need to gain further knowledge on human behavior in cyber security incident response and use this knowledge to strengthen the response capacity."
>
> – Institute for Energy Technology (IFE) [16].

Through our study, we found only a dozen cyber ranges related to smart grids and cyber security. In particular, only one is located in Norway, called the Norwegian Cyber Range (NCR). The NCR was officially opened on September $4^{\text{th}}$, 2018 by the Norwegian prime minister, Erna Solberg, as a consequence of the growing digitalization of our society [17]. Additionally, the need for educating cyber security personnel in terms of facing the ever-increasing cyber threats to our society has never been greater, including the cyber security awareness and preparedness among organizations. Hence, the primary focus of NCR lies on testing, training and practicing cyber security in different critical infrastructure sectors. The vision is to build competence based on simulation of real-world cyber security incidents, observations and scenarios [17].

Unfortunately, it's very hard to design and build a cyber range, and even harder a CPR, due to the natural complexity of a CPS, including networks and system of systems. Additionally, it requires the appropriate skills and proficiency from various disciplines, especially within the field of IT and OT. Moreover, the field of cyber ranges are currently facing various knowledge gaps, and our study identified multiple challenges, such as scalability, flexibility and realism. In this thesis, we aim to cope with some of these challenges by designing and validating a novel and virtual SGCR – based upon up-to-date stakeholder goals – that is suitable for cyber security training in the smart grid domain. We name the cyber range architecture; *Smart Grid Cyber Security & Cyber-physical range for CINELDI* (SG3C).

## 1.1 Objectives and Contributions

By using design science methodology as a guiding tool, our aim is to elicit the stakeholder goals and the necessary requirements for a SGCR. Moreover, we intend to use these requirements to build a novel architectural design for a SGCR. In particular, this SGCR must support cyber security capabilities in terms of incident response training.

The research goal is equivalent to our specified design problem, which is to;

> ***Improve stakeholders ability to create and execute smart grid cyber-security training scenarios by creating a novel design for a SGCR.***

In summary, the thesis objectives are:

- Identify the stakeholders and elicit the stakeholder goals.
- Apply the identified goals to define a set of artifact requirements.

- Validate the potential design by testing various mechanisms, and discuss whether the design fulfills the stakeholder goals, requirements, and ultimately, whether or not it solves the design problem.

By its nature, a cyber range has a wide-range of applications other than cyber security training, for instance, testing of system components, team building, research, and product development [18]. However, our main focus lies on the contribution towards hands-on training and improvement of cognitive skills of cyber security professionals. Designing and creating training scenarios are outside the scope of this thesis, but we aim to provide the ability to do so.

We contribute with the following:

- Stakeholder goals and requirements for a virtual smart grid cyber-physical range (SGCR) with cyber security training capability and;
- A novel architectural design for a fully virtualized SGCR.

## 1.2 Outline

Beginning with Chapter 2, we introduce the traditional electric power grid, the emerging smart grid and critical infrastructures in general. Followed by Chapter 3, where we move into related topics of security, attacks and threats. We explain the capabilities of an advanced persistent threat (APT) and the cyber kill chain (CKC) applied to ICS. We also describe previous cyber attacks on critical infrastructures. The previous cyber attacks are important to understand as they are a fundamental motivation for conducting our thesis. In Chapter 4, we explain information security incident management through a review of the ISO 27035 standard. In Chapter 5, we provide in depth knowledge of the state-of-the-art cyber ranges, including taxonomy, requirements, architecture, and ongoing challenges. In Chapter 6, we explain design science methodology, as well as the adapted framework we used to conduct our research. The chapter includes an introduction to design science terminology, design cycles and empirical cycles, and explains how they are connected. In terms of the supplementary methods, we explain how the literature study was carried out and how the semi-structured interviews were conducted through narratives. In Chapter 7, we present our main findings, such as the stakeholder goals and the artifact requirements. Final artifact design, tools and roles are also presented. Lastly, the prototype testing and validation is described and results are given. In Chapter 8, we discuss the fulfillment of requirements in terms of the SG3C artifact design, outline limitations and provide suggestions for future work. Finally, in Chapter 9, we provide a brief thesis summary and conclude our research.

# Chapter 2
# Smart Grid and Critical Infrastructures

This chapter represents the first of four fundamental background chapters, and will introduce terminology and theory to establish a solid context for further reading. Section 2.1 introduce the conventional power grid and highlights some its current challenges. This is then followed by Section 2.2, where the emerging smart grid is described and how it is thought to solve some the challenges related to the conventional grid. Finally, Section 2.3 explains critical infrastructures in general, including the common architectural Purdue model, interdependency with other critical sectors, as well as communication flow and protocols.

## 2.1 The Conventional Power Grid

The conventional power grid supplies its customers with on demand electricity and is structured around centralized power generation [19]. On a high level, today's grid is comprised of three major elements: generation, transmission and distribution. An overview of the three systems can be seen in Figure 2.1. In the generation section, bulk power is generated by large generator stations from primary energy sources such as hydropower, nuclear fission, fossil fuels and others [19]. The transmission grid acts as a high-voltage bridge between the generation units and the distribution grid. It also serves to interconnect power grids across national borders. Before entering the transmission grid, the electric current is transformed up to high-voltage. This is done in order to mitigate power loss during transmission across large distances [20]. The distribution grid is where power is delivered to end users. The electricity is then transformed down to voltages suitable for home appliances and routed to end-users.

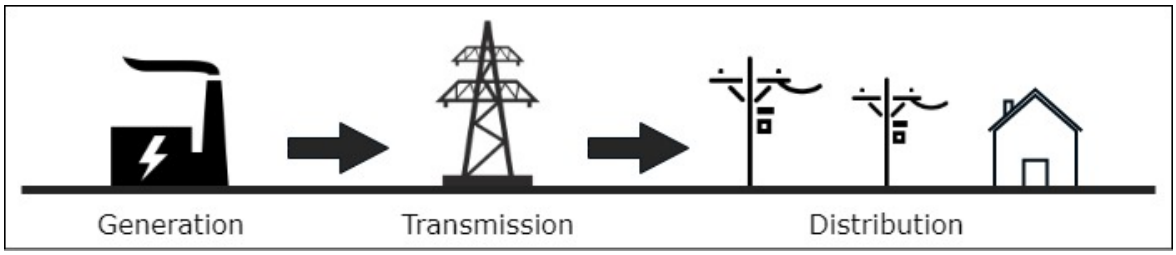


**Figure 2.1:** Graphical illustration of energy generation, transmission and distribution in the conventional power grid. Direction of power flow is indicated by the black arrows. Adaptation from [21]

Two central entities in the conventional power grid is the distribution system operator (DSO) and transmission system operator (TSO). The following is a brief introduction to their roles and functions.

**Distribution System Operator**

The  defines in their 2017 article "*Open Networks Project DSO Definition and R&R* a DSO" as the following [22]:

> *A distribution system operator (DSO) securely operates and develops an active distribution system comprising networks, demand, generation and other flexible distributed energy resources (DER). As a neutral facilitator of an open and accessible market it will enable competitive access to markets and the optimal use of DER on distribution networks to deliver security, sustainability and affordability in the support of whole system optimisation. A DSO enables customers to be both producers and consumers; enabling customer access to networks and markets, customer choice and great customer service.*

ENA also lists the following DSO roles and responsibilities:

- *Maintain distribution network resilience and security*
- *Maintain system stability*
- *Provide fair and cost-effective distribution network access*
- *Provide capacity in an efficient, economic, coordinated and timely manner*
- *Support whole system optimisation*
- *Enabling and facilitating competition in energy markets*

– *Provide and maintain systems, processes and data to facilitate markets and services.*

**Transmission System Operator**
Directive 2012/27/EU of the European parliament defines a transmission system operator (TSO) as the following [23]:

> *Transmission system operators are responsible for providing and operating high and extra-high voltage networks for long-distance transmission of electricity as well as for supply of lower-level regional distribution systems and directly connected customers.*

Furthermore, the ENTSO-E Supporting Document for the Network Code on Operational Security lists the following TSO responsibilities [24]:

– *Continued power supply to the demand facilities connected to the transmission system*
– *Power flow control to avoid congestion*
– *Frequency stability*
– *Voltage stability*
– *Emergency control and restoration.*

In effect, it is the TSOs objective to maintain safe and reliable high-voltage electricity from the generation units to the distribution network.

**Challenges with the Conventional Grid**
As the global climate is seeing steadily increasing temperature averages, linked to the emission of green house gases (GHGs), it is important for society to transition to renewable energy sources (RESs). In fact, according to Lo and Ansari [25], 80% of all globally generated energy, is fossil fuel-based, directly linked to the GHG that causes environmental effects such as global warming.

However, the centralized structure of the conventional grid is not ideal for integrating large-scale integration of RES, as many RES also fall in the category of DER [26]. Wind farms and photovoltaic systems (PVs) being two prominent examples. As both sunlight and wind is free to all and available most places, these energy sources will open up for many new actors on the energy generation side. The distributed architecture of the smart grid takes this availability into account, and enables generator units to be connected from nearly "anywhere". Not only new commercial actors, but traditional

consumers is also thought to participate as energy producers, by installing micro generator units such as PVs at their property. In order to achieve this, the grid must not only be distributionally structured, but also support bidirectional power flow. The latter being necessary for the consumers to transmit excess power back to the grid [27].

Another archaic feature of the conventional grid is the unidirectional communication throughout the grid. The lack of bidirectional communication prevents interaction between utilities and their users. For instance, it is not possible to measure the amount of energy consumed by a particular consumer [19]. This complicates billing as well as grid state monitoring. A DSO can not tell if a residential area is experiencing a blackout or not. Instead the DSO must rely on the end user reporting failures by manually contacting the DSO.

In the sections above we have given a high-level overview of the conventional power grid and some of its key challenges. Most importantly the fossil-based centralized architecture, unidirectional power- and communication flow. These issues are the main driving factors for the development and implementation of the smart grid. Next section will give a introduction to the smart grid and what challenges it is designed to solve.

## 2.2 The Emerging Smart Grid

In order to increase power utilization, efficiency, and reliability as well as facilitate the integration of renewable energy resources (RES), a framework for the next generation power grid, the smart grid concept has been proposed. Key features are: bidirectional communication and power flow, as well as enhanced monitoring, fault detection, and maintainability through expansive sensor networks, coupled with high bandwidth communication technologies and computational intelligence. Other highlighted features are increased grid resilience through defensive islanding, as well as consumer participation enabled by the bidirectional power flow and integration of micro generator units. These features are largely achieved by coupling modern ICT solutions with the existing power grid [19, 27].

As mentioned in Section 2.1, it is crucial for the global community to transition to RES, such as wind and solar. This is essential in order to reduce greenhouse gas emissions and stay within the 2 °C limit of the Paris Agreement [28]. However, as most RES are weather dependent and require dispersion across large areas, they do not integrate optimally with a centralized grid structure. To tackle this issue and increase the overall flexibility of the grid, the smart grid will adopt distributed or decentralized energy generation (DG). The DG enables integration of distributed energy sources, reduces the distance from production to load-site, and decreases energy loss during

transmission. Combined with smart infrastructure, smart management, and smart protection systems, DG provides effective monitoring and control systems during faults without affecting the whole transmission and distribution chain [27]. Figure 2.2 contrasts the current, centralized grid to the decentralized energy production in the future smart grid.

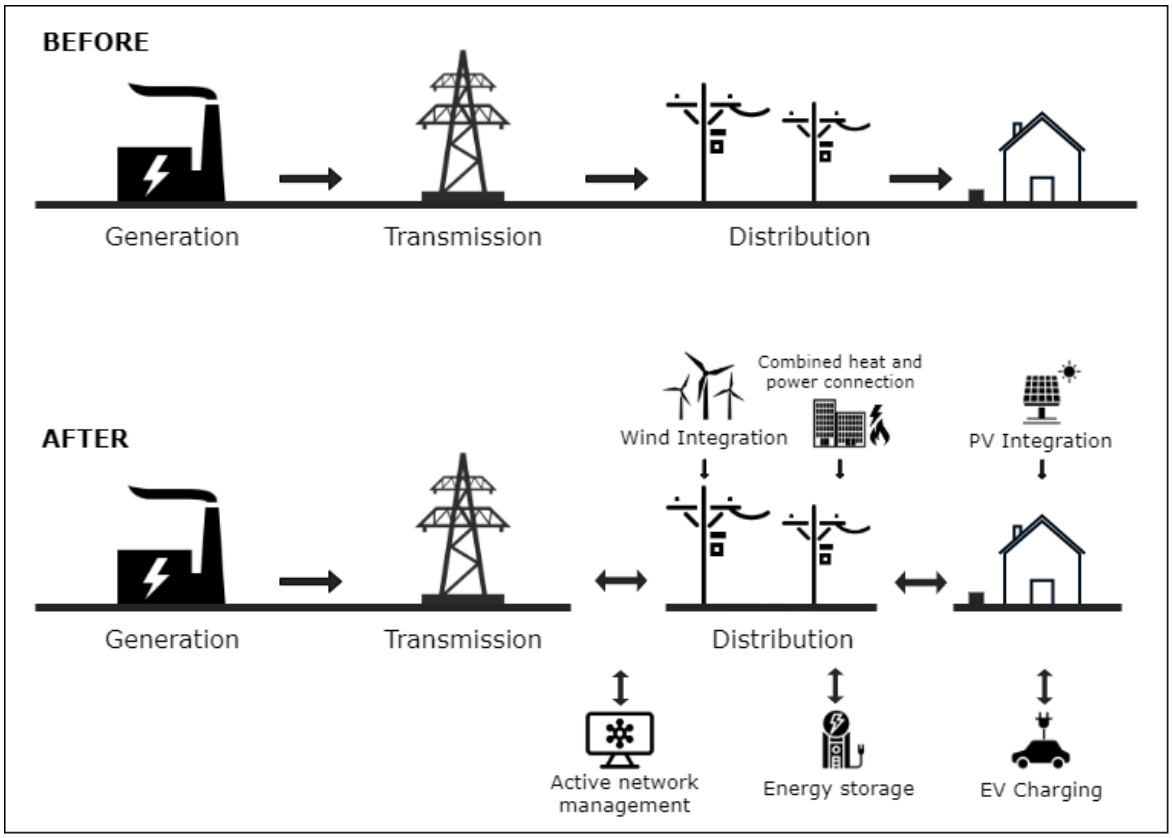


**Figure 2.2:** Graphical comparison of the centralized architecture with one directional power flow in the conventional grid, versus the distributed architecture and bi-directional power/communication flow in the smart grid. Adaptation from [21].

Integration of bidirectional energy flow enables consumers to install microgenerator units on their property, such as wind or solar, and sell excess energy back to the grid via the energy market. Transitioning the consumer into a producing consumer or prosumer as they have come to be known in the literature [19]. As renewable energy sources are weather dependent, they create a somewhat intermittent supply of power. To mitigate this intermittence, the use of distributed energy storage (DES) systems has been proposed. Storing excess energy in times of high supply, and then resupplying the grid when demand is higher than production—effectively smoothening the demand curve. Technologies such as electrochemical batteries,

pumped hydroelectric energy storage, hydrogen storage, and flywheels have been proposed as components in the distributed storage model. But also electric vehicle (EV), where the owner of an EV can charge its batteries when demand in the grid is low (G2V), and then resupply the grid when demand is high (V2G). Combined with real-time pricing, the car owner can be incentivized by monetary gain by providing his EV as an asset in the distributed energy storage system [21].

An advanced metering system (AMS) is an essential element to support the improved monitorability and efficiency of the smart grid. AMS, also known as smart meters, are endpoints located at load-site that measures real-time energy consumption by capturing metrics such as voltage, current, frequency, and phase angle [19]. The AMS can also receive control signals, and come equipped with an actuator, enabling the AMS to disconnect the respective load-site from grid. Measurement of real-time power consumption enables precise billing, but more importantly, it is thought to enhance demand-side management (DSM) [27]. Demand-side management is the idea that consumers can more efficiently adjust their energy usage, either manually or by automated smart appliances, if they can easily monitor their energy consumption in real-time. The AMS is also supported by bidirectional communication technology, and thus enables DSOs to detect outages early. Not needing to rely on customers manually reporting outages by phone or similar means.

Bidirectional communication is one of the most attractive new features in the smart grid. Combined with high data throughput, wireline, and wireless communication systems, it is the key enabler of the sensor and actuator networks as well as the advanced metering systems. Together, these systems aid fault prevention, detection and localization as well as improve the ease of maintainability. Fault prevention can be done by utilizing the sensor network to observe voltage and currents amplitudes, thermal variations, transient and steady-state parameters [19]. Detecting signs of failure early and avoiding major faults. Fault detection, diagnosis, and fault localization can be achieved by widespread gathering of measurements from phasor measurement units (PMUs) and smart meters. Maintainability is enhanced by the same factors, as faulty parts can be detected, located, and replaced based on collected measurements.

In order to support the large amount of smart meters and sensors proposed for the smart grid infrastructure, the smart grid will be dependent on having cost-effective, high bandwidth communication systems that covers large geographical areas [27]. There are two categories of communication technologies, wireless and wireline. Wireless is advantageous for its low installation cost, large area of coverage as well as high scalability. Its main drawbacks are unrealiability due to radio interference and electromagnetic interference (EMI). Whereas many wireline solutions are less affected by EMI and provide better reliability, but generally comes with

higher installation costs. For certain areas, installation of wireline solutions may be impractical altogether. The debate on precisely which communication technologies should be implemented in the smart grid is still ongoing [29]. However, the following is an overview of the, so far, most promising technologies available and some of their proposed applications.

**Optical Fiber Communication**
An optical fiber communication (OFC) delivers nearly unlimited bandwidth across large distances, with strict quality of service (QoS) measures. It is also immune to electromagnetic interference. As such, it is one of the most promising technologies to offer reliable high throughput data transmission in the smart grid infrastructure [19]. The main drawback is high installation cost, with some areas being infeasible for OFC installation at all.

**Cellular**
Cellular communications, especially UMTS (3G) and LTE (4G/5G), are attractive solutions for wireless, high bandwidth applications, as many geographical areas already have existing (3G/4G) coverage [19]. Possible smart grid applications for the coming fifth-generation LTE (5G) are also currently being researched. One such application is short distance communications using very high frequencies (60 GHz). Researcher Dheena found that 5G transmission using the 60 GHz band is as reliable as optical fiber communication. Making it the only currently known wireless communication technology nearly immune to electromagnetic interference [30]. The drawbacks of the 60 GHz band is short transmission range and poor material penetration, requiring clear line of sight for optimal use. However, the very high transmission rate (up to 1 Gbps) and resistance to EMI, makes it an attractive solution for short distance, high throughput applications.

**WiFi over WLAN**
Shaukat et al. [27] states that a selection of the IEEE802.11 (Wi-Fi) standards is likely to be used in the smart grid infrastructure. In particular, their paper mentions: 802.11e for applications requiring strict quality of service (QoS) on the wireless medium, 802.11p for vehicle to grid (V2G), and 802.11s for applications requiring multi-hop support.

**Digital Subscriber Line**
A digital subscriber line (DSL) enables digital data transmission over telephone lines. DSL technology includes: asymmetrical DSL (ADSL), ADSL2+, and very high DSL (VDSL). Ranging in speeds from 8 Mbps download/64 kbps upload, to 54 Mbps download/16 Mbps upload. As installation costs can be significantly reduced by utilizing existing telephone lines and infrastructure, DSL is thought to be a cost-effective alternative wherever suitable [19].

**Satellite Communication**
A satellite communication (SC) offers the best solution to remote access control and monitoring for rural areas where other communication infrastructures do not exist [19]. SC can also be used as a backup system in case primary communication links fail. The drawbacks are higher delay, channel fading, and high cost [27].

## 2.3 Critical Infrastructures

A critical infrastructure (CI) is described as all systems and constructions that maintain the critical functions of a society, which in turn covers the basic needs of the population, as well as the sense of safety [31]. Definitions of a critical infrastructure (CI) are slightly different between governments or unions of countries, but are essentially the same. The United States Department of Homeland Security defines a CI as; "the assets, systems, and networks, whether physical or virtual, so vital to the nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof." [32]. Most countries have multiple CIs within its borders, in fact, they exist in every country worldwide [32]. Many but not all CIs are dependent on a so-called cyber-physical system (CPS) [33]. According to NIST; "A cyber-physical system comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas" [34]. Thus, a CPS is allowing for the *interaction* between the cyber world and the physical world, such as a smart grid in its entirety.

Furthermore, a smart grid could also be viewed as a system-of-systems, since it comprise multiple smaller CPSs (e.g. ICSs, PLCs, RTUs, etc.). An industrial control system (ICS) is highly leveraged in the traditional power grid, as well as industrial manufacturing, distribution, transportation, and other practical industrial applications [33, 35]. An ICS is relying on a ICT network and communication infrastructure, and is primarily used for remote command and control of dispersed assets, usually over thousands of square kilometers. About a decade ago, such industrial remote controlling was nearly infeasible, and plant operators were facing time-consuming and manual endeavors [35]. Since then, a rapid development of networking technology facilitates remote command and control through an ICS, and thereby promoting reduced costs [36]. Moreover, an ICS can share communication and signalling data from a local control center to remote operational field sites using wide area network (WAN) technologies, thus, span large geographical areas. However, the interdependency between ICS and ICT raises a safety and privacy concern when addressing CI security, as the telecom industry or any other third-parties providing WAN technology are usually not in the control of the same organisation. It is important to note

**Table 2.1:** European sectors and industries identified as critical infrastructures [32].

| No | Sectors | Industries |
|---|---|---|
| 1 | Energy | Electricity, Natural gas, Oil |
| 2 | ICT | Telecom, Broadcasting systems, Software, Hardware and Networks |
| 3 | Traffic and Transportation | Shipping, Aviation, Rail traffic, Road traffic, Logistics |
| 4 | Healthcare | Healthcare, Medicines and Vaccines, Laboratories |
| 5 | Water supply | Dams, Storage, Treatment and Distribution networks |
| 6 | Finance and Insurance | Banks, Stock exchanges, Insurance companies, Financial services |
| 7 | Government and Administration | Government, Parliament, Legal institutions, Emergency services |
| 8 | Nutrition and Agriculture | Food trade, Agriculture |
| 9 | Media and Cultural assets | Radio, Press, Symbolic buildings |

that this is just one of multiple examples on the interdependencies that can arise when studying CIs [37]. The various critical sectors and the corresponding industries identified by the European Commission are listed in Table 2.1 below.

The European Union Agency for Cyber Security (ENISA), formerly known as the European Union Agency of Network and Information Security, is the center of expertise for cyber security in Europe. They have been working to make Europe cyber secure since 2004, and have contributed with several publications relevant to this thesis. One of these publications discusses the topic of communication network interdependencies in ICS systems and provides, among other things, a concept of interdependencies between the main CI sectors, which is illustrated in Figure 2.3 [37].

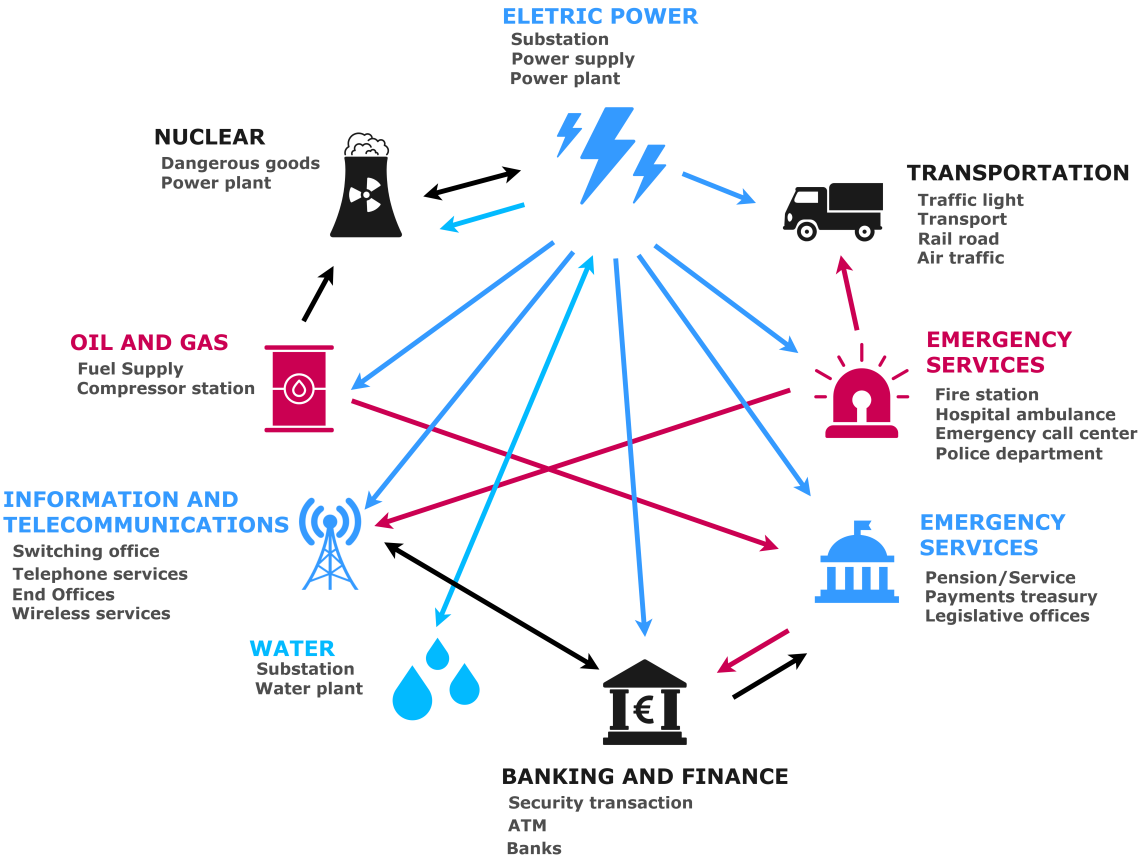


**Figure 2.3:** Illustration highlighting interdependencies between critical infrastructures. Source: Adapted from [37].

It should be clear from Figure 2.3 that the energy sector is one of the most influential and important infrastructures, as it has multiple connections to others. Moreover, the figure shows that the interconnections are bidirectional in most cases. As a result, the cascade or intercorrelation between these essential infrastructures can lead to a potentially unwanted chain reaction or a domino effect of harmful events, which can be initiated by for example a cyber attack, causing widespread malfunction or otherwise catastrophic effects [36].

There are four types of interconnections according to ENISA [37]:

- **Physical:** when a physical product from one infrastructure is a physical input for the other, they are said to be physical dependent. For example, a lot of transportation is dependent on oil or electricity as input.
- **Geographical:** when an environmental event is able to cause a change in state of an infrastructure, it is said to be geographical dependent. For example, a

water plant can be affected by the amount of rainfall or precipitation over a time period.

- **Cyber:** when the information broadcast through the underlying ICT technology is a condition for the state of an infrastructure, it is said to be cyber dependent. For example, the electricity production is conditioned on information transfer of customer consumption.
- **Logical:** when the state of one infrastructure depends on the state of another through some kind of mechanism that is not physical, geographical, or linked by any form of ICT, then they are said to be logical dependent. For example, a decision made by the human factor (i.e., process of decision-making).

The different sectors within a country are not only getting more interconnected with each other, but also to the CI sectors of neighbouring countries, due to the air environment, rivers, seas, roads, etc., and of course, the cyberspace [32]. Leading to multiple advantages, but on the downside, a single point of failure could lead to a devastating chain reaction both within countries and between countries. For example, as to what concerns the energy sector, a power outage of one country could potentially spread and affect another country that is relying on the former to deliver electrical power. Thus, likely causing instability or any other unwanted impacts on the neighbouring power systems. Unfortunately, the topic awareness is low and this type of risk is not usually considered. However, for obvious security reasons, it is necessary and very important for CI operators among countries to become aware of the risks they are exposed to, by the presence of interdependencies in ICS-SCADA communication systems [37].

Dr. Stockton asserts there is evidence that adversaries are positioning themselves to cause multi-state blackouts, and additionally, ramping up their efforts to embed sophisticated malware across bits per second networks. Stockton is further stating the importance together with the anticipation of taking these threats seriously in a crisis environment [38]. Next subsection will introduce a purdue model for ICS-SCADA, where the typical and technical essentials of a CI resides.

### 2.3.1 ICS-SCADA Architecture

Analysing the ICS-SCADA architecture at the network communication and protocol level is necessary in order to understand and identify possible security vulnerabilities, as well as cyber security threats towards CIs. In Chapter 3, some of the current and global cyber threats will be identified. A general ICS-SCADA architecture was developed by the International Standard on Auditing (ISA). Hence, the ICS-SCADA architecture will hereinafter be known as the ISA95 architecture. The specific ISA95 architecture is thoroughly analysed from a security perspective by ENISA [37].

The different CI sectors and industries from the previous subsection, such as electrical power utility, oil and gas, emergency services, which serves a country with different purposes, but they usually have commonalities in the underlying technology, with embedded off-the-shelf software and strict standards (e.g. ISA95 or ISA99) [36][39]. This common technology is known as an ICS, which in turn consists of a supervisory control and data acquisition (SCADA) system, with one or more HMIs. The ICS-SCADA system orchestrates the use of programmable logic controllers (PLCs) and/or remote terminal units (RTUs). The ICS, including SCADA, HMIs, PLCs and RTUs is of great importance when addressing the industrial telemetry system, as they are networked together to allow sharing of data. Furthermore, the clash of operational technology (OT) and IT disciplines comes with a myriad of terms and acronyms, it is important to acquire an overview, here through figures and tables.

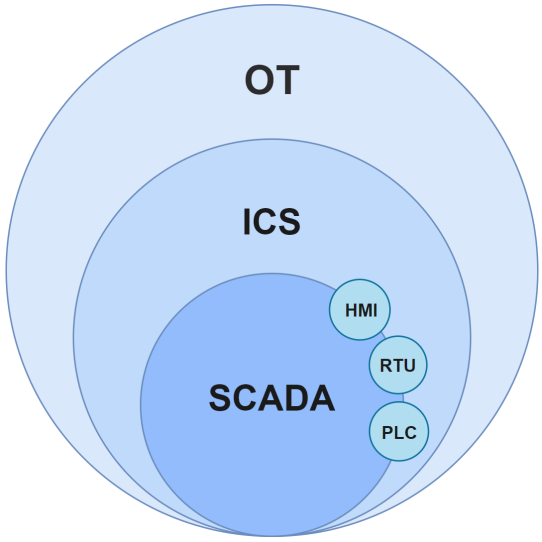


**Figure 2.4:** Showing the relation between the main OT concepts. Adapted from [40]

OT is the main umbrella term for all systems that manage industrial operations, as opposed to administrative operations [41]. In other words, OT operates the networks that allow for common norms and functions, such as the electricity turning on in the house or the clean water coming out of the facets. It is important to note that OT-ICS requires high-availability, usually real-time data. In contrast to OT, the security in IT-systems is a high priority and is mainly covered by the confidentiality, integrity and availability (CIA) triad, while both confidentiality and integrity come second to availability in OT. This is one of the main differences between IT and OT, in terms of security. As depicted in Figure 2.4, the ICS is a large segment of OT. As previously mentioned, the ICS is a general term for the entire monitor-and-control function provided by SCADA. The SCADA system consists of three main components; a central control center, local control systems and communication systems. The main

purpose of SCADA is data-acquisition and control from the help of PLCs and RTUs [40]. All of which are contained within the Purdue model, which in this case, is the ISA95 architecture, depicted in Figure 2.5.

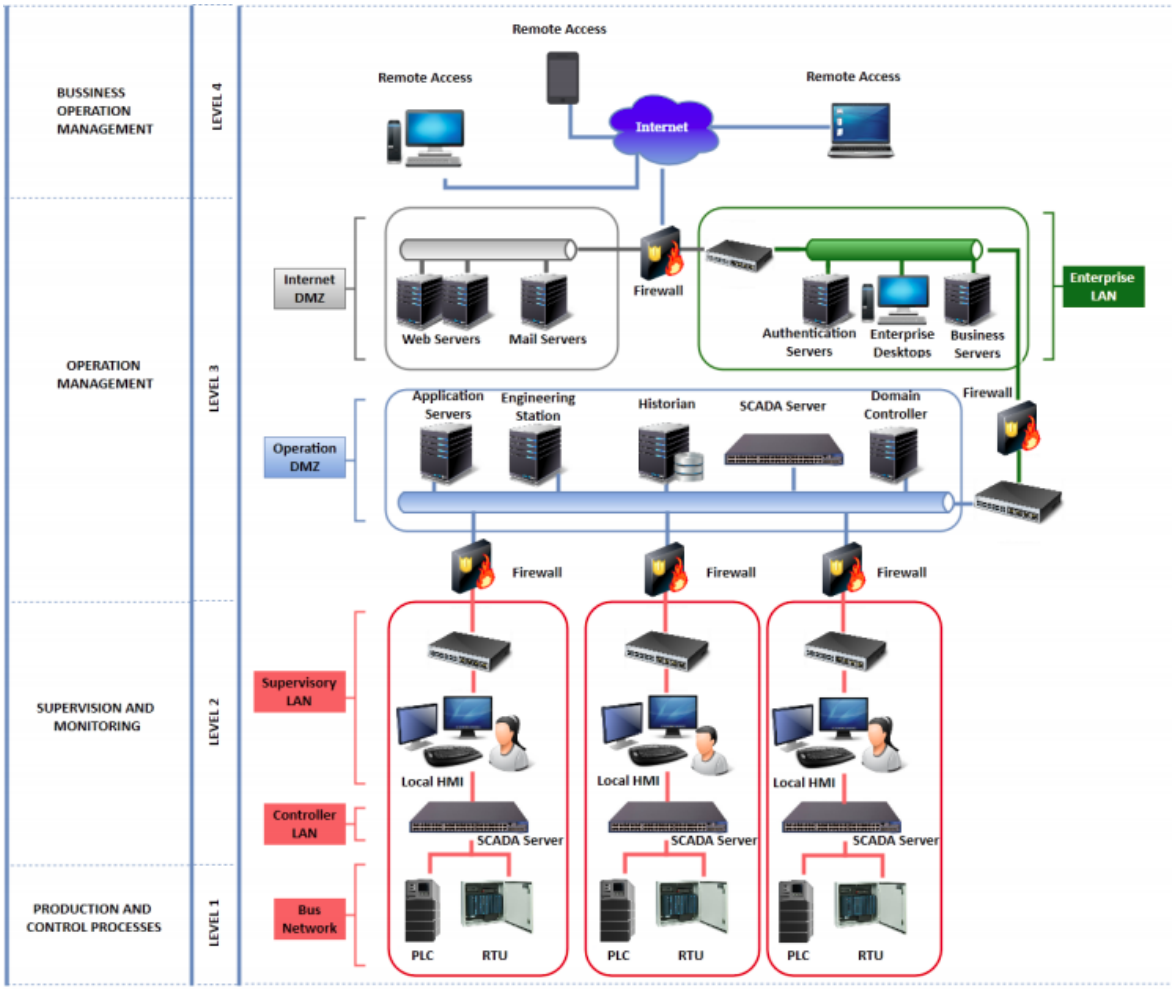


**Figure 2.5:** ISA95 levels applied to a ICS-SCADA Architecture. Reused with permission from [37].

### Level 1

Consist of all the field devices, and constitutes the production and control processes. Examples of such field devices are PLCs, RTUs, motors, actuators, transducers, pumps, valves, relays, sensors, etc. The field devices communicate between each other, and the PLC acts as a puppet master, by giving commands, receiving and processing data, to or from the other devices. Normally, the PLC forwards the command to several RTUs, which in turn are positioned nearby the other field devices and control their operational state [37][41].

**Level 2**
Consist of the SCADA server and local human machine interface (HMI), and constitutes the supervision and monitoring. The main role of HMI/SCADA is to gather and combine data from level 1, using a specific protocol that is compatible with the PLCs. HMI is, as the name suggests, an interface for a human operator to interact with a system, in this case SCADA, in a simple and intuitive way, often by the push of a button on a touch-screen console. In the real-world, it is common to find the HMI applications running on deprecated or obsolete operating systems (OSs), such as old Windows[1] or Linux versions [37].

**Level 3**
Contains the more complex devices that constitute the operational management, and is tasked to optimize and execute the manufacturing processes, also known as manufacturing execution systems (MES). This level contains different servers for application and business functionalities, engineering workstations, historian, domain controllers among others. The engineering station is usually a very reliable computing platform designed for distribution of system modifications, maintenance, diagnostics and configuration of control system applications and any other control equipment, such as PLCs or RTUs [42]. Historian is the system in charge for collecting and storing all data logs, alarms and other assets generated by the different field devices. The domain controller manages the addresses and domains of the SCADA network. All of these devices are logically connected through a switch and communicating using specific protocols, as shown in Table 2.2 [37].

**Level 4**
Is the highest level in the ISA95 architecture, and constitutes the business and operation management. This level represents all form of remote communication to/from the CI over the Internet (WAN) (e.g. over a virtual private network (VPN) connection). The software on this level is not specific, but the same used in other IT areas. Software on this level includes enterprise resource planning (ERP), control room management (CRM), and business intelligence (BI). The ERP can integrate planning, manufacturing, sales, and other business phases. CRM software is mainly used by operators in a control room to govern the entire pipeline system through a SCADA system. BI is a business analyzer software used for understanding strengths and weaknesses within the organization [37].

### 2.3.2 Communication Flow and Protocols

A brief overview of the ISA95 communication flow and common protocols are given in Figure 2.6 and Table 2.2, respectively. As shown, there are multiple protocols serving

[1]Windows 7 obsolete 14 January, 2020 – https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020

**Table 2.2:** Examples of protocols for each level in a typical ICS/SCADA system. There exists many more, but these are very common in use [37].

| Level 1 | Level 2 | Level 3 | Level 4 |
|---|---|---|---|
| Profibus | DNP3 | MODBUS | OPC |
| WiMAX | IEC 60870 | TCP/IP | TCP/IP |
| ISA SP100 | SOAP | Profinet | WiFi |
| MODBUS | OPC | DDE | DCOM |

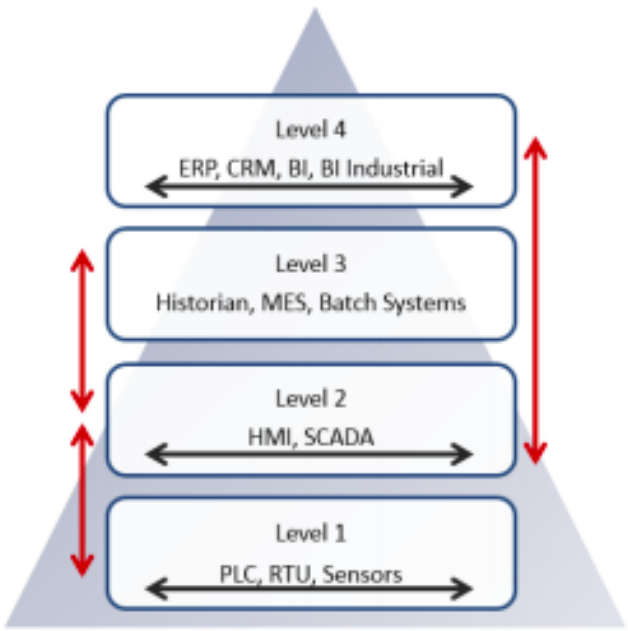


**Figure 2.6:** Relation of the communication between the different levels of ISA95. Reused with permission from [37].

its purpose for each level. Notice that some protocols are flexible and can be used in more than a specific level (e.g. TCP/IP). From the figure, numerical values are horizontally exchanged on level one, as well as a bidirectional vertical communication with level two. Furthermore, the interchanged information or actions acquired by SCADA are forwarded to the HMI for graphical representation. A bidirectional communication between level two and three is exchanging the originated information from level one, that was processed in level two and finally sent to higher-level systems to register (Historian), verify (MES) and transferred to other processes (Batch) if necessary. Between level two and level four, the operational status, progress etc. are exchanged between ERP, BI, etc. systems [37].

# Chapter 3
# Security, Attacks and Threats

Section 3.1 discovers the characteristics of an advanced persistent threat (APT), and point out the possible danger of facing such a threat. Section 3.2 provides a step-by-step explanation of the ordinary cyber kill chain (CKC) model. More importantly, the improved and tailored CKC model applied to ICS will be explained in detail. Section 3.3 investigates previous cyber attacks, such as Stuxnet and Havex. In particular, an in-depth case study of a previous and real-world cyber attack, called Industroyer/Crashoverride, on the Ukrainian power grid will be provided.

## 3.1 Advanced Persistent Threat

In the recent years, an alarming escalation of the prevalent cyber security incidents has emerged, and have created a major cyber security concern on a global basis [43]. However, it is not a question of single incidents and breaches when talking about cyber attacks on ICS in critical infrastructures, but rather a campaign of efforts to devise an effect, which also represents the attack as a whole [44]. This campaign is usually carried out by a group of well-funded attackers, and is recognized as an APT using a multi-staged approach by utilizing the entire, or parts of the cyber kill chain (CKC), as further elaborated in Section 3.2. The diversity of APTs are large due to each attack being unique and different, but are commonly recognized as stealthy, targeted, and data focused. APTs are not advanced because of a sophisticated attack, but rather the sophistication of the attacker [45]. Moreover, APTs are often described differently, but probably best by author and cyber security expert, Dr. Eric Cole, as he compares an APT to human cancer and explains that; "the advanced persistent threat is cyber cancer which means traditional detective and reactive measures will not work. At point of compromise there is nothing visible and by the time there are visible signs of attack, the damage has already occurred. We have to assume that even though everything looks fine on the surface, underneath the surface the network might be compromised." [45]. The persistent part in APT, comes from the persistent nature and willpower of the attackers to never quit until they are successful, and this

is where the true damage emerges. Nowadays, the attack is non-stop, the attackers are not going away and they keep "hammering" on the defender's door. Consequently, Cole is suggesting that organizations keep the guard up at all times by running defense mechanisms and other countermeasures 24-7, every day of the year [45].

APTs have been one of the most challenging threats to the safety and security of critical infrastructures, and are hard to deal with in general, mostly due to the human-driven nature of the attacks, and ability of exploiting zero-day vulnerabilities that are normally unknown to the public [46]. APTs are a particular class of threats targeting cyber-physical systems, and are known to be very goal or target oriented. Meaning the attackers make sure they have sufficient knowledge of system architecture, valuable assets, and even defense strategies, as opposed to opportunistic adversaries who spray and pray. Additionally, APTs are stealthy and can disguise themselves to appear as a valid user, thereby achieving a long dwell or sojourn time [45]. The dwell-time is defined as "the number of days an attacker is present in a victim network before they are detected" [47]. Furthermore, APTs can invalidate cryptography, firewalls, and intrusion detection systems (IDS) [48]. Thus, APTs pose a cyber security challenge for organizations including critical infrastructures. The modern APTs can evade cyber security efforts, and cause severe damage to organizations. Multiple attack vectors and entry points can be used by a skilled and resolute cyber criminal to navigate around defenses, breach the enterprise network and dwell or remain hidden in the system for months or even years [49]. However, as indomitable and scary as it sounds, there are several security measures and mitigation steps for an organization to consider [45].

## 3.2 Anatomy of the Cyber Kill Chain applied to ICS

Security personnel can see how defense is doable by proactively detect (advanced) persistent threats using the CKC. The original CKC is well-recognized in the security community and was developed by the American corporation Lockheed Martin[1] in 2011. The CKC is a stepwise and chained model for analyzing the offensive actions of a cyber attack, and is used by ICT-system defenders such as incident response teams, digital forensic investigators and malware analysts [50]. The model is an auxiliary tool for defenders to better understand the thinking of an adversary, and/or detect, disrupt and respond to the progress or state of an ongoing cyber attack, as well as using this knowledge to enhance information and cyber security wherever possible [44, 51]. The model is much based upon the fact that; "If you know how they work, you can learn how to stop them" [49]. The seven steps of the "ordinary" CKC are shown in Figure 3.1 below.

[1]Lockheed Martin and CKC – https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html#

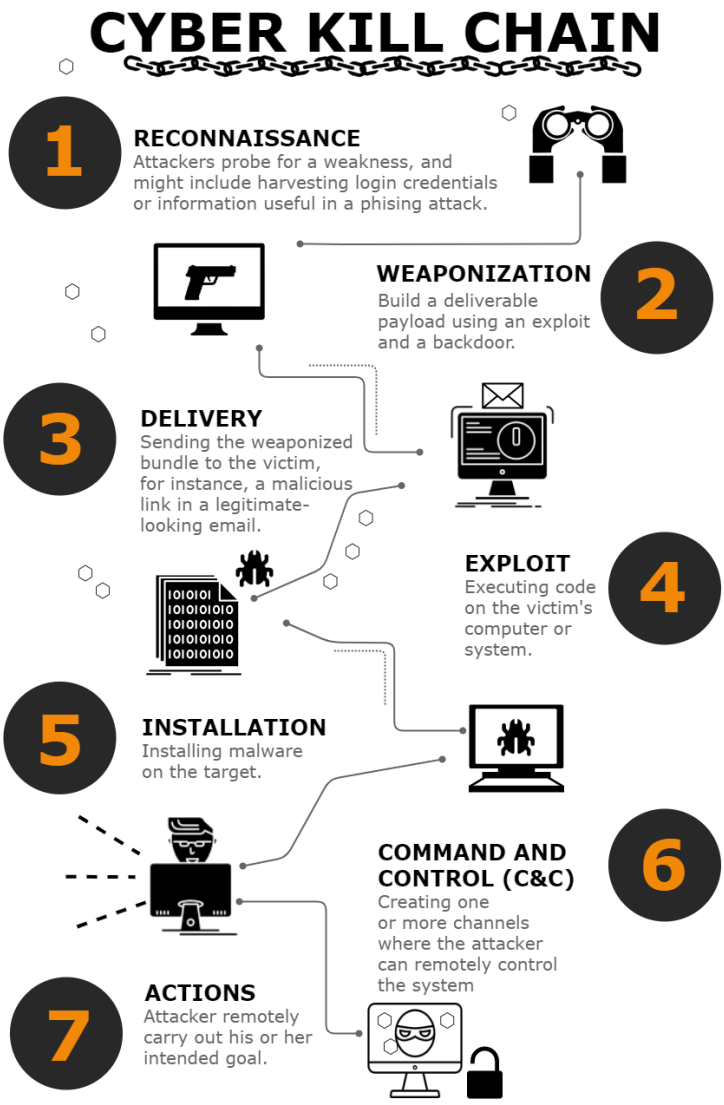


**Figure 3.1:** Depection of the original cyber kill chain. Adapted from [52].

The CKC model has been highly successful in ICT and enterprise networks, however, not so well suited for OT/ICS specific systems, as those utilized in critical infrastructures. The traditional CKC model has certain drawbacks and disadvantages; (1) It leads the defender's focus away from insider threats, and towards a more perimeter-based security[2]; (2) It does not work well for insider threats, and; (3) every cyber attacker is a potential insider [51]. An insider threat is a conundrum or major challenge in cyber security, where an insider could trade valuable and vital information with an attacker on the "black market". The adversary is then capable to compromise the system by applying that information and escalate from there.

[2]Perimeter-based security is a technique to protect a network by controlling access to the entry and exit points.

A proactive security approach should be favored to deal with these insider threats, rather than a reactive action [53].

The CKC model, as shown above, is not directly applicable to an ICS-specific cyber attack, but serves as a guideline and concept on which to build further [44]. Hence, various proposals have been made by researchers to extend the traditional CKC towards a more industry friendly version. This extended CKC is what we call an ICS-CKC model, which supports the defenders in visualizing and understanding an attacker's campaign. One such proposal is given by Zhou et. al [51], the paper presents an improved and extended version of the CKC model with respect to ICS, including three different levels of kill chain:

1. "External Kill Chain" – used to invade the enterprise network.
2. "Internal Kill Chain" – used to gain access to ICS.
3. "ICS Kill Chain" – used to develop and implement a final tailored attack of an ICS production process.

All of which are introduced as a hierarchy or layers of circles, where (1) is the outermost, (2) is the middle part, (3) is the innermost circle including a sub-circle representing the targeted core production process. In order to deliver a successful attack, an attacker must traverse all three layers, starting at (1) and moving inwards. Furthermore, the researchers utilized the matured model by performing a case-study of a real-world cyber attack, and ultimately, concluding a well-suited kill chain model for industrial control systems [51].

The SANS Institute have proposed a slightly different foundation of such a model, with Michael J. Assante and Robert M. Lee as the authors [44], shown in Figure 3.2. The main difference between the traditional and ICS-specific cyber attacks, comes from the underlying engineering in ICS components. The ICS components are configured and designed in unique ways that requires an intelligent attacker to gain extensive knowledge in order to impact them in a meaningful way [44]. Thus, a new kill chain model is necessary in order to visualize and prepare for this kind of attack. The ICS-CKC model, as shown in Figure 3.2 below, is the proposed generic campaign of a possible adversary, and can be used as an auxiliary aid for defenders to detect, disrupt, and increase the cost of an ICS-specific attack. The model consists of two stages, Stage I; Preparation for Cyber Intrusion and Execution, and Stage II; ICS Attack Development and Execution [44]. From Figure 3.2, it is easy to see that Stage I is reusing steps from the original CKC in Figure 3.1, only divided into different phases with additional accessories. In particular, these are the two stages an attacker

has to initiate in order to perform a true cyber-physical attack against an ICS, both stages are further explained below.

**Explanation of Stage I: Cyber Intrusion Preparation and Execution**

Stage I constitutes a breach on traditional IT networks. Hence, Stage II can be seen as the ICS-specific part including a final move towards an ultimate impact. The main goal of Stage I is to plan, prepare and execute a cyber intrusion. Upon a successful intrusion, it is normal to establish a persistent C2 connection for access management and enablement. Once the attacker is inside, a C2 connection can be utilized to move laterally through the system environment in the attempt of stealing information, among other diligent actions that fulfill the end goals of an adversary. Furthermore, Stage I is where the most significant portion of malware and network intrusion occur, due to a high activity of nation-state intelligence and espionage. Stage I is also where criminals can enjoy a sustained access, and most likely achieve financial gains. For example, by monetizing the exfiltrated information. Thus, even if the danger is immediate or not, it is important to identify and remediate adversary intelligence efforts [44].

***Phase 1: Planning***
The main objective of the Planning phase is to reveal weaknesses, identify information and shape the target options available to adversaries by carrying out reconnaissance. Reconnaissance is the process of gathering or accumulating information about the target without being discovered or observed. A lot of the gathered information that is useful for an adversary is normally public, such as social media and announcements, network, host and protocol information. In addition, any information that identifies how the target operates, including policies, processes and procedures are of particular interest. For example, Google and Shodan are two popular information gathering-tools used for reconnaissance. Furthermore, attackers can be expected to conduct an ICS research and read up on technical vulnerabilities and features in order to understand the ICS attack surface, sooner or later, an adversary will discover how a process or system is susceptible to exploitation. Particularly, the one thing defenders cannot decide is whether or not an organization is worth targeting [44].

***Phase 2: Preparation***
The main objective of the Preparation phase is to make the choice of weapon(s) for exploitation and identify potential victims to be exploited. Weaponization is where the attacker determines the type of exploit to be used, which is based on the findings from the previous Planning phase. The exploit is usually a type of malicious software or better known as a *malware*. A malware is considered to be any software that causes harm in one way or another, to a user, computer or network, including viruses, worms, trojan horses, ransomware, spyware, scareware and rootkits [54].

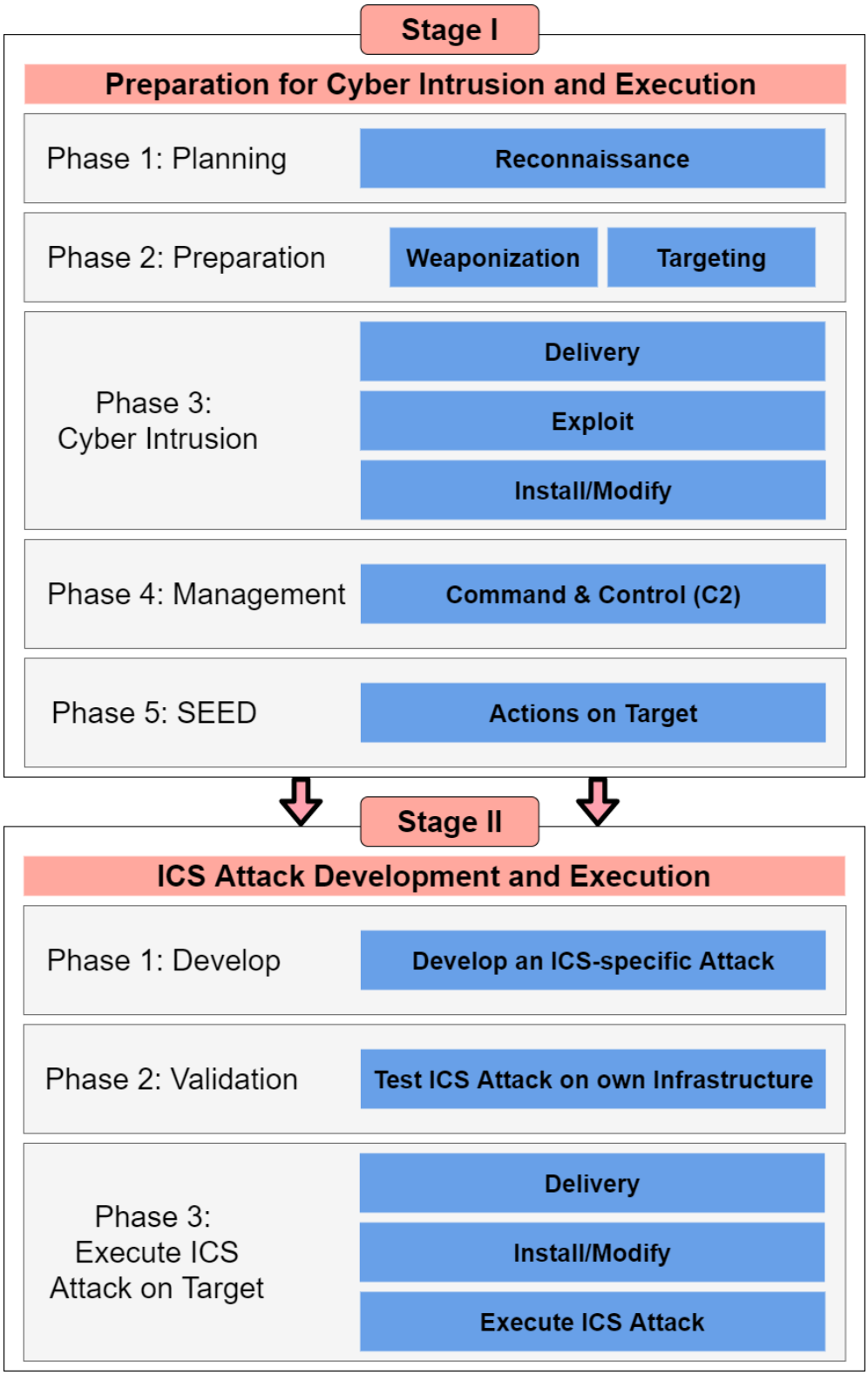


**Figure 3.2:** Depicts the ICS-CKC framework model. In Stage-I, the attacker prepare for a cyber intrusion, executes it and acts on target. Depending on what information was exfiltrated during Stage-I, the attacker use this information in Stage-II to learn the system, develop, test and execute an ICS-specific attack. Adapted from [44].

A trojan horse is defined as a "malicious program that masquerades as a benign application" [55], and is often a weapon of choice. As it's purpose is to cloak itself within a legitimate looking program or a document, such as DOCX and PDF files, which is commonly weaponized by attackers. Hence, a trojan is stealthy in terms of executing the malicious code that is hidden in the background when the user starts the program or otherwise opens the downloaded file.

In addition, or as an alternative to the above mentioned, the cyber attacker can identify potential victim(s) vulnerable to exploitation by using a so-called agent (i.e. a script or tool). This process is called Targeting, and is where attackers determine the offensive tools or methods to be used against the target, which is based on the many trade-offs between likelihood of a successful attack, risk of detection and amount of work over time. For example, based on the results from the planning and reconnaissance, an attacker may decide to target the VPN environment of an enterprise. As it could be the best approach or shortest path to a more cost-effective attack, as well as minimizing the waste of time and resources.

It is possible to perform both Weaponization and Targeting, but this is not a requirement. For example, if the adversary was able to identify login credentials in the VPN example, it would be possible to skip or bypass the need for weaponization. Likewise, the weapon of choice could be delivered to a number of targets, from thenceforth, filter out those affected or compromised. Thereby, excluding the need of doing targeting first [44].

***Phase 3: Cyber intrusion***

The aim of the third phase is to perform a cyber intrusion, which is defined as an; "unauthorized access to a network or a network-connected system, that is, deliberate or accidental unauthorized access to information systems, to include malicious activity against information systems, or unauthorized use of resources within information systems" [55]. In other words, the cyber intrusion phase is all about gaining access to the defender's system or network.

The very first step, is the Delivery step, in which a method of choice is used to interact with the defender's network. For example, a weaponized PDF could be sent through a phishing mail as the delivery mechanism. Another example, the malicious adversary could be delivered directly to the enterprise network through the trusted VPN connection. The next step is the Exploit step, and is where an attacker performs the malicious activity. This step is triggered in the moment the attacker uses the credentials for a VPN, or when a weaponized PDF or any other file opens, thus exploiting a vulnerability which allows adversaries to access the network.

Once the exploit is successful, the insidious attacker will install a malicious capability, such as a backdoor, also known as a remote administration tool (RAT). A RAT is used

to remotely manage a computer or computers, and is commonly used by nefarious adversaries in targeted attacks, which ensures the attacker a persistent connection to the target [54]. In addition to installing, or as an alternative, the attacker could modify and make use of already existing capabilities in the compromised system, otherwise known as living off the land (LotL) techniques[3]. For example, by using legitimate Windows tools, such as enabling an off-the-shelf remote desktop tool, or utilizing the PowerShell tool that is powerful enough to replace or omit the need for intrusion-malware. On a side note, it is very important to identify and understand the threat, but assuming that the threat is only malware-based is a sincere mistake by the defender [44].

***Phase 4: Management & enablement***

If the cyber intrusion is successful, the adversary moves on to the next phase, Management and Enablement. Here the threat actor will establish the C2 by using the previously installed or modified capability, and is where the dwell-time really begins. Multiple C2 paths are usually established to make sure the connection is persistent and uninterrupted. If a defender or threat hunter detects or removes one such intrusion path, the adversary still has options. It is important to note that the adversary pursue stealth and is continually seeking ways to be invisible, thus hiding in normal outbound and inbound traffic is commonly used in C2 connections. Some C2 connections does not always rely on full-duplex or bidirectional communication. Hence, a half-duplex or one-way communication might require more time for the attacker to do coding, move information and escalate the attack. However, as the access is managed and enabled, the adversary can move on to the last phase in Stage I, and ultimately, achieve his or her goal [44].

***Phase 5: Sustainment, Entrenchment, Execution & Development (SEED)***

The main goal in this phase is to document all end goals, which then is further acted upon. The complete list of all actions an adversary might have in mind would be cumbersome to derive here. However, adversaries are commonly utilizing tools for host, system and vulnerability discovery, lateral movement in the network, installation or modification of additional capabilities, as well as launching these. Furthermore, eavesdropping and collecting communication information such as credentials or other sensitive information to be exfiltrated out of the environment, and apply several anti-forensic techniques such as cleaning all their traces to the best of their ability, and methods for defending their foothold upon encounter with incident response and defender teams. Notice that the adversary does not attack anything in this phase, other than learning the compromised system by traversing the surrounding environment and fishing for information. Hence, depending on the information

[3]LotL is best explained by Symantec's "Living off the Land and Fileless Attack Technqiues" (https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf)

gathered, this might be a critical phase with respect to the planning and execution of Stage II [44].

It is very important to notice that Stage I can be omitted or bypassed if the ICS, or any interconnected third-party, is successfully compromised through Internet-facing components. For example, the recent cyber attack campaign, BlackEnergy version 2/3, which attempted a direct exploit on Internet-facing devices within the ICS [56]. Lee and Assante are further explaining the utter importance of being careful in making design choices, as well as how to integrate systems. A properly architected ICS may give several security advantages, even if the vendor components are made without security in mind. The ICS contains multiple layers of systems, firewalls and other detection sensors, as described in Section 2.3.1 on CIs. Hence, there is much an adversary has to traverse in order to gain access to the internal ICS components. However, by implementing Internet-facing devices and thereby directly connecting ICS components to the Internet, will surely undermine the security to some extent, regardless of architecture [44].

**Explanation of Stage II: ICS Attack Development and Execution**

The main goal of Stage II is to utilize the knowledge gained from Stage I by applying three different phases, which will lead to a meaningful attack on the ICS. Unfortunately, an unintended attack might occur in Stage I due to sensitive ICS equipment and might lead to unforeseen consequences. For example, an adversary operation attempts to discover hosts on the ICS network, but in the process, interrupt necessary communication and accidentally cause vital communication cards and protocols to fail. This is an unintended activity in the Act step, and would still be contained within Stage I. Hence, only intentional and meaningful attacks are recognized as a part of Stage II [44].

***Phase 1: Attack Development & Tuning***
Normally, it is very difficult to detect an adversary in this phase, as the development and tuning are done through the scrutiny of exfiltrated data. Only the bravest of adversaries would attempt to perform the development through a live in-production testing. Hence, a significant and prolonged-time might emerge between Stage I and Stage II, due to the development time needed for a tailored capability [44].

***Phase 2: Validation***
The purpose of the Validation phase is to test the newly developed capability on a similar or identical configured system. The testing is necessary to ensure the attack will have any meaningful and reliable impact. An attack with a big impact require sophisticated testing and might acquire the use of ICS software and physical components, but even simple attacks need some level of testing. Hence, governments and organisations should use their sources to monitor or collect necessary intel on

unusual acquisitions of such items, which may indicate a Stage II attack [44].

***Phase 3: ICS attack***
The last phase encompass delivery and installation of the capability or modification of the internal system functionality, and finally, execute the attack. In order to achieve the ultimate effect, the attack may consist of several concurrent attacks in parallel or in tandem, which is either initiating, enabling, or supporting the totality of the impact. For example, an attack could initiate a change in the process attributes and variables, while another instance of the attack might be tasked to fool plant operators into believing everything is normal by spoofing state information of ICS-SCADA processes [44].

In addition to those presented above, there are a growing number of ICS-CKC models, and ICS defenders can choose the most suitable model based on their organizational needs, system and architecture. The concepts revealed in the ICS-CKC model may increase cyber security awareness to security-minded personnel, as well as advancing the security in their organization and ICS community [44]. The result of not being adequately aware and prepared of potential cyber threats is becoming evident in the next section on previous cyber attacks on critical infrastructures.

## 3.3 Previous Cyber Attacks

The investigation of selected cyber attacks from the past decade on critical infrastructures are established in this section. The Black Energy and Crashoverride attacks are of particular interest for this thesis as they are directly targeting the electric power grid.

Five different attacks specifically tailored for ICS has been discovered over the past decade; Stuxnet (2010), Havex (2013), Black Energy 3 (2015), Industroyer/Crashoverride (2016) and Trisis/Triton (2017). Stuxnet and Havex will be further examined below, while a more throughout case study will be carried out on the most relevant attacks, that is, Black Energy 3 and Crashoverride. Equally intriguing is the Trisis attack, but is left out for the sake of brevity.

**Stuxnet** was a highly complex and infamous attack on a critical infrastructure at Natanz in Iran, and is still considered as the most advanced attack as opposed to the other ICS-attacks [57]. Stuxnet is the most sophisticated family of Internet worms ever discovered, and is also the first to attack SCADA [58]. The self-propagating worm consisted of approximately 500 kB of well-written code [59]. Furthermore, Stuxnet was mostly active during 2010, but experts think the campaign may have taken place over several years, with earliest estimates around 2006 and 2007, but the precise dwell-time is unknown. The mission or main purpose of Stuxnet was to

paralyze or incapacitate the uranium enrichment program at Natanz in Iran, which at the time was of significant concern for various countries. The nuclear facility was relatively secure and even had an air-gapped network[4], so it was out of reach for traditional cyberattacks, but the malware still found its way through.

Remarkably, investigators believe the malware delivery was done by an insider threat which – knowingly or unknowingly – compromised the network through the use of a physical component, such as a USB or infected engineering laptop [44]. The main target was a WinCC SIMATIC server controlling the PLCs running software from Siemens, which in turn controlled the uranium centrifuges[5] [44, 60]. The malware was gradually accomplishing the mission through manipulation and modification of systems and processes. Meanwhile, the malware was returning normal operation feedback values to the facility operators as a part of the stealth and tactics to make it look like an accident [60]. Eventually and reportedly leading to one-fifth of Iran's fast-spinning centrifuges to physically destroy themselves [44].

Stuxnet is an example of a worst-case scenario, as it managed to go throughout the entire ICS-CKC [44]. The exact perpetrators has not been conclusively identified, but several papers are strongly indicating a joint effort between the US and Israel. After all, it was a time when the ethical and geopolitical tension was utterly high [58, 59]. Stuxnet has proven that cyber-espionage perpetrators with their nefarious activities can reside in the systems for years without detection, and by the time malware like these do their damage, it is too late to defend against them [61]. For further reading, a case-study and ICS-CKC walkthrough of Stuxnet is to be found in [44].

**Havex**, also known as Backdoor.Oldrea, is another ICS focused malware campaign discovered in 2013, which has evolved into becoming a criminal toolset. The main purpose of Havex is to gather sensitive data and information about multiple ICS systems and their corresponding network infrastructure, by utilizing a botnet of unknown size and a remote trojan for general-purpose espionage. The attacker or threat actor uses several methods in the attempt to gain access; (1) Spear phishing-mail, containing malicious attachments; (2) Infect the ICS provider or vendor websites, and intervene with ICS processes when an operator visits the page; (3) provide trojanized software versions used by ICS, for example, during an upgrade it could download and install the malicious version in place of the legitimate version [44, 51]. The origin of Havex is traced back to the Russian APT group "Energetic Bear" or "Dragonfly", and was the first advanced ICS attack since Stuxnet [61]. Several countries, such as Spain, the US, France, Italy, and Germany, have been victims of the Havex Trojan, according to Symantec [62]. For further reading, a

[4]Air-gapped network is disconnected from the enterprise network and the Internet in general.
[5]Nuclear uranium centrifuges – https://science.howstuffworks.com/uranium-centrifuge.htm

case-study and ICS-CKC walkthrough of Havex is to be found in [44].

### 3.3.1 The Cyber Attack on Ukraine's Power Grid

In late December 2015, the customers of three Ukrainian regional DSOs were informed about power outages [63]. The power cuts was due to an illegal third-party entry of the enterprise computers and SCADA systems, which later was confirmed to be a cyber attack, better known as Black Energy 3 [64]. It is known to be the very first cyber attack to ever disrupt electric power grid operations [65]. In summary, a series of synchronized and coordinated cyber attacks disconnected seven 110 kV and twenty-three 25 kV substations for approximately three to six hours, before the operators were forced to switch to manual mode and restore power. Consequently, impacting the regional power distribution level and leaving 225 000 customers without power across different regions [64]. Other parts of the distribution network was overloaded, and a number of electric substations had to be manually operated for several weeks after the attack [57].

The perpetrators used different attack vectors during the cyber intrusion, and is believed to include spear-phishing emails delivering trojanized Microsoft office documents, and a third version of the Black Energy malware [64, 15]. However, this was not the main cause of the power outage. An important fact is that the power outage was not attributed by the malware per se, but by direct interaction using various hand operated LotL techniques, including SCADA hijacking and the use of ICS tools in order to leverage the systems against themselves [65]. Thus, the attackers dwelled in the system long enough to become a legal account (admin) user for instance, and blend in as authorized users [64, 66]. The SCADA hijacking is considered as the primary attack, and was facilitating the remote opening of circuit breakers by infecting the field devices with a tailored malicious firmware [15]. Nevertheless, Black Energy 3 is considered to be a small-scale attack compared to the overall power consumers in the country and due to the short duration of the attack. Additionally, the investigative cooperation between entities of different countries, especially the American and Ukrainian government, as well as the willingness to share technical information is described as the best to date for a confirmed cyber attack [64].

The Black Energy attack was the prelude to a more sophisticated attack, called Industroyer, also known as Crashoverride [67]. A high-level illustration of the Industroyer attack is given in Figure 3.3.

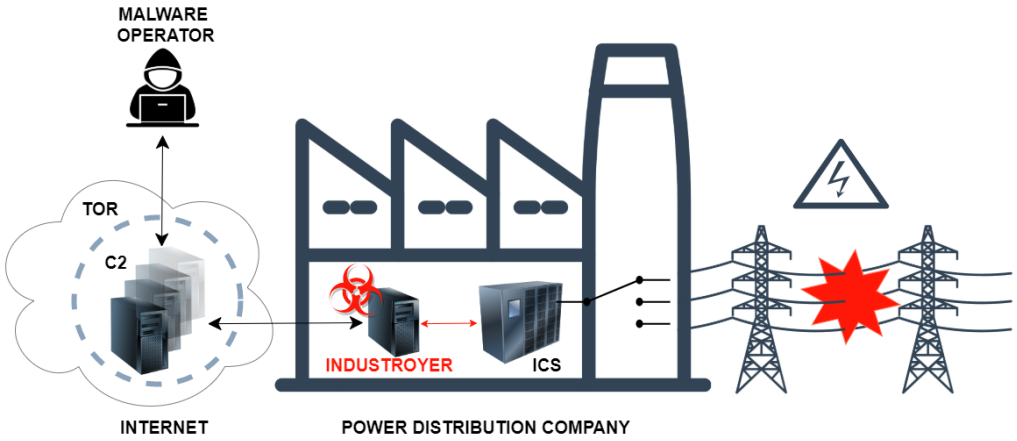


**Figure 3.3:** High-level illustration of Industroyer/Crashoverride. Adapted from [67].

In December 2016, roughly a year after the Black Energy events, there was once again a cyber attack in Ukraine. Only this time in the capital Kiev, causing approximately one hour of power outage [68, 66]. The number of affected customers are unspecified, but the attack is described to have a lower impact than the power event in 2015 [65]. However, Industroyer is considered to be the "biggest malware threat to critical infrastructure since Stuxnet" [67], and is the first known successful cyber attack on the electrical power grid induced by malware [68].

> "Industroyer's ability to persist in the system and to directly interfere with the operation of industrial hardware makes it the most dangerous malware threat to industrial control systems since the infamous Stuxnet."
>
> – ESET Senior Malware Researcher, Anton Cherepanov [67]

The Slovakian Internet security company, ESET, was the first to investigate and publish a technically detailed report on the Ukrainian incident [68]. In the report, ESET identified a new and sophisticated malware as the main suspect, and named it Win32/Industroyer or simply Industroyer [67]. Shortly after, ESET notified Dragos about the incident in June 2017, leading to their own investigation and publication under the name Crashoverride [65]. The Dragos naming convention comes from the malware identifying itself as "crash" in several locations [65]. Dragos is an American company specialized for OT/ICS cyber security, and was founded by Robert M. Lee, which also is the CEO of Dragos and lead investigator of the Ukrainian attack [69]. A recent report, published by Dragos in January 2020, provides a general threat intelligence and overview of the Ukrainian Industroyer attack, built upon

assumptions, but with a high level of confidence [68]. Notice the names, Industroyer and Crashoverride, represents the highly modular malware framework shown in Figure 3.4, but is occasionally interpreted to be the malware itself.

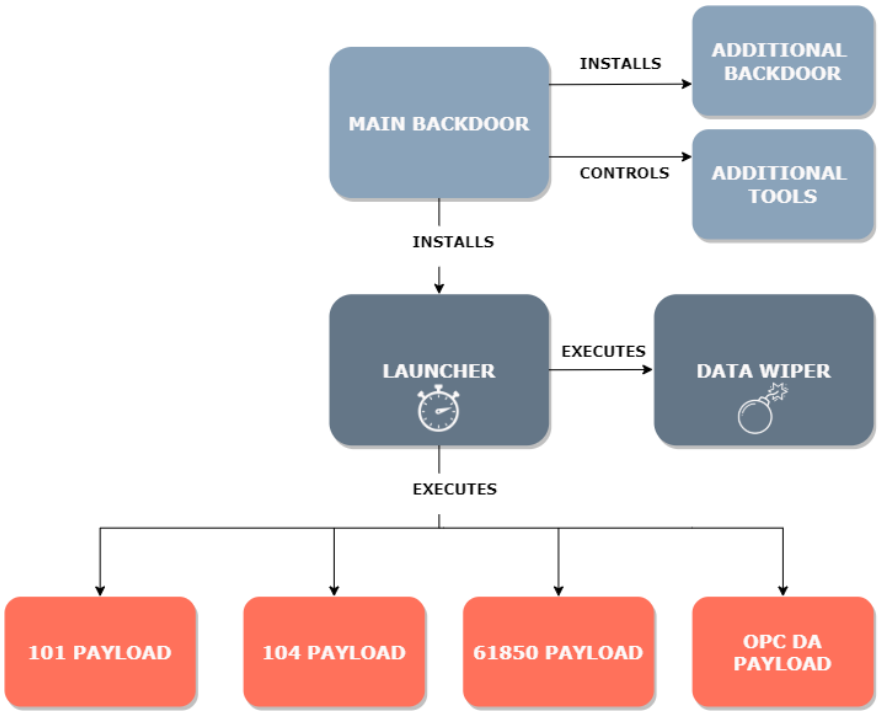


**Figure 3.4:** The Industroyer/Crashoverride malware framework. Adapted from ESET [11].

The **Main Backdoor** is the core component of the Industroyer malware. By remotely connecting to the C2 servers over HTTPS, the attackers can control all other components of the malware. The backdoor has two interesting features; C2 servers and backdoor activation at will. The C2 servers are using the onion router (TOR) software, thus making it very hard if not impossible to trace back. The other feature is enabling the attackers to deactivate or activate the backdoor at any time of the day. For example, the backdoor could be set to only communicate with the C2 servers outside of working hours [11].

The **Additional Backdoor** is used by attackers to regain access if the main backdoor is disclosed by defenders or otherwise fail to function. In this case, the additional backdoor appears as a trojanized version of the Windows Notepad application, in which the malicious code is heavily obfuscated [11].

The **Launcher** is installed by the main backdoor, and appear as a separate executable that is responsible for executing the **Data Wiper** or any of the custom-made **ICS payloads**. The Data Wiper is a destructive component which is used in the endgame.

It attempts to hide traces and make recovery difficult by rewriting content and deleting files. It also attempts to make the operating system unbootable by editing configuration files, removing registry keys and terminating all system processes except its own. The Data Wiper and ICS-custom payload components are standard Windows DLL files, as further explained in ESET's technical report [11].

Industroyer was supporting four different industrial protocols that were implemented by the malware authors. These protocols are utilized by the malware as executable payload components, as shown in Figure 3.4. The industrial protocols are further specified in the standards below [11]:

- IEC 60870-5-101 (aka IEC 101)
- IEC 60870-5-104 (aka IEC 104)
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

The above mentioned ICS protocols are believed to be used in the malware with the intention to disrupt power grid substations, as it was able to directly control circuit breakers and switches. Additionally, the malware contained a custom-made port scanner tool that can be used for mapping the network [11]. Another tool was specifically design to perform a denial of service (DOS) attack against a family of protection relays belonging to the Siemens SIPROTEC series [70]. In this fashion, the Industroyer was a far more advanced malware than Black Energy 3, especially as the malware authors were leveraging a comprehensive and specialized knowledge in industrial control systems. Despite the fact that some malware components were conceptually similar, such as the Data Wiper, malware analysts could not find any other similarities between the two [11].

At first, the Industroyer incident seemed to be a typical single-intruder event, where an attacker try to traverse the cyber kill chain steps in the attempt to compromise the system. The incident appeared to originate from a backdoor, with the objective of connecting to remote command and control servers and receive control commands from the attacker. Thus, facilitating the enterprise intrusion or network access and assisting the deployment of an ICS-disruptive payload. However, the incident was far more sophisticated than a single backdoor, but the initial investigation suffered from a lack of available research. The analysis available was not providing the complete picture due to the absent of in-depth technical reports [68]. It was not until, 2018 and 2019, when such reports were emerging, which indeed made an important discovery of how multiple tools were utilized in the victim network. Moreover, and more

importantly, the previously discovered backdoor was not necessarily linked to the execution of the ICS portion of the attack. Among other observations, it appears to be affirming the hypothesis of a multiple threat-actor intrusion and not a single, monolithic intrusion, as previously anticipated [68].

A few years after the Industroyer incident, a new malware was discovered by ESET, called "Exaramel". It was discovered in the context of a new malicious activity, and was surprisingly comparable – both in functionality and code – with the previous backdoor discovery. A more scrutinized and malware-centric analysis approach revealed that the perpetrators or authors of the Exaramel malware were those accountable, not only for the Industroyer's backdoor, but the overall 2016 Ukrainian power event [68]. More importantly, ESET was able to link the Exaramel backdoor to the Sandworm team [68], which is a russian APT group mainly targeting Ukrainian entities, and has been operational since approximately 2009 [71]. Thus, the overall investigation points out a far more subtle operation than initially thought. According to Dragos, the power event is believed to involve at least two distinct teams collaborating. Depending on skills and techniques, each team could be assigned to different stages in the ICS cyber kill chain. Furthermore, the teams involved are believed to be; Sandworm as the cyber intrusion specialist, and; Electrum as the specialist in attacking ICS infrastructure [68]. In a certain sense and metaphor, the teams were operating as a "swiss army knife" with multipurpose tools as a means to open a "black box", and subsequently, aiming to do something vicious.

In spite of the challenge to discover a post-incident intrusion – based on the log data and other evidence – the initial cyber intrusion was based on a phishing campaign starting as early as January 2016. Thus, the intrusion was most likely done by leveraging credential capture and VPN access over the same year. After positioning themselves in the compromised system, the perpetrators made further advances to download and execute the Industroyer malware as a system service. Nevertheless, the precise information of the adversary's movement from IT to OT-ICS remains elusive [72].

In similarity to Stuxnet, the Industroyer malware was codifying and learning the system and network operations. Additionally, the malware was utilizing the OPC protocol in order to map the environment and select its targets, as the Havex malware did [65]. Obviously, the evolution of tradecraft is revealing the adversaries intentions to leverage, both their knowledge and techniques gained from past attacks, with the purpose of constructing even more sophisticated APT attacks designed for ICS, in the future. Moreover, and probably more disturbing, is the fact that many elements of the Industroyer attack were rather experimental or concept validation, thus the malware was not living up to its full potential [65]. In addition, the review of event log data among other artifacts revealed that the intended scale of the attack was

far larger than achieved. A fully successful Industroyer attack would be orders of magnitude larger than the 2015 Ukraine event. This is causing concern among the electric utility operators, as well as the security community of critical infrastructures [66].

> "The relatively low impact of December 2016's blackout stands in great contrast to the technical level and sophistication of the suspected malware behind Industroyer. The possible explanation for this – and the opinion of many security researchers – is that this was a large-scale test. True or not, this (analysis) should be a wake-up call for those responsible for the security of critical infrastructure (systems) worldwide."
>
> – ESET Senior Malware Researcher, Robert Lipovsky [67]

Security experts seems to contemplate on why someone would even bother to blueprint such an highly technical and sophisticated attack, only to gain a minor impact. Nevertheless, as Lipovsky – one of the Industroyer researchers – mentioned above, this should be a wake-up call for those concerned [67]. Crashoverride's lack of significant impact can be seen as a failure, but the Electrum team will most likely learn and adapt from this event in the future. Accordingly, the event should not be ignored or underestimated by ICS owners [66].

This section is concluded with a table overview of Black Energy 3 and Industroyer/Crashoverride, shown in Table 3.1.

**Table 3.1:** Overview of Black Energy 3 and Crashoverride.

| | **Black Energy 3** | **Industroyer / Crashoverride** |
|---|---|---|
| **Location** | Three different oblenergos (DSOs) within the northern district of Ukraine | Kiev, Ukraine |
| **Date of impact** | December 23, 2015 | December 17, 2016 |
| **What** | Service and power outage done by direct interaction | Service and power outage done by malware |
| **Perpetrator(s)** | Sandworm | Electrum (and possibly Sandworm) |
| **Attacker dwell-time** | Unspecified | Unspecified |
| **Includes** | Spear-phishing emails, Trojans, LotL techniques, Handcrafted ICS firmware and SCADA hijacking | A malware framework tailored for ICS/SCADA in electric power grids |
| **Affected customers** | Approx. 225 000 | Unspecified |
| **Affected substations** | 30 distribution level substations; seven 110 kV and twenty-three 35 kV substations were disconnected | A single distribution level substation |
| **Attack Duration** | Approx. 3 to 6 hours | Approx. 1 hour |
| **Other things** | Used existing tools (LotL) | Designed ICS-custom tools using industrial control protocols |

# Chapter 4
# Information Security Incident Management

An information security incident management (ISIM) is a structured process for efficiently preparing, handling, and learning from information security incidents (ISO 27035:2 2016) [73]. The core elements are the establishment of procedures with regards to detecting, reporting, prioritizing, and responding to information security incidents. Other important aspects are: Establishing and maintaining external and internal relationships that could assist in the response, as well as having clear procedures for post-incident analysis and learning (ISO 27035) [74]. The end goal is to minimize harm to the organization, such as productivity loss, direct financial costs, loss of business reputation, or legal issues [75].

Several standards have been produced on the topic of ISIM. Some internationally well-recognized standards are NIST SP 800, ISO 27035, ENISA, and ITIL incident management [14]. However, Nural and Choo highlights in their survey; *A survey of information security incident handling in the cloud*, that despite the relative maturity of the field there exists inconsistencies in the use of terminology [76]. In particular, the terms incident response, incident handling, and incident management are frequently used interchangeably [76].

However, ISO 27035 does make a clear distinction between the three terms and is, according to Tøndel et al. [77], one of the most recognized standards on the topic. The reasoning being that it is based on consensus between international experts, as well as being developed by the non-profit and independent organizations: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). With respect to these arguments, this thesis will base its theoretical framework regarding ISIM on ISO 27035.

ISO 27035 gives the following definitions:

- **Incident management:** Exercise of consistent and effective approach to the handling of information security incidents

- **Incident handling:** Actions of detecting, reporting assessing, responding to, dealing with, and learning from information security incidents
- **Information Security Event:** Occurrence indicating a possible breach of information security or failure of controls
- **Information Security Incident:** One or multiple related and identified information security events that can harm an organization's assets or compromise its operations
- **Incident response:** Actions taken to mitigate or resolve an information security incident including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

Concerning incident handling, Nural and Choo found that, despite the use of different terminology, the most prominent standards frequently have four phases in common as part of their framework. These were identified as Preparation, Detection and analysis, Incident Response and Post Incident [76]. The findings are consistent with ISO 27035, with the exception that ISO splits the "detection and analysis" phase into two separate phases: "Detection and Reporting" and "Assessment and decision." ISO 27035 also mainly uses the term "Information Security Incident Management" to describe the process encapsulating these phases. This thesis will use the same terminology in order to stay consistent with ISO 27035.

ISO 27035 argues that information security policies and controls are not enough to ensure an appropriate response to an information security incident. Additionally, the organization should also employ a structured process for information security incident management in order to handle and learn from information security incidents appropriately. In order to put such a process into operation, ISO 27035 suggests using a cyclic process separated into five phases, whereas the last phase loops back to the first. The phases described are plan & prepare, detection & reporting, assessment & decision, responses and lessons learned. For each phase, the standard suggests a set of activities in order to enable an efficient response. Figure 4 gives a graphical overview of the process. The next subsections will explain the phases of ISO 27035 in more detail [78] .

## 4.1 ISO 27035 - Phase 1: Preparation.

ISO 27035 argues that appropriate planning and preparation are required for effective information security incident management. In order to develop an efficient ISIM plan, the standard suggests that the organization should complete the following activities.

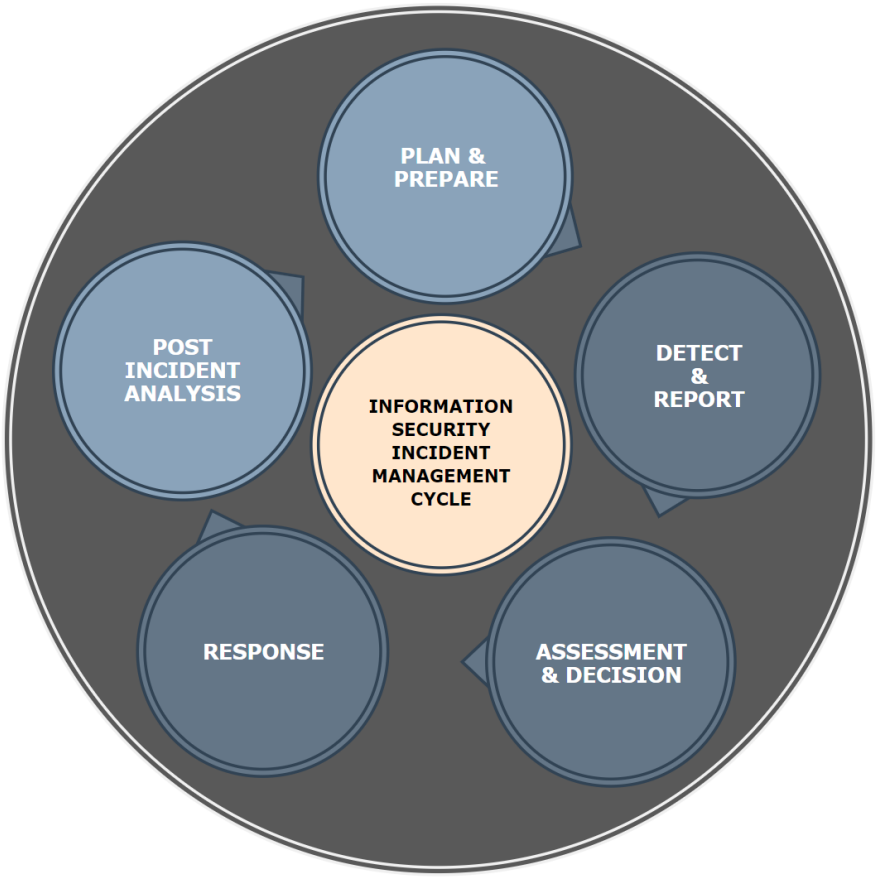


**Figure 4.1:** ISO 20735 Information Security Incident Management cycle, starting at phase 1: Plan & Prepare. Adaptated from [79].

– Develop an ISIM policy and obtain commitment from top management. ISO 27035 states several points to be included in the policy, however, some of the most essential are: A definition of what the organization considers to be an information security incident. A description of how, when, and to whom incidents should be reported. A flow chart or other visual overview of the incident management process from detection to resolution. An example of such a process can be seen in figure 4.1.

– Develop an Information security incident management plan. The ISIM plan should document concrete activities and procedures for dealing with information security events, incidents and vulnerabilities, and the communication of them. The organization should develop an incident classification scale in order to grade incidents and prioritize appropriately if several incidents coincide. ISO 27035 suggests classifying on the following factors (however, other schemes can be used):

  - Information system importance
  - Business loss
  - Social impact.

- Establish an incident response team (IRT). The IRT function is to ensure that an organization can assess, respond, and learn from information security incidents. As well as providing necessary coordination, management, and communication during a response. IRTs can be configured in numerous ways, but ISO 27035 provides the subsequent composition as an example: Team lead and group leaders to provide strategic direction. Help desk/triage staff to sort and prioritize incoming events, alerts and information. Incident handlers to undertake incident analysis, tracking, recording and response. Vulnerability handlers to disseminate information regarding vulnerabilities and corresponding fixes, patches or workarounds. Technical writers to facilitate publications such as advisories, technical tips and best practices. For small organizations, the same individuals can fill several roles. (IRTs are often also described as computer emergency response team (CERT) or computer security incident response team (CSIRT). In the context of ISO 27035, these terms are regarded as equivalent.

- Establish and maintain relationships between its IRT and relevant internal and external parties. Examples of such parties can be law enforcement, external IRTs, internal business managers, legal and public relations departments. Communicating and coordinating with such entities are frequently necessary in an ongoing incident response.

- Acquire and test technical and auxiliary support systems. In order to facilitate a rapid and effective response to an information security incident, the organization should obtain, prepare, and test all necessary technical and auxiliary support systems. Examples of such systems are:

  - Intrusion Detection Systems
  - Log monitoring software
  - Backup systems
  - Systems for digital evidence collection
  - Network monitoring tools and security devices

- Regularly test and verify the ISIM plan. The organization should conduct regular testing of the ISIM process and procedures in order to uncover flaws

and problems. Testing can be done by arranging simulated scenarios, ranging from realistic technical attacks and faults to discussions and tabletop exercises. The scenarios are not limited to only the IRT, but also some or all internal and external parties relevant to the organisation's ISIM plan. Four types of exercises are mainly used in this context. These are: Discussion-based, tabletop, live, or a combination. The exercise type is dependent on the goal as well as the time and resources available. However, ISO 27035 suggests all exercises should go through the following phases: Planning and preparation, execution, debrief, and post mortem analysis. Where the result of the debrief and post mortem analysis should be used as actionable input to improve the current ISIM plan.

## 4.2 ISO 20735 - Phase 2: Detection.

The detection phase is described ISO 27035 as a set of activities regarding the detection of information security events and vulnerabilities, collection of information related to the detected events and vulnerabilities as well as the reporting of discovered events and vulnerabilities. Detection, information gathering and reporting may be achieved by automatic or manual means. Key activities include:

- Maintaining situational awareness by ensuring that appropriate network and system activity is monitored and logged.
- Monitoring news feeds concerning economic, political and social activity that may affect incident activity. Monitoring external news feed on current attack vectors and indicators, incident trends, as well as any new mitigation strategies and technologies.
- Detecting and reporting of information security events and vulnerabilities either by automated systems or manually by personnel.
- Collecting information related to discovered information security events and vulnerabilities.
- Ensuring secure collection of digital evidence in accordance to local investigative standards, in case legal prosecution should be necessary.
- Escalating an event whenever needed in order to obtain further assessment and decision making.

The standard suggests that logging should be done in this and all the subsequent phases, with exception of the final phase, lessons learned. In particular, the IRT should maintain an information security database where all information collected

and reported relating to an detected event, vulnerability or incident should be stored. Related actions performed and decisions made should also be recorded. The information should then be used throughout the process to assist assessment and decision making, as well as after the incident is resolved for post incident analysis.

## 4.3 ISO 20735 - Phase 3: Assessment and Decision.

Phase three in the incident handling cycle involves assessing the information collected in relation to an information security event and deciding whether to escalate the event to an incident. Key activities in the phase:

- Distribute tasks regarding assessment, decision making and actions through a predefined hierarchy of security and non-security personnel.
- Provide each notified person formal procedures to follow
- Run an assessment by the incident handler to establish if the detected event is a possible or confirmed information security incident or a false positive.
- Ensure that all relevant activities, results and decisions conducted by the involved parties are properly logged for post incident analysis.

## 4.4 ISO 20735 - Phase 4: Responses

The cycle moves to phase four if the event is confirmed as an information security incident. According to ISO 27035, the organisation should respond to the information security incident in accordance with the decisions made in the assessment and decision phase. As for the previous phases, logging of activities and decisions is important. As well as collecting information and digital evidence related to the incident. Digital evidence should be stored cryptographically secure and its preservation continually monitored. Following key activities are recommended:

- Investigate incidents in accordance to the information security incident classification scale rating. The Incident's scale rating may be upgraded or downgraded continuously throughout the phase as more information is uncovered regarding the incident.
- Assess whether the information security incident is under control.
- Designate internal and external resources in order to enhance incident response.
- Communicate and share relative details and information with other internal and external parties that can assist in the incident response. Some examples are: External IRTs, law enforcement and internet service providers.

After recovering from an incident, a set of post incident activities should be initiated. Such as investigating the information gathered throughout the incident handling process and eliciting first hand information and experiences from the individuals involved. Following that, a summarized report should be produced based on the investigative findings. Finally, the incident should be formally closed and all stakeholders notified.

## 4.5 ISO 20735 - Phase 5: Lessons Learnt

Phase five occurs after an information security incident has been resolved. ISO27035 describes the aim that the aim of this phase is to make improvements to the organization's information security incident management plan and policy. This is achieved by extracting information and lessons learned from the handling of preceding incidents and vulnerabilities. ISO 27035 specifies the following key activities:

- Review gathered information in relation to previous information security incidents and vulnerabilities and identify lessons learnt. Apply findings to decide where to enhance information security controls.
- Review process procedures, reporting formats and organizational structure in terms of its effectiveness in responding to, assessing and recovering from information security incidents and vulnerabilities. Update the information security incident management plan and its documentation accordingly.
- If desired, share the review results with a trusted community.
- Examine if the incident information, related attack vectors or vulnerabilities may help partner organisations prevent the same incident from occurring in their systems.

The ISO standard emphasizes that ISIM activities are iterative and that an organisation should make frequent improvements to their ISIM plan and security measures over time. The improvements should be based on reviews of the data collected during previous incident handling cycles.

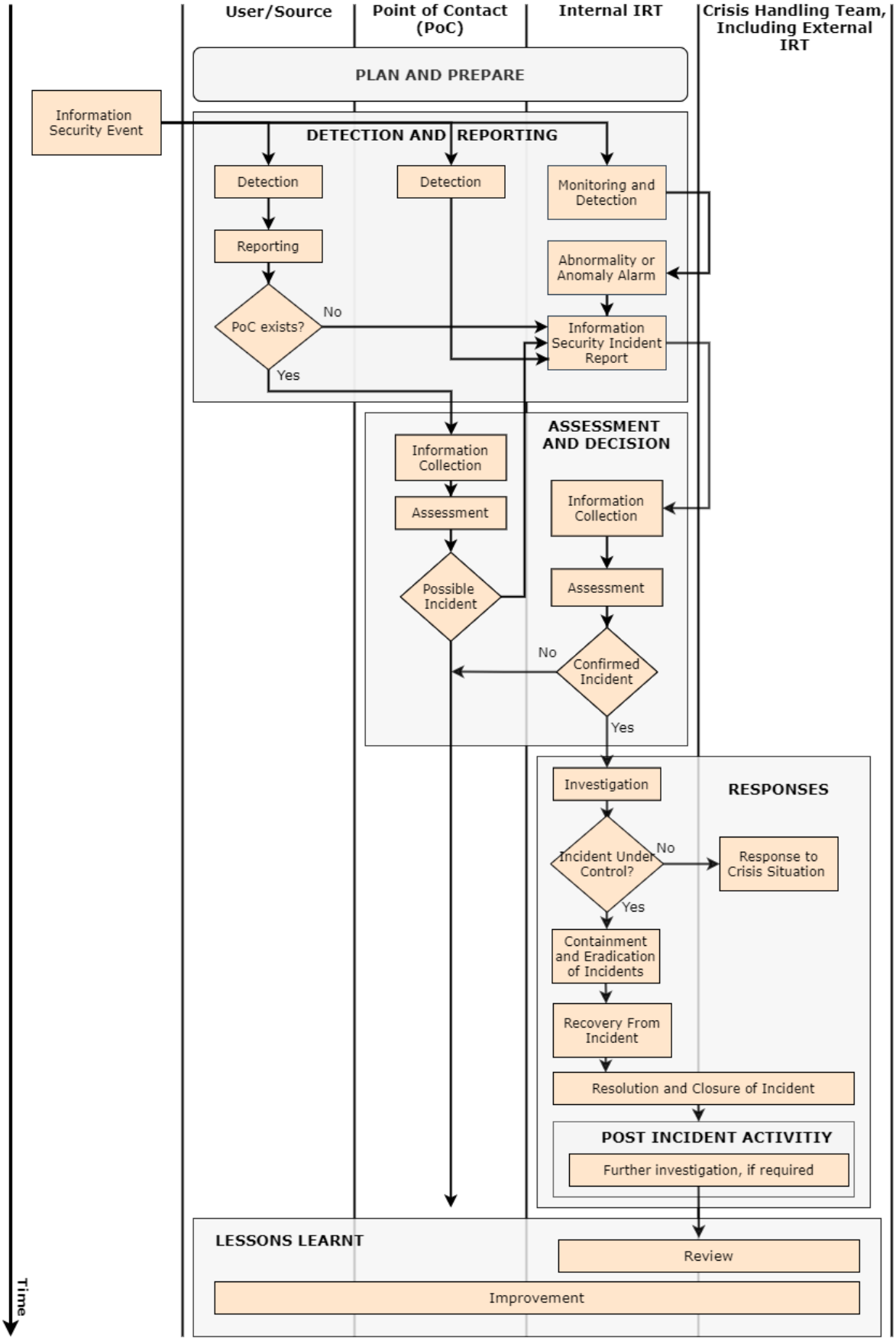


**Figure 4.2:** Flowchart of the Information Security Incident Management Process. Adaptation from [78].

# Chapter 5
# State of the Art Cyber Ranges

This chapter includes five different sections that are structured as follows; Section 5.1 will briefly explain and define a cyber range (CR), a cyber-physical range (CPR) and a smart grid cyber-physical range (SGCR). Followed by Section 5.2 and Section 5.3 which is further dissecting the concept of cyber ranges; in order to investigate the state-of-the-art taxonomy, design and implementation. Section 5.4 explains a wide range of tools, protocols and attacks currently used by contemporary cyber ranges. Finally, Section 5.5 introduce the state-of-the-art problems or ongoing challenges in terms of cyber range design and implementation.

## 5.1 What is a Cyber Range?

High computational power makes it possible to mimic a real world system through the use of virtualization, which in turn makes the foundation for simulation and emulation that embodies a cyber range (CR) [18]. According to NIST; "Cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing" [80]. Furthermore, a CR is used for a variety of purposes such as cyber training, team building, recruitment, assessment, testing, research and development. The CR should therefore constitute a configurable and extensible platform [18].

In this regard, a cyber-physical range (CPR) is designed and implemented in terms of a real-world cyber-physical system which, among other things, allows for testing, verification and development of an organization's cyber security posture [6]. Recall from Section 2.3, that a cyber-physical system (CPS) is allowing for the interaction between the cyber world and the physical world. CPRs are recognized as being connected to real-world equipment, such as PLCs, RTUs, actuators and other field devices typically found in a CPS. It is important to note that a CPR can be

classified into one of three types; virtual, physical, or a hybrid. For instance, a CPR could include a virtualized PLC or a physical PLC, or both. Furthermore, a CPR is reportedly used within different domains including smart grid, transportation systems, IoT, medical devices and water distribution [6]. Accordingly, a smart grid cyber-physical range (SGCR) is therefore a CPR within the energy domain that specifically focuses on the emerging smart grid.

The impact of successful APTs and cyber attacks on critical energy infrastructure can be devastating, in particular towards the smart grid, as previously described in Section 3.3. For instance, the cyber attacks on the Ukrainian power grids; affecting many people by causing blackouts for several hours in 2015-16. However, not all cyber attacks are caused by cyber bandits or malicious groups, but might as well be a result of countries in conflict. The US considers a cyber attack as an "Act of War" and will engage its Cyber Command upon future conflicts, thus, leading to a potential cyber warfare [81]. Accordingly, the interdependent critical infrastructures, explained in Section 2.3, will most likely be primary targets for those involved. Hence, it is important to protect CIs against all internal and external malicious actors [82]. It is of further importance to conduct research and risk assessments on cyber-physical systems including safety and defence mechanisms, as well as ensuring an effective triage and incident response in general, thereby, reducing the gap between threat and defence [6]. On the other hand, the cyber security study and experimentation is, unfortunately, not advisable nor feasible to conduct on a real-world CPS [6, 83]. Thus, the golden opportunity to study "in vitro" possible system vulnerabilities and potential cyber threats towards a CPS is one of the fundamental reasons for designing, implementing and even deploying a CPR [6].

Many CPRs have already been developed, however, only a few of these are designed and specifically tailored for cyber security experimentation and training, more importantly, enabling that kind of security functionality in a CPR is a matter of design [6]. Regarding cyber security training, the human element is normally considered as the first line of defence when it comes to being aware, prepared and up to date on possible cyber threats and crimes, as well as the latest techniques and tools applied in such manners [84]. The human element is therefore considered as a key part when building an adequate training environment, and is taken into account when designing a CPR [6]. Yamin, Katt, and Gkioulos, describe two forms of training; the first is concentrating on security professionals, aiming to increase the participants' skills and understanding of the latest cyber threats. By means of practicing and drilling on attacks and/or defence and mitigation procedures through a well-developed training program or exercise. The second form of training is concentrating on improving the cyber security awareness among non-security professionals and the general public, however, this form of training is less popular [84].

There is a high risk that a CPR does not accurately replicate the CPS. Moreover, a CPR can be used with security in mind to conduct [6]:

- Vulnerability analysis
- Testing defense mechanisms
- Impact assessment
- Threat analysis
- Testing cyber security in general
- Educational training in cyber security

Notice that Cyber-Physical Battlefields, Cyber Warfare Testbeds, Cyber-Physical Testbeds or simply Testbeds are some of the CPR synonyms applied in the literature. The SGCR abbreviation is used to denote a general smart grid CPR throughout the rest of this thesis. The next sections will scrutinize the state-of-the-art tools, attacks, design and implementation of contemporary cyber ranges, as well as the current challenges.

## 5.2 The Taxonomy of a Cyber Range

A taxonomy is a hierarchical structure used to classify and organize data [85]. In the context of cyber ranges, the use of a well defined taxonomy becomes helpful as it aids to create a common understanding of what constitutes a cyber range in regard to its functionalities, and the communication of the terms related to these. If the taxonomy is created from the perspective of its capabilities, it may also aid cyber range designers as a framework to work within.

During our literature study of cyber, we identified three papers describing CR taxonomies. Two of which are describing a general-purpose cyber range, whereas one is specifically targeting the smart grid domain. The latter was created by Cintuglu et al. [2] and classifies smart grid cyber ranges in terms of research goals, NIST domains, platform type, and the communication protocols utilized. Except for type classification and communication protocols, the taxonomy does not account for the other design choices and functionalities that relate to cyber ranges. This makes it unsuited as a framework for cyber range design. Yamin, Katt, and Gkioulos created a taxonomy describing cyber ranges in terms of the range's capabilities and functions [84]. The taxonomy was the result of surveying 100 security-related cyber range articles, selected from the period 2002-2015. One objective of the survey was to identify and classify the capabilities and functionalities, the roles and teams, as well as the tools and hardware used within contemporary ranges. As such, the taxonomy of Yamin, Katt and Gkioulos gives a well-founded snapshot of the current state of

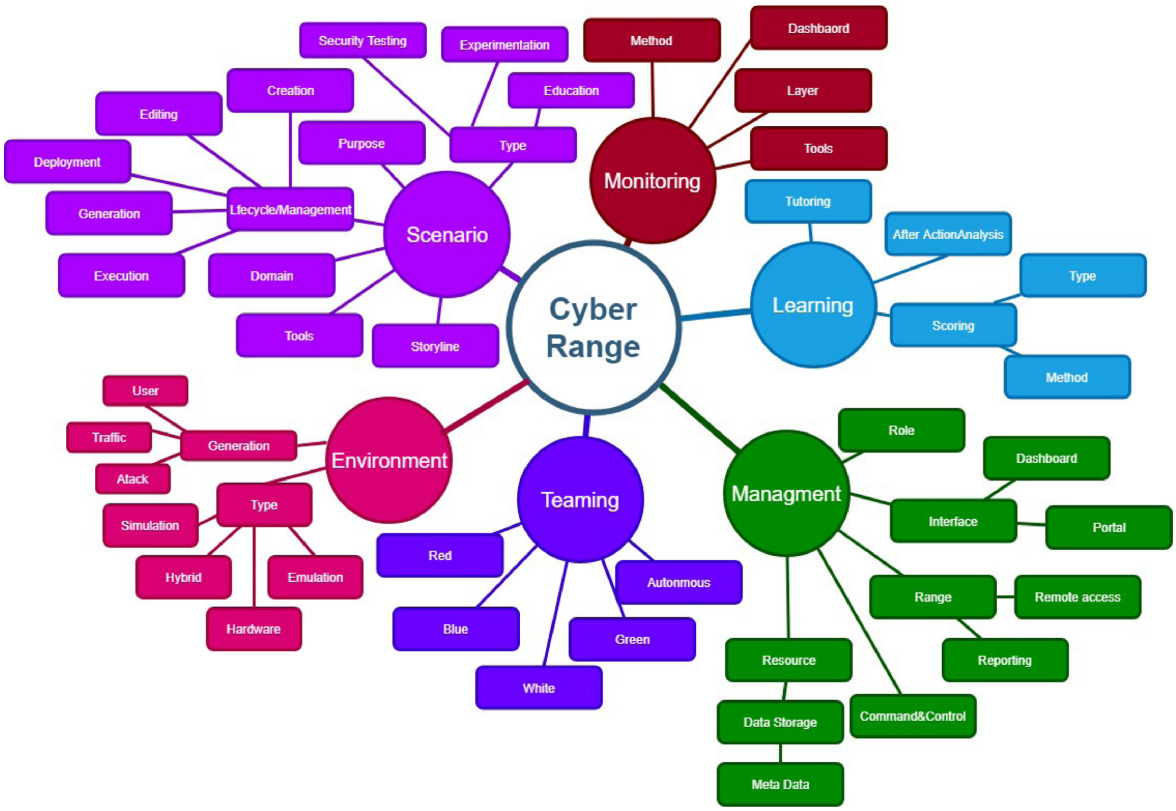


**Figure 5.1:** Overview of the cyber range taxonomy created by Yamin, Katt and Gkioulos. Reused with permission from [84].

the art in regards to contemporary cyber rages. Priyadarshini surveyed cyber ranges located in the US and made a model of the ideal general-purpose cyber range [86]. In particular, she classifies and describes a set of parameters and ranks them in order of importance. The model is in agreement with the taxonomy described by Yamin, Katt and Gkioulos, but is smaller in scope and only contains a subset of the properties.

Based on the findings above, the taxonomy created by Yamin, Katt and Gkioulos will be used in our thesis as a central reference in order to communicate the design choices and justify the specifications. Given below is a description of the taxonomy and its elements.

### 5.2.1 Scenario

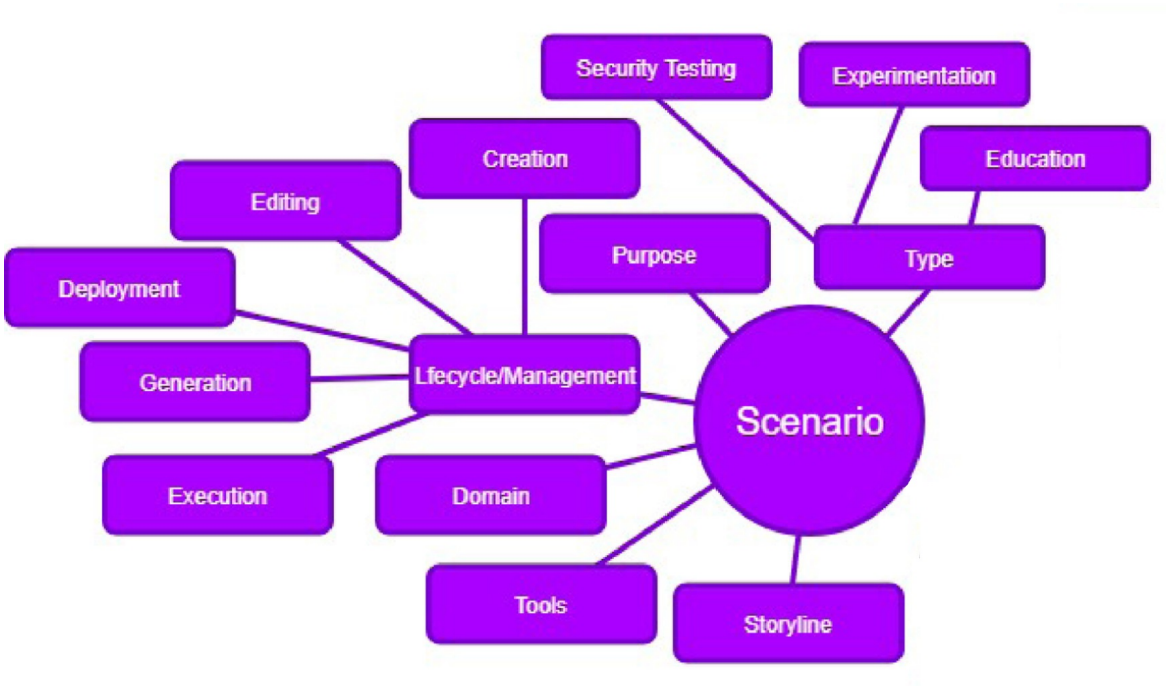


**Figure 5.2:** Taxonomy of cyber range scenario. Adapted with permission from [84].

A scenario describes the purpose as well as the storyline for a training exercise. The scenario also defines training requirements and should give an accurate representation of the operational environment in order to achieve the training objectives [87]. Yamin, Katt and Gkioulos further classify the scenario to contain information about the scenario type, purpose, domain, the tools needed and the scenario lifecycle management [84]. A description of each is given below.

- **The purpose** can either be testing new technology, education, or experimentation. The purpose dictates the objectives of the scenario and environment.
- **The storyline** tells one or several stories and guides the sequence of actions and events throughout the exercise. In addition, the storyline aids the overall understanding and controlling of larger technical scenarios and helps evaluate the exercise outcome [87].
- **The scenario type** can either be static or dynamic. Static, as the name implies, does not include dynamic changes during execution. Whereas dynamic types include components that add variations for each run of the scenario. Examples are traffic generators and simulators. Static types were the most common until 2011, when it was overtaken by dynamic types.

– **The domain** describes which application domain the scenario is built for, examples are, networks, critical infrastructure, SCADA, IoT, etc.

– **The tools** specify which software and hardware solutions are used for environment creation as well as scenario and storyline development.

– **Scenario lifecycle management** describes the methods and techniques used to create, edit, deploy, and execute a scenario. Based on implementations reviewed in their survey Yamin, Katt and Gkioulos provides the following examples on lifecycle management tools and methods [84]:

  ◦ Designer dashboards for presenting a collection of premade scenario components, enabling scenario creation and editing.

  ◦ Automated scenario creation and deployment by the use of human-readable scripting languages such as XML and JSON.

  ◦ Control modules for starting, pausing, and resetting the scenario.

  ◦ Use of a deployment component for deploying network resources, like routers, firewalls, and vulnerable software applications.

### 5.2.2 Environment

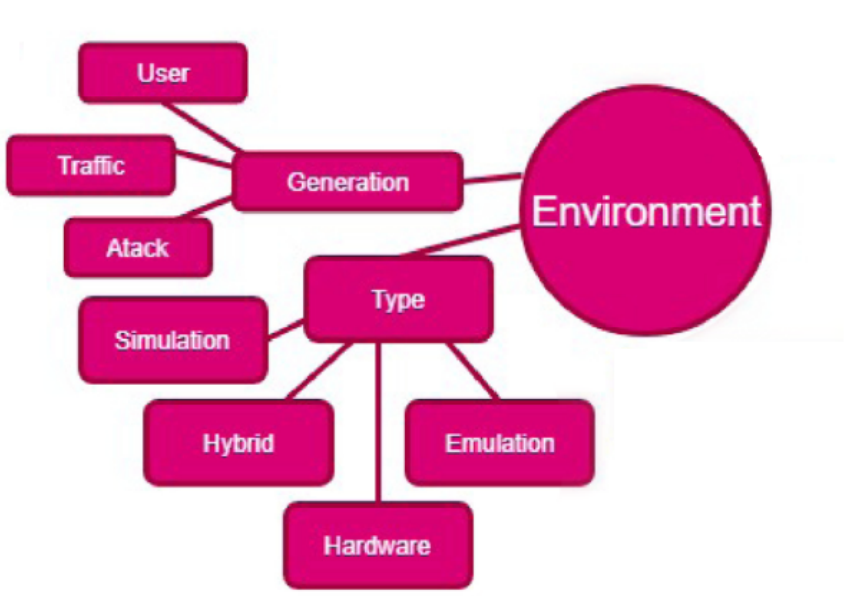


**Figure 5.3:** Taxonomy of cyber range environments. Adapted with permission from [84].

Environment is described by Yamin, Katt and Gkioulos as the topology where the exercise is executed. The choice of topology and infrastructure depends on the

exercise type and its objectives. For operation based exercises, the infrastructure will be physical or computer-based. Whereas for tabletop exercises a non-technical infrastructure can be used, as the objective may be to train decision making and communication. Computer-aided tabletop exercises have also been observed, where an additional exercise objective can be to evaluate or improve the communication between technical staff and non-technical management. For environment types Yamin, Katt, and Gkioulos classified the following [84]:

- **Emulated** environments incorporate virtualization software such as VMware, Virtualbox, and Emulab. Emulated environments have been the most common environment type since 2016 and are still gaining popularity.
- **Hardware** environments consist of real hardware components such as PLCs and SCADA controllers. However, purely hardware-based environments are uncommon.
- **Simulated** environments incorporate simulation software, such as Simulink, Opnet, and QualNet.
- **Hybrid** environments use a mixture of emulation, simulation, and hardware solutions. Hybrid environments are the second most common environment type.

### 5.2.3 Teaming

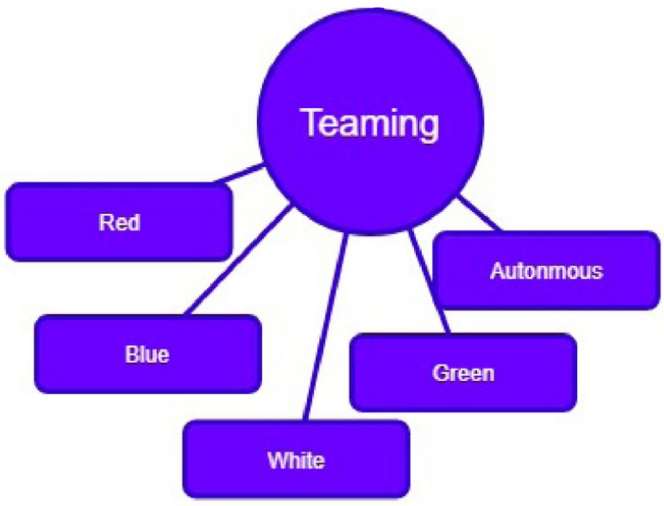


**Figure 5.4:** Taxonomy of the different teams related to cyber ranges. Adapted with permission from [84].

Teaming refers to the assignment of roles and objectives for the individuals that participate, design, develop, and manage a cybersecurity exercise [84, 87]. Each team has a color that identifies their roles. Below is a description of the most common teams as described by Yamin, Katt and Gkioulos:

- **The red team** identifies and exploits vulnerabilities located in the exercise environment.
- **The blue team** actively defends the exercise environment by identifying and patching vulnerabilities as well as monitoring and responding to signs of cyber attacks.
- **The white team** designs the exercise scenario, its objectives, rules, and evaluation criteria. They decide the rules of engagement between the red and the blue team as well as which vulnerabilities are to be present in the exercise environment. In some cases, they act as instructors or give hints to the participants [84, 88].
- **The green team** develops, monitors, and maintains the exercise environment designed by the white team. This includes bug fixing, crash handling and other faults that may arise.
- **The yellow team** enhances scenario realism by simulating the behavior of normal users in the scenario environment. The yellow team participants generate legitimate traffic by using applications and services deployed in the environment by the green team.
- **Autonomous team** refers to the automation of any of the aforementioned teams. Yamin, Katt and Gkioulos further highlight that autonomous cyber range agents have gained attention in literature since 2014.

### 5.2.4 Management

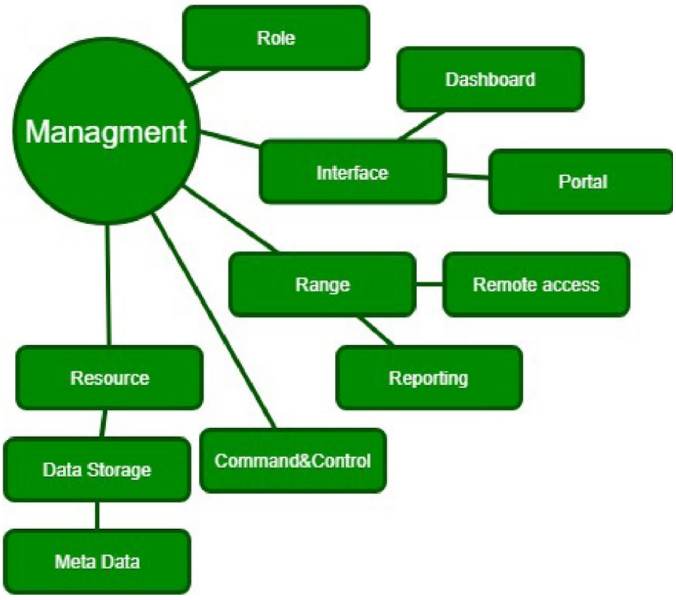


**Figure 5.5:** Close-up of the Management sub category from the cyber range taxonomy created by Yamin, Katt and Gkioulos. Adapted with permission from [84].

Management classifies the methods or tools used for managing roles and tasks for individuals related to the exercise, as well as the allocation of computational resources and the general management of the range.

- **Role management** refers to the methods or tools used in managing role segregation and user privilege allocation. Blue team and red team participants will, for instance, have different system rights and privileges in the scenario environment.
- **Resource management** refers to the methods or tools used for allocating and managing computational resources such as processing power, data storage and network capacity. These resources can be allocated to users and applications in the scenario, or to separate scenarios if several are running in parallel on the same system.
- **Range management** refers to the methods and tools utilized in managing the overall cyber security environment and exercise. Yamin, Katt and Gkioulos give the following examples from their survey:
  - Range management portals and dashboards which graphically represent the state of the range or current exercise.
  - Remote access for managing components, applications, or virtual machines.

- Application Programming Interfaces (APIs) that enable external applications to communicate and control components in the scenario.

### 5.2.5 Learning


**Figure 5.6:** Taxonomy of cyber range learning functions. Adapted with permission from [84].

The Learning component consists of after-action analysis, scoring and tutoring functions. Yamin, Katt and Gkioulos do not give a description of the learning component itself, but highlight a selection of implementations reflecting each subcomponent. Subaşu et al. [89] support tutoring functions in their cyber range by displaying text, images and multimedia clips to the participants. Vigna et al. [90] utilize a scoring bot which monitors the status of selected services in the exercise environment and calculates a score for the red and the blue team. Ernits et al. [91] uses a scoreboard displaying the progress of participants based on which tasks they have completed. Yamin, Katt and Gkioulos further suggest that scoring should consist of the following sub classifications:

- Scoring methods describe whether the scoring is objective based, i.e. by capturing flags or completing tasks, or if it is done by analyzing events, logs and metrics generated during the exercise.
- Scoring tools describe the software or hardware solutions utilized for scoring in a cyber security exercise. Examples are log analyzers, flag submission dashboards, event listeners, etc.

### 5.2.6 Monitoring

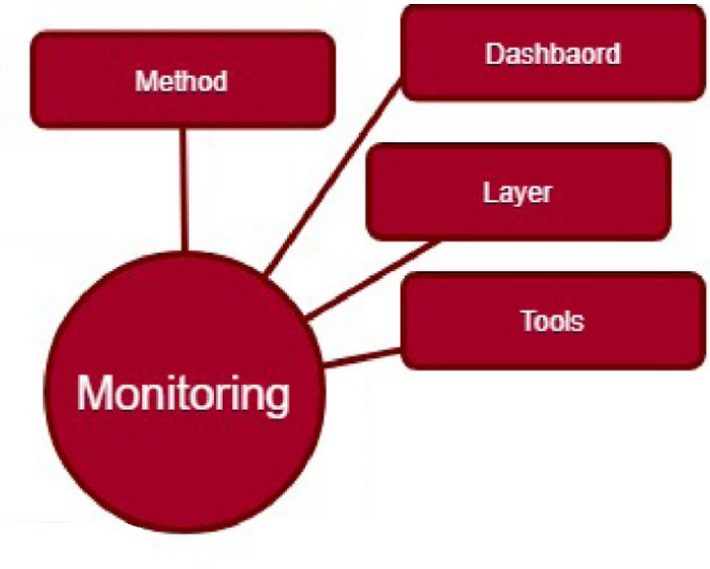


**Figure 5.7:** Close-up of the Monitoring sub category from the cyber range taxonomy created by Yamin, Katt and Gkioulos. Adapted with permission from [84].

Monitoring classifies the methods, tools, and layers used for real time monitoring of the cyber security exercise and its participants. It includes automated collection and analysis of logs from several sources, such as network devices and operating systems, as well as manual observation performed by designated observers. Yamin, Katt and Gkioulos gives the following descriptions [84]:

- Monitoring methods can either be done manually by human observers, or automatically by tools that gather data for analysis.
- Monitoring tools classifies the hardware and software solutions used to monitor an cyber security exercise. Common examples are intrusion detection systems(IDS) like Snort and network analyzers such as Wireshark and TCPdump.
- Layers classifies at which layers the monitoring is being performed. Layer choice depends on the exercise type. For instance, in a technical based exercise the monitoring is commonly done at the application, transport or network layers in the OSI network model. Whereas in case of a table-top exercise the monitoring can be performed at an abstract social layer.

## 5.3 Requirements and Architecture

It is a challenging task to construct and build a CPR, because many requirements must be considered and fulfilled in order to support, for example, training scenarios

and exercises, among other desired features and functions. One way to combat this problem is to design from scratch [92].

Kavallieratos, Katsikas, and Gkioulos have conducted an extensive survey [6] of cyber security related CPRs within five major application domains; Smart Grid, ICS, IoT, Transportation and Medical devices. The main objective of the survey, as well as the entire research, was to define the requirements for future cyber-physical ranges with the capability to test cyber security posture. The requirements were mostly adapted from Vykopal et al. [93]. Based on the requirements, a CPR reference architecture was made by the researchers in favor of future CPR builders [6]. The CPR requirements and proposed architecture are further explained below. Likewise, Osama et al. [2] have provided a list of general architecture requirements, but they were rather vague and not specifically made for a CPR, and are therefore not considered.

- **Flexibility:** The CPR should be flexible in the sense of being able to manage different CPSs across different domains, either by the exchange of information and/or substitution of components. Thus, a CPR must be able to reflect various CPS functions.
- **Scalability:** The CPR should have the ability to scale with regards to the number of CPS components, computing power, support of several users, as well as other component resources in the CPR.
- **Isolation:** Both users and the CPR itself should be isolated from the outside world. In addition, the users should be separated from each other.
- **Interoperability:** The CPR should support interoperability in terms of being compatible with external systems, and should be able to integrate external systems with reasonable effort.
- **Cost-Effectiveness:** Off-the-shelf hardware and open-source software solutions should be leveraged as much as possible, with the aim of keeping a low cost in maintenance and operations. In addition, the deployment of CPR hardware should be possible without the need for a dedicated data center.
- **Built-In Monitoring:** The CPR should support real-time and post-mortem access to detailed monitoring data from individual topologies, including captured network packets, flow data, host metrics and logs of the reflected CPS processes.
- **Easy Access:** The CPR should support web-based access to core functions, such as remote SSH terminal. It should also be relatively easy for users to learn the CPR.

- **Adaptability:** The CPR should have the ability to add and remove different components in terms of installation, uninstallation and reconfiguration, with a reasonable amount of effort.
- **Shareability:** The CPR should be able to share single components.

Furthermore, Kavallieratos, Katsikas, and Gkioulos [6] analyzed the surveyed cyber ranges together with the identified requirements, and made the foundation of the CPR reference architecture, depicted in Figure 5.8. The state-of-the-art CPR reference architecture is composed of four different modules: (1) The Cyber Range Control Center (2) Physical Components Module, (3) Virtual Components Module, and (4) Cyber Security Defence Module. These will be explained in more detail:

- **Cyber Range Control Center Module:** This module represents the possible interaction the cyber range operators (green team) have with the cyber range [6].
- **Physical Components Module:** This is comprised by all the physical components within the range, such as PLCs, RTUs, IEDs, Raspberry PI's, Arduino's, smartphones, vehicle telemetry displays, medical devices, etc. Additionaly, routers and switches for networking, as well as sensors and actuators are included in this module. As a consequence, multiple different communication protocols are needed for these various components to communicate. [6].
- **Virtual Components Module:** This module represents the virtual environments, including all simulated/emulated CPS components. Figure 5.9 depicts one such module; simulated power grid / ICS environment [6].
- **Cyber Security Defensive Mechanisms Module:** This module contains multiple defensive mechanisms in terms of conducting cyber-security assessment of the particular CPS domain, including configurations. Such mechanisms can be, for example, IDSs, IPSs, Firewalls, security enhanced gateways, among others [6].

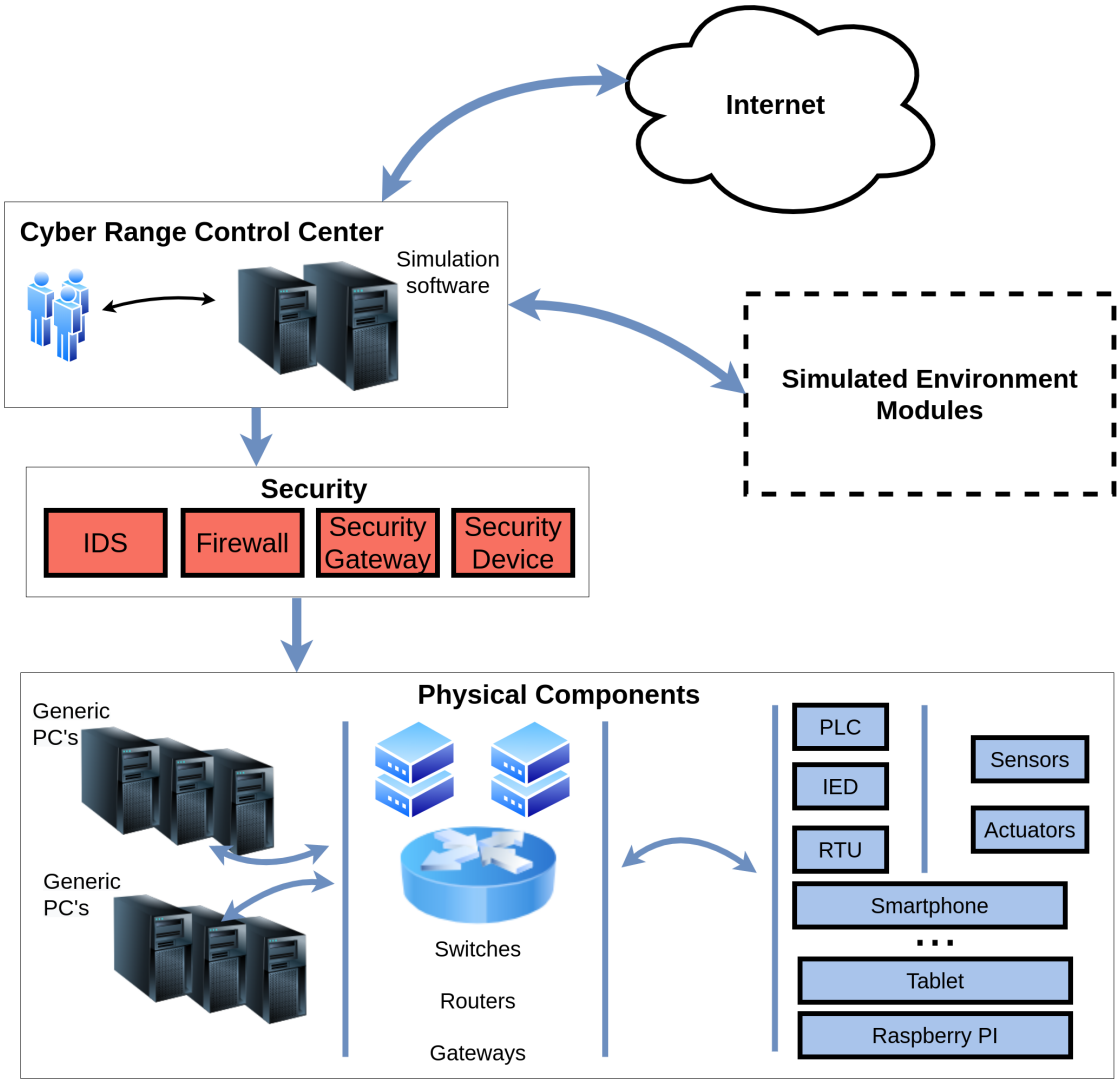


**Figure 5.8:** The state-of-the-art CPR reference architecture. Adapted from Kavallieratos, Katsikas, and Gkioulos [6].

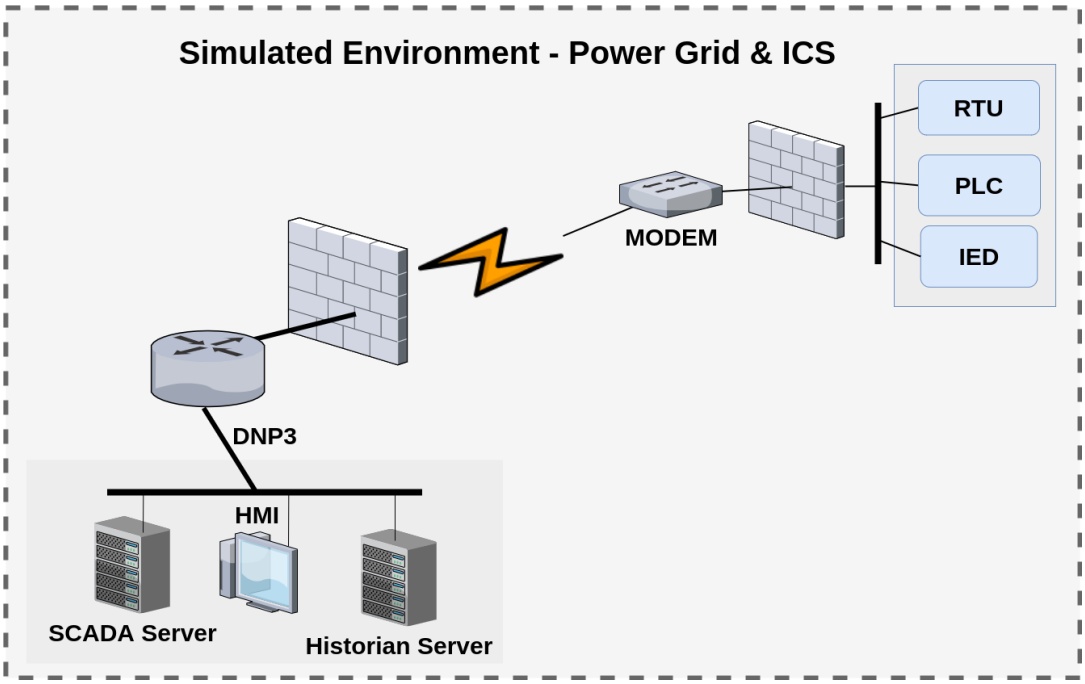


**Figure 5.9:** Illustration of a simulated environment module for Power Grid & ICS. Adapted: Kavallieratos, Katsikas, and Gkioulos [6].

In their paper, Kavallieratos, Katsikas, and Gkioulos illustrate a simulated environment for each of the five application domains, as mentioned above. In particular, the "Simulated Environment" in Figure 5.8 can be "replaced" with one of the simulated CPS environments that is described in the paper. For instance, by inserting the simulated environment for Smart Grid & ICS, depicted in Figure 5.9. Thus, the general CPR becomes a SGCR by definition, and demonstrates the ability to swap different CPS environments with ease; this is a feature that covers the flexibility requirement. Furthermore, the illustrations provided by Figure 5.8 and Figure 5.9 are of special interest as they can be associated to the Purdue model from Section 2.3.1. The illustrated figures, requirements and architecture will serve as a good guidance in later treatment design.

## 5.4 Contemporary Cyber Ranges: Tools, Protocols and Attacks

The following section gives an overview of the tools, protocols and attacks commonly implemented in today's cyber ranges. While conducting our study, we found that most articles either describe the tools used in their own cyber range, some selected tools used in other ranges, or some general category of tools. However, the survey conducted by Yamin, Katt and Gkioulos gives a comprehensive overview of the tools

used across 90 cyber ranges, including several ranges from the critical infrastructure and the SCADA domain [84]. As such, the information regarding the frequency of use and domain for each tool is based on the works of Yamin, Katt and Gkioulos. The protocols and attacks were gathered from a smaller, more specialized survey conducted by Cintuglu et al. [2], where they reviewed 37 smart grid cyber range implementations. A short description is also given of each tool and protocol. These descriptions were constructed by reviewing the documentation of that particular tool.

**Emulation Tools**
For emulation, VMware, XEN, Emulab and OPENNEBULA were the most common software solutions found in contemporary cyber ranges. VMware and XEN both emulate operating systems and support communication over virtual networks[1,2]. XEN is most commonly used to host virtual machines in cyber ranges targeting the network infrastructure domain, while VMware sees use in several domains, such as critical infrastructure, networking and SCADA applications [84]. Although XEN is free and open source, VMware is seen to be applied more frequently and across a more extensive selection of domains.

Emulab and Opennebula are cloud based virtualization tools and the most common solutions for network emulation [84]. Emulab is a distributed network testbed, containing 500 computing nodes. The service is free and researchers can apply for access in order to create, test, and interface with a virtual network running on top of the Emulab cluster[3]. OpenNebula[4] is a commercial cloud computing and virtualization service. A highlighted feature is native support for VMware and Docker. Jirsik et al. [94] and Vykopal et al. [93] used Opennebula to create virtual infrastructures for their cyber ranges, running mostly in the cloud.

**Simulation tools**
Matlab, Simulink, OPnet and Network Simulator 3 (NS-3) were found to be the most common simulation tools used in contemporary cyber ranges. Matlab is a powerful computing language often used in academic research, and Simulink is a Matlab extension that allows for dynamic system modelling by graphical block diagramming. Both Matlab and Simulink see extensive use in simulation applications related to the SCADA domain, whereas Simulink is also frequently used in cyber ranges targeting critical infrastructure [84].

NS[5] and OPnet[6] are both network simulators. As simulators, NS and OPnet attempt

[1] https://www.vmware.com/products/player/faqs.html
[2] https://xenproject.org/about-us/
[3] http://docs.emulab.net/
[4] https://opennebula.io/docs/
[5] https://www.nsnam.org/about/
[6] http://opnetprojects.com/opnet-network-simulator/

to mimic real-world network behaviour and traffic, as opposed to Emulab and Opennebula which runs network operating systems and protocols on virtual machines. NS and OPnet are both frequently used to simulate local IT-network infrastructure, whereas OPnet is also used in OT-network simulations.

**Communication protocols**

The protocols used in cyber ranges depend on the domain. This section will only look at the protocols relating to IT and OT as those are the communication domains most relevant to the thesis. For IT applications the usual suspects appear as the most common: Ethernet, IP, TCP and UDP. This is a natural consequence of their widespread use in real-world applications. Regarding the OT domain, Modbus[7] and DNP3[8] are the most common [2]. Modbus and DNP3 are both master-slave protocols, meaning the slaves do not transmit any data unless requested by the master node. Modbus is the oldest of the two, released in the 1970's, and is slightly slower than DNP3. This is due to modbus transmitting all data stored in a field device's registers, at every request. Whereas DNP3 only transmits values that have changed since the last request. Modbus is however more frequently used in cyber range implementations[2], likely due to it being royalty free and coming with an open standard.

**Monitoring tools**

Monitoring tools can be used both by the green team, to monitor the state of the cyber range, as well as the blue team to monitor the network traffic for malicious activity. TCPdump[9], Wireshark[10] and IPFIX[11] was found to be the most prevalent monitoring tools. TCPdump and Wireshark are open source packet analyzers, and have the ability to capture packets sent and received on a network interface. The main difference between them is the workflow. TCPdump is a command line tool, whereas Wireshark has a graphical user interface [2]. Wireshark also has a selection of more advanced functions, for instance the ability to filter out TCP streams, only showing packets related to that particular stream[12]. IPFIX (IP Flow Information Export) is an open protocol developed by the Internet Engineering Task Force (IETF), used for network flow monitoring. All three were found by the survey, to be used in networking, cloud, SCADA and critical infrastructure domains.

**Cyber Physical Attack implementations in Smart Grid Cyber Ranges**

Of the 37 cyber ranges surveyed by Cintuglu et al. [2], 12 of them were targeting smart grid cyber security and eight different attacks were identified. The identified

[7] https://www.csimn.com/CSI$_{p}ages/Modbus$101.$html$

[8] https://www.dnp.org/Portals/0/AboutUs/DNP3%20Primer%20Rev%20A.pdf

[9] https://www.tcpdump.org/manpages/tcpdump.1.html

[10] https://www.wireshark.org/index.htmlaboutWS

[11] https://tools.ietf.org/html/rfc7011

[12] https://www.wireshark.org/docs/wsug$_{h}tml_{c}hunked/ChAdvFollowStreamSection.html$

**Table 5.1:** Commonly implemented cyber attacks in smart grid cyber ranges

| Attack Type | Frequency | Attack Type | Frequency |
|---|---|---|---|
| Man-in-Middle | 4 | ARP Spoofing | 4 |
| Denial of Service | 2 | Malformed Packet | 2 |
| Database Attack | 2 | Eavesdropping | 1 |
| Precision Insider | 1 | Rogue Software | 1 |

attacks are presented in table 5.1 above, sorted by the number of ranges employing the particular attack type:

## 5.5 Ongoing Challenges

In their survey, Yamin, Katt, and Gkioulosi also identified a list of main future plans and directions reflecting the ongoing and current challenges in the cyber range field. Based on the identified list and literature review findings, the following problems will be further elaborated [84]:

- Scalability, Realism and Virtualization
- Education and Learning
- User Behaviour Simulation
- Monitoring
- Testing and Evaluation
- Data Interoperability

**Scalability**
Scalability is marked as a challenging task, especially in terms of large-scale network topologies, as well as the ability to support multiple trainees at once. Thus, several papers mention scalability in their plans for cyber range improvement [84, 6, 95, 96, 97]. Two proposed solutions are Software Defined Networking (SDN) and Container technology, both of which are relatively new virtualization techniques that are continually under development. Moreover, SDN introduces several benefits such as easier management and network resilience, scalability, programmability, and other advantages [2]. SDN contributes to scalability because the control layer is separated from the data layer, allowing for logical dynamic and centralized control over hardware devices, as well as efficient traffic flow. However, the majority of organisations have

not adopted SDN due to remaining challenges, like high complexity and security issues [98]. The second solution is suggesting to utilize application container technology, which are running applications in isolated environments, that can be setup in a matter of seconds and support a running service with more resources. It is often used instead of virtual machines to improve scalability in general [97, 99].

**Virtualization and Realism**
In order to build realistic training scenarios and exercises, the run time environment should mimic the real world as much as possible [93, 84, 2]. However, it seems to be quite a challenge to achieve adequate realism as it heavily depends on the limits of virtualization. For instance, it is hard to simulate and/or emulate certain components, such as PLCs and RTUs. Osama et al. [2] suggest to increase realism by implementing support for numerous ICS-SCADA protocols in future designs. Additional ongoing work is aiming to close the gap of realism between virtual CPRs and physical CPRs [100]. Furthermore, virtualization can usually be improved in some way or another, for instance, by minimizing the creation time of a virtual machine. Virtualization is usually the backbone of any cyber range. The use of virtualization technology can be a solution to the problem of inefficient scalability and expensive dedicated computer infrastructures [95]. It can be used to repeatedly create massive virtualizations of network topologies, including machines running full-fledged operating systems and network devices, such as switches and routers, to closely mimic the real-world systems [93].

**Education and Learning**
Conventional cyber ranges are often used for field expert training or academic research, however, these are in many cases not suitable for general cyber security exercises due to inadequate scalability and flexibility [92]. Moreover, multiple cyber ranges are missing support for educational and learning features. Accordingly, ongoing research is aiming to provide educational evaluation techniques and methods [84]. A proposed solution is a so-called learning management system (LMS) where all educational progress is centralized in one place, facilitating the delivery of instructions and learning materials, tracking trainee progress, and grading. The LMS includes a scoring system that provides not only a scoreboard but also statistics and metrics for improved training and increased learning effectiveness [95]. Somarakis et al. [101] suggest another solution by using a model-driven approach for cyber range training, based on the security assurance model.

**User behaviour simulation**
Beuran et al. [95] are using pre-recorded network capture files of emulated cyber attacks in their cyber range, called CyRIS. More importantly, CyRIS offers the option to mix this capture file with pre-recorded normal user traffic in order to make it more realistic, as well as more challenging to the participants. This technique seems

to be one of the better ways of simulating user behaviour. However, it is otherwise done manually in multiple cyber ranges in order to contribute with a more realistic training, but this may be a very time consuming factor. The current tools for user traffic generation can emulate enterprise users, but are limited [93]. Accordingly, the primary challenge resides in the fact that a real-time user behaviour simulation is hard to achieve with a satisfying realism. As a means to mitigate these limitations, the future enhancements are proposing to introduce cognitive factors and agent based simulations [84, 93, 102].

**Monitoring**
Built-in continuous monitoring capabilities are one of the must have requirements, thus, important to have for any cyber range. Monitoring is used to supervise utilization of processor and memory, open or closed connections, interface statistics, among other host characteristics [81]. However, the degree of using monitoring in cyber ranges are various and might be limited in particular solutions. Future work are linked to data collection techniques as well as advanced security monitoring [84].

**Testing and Evaluation**
Only a few papers were suggesting to extend the cyber security testbeds with capabilities for testing and evaluation in future designs [84]. In particular, the cyber ranges were suggested to have the ability to:

- Test security solutions and technologies
- Test attack vectors and techniques
- Test new security features (e.g. reliability and availability)
- Improve the testing techniques

**Data Interoperability**
"Interoperability is the ability of two or more devices to exchange information and work together in a system" [2]. This is achieved by using technical standards, protocols, definitions and compatible formats for data exchange, which is agreed upon between all stakeholders. Accordingly, the interoperability will most likely introduce a challenge or two when building a novel cyber-physical range that comprise multiple components and modules including software, protocols and devices from different vendors [2]. Naturally, some architectural designs cannot be implemented due to incompatibility between different cyber range components, modules or tools [92]. Consequently, it is important to recognize the possible problems that can arise when building a SGCR, especially, with respect to interoperability.

# Chapter 6
# Methodology

In this chapter, we introduce the combination of methods that were used to conduct our research. Beginning with Section 6.1, we provide a brief introduction to the the design science methodology and its terminology. In Section 6.2, we explain the design science framework in terms of the problem-solving cycles, which allows us to develop a final treatment to the design problem. Section 6.3 gives an description of the literature study, followed by Section6.4 which describes the chosen interview methodology.

## 6.1 Design Science

The research methods are based on a qualitative approach by means of performing a literature study, semi-structured interviews (SSIs) and prototype development using design science methodology. The primary information was established through the literature study, while the secondary information was collected through the SSIs. These methods were employed to add depth and supplement the design science framework; from where the final architectural design was established.

The literature study and interviews in conjunction with design science methodology are a suitable combination due to the nature of our study. Regarding the research problem, the combined methods are providing a thorough understanding of previous, related and current work. In particular, the design science methodology is providing us with the necessary tools and guidelines to pursue a final treatment design.

### 6.1.1 Introduction

Design science is a scientific research approach that aims to sole problems, instead of explaining existing patterns and phenomena in nature [103]. The Design science methodology provides the necessary guidelines to study, design and investigate an artifact in context. It is a framework that allows for constructive ideas and reflections in order to ask the right and relevant questions, and ultimately, achieve inferences

[104]. However, the framework does not provide the answers to the questions that arise for a specific project, but are left to be concluded by the researchers. Since our main focus in this thesis is to provide valuable knowledge, the design science framework serves us well as a guiding tool.

In particular, design science consists of two main processes, called cycles. These are the design cycle and the empirical cycle and [104]. As the name suggests, the design cycle is used to solve or treat the so-called "design problems", which is primarily done by iterating over three steps to obtain one or more artifacts. On the other hand, the empirical cycle is used to solve or answer the so-called "knowledge questions" that arise, for example, in a design process. Separately, both cycles can be used to solve different problems in their very nature, but the combination of the two are establishing a solid methodological approach, as they complement each other well [104]. The cycle combination is the essence of design science, and make up the core of our scientific methodology. The following sections are further elaborating on these concepts.

### 6.1.2 Terminology

Design science brings interesting and characteristic terminology, such as "artifact", "treatment", "knowledge questions", etc. This is mainly due to avoid confusion with other terms and scientific approaches [104]. Note that Section 7.1, presents the design problem, identified stakeholders, elicited stakeholder goals, specified knowledge questions, as well as the derived artifact requirements. Here we define the most important terms to be used in the forthcoming sections.

- **Design problem:** The problem to design or redesign an artifact such that it better contributes to some goal is called a design problem. The design problem is treated by following the design cycle [104].
- **Mechanism:** Design science defines a mechanism to be an interaction between system components [104].
- **Artifact and Context:** An artifact is the object of study in a particular context. An artifact could be, for example, techniques, services, methods, algorithms, or systems that are used in software and information systems. The context could be, for example, development, design, maintenance, and use of software and information systems [104]. In our case, the artifact to be designed is a smart grid cyber-physical range in a user context, where the possible users are the identified stakeholders. Since we design an artifact for this specific context, we should also investigate it in this context [104].

- **Knowledge questions:** An answer to a knowledge question (KQ) will always be a proposition that is made by inferences [104]. The answer will serve as input to the design cycle, and thereby, helping to solve design problems. As we try to answer a KQ, we also assume it is the only answer. However, we don't really know the answer; it might be wrong, it might be true in some cases, it might be a partial answer, or even an answer to a slightly different question. The KQs are answered by following the empirical cycle, but these questions must be *fallible*; we can never know if we have actually found the answer [104]. An example of a KQ could be; "is the simulation in <some artifact> realistic enough?", or "is the <artifact> usable and useful to cloud service providers?".

- **Stakeholders:** The stakeholders are contained within the social context of design science, and may be anyone that directly affect or may be affected by the project. Stakeholders are, for example, all possible users, operators, maintainers, etc. of the artifact to be designed [104].

- **Treatment:** A treatment can also be thought of as a solution, but a solution is something that completely solves a problem, while a treatment is something that might contribute to solving the entire or parts of a problem, or maybe not at all [104]. Wieringa uses the following example to illustrate the difference:

  > *"Consider a person visiting a doctor in order to receive some medicine to solve a specific health issue. The treatment is the interaction between the artifact (medicine) in a problem context (the human body)."*
  >
  > – Roelf J. Wieringa, Design Science Methodology (2014)[104].

  Just like the knowledge questions, the treatment is also *fallible*, as further explained in the following section. Ultimately, the artifact(s) to be designed should help the stakeholders by *treating* a problem [104].

- **Prior and posterior knowledge:** The knowledge context distinguishes between the "prior knowledge" and "posterior knowledge". All knowledge that is prior to the project is called *prior knowledge*, whereas all knowledge gained as a result from the project is called *posterior knowledge* [104]. Accordingly, we have prior and posterior knowledge questions, as mentioned below.

## 6.2 Design Science Framework

In this section, we explain the purpose of design cycles and empirical cycles, depicted in Figure 6.1 and Figure 6.2, respectively. Additionally, a brief description of how we proceeded is explained within each iteration step. We also provide a holistic overview of the design science framework and how the cycles are connected.

### 6.2.1 The Design Cycle

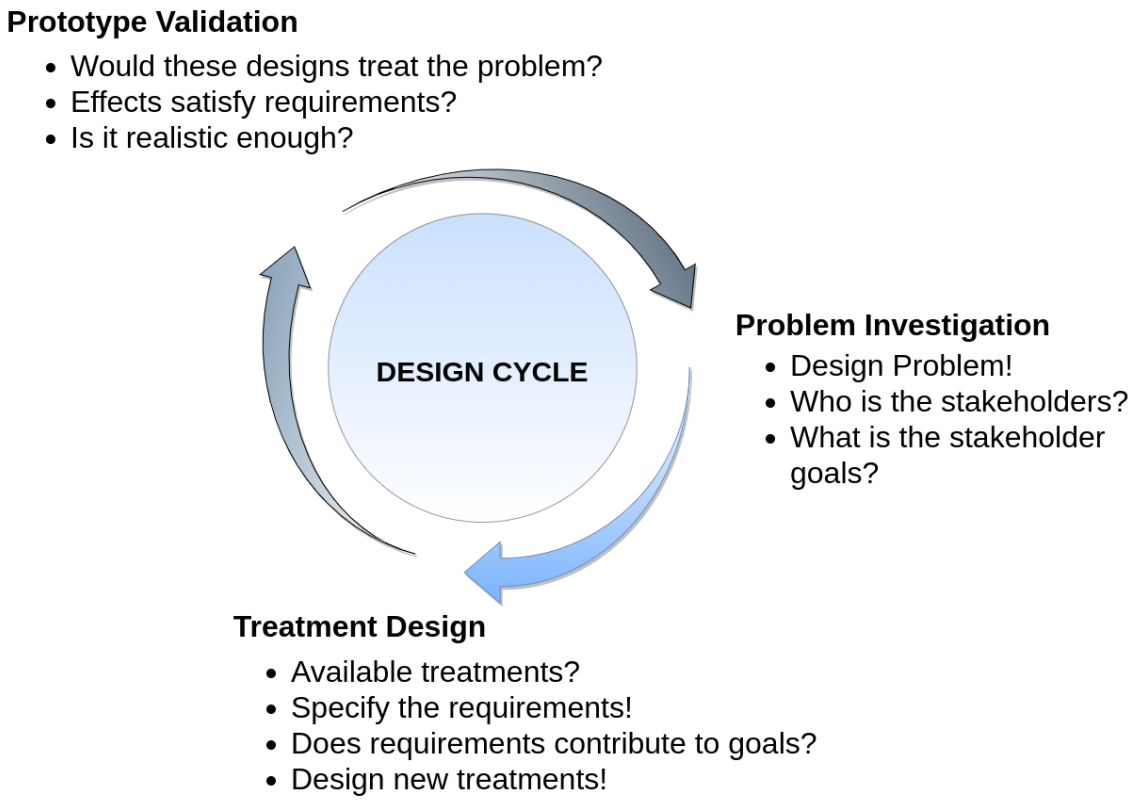


**Figure 6.1:** Depicts the design cycle. Each iteration step is exemplified with problems. The question marks denotes a knowledge question, while the exclamation marks denotes a design problem. Adapted from Roelf J. Wieringa [104].

#### Problem Investigation

The problem investigation is the first iteration step in the design cycle, and is where our research begins. This is a step where we prepare for the design of a treatment by learning and understanding the problem to be treated. The purpose is to discover what real-world phenomena must be improved and why [104]. Moreover, problem investigation is a step where we process and turn important data – collected from literature studies and interviews – into meaningful and useful information. From this information, we gain insight into the problem context that help us to specify a design problem to be treated, as well as any stakeholders that would like to see the problem be treated. In design science, it is important to obtain the stakeholder goals, because the goals define the problems we intend to treat [104].

After we determined a problem investigation plan, we specified the initial design problem to be treated. The design problem was improved and ensured by iterating over the initial problem as new information were collected. Additionally, the stakeholder goals were elicited from the collected information, especially from the interviews. Further, the artifact requirements were created and derived from the stakeholder goals. Notice that the artifact requirements actually belong to the step for treatment design, because the requirements are in fact a matter of design. However, we defined the requirements in this step due to improved readability and a natural flow. Furthermore, the prior knowledge questions that emerged throughout the iteration(s) were answered by the literature study, whereas the posterior knowledge questions were answered by us, the researchers, during the prototype validation step. The specific methods we used to obtain prior knowledge, that is to say, the literature studies and interviews, these are explained in Section 6.3 and Section 6.4.

Based on design science methodology [104], we arranged the problem investigation as shown below. The results are presented in Section 7.1:

1. Specified the design problem to be treated.
2. Identified project stakeholders.
3. Elicited stakeholder goals from the semi-structured interviews.
4. Specified the (initial) knowledge questions based on the design problem and collected information.
5. Researched the knowledge questions using the empirical cycle, which included the interviews and literature study.
6. Requirements were then formulated from the stakeholder goals and findings from the literature study.

**Treatment Design**

Treatment design is the second step in the design cycle, and is where we initiate the artifact design process. Because the literature contains what is already known about the problem, a survey of the state-of-the-art is always included in the treatment design step, and this is done by a literature study [104].

Based on design science methodology [104], we arranged the treatment design as shown below. The results are presented in Section 7.2:

1. Conducted a literature study; trying to answer knowledge questions.

2. Specified a high-level design, including modules and components.
3. Itemized and defined all selected tools to be used in the artifact.
4. Specified a low-level design, including communication layers and protocols.

**Prototype Validation**
Treatment validation and evaluation are both concepts in design science, but we are only considering the treatment validation. However, in order to fully understand treatment validation, we need to briefly explain treatment evaluation. Treatment evaluation is done in the field in order to evaluate an applied and already implemented treatment by observing it in a problem context [104]. On the other hand, a treatment validation is usually done in a laboratory or under similar conditions. It is important to note that, in contrast to evaluation, the validation tries to *justify* that a treatment (prototype) would contribute, or fulfill, the goals of its stakeholders if implemented in the real world. Thus, the ultimate goal of treatment validation is to examine, and make *predictions* about how the artifact will interact within its respective context [104].

To perform treatment validation we developed a small-scale prototype which we used to performed a selection of tests. These tests were designed to answer knowledge questions about the practicality of key concepts in our design. The knowledge questions and the results of the testing are described in section 7.4 Validation. Interpretations of the results and their implications are further discussed in Chapter 8.

### 6.2.2 The Empirical Cycle

The adapted empirical cycle, as depicted in Figure 6.2, were used to supplement the design cycle. Such that, when we got a new knowledge question or a group of knowledge questions, a spin-off empirical cycle was performed in order to find an inference. How we performed each step from Figure 6.2 is briefly explained below.

**Research Problem Analysis**
In this step, we used the design problem to derive a list of relevant topics:

- Smart grids and critical infrastructures
- Security, attacks and threats
- Information security incident management
- State-of-the-art cyber ranges

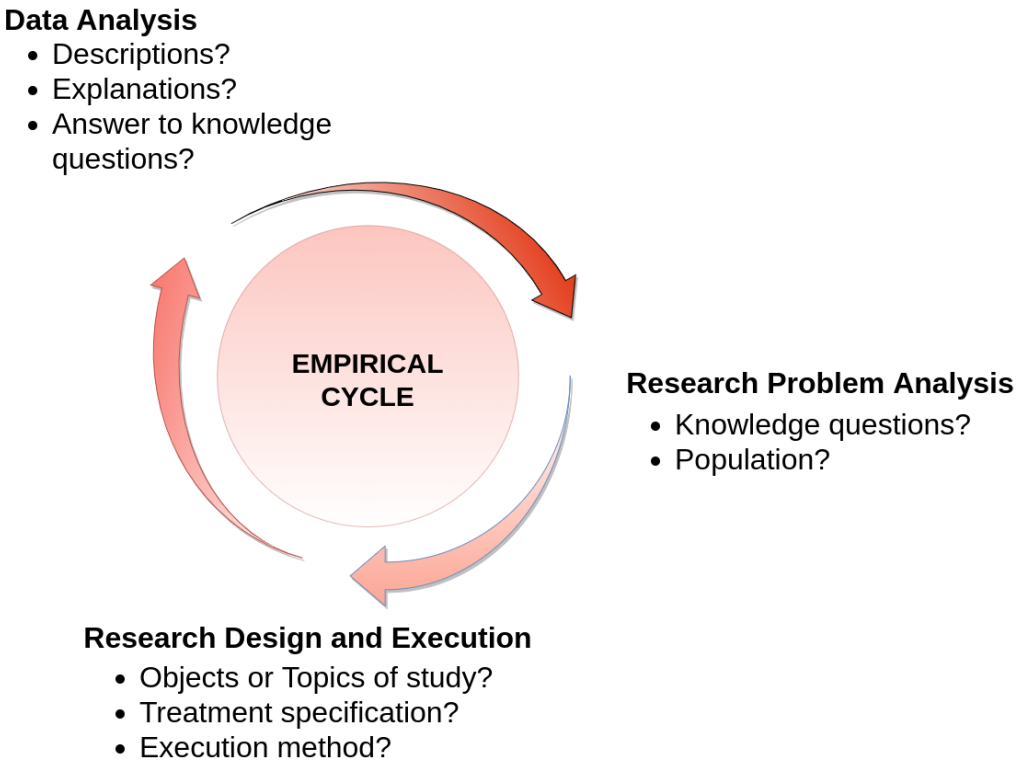


**Figure 6.2:** Depicts the empirical design cycle. Each iteration step is exemplified with knowledge problems. Adapted from Roelf J. Wieringa [104].

Furthermore, we derived several knowledge questions (KQs) from these topics. The KQs are listed in Section 6.3, for the sake of context. Furthermore, we defined what to do in terms of solving the specified knowledge question(s). In our case, it was a matter of conducting semi-structured interviews and the literature study.

**Research Design and Execution**
Here we accumulated all KQs in order to define a research problem to be solved. Followed by the execution of either a semi-structured interviews or the literature study, as deemed appropriate. The execution steps are further described in Section 6.3 and Section 6.4.

**Data Analysis**
In this step, we analyzed all collected information and decided what to include. In terms of the literature study, we performed a selection of search engines and defined inclusion criterias and word search. Regarding the interviews, the transcriptions were examined and necessary information was further drawn out with respect to the stakeholder goals.

### 6.2.3 A Holistic Overview

Figure 6.3 illustrates the connection between the design cycles and empirical cycles, as used in our thesis. Starting from the top of the blue spiral, representing the iterations of the design cycle, and moving vertically downwards. Whereas the red circles, representing the empirical cycles, are temporary spin-offs in order to answer the KQs. Ultimately, approaching a final artifact design and prototype.

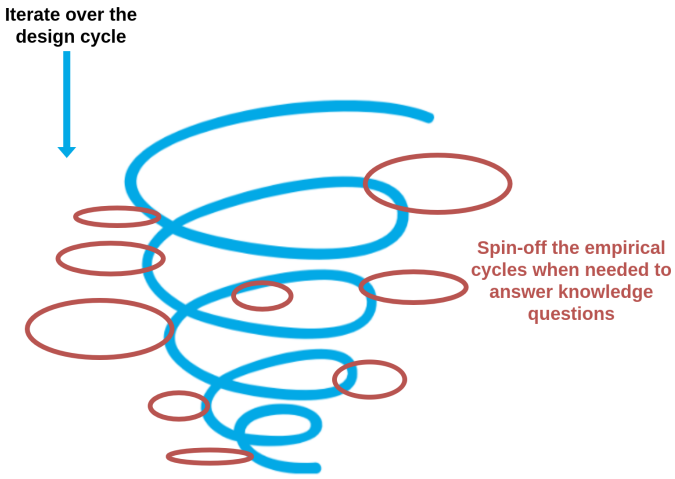


**Figure 6.3:** Illustrates the connection between design cycles and empirical cycles.

As previously mentioned, a very important observation about the problem-solving cycles is that all results are *fallible*. Meaning that an artifact may not fulfill all stakeholder goals, or knowledge questions might have validity limitations [104]. Accordingly, the artifact design and answers to KQs must be justified in terms of stakeholder goals, the structure of problems and artifact requirements [104].

We are now ready to provide an holistic overview of the design science framework, depicted in Figure 6.4. The framework consists of a social context, a design context and a knowledge context. These are further explained below.

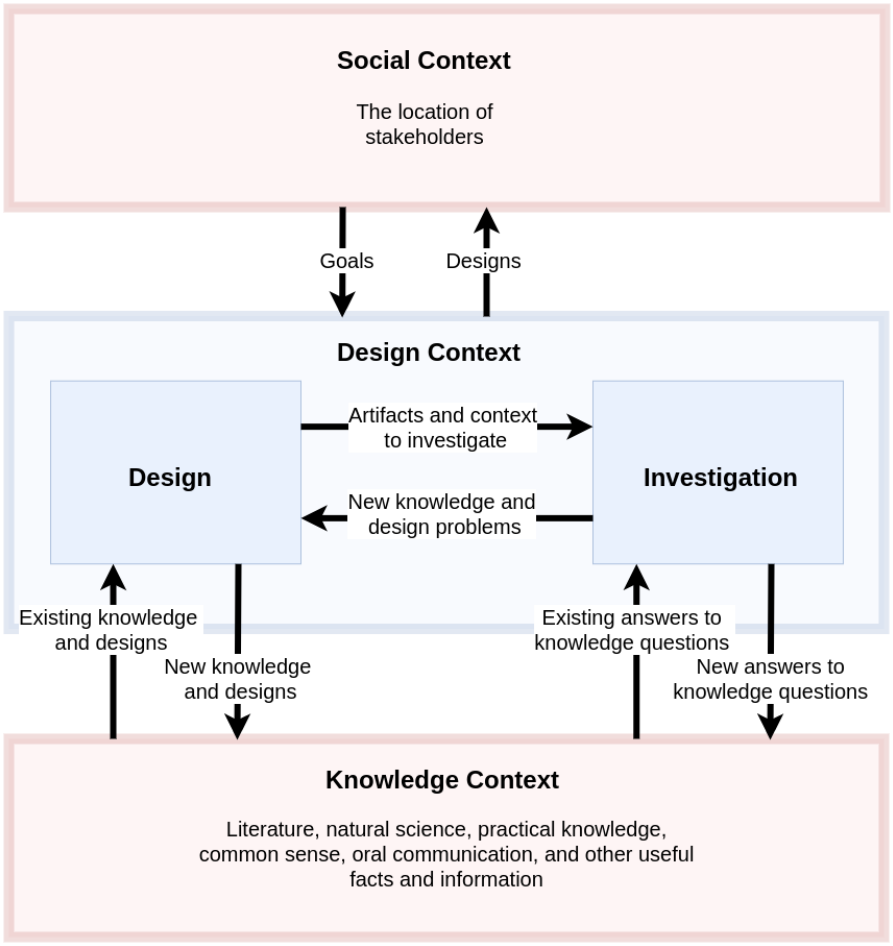


**Figure 6.4:** Depicts an overview of the design science framework that is used as our principal research method. Adapted from Roelf J. Wieringa [104].

- **Social Context:** Is where the project stakeholders and potential sponsors are located. They are the ones that want a particular problem solved and provides the project goals (and budget) to be fulfilled. However, they may not know the problem and/or the goal, thus, the formulation of these might be part of the research [104]. Ultimately, the researchers reply with new designs and prototypes that may satisfy these goals. Based upon the researchers' justification that an artifact might treat a problem, the stakeholders decide whether the artifact should be implemented or not. It is important to note that the researchers do not necessarily implement the artifact, but validate its design by, for example, partial implementation and testing [104].
- **Design Context:** Is where the researchers conduct the necessary investigation and construct artifact designs and prototypes. Design science, as explained above, makes use of both problem-solving cycles to generate an iterative process of design and problem investigation [104].

– **Knowledge Context:** Is where all the existing theories, lessons learned, and practices are located, including available products, specifications, ongoing challenges and currently known designs, amongst other useful information. This information is obtained in various ways, such as professional literature reviews, oral communication and expert interviews [104]. The knowledge context is used by design science in order to create something new, and may also add something to it by answering knowledge questions and produce new designs [104].

### 6.2.4 The Iteration(s)

In order to collect the prior knowledge, we engaged the social context and knowledge context. We reached out to the identified stakeholders; a selection of them were invited for an interview. The most significant part of the prior knowledge was gained through an extensive literature study. Whereas the posterior knowledge was obtained and presented throughout the resulting Chapter 7.

In a step-wise and convergent manner, we approached a final treatment design. One large design cycle iteration led to several KQs being answered, which in turn, improved our design. In the beginning, we intended to conduct several smaller design cycle iterations, however, we determined otherwise due to time constraints. The final results may have been affected by this choice, and is further discussed as a limitation in Chapter 8. Nevertheless, we decided to perform a single comprehensive design cycle iteration, that resulted in a total of 8 empirical iterations. Four from the interviews; one iteration for each interview, and four from the literature study; one iteration for each topic of study.

## 6.3 Literature Study

In design science, a literature study is used to collect necessary information that is already known about the problem, this knowledge is then used to create and design new artifacts [104]. Design science does not require any specific method, thus, we chose to conduct our own method.

We used the following plan for our literature study:

1. We performed a selection of academic search engines
2. We specified a chapter name based on the topic of study
    a) Inclusion criteria
    b) Word search
3. We analyzed the paper findings

### 6.3.1 How we conducted the literature study

As we advanced in the design cycle, several KQs were specified and gave rise to multiple spin-offs. The spin-off empirical cycle, as explained above, has been a great tool for problem-solving in terms of KQs. Table 6.1 provides an overview of each prior KQ that corresponds to a background chapter. The initial and majority of KQs are directly derived from our design problem. Notice that these questions are accumulated over time, and are provided here for the sake of context in terms of the four background chapters. The list is not extensive, but includes the ones of most importance.

The entire literature study was based on the prior knowledge questions, as depicted in Table 6.1. As such, the literature study aimed to provide answers to our KQs. Furthermore, we performed a selection of academic search engines, and found that the following were suitable; Google scholar, ACM Digital Library, Springer Link, Wiley Online Library, NTNU Online University Library (Oria). The respective chapter topics and their inclusion criterias and word search are listed below. The word search were used to create various search strings to be used in the selected search engines. Whereas the inclusion criterias were used to identify the relevant papers, mainly by a quick investigation on the paper's abstract. Finally, we analyzed the paper findings which had passed the inclusion criterias. All the results from our literature study are provided in Chapter 2 through Chapter 5, and constitute our research background.

- **Chapter 2: Smart Grid and Critical Infrastructures**
  - Inclusion criteria: All papers that are exclusively about power grids, smart grids, and critical infrastructures in general, with a focus on national and international standards in the electric power and utility industry.
  - Word search: Smart grids, future power grids, electrical power grids, critical infrastructures, industrial control systems, supervisory control and data acquisition, ICS/SCADA, SCADA, traditional, power grids
- **Chapter 3: Security, Attacks and Threats**
  - Inclusion criteria: All papers that are related to the security, attacks and threats of the traditional power grid or smart grids. Topics of interest should be; previous cyber attacks on ICS or critical infrastructures, advanced persistent threats, and the cyber kill chain.
  - Word search: Cyber attacks, critical infrastructures attacks, smart grids, power grid cyber attacks, electrical power grid attacks, advanced persistent threats, cyber kill chain, apt, ckc, ICS cyber attacks, smart grid cyber security, smart grid threats.

**Table 6.1:** Showing the most important prior KQs and respective chapters they are answered in.

| **Prior Knowledge Questions** | **Answered in** |
|---|---|
| What is a Smart Grid?<br>What is the core functions of a Smart Grid?<br>How does the technical internals of a<br>typical and critical infrastructure work?<br>What are the standards? | Chapter 2 |
| Is it possible to impact a real-world<br>smart grid or power grid with a cyber attack?<br>Any real-world scenarios?<br>How does a cyber attack on a<br>critical infrastructure work?<br>What are the typical steps done<br>by an ICS adversary?<br>What are the possible threats? | Chapter 3 |
| Which steps are involved in an<br>incident response process?<br>Which tasks must the blue team participants<br>be able to carry out in the cyber range? | Chapter 4 |
| What is a cyber range?<br>What are the requirements?<br>What is the state-of-the-art cyber range<br>architectural design?<br>What are the typical components<br>of a cyber range?<br>Any cyber ranges that is related to<br>cyber security and/or smart grids?<br>Is it possible to simulate a smart grid<br>within a cyber range in a satisfactory manner?<br>What about network components?<br>Is it possible to generate and mimic<br>real-world user network traffic?<br>What are the ongoing challenges<br>in current cyber ranges in terms of design? | Chapter 5 |

- **Chapter 4: ISIM**
  - Inclusion criteria: The topic of incident response must be related to security. It must also be a recognized international standard, either from ISO, ITU, IEC, IETF, IEEE, or similar.
  - Word search: Information security, incident response, incident management, ISO-, ITU-, IEC-, IETF-, IEEE incident response, cyber security, CERT, CSIRT, Blue team.
- **Chapter 5: State of the Art Cyber Ranges**
  - Inclusion criteria: All cyber ranges related to cyber security, smart grids and electrical power grids. Topics about software and hardware implementation, development, design choices, requirements, state-of-the-art designs, taxonomy and problems/challenges.
  - Word search: Cyber ranges, cyber physical range, cyber physical testbed, smart grid, cyber range, smart grid testbed, ICS/SCADA cyber range, ICS testbed, industrial control system, cyber-physical battlefield, testbed, warfare, simulation, Norwegian, national cyber range, industrial control system testbed, design, architecture, taxonomy, cyber-physical range.

## 6.4 Semi-Structured Interviews

Design science suggests multiple forms of surveys to obtain real-world data. Surveys can be conducted by, for example, paper questionnaires, oral interviews, emails, chat messages, web forms, among others [104]. Surveys are an important contribution to the problem investigation, because they can collect information about real-world phenomena [104]. Nevertheless, design science does not require any specific method, however, we chose to conduct semi-structured interviews (SSIs). SSIs are a suitable way of collecting secondary and real-world information due to the nature of our study. An SSI is a simple and descriptive method that allows us to ask open-ended questions, also known as qualitative interviewing. By using open ended questions we are able to gather information from the candidates past experiences, expertise, opinions and ideas about the future [105]. It is conducted with one respondent at a time, and is a method that supports follow-up questions in terms of why and how questions [105]. Although the SSI is considered a labor intensive method, we approved it to be used in our research.

We conducted the SSIs by following the research of William Adams [105] on "Conducting Semi-Structured Interviews". We established the SSIs in the following order:

1. We identified the stakeholders/respondents and arranged the interviews.

2. We specified the questions and interview guide.
3. We conducted the interview.
4. We polished the transcription.
5. We analyzed the SSIs.

### 6.4.1 How we used the SSI method

The interviews were taken into account in an early stage of the research. First, we decided on the topics to be contained in the interview guide; after some discussion we concluded with "incident response" and "cyber ranges", as the main topics. Accordingly, we continued by drafting the questionnaires in accordance to the SSI method. It was shortly followed by the formulation of invitations, that were sent to the stakeholders by email. The identified stakeholders are listed in Section 7.1.

Furthermore, the SSI meetings were scheduled and organized by using a web-application service, called Doodle. The creation of a Doodle account was done with ease and free of charge. It allowed us to set immutable and convenient time slots for the upcoming interviews. A shareable link to the Doodle appointment service was created and attached to the invitation email, allowing the participants to enter the service and select between a variety of predetermined time slots. Thus, it were several benefits of using the Doodle service, for example, only one shareable link was needed, time slot collisions were prevented, and a given dashboard containing the overview of all enrolled participants.

The interviews were performed online by using Teams, Skype, or any other suitable conference software. We started each interview with an informative introduction to our interview policy, including statements of participant anonymity, non-confidentiality, privacy and the use of sensitive information. The sensitive information, such as, names, current job positions, emails, etc., were not to be stored, used or processed in any way. Hence, the participants will remain anonymous throughout the thesis. Additionally, the participants were informed that the answers gathered during the interview would not be held confidential as they were to be used in our thesis.

As expected, the different interviews were relatively dispersed in time due to the respondents having varying availability. Thus, the intervals between one interview and the next could be significant. Meanwhile, we continued the work of improving the questionnaires and sustaining the progress in literature reviews. Moreover, based on the number of questions, as well as the preferred and reasonable maximum length of SSIs, we planned the interview duration to be about 1 hour each. However, some interviews lasted for approximately 2 hours, most likely due to open-ended questions and our intent to not interrupt the respondent. After each interview

we used approximately 2-3 hours to refine and polish the documented results, and stored them in Google Docs. Finally, the polished transcription was sent back to the corresponding respondent for verification of quotations.

A total of ten individuals were contacted, from which five accepted the invitation. One of which declined at a later date. In total, four interviews were conducted. The enrolled participants are briefly presented below. Their answers are mainly used to define the stakeholder goals.

The general interview guide is provided in Appendix B.1. The guide is not exclusive, as the questions were slightly different from participant to participant, depending on the expertise and proficiency. For brevity, the specific questions including the follow-up questions are omitted. The questions that were common to each interview are given in the guide. Moreover, a selection of the most important quotes are provided in Appendix B.2, and are used in conjunction with the stakeholder goals.

### 6.4.2 Anonymous presentation of respondents

- Person 1: Technical lead at a European cyber range, having experience in design and implementation of a large scale cyber range with cyber physical components.
- Person 2: A researcher and expert in the field of cyber ranges. Experienced with designing and building a CPS cyber range.
- Person 3: A representative from a TSO with experience within incident response and cyber security.
- Person 4: An executive and cyber security professional experienced in various preventive work and incident response tasks related to industrial control systems.

# Chapter 7
# Results

In accordance to the design science methodology, as described in Chapter 6, we put forward our main findings in this chapter. This chapter represent the outcome of a comprehensive design cycle iteration, and is divided into three sections; each reflecting the results from the design cycle steps. In Section 7.1, we follow the problem investigation step, and itemize all the identified stakeholders and elicited goals. We further list all the SG3C artifact requirements. Section 7.2 and 7.3 presents the high- and low-level architectural design of the SG3C artifact. Additionally, the artifact roles and tools are listed and described. Finally, a partial implementation of the design is presented in Section 7.4. The prototype implementation allowed us to test and conduct single-mechanism experiments in order to validate the SG3C artifact design.

## 7.1 Problem Investigation and Artifact Requirements

In this section, we present the problem investigation, in which, we conduct real-world research to identify the possible stakeholders and the stakeholder goals in compliance with the method described in Chapter 6. The stakeholder goals and possible project constraints are elicited from the stakeholders, and used to derive and define the necessary artifact requirements. Thus, the ultimate goal of this section is to present the resulting requirements that we created for the SG3C artifact to be designed. Additionally, we chose to further assist the main requirements with more specific subrequirements, assuming it would be easier to test the final treatment design.

Recall from the introduction chapter that the design problem is to;

> ***Improve stakeholders ability to create and execute smart grid cyber-security training scenarios by creating a novel design for a SGCR.***

Throughout the design cycle iterations, we tried to find a treatment to the selected problem, and the final result is presented in the following section. Based on the problem investigation, we defined the possible stakeholders to be:

- The CINELDI project.
- Norwegian Cyber Range (NCR).
- NTNU Department of Electric Power Engineering, including researchers in the national smart grid laboratory.
- All TSOs and DSOs in current need for smart grid cyber-security training.
- Security professionals aiming to improve their expertise in the smart grid domain.

Based on the interviews conducted with stakeholders, we elicited and identified the stakeholder goals (SGs) listed below. Table 7.1, shows the mapping between the SGs and the quotes they originate from. The quotes are enumerated and listed in Appendix B.2.

- SG1 Design: Design realistic training scenarios for smart grid cyber-physical security.
- SG2 Attacks: Arrange realistic attacks against a realistic training environment.
- SG3 Simulate: Simulate parts of own infrastructure in the cyber range with low costs.
- SG4 ICS: Learn more about ICS-specific attacks and how adversaries operate.
- SG5 Triage: Learn to triage effectively and detect signs of attacks in a smart grid context.
- SG6 Isolate: Learn to isolate attacks and minimize damage from smart grid cyber attacks.

- SG7 Incident Response: Practice incident response routines and protocols.
- SG8 Cooperation: Have several defenders train and cooperate simultaneously.

**Table 7.1:** Relation between stakeholder goals and interview qoutes.

| **Stakeholder Goals** | **Quote No.** |
|---|---|
| SG1, SG3 | 1 |
| SG1, SG4, SG7, SG8 | 2 |
| SG4, SG5, SG7 | 3 |
| SG4, SG7 | 4 |
| SG2, SG6 | 5 |

We then moved on to derive the necessary artifact requirements. We defined the requirements and the corresponding subrequirements for the SG3C artifact as follows:

**R1 Versatility:** SG3C must be flexible in order to manage different functions across the IT, OT and smart grid domain, either by substitution or modification of individual components.

- R1.1 Subrequirement: SG3C must support customizable IT and OT infrastructures.
- R1.2 Subrequirement: SG3C must support the ability to import/create replicas of different smart grids components and systems.

**R2 Scalability:** SG3C must be scalable in terms of number of users, components, and services represented in the training scenarios.

**R3 Compatibility:** SG3C must support compatibility in terms of being compatible with external systems, and should be able to integrate (or connect to) external systems.

**R4 Open-Source:** SG3C should employ open-source solutions whenever possible, to keep costs down and maintain adaptability.

**R5 Monitoring:** SG3C must support real-time monitoring and after-action analysis of traffic data, packet capture and alert logs from the training environment.

- R5.1 Subrequirement: SG3C must give the control center (green team) an overview and adequate control over current activities and processes within the cyber range.

**R6 Customizability:** SG3C must have the ability to add, remove and modify applications and services represented in the training environment in order to support custom learning objectives.

**R7 Reusability:** SG3C must support storage, re-use and customization of previous training scenario configurations.

- R7.1 Subrequirement: SG3C should be able to extract individual components.

**R8 ISIM:** SG3C must support practicing cyber security incident response frameworks such as ISO 27035 [78] and NIST SP 800 [74]. This implies the following; the blue team must be able to perform the technical steps in the information security incident management (ISIM) phases; Detect, Isolate, Eradicate and Recover.

- R8.1 Subrequirement: SG3C should include the tools necessary to monitor, detect, isolate and recover from attacks, as well as analyse the attacks post mortem.
- R8.2 Subrequirement: SG3C should have the capability to let defenders (blue team) control host communication and other security mechanisms in the network, such as firewalls, gateways, etc.
- R8.3 Subrequirement: SG3C should give defenders (blue team) the necessary control and overview of safety and security mechanisms in order to protect and recover the system.

**R9 ICS-CKC:** SG3C must support exercise scenarios that include one or more of the following ICS-CKC phases; (Stage 1) Recon, Delivery, Exploit, Installation, C2; and (Stage 2) Deliver, Install, and Execute ICS-specific attack.

- R9.1 Subrequirement: SG3C should support custom automated and manual attacks.
- R9.2 Subrequirement: SG3C should support a selection of realistic prescripted attacks that should be relative to those observed in the real world.

- R9.3 Subrequirement: SG3C should support easy configuration of automated attacks.
- R9.4 Subrequirement: SG3C should include necessary pre-scripted flaws or vulnerabilities in order to give the attackers (red team) a starting point.

**R10 Applicability:** The SG3C must reflect one or more core smart grid functions, such as distributed management, power, storage and generation, V2G or G2V, sensor networks, actuator networks, bidirectional power or communication, and computational intelligence.

- R10.1 Subrequirement: SG3C must support physical or simulation/emulation of common and security critical smart grid functions.

**Table 7.2:** Showing how the stakeholder goals are covered by the requirements

| **Stakeholder Goals** | **Requirements** |
|---|---|
| SG1 Design realistic training scenarios for smart grid cyber-physical security. | R1, R5, R6, R8, R9, R10 |
| SG2 Arrange realistic attacks against a realistic and virtual environment. | R6, R9, R10 |
| SG3 Simulate own infrastructure in the cyber range with low costs. | R1, R4, R6, R7, R10 |
| SG4 Learn more about ICS-specific attacks and how adversaries operate. | R9, R10 |
| SG5 Learn to triage effectively and detect signs of attacks in a smart grid context. | R3, R5 R8, R9 |
| SG6 Learn to isolate attacks and minimize damage from smart grid cyber attacks. | R5, R8, R10 |
| SG7 Practice incident response routines, mechanisms and protocols. | R2, R5, R8, R9 |
| SG8 Train several ICS / smart grid defenders simultaneously. | R2, R8 |

Table 7.2, depicts how the defined requirements were meant to satisfy and fulfill the stakeholder goals. Although, the requirements were derived with the stakeholder goals in mind, we gained inspirations from the literature study. All requirements were inspired from the prior knowledge, especially in terms of the identified must-have requirements for a cyber-physical range. We were surprised to see how much prior knowledge from different sources were able accommodate the predefined stakeholder goals. Indicating an adequate approach in terms of deriving the initial topics from the design problem. Finally, we used the prior knowledge to culminate, devise and create the artifact requirements in order to accommodate the stakeholder goals. Table 7.3 gives an overview of where we obtained our inspirations. The artifact requirements are further discussed in Chapter 8, while the next section presents the final treatment design.

**Table 7.3:** Showing source of inspiration in terms of the SG3C artifact requirements.

| Requirements | Source |
|---|---|
| R1, R3, R4 | [6, 93, 106] |
| R2, R5, R6, R7 | [92, 93, 106, 6] |
| R8 | [76, 78, 74, 79] |
| R9 | [44, 51] |
| R10 | [82, 22, 19, 24] |

## 7.2 High-Level SG3C Treatment Design

The following sections explains the smart grid cyber-physical range design that was created as a result of this project. Subsection 7.2.1 gives a high level description and outlines the architecture, the tools used and the teams that operate in the range. This is then followed by Section 7.3 Low Level Description, which goes into greater depth about design choices and how the different components and tools works together to form a complete cyber range solution.

### 7.2.1 High-Level Description

Figure 7.1 illustrates the architectural design of the cyber range. The architecture is split into three main modules; the range management center (RMC) module, the virtual scenario environment (VSE) module, and the virtual participant environment (VPE) module.

The RMC module is where the training scenarios are created, edited, and then deployed into the VSE module. The RMC module also controls and monitors the training scenarios running in VSE. The VSE module hosts the topology, components, applications and services that constitute the training environment. Finally, the VPE module consists of virtual machines (VMs) for the blue and red team participants to access via remote desktop software. The VMs contained in the VPE is pre-configured with network access to the VSE, as well as the tools needed by the blue and red team members to achieve their objectives. The three modules can be hosted in one single physical machine for smaller scenarios, a cluster of machines, or be hosted on a cloud service platform for larger scenarios.

#### Virtual Scenario Environment (VSE) module

The purpose of the VSE is to host a virtual environment where the red and blue teams can carry out their objectives, such as practicing offensive and defensive techniques in a realistic scenario. This is realized in the design by the VSE supporting the

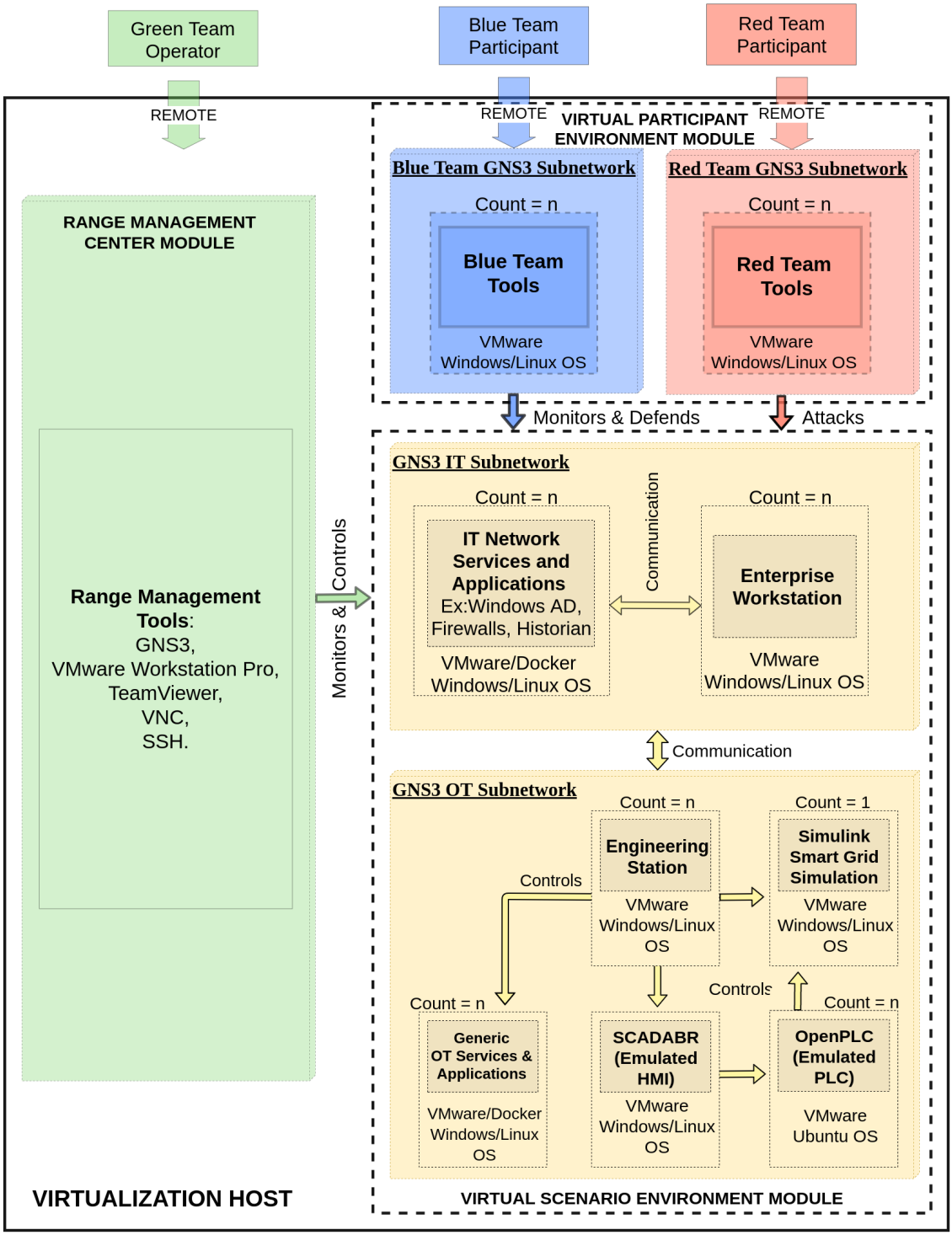


**Figure 7.1:** The Final SG3C Architecture.

deployment of realistic IT and OT networks, simulated smart grid topologies, as well as a wide array of applications and services common to the IT and OT domains. The IT and OT networks consist of emulated real-world network equipment and protocols, running on virtual hardware. Applications, services, and smart grid simulations are further hosted inside a combination of virtual machines, which all communicate over the emulated network.

#### Range Management Center (RMC) module

The purpose of the range management center (RMC) module is to enable the green team to administrate, monitor, and maintain the cyber range. It also contains the functionalities needed to create, edit, and deploy training scenarios in the range. The green team either connects to the RMC via remote desktop access, or they can work directly on the main host of the cyber range.

#### Virtual Participant Environment (VPE) module

In order to access the scenario environment (VSE), the blue and red team members connect to the virtual participant environment module (VPE) via a remote desktop client. In particular, the red and blue team members connect to preconfigured virtual machines contained within the VPE. As a consequence, there is little or no setup required by the participants. The VPE is segregated into two VLANs, one for each team, and connected to the VSE over the emulated network. Depending on the scenario, the red team can either have native access to the VSE or must find and exploit vulnerabilities in order to gain access.

### 7.2.2 Artifact Roles

This subsection gives a brief description of the teams involved with the cyber range. Note that an individual may have roles in several teams. For instance, a white team member can design a training scenario and transition to a green team role by implementing the scenario in the range.

#### White Team

The white team is responsible for designing the training scenarios, storylines and learning objectives. They may also act as instructors during the scenario execution.

#### Green Team

The green team operates as the administrators of the cyber range. Their tasks are to maintain the cyber range and implement the scenarios defined by the white team. During scenario execution, the green team also monitors and controls the scenario environment (VSE). The green team tasks are carried out from the range management center (RMC).

**Blue Team**
The blue team consists of cyber security professionals. They represent the problem to be treated in terms of design science, where they are supposed to learn and achieve new knowledge by interacting with the cyber range (artifact). Thus, the treatment is to let the blue team interact with the SG3C artifact and give them a hands-on experience that yields learning effects. The blue team objectives are specified by the training scenario, but usually include detection, isolation, eradication, and recovery from cyber attacks, as well as monitoring of the network environment.

**Red Team**
The red team's objective is to attack the scenario environment and disrupt applications, services and the smart grid topology. Depending on the scenario, they can start out in any of the ICS-CKC phases; Recon, Delivery, Exploit, Install/Modify or the Command & Control phase. The red team can either be given direct access to the IT or OT network, or they can be required to gain access through exploiting security vulnerabilities in the virtual environment. The Red team can consist of human participants using Kali Linux, or the Caldera adversary emulation engine can be used in order to create an automated red team.

### 7.2.3 Artifact Tools

The tools used within the cyber range are listed below and given a brief description as an overview.

**GNS3:** Open source network emulator that supports emulation of real network devices and operating systems, as well as complex network topologies.

**VMware Workstation Pro:** Commercial virtual machine hypervisor that supports parallel hosting of uptil 80 separate virtual machines from one single computer. VMware Workstation Pro also supports GNS3 integration.

**Docker:** Software tool for creating and running containers. Containers are the result of bundling a single application together with a stripped-down operating system, only containing the libraries and functions required by that particular application. The purpose of containers is to enable hosting of singular applications on very lightweight virtual machines.

**Simulink:** Matlab based graphical programming environment for system modeling and simulation. Simulink can run complex and realistic simulations of grid topologies and components.

**SCADAbr:** Open source SCADA system, which includes a customizable Human Machine Interface (HMI)

**OpenPLC:** Open source PLC emulation which can be hosted on a virtual machine and can be interfaced with SCADAbr and Simulink.

**SimLink:** Interface between Simulink and OpenPLC.

**Kali Linux:** Open source Unix distribution designed for digital forensics and cyber security testing. It comes prepackaged and preconfigured with a wide array of industry-standard tools for these purposes.

**Caldera:** Open-source adversary emulator built upon the MITRE ATTCK framework. It can simulate hostile agents and be configured to launch chains of pre-scripted cyber attacks.

**Security Onion:** Open source Unix distribution designed for enterprise security monitoring, threat hunting and log management.

**Wireshark:** Open Source Packet Analyzer, which enables the user to monitor, capture and analyze network packets transmitted over network interfaces.

**TeamViewer:** Commercial tool for remote desktop access. Provides the user with graphical desktop access to Unix and Windows machines over the Internet or LAN.

**SSH:** Unix based command-line tool and protocol for authentication, secure remote access, and encrypted file transfers.

**Macro Recorder:** User task automation software that lets the user record mouse movements, clicks, and keyboard strokes.

**AutoHotkey (AHK):** Powerful scripting language for user task automation. Enables rapid task automation through code.

**Table 7.4:** Overview of the relation between design modules and tools. A link to the source of each tool is provided.

| Module | Tool | Purpose | Source |
|---|---|---|---|
| RMC, VSE, VPE | GNS3 | Virtual Network | https://www.gns3.com |
| RMC, VSE, VPE | VMware Workstation Pro | Virtual Machines | https://www.vmware.com |
| RMC, VSE, VPE | Docker | Applications and service hosting | https://www.docker.com |
| VSE OT | Simulink | Smart grid simulation | https://se.mathworks.com/products/simulink.html |
| VSE OT | OpenPLC | PLC emulation | https://www.openplcproject.com |
| VSE OT | SCADAbr | HMI emulation | https://www.openplcproject.com |
| VSE OT | SimLink | Simulink/OpenPLC interface | https://github.com/thiagoralves/OpenPLC_Simulink-Interface |
| VPE Red Team | Kali Linux | Cyber Offense and Digital Forensics | https://www.kali.org |
| VPE Red Team | Caldera | Automated Red Team | https://github.com/mitre/caldera |
| VPE Blue Team | Security Onion | Network Monitoring | https://github.com/Security-Onion-Solutions/security-onion |
| VPE Blue Team | Wireshark | Packet Analysis | https://www.wireshark.org |
| VPE Blue Team | SSH | Remote CLI Access | https://www.ssh.com/ssh/ |
| VPE Blue Team | TeamViewer | Remote Desktop Access | https://www.teamviewer.com/ |
| VSE | Macrorecorder | User Traffic Generation | https://www.macrorecorder.com |
| VSE | AutoHotkey | User Traffic Generation | https://www.autohotkey.com |

## 7.3 Low-Level SG3C Treatment Design

### 7.3.1 Virtual Scenario Environment (VSE) Module

In order for the scenario environment to be realistic and relevant, we decided that the VSE module must be able to represent core elements from the Purdue model of industrial control systems, as described in Section 2.3. This was because we found the Purdue model to be frequently applied in order to organize the architectural infrastructure of industrial organizations, including the power industry. The following are the Purdue zones and the components that were deemed necessary to support in the VSE.

**Table 7.5:** Purdue zones and components, used as base for the treatment design

| Zone | Components/Funtionality |
|---|---|
| Level 4-5: IT Enterprise | User Workstations, Domain Controller, File server, Web Server, Mail Server |
| Level 2-3: Supervision and Monitoring | Engineering stations, OT domain controller, OT historian, |
| Level 1: Basic Control | Human Machine Interface (HMI), PLC, DNP3 |
| Level 0: Process: | Distributed Energy Generation, Transmission and, |
| | Distrubtion Systems, Distributed Energy Storage, |
| | Renewable Energy Sources, Load Sites (Consumers) |
| IT/OT DMZs | Network segregation functionality, firewalls and bastion hosts. |

As can be seen from table 7.5, the VSE needs to contain a wide range of different systems, devices, applications and services. Using physical components in the design would be both expensive and inflexible, nor would it be an easily scalable solution. As such, we aimed to design the VSE module as a full-fledged virtualization.

Figure 7.2 shows the final design of the VSE architecture, where the VSE module is divided into four layers; the virtual network layer, virtual host layer, application layer, and the simulation layer. The virtual network layer is handled by GNS3, which hosts a virtual network and provides LAN and Internet access for the layers above. The virtual host layer is consisting of VMware Workstation Pro and Docker, which populates the virtual network with virtual machines. These virtual machines host operating systems, applications and services in the application layer. Finally, the smart grid simulation is hosted inside Matlab Simulink, which is capable of executing realistic simulations of real-world systems, including smart grids. The communication for all layers is realized by passing traffic to the virtual network layer.

This structure enables the VSE module to host virtual, emulated, and simulated versions of all the components deemed necessary to recreate a realistic environment. It is, however, not limited to the systems and components described in Table 7.5, as it should theoretically be able to host all systems where a virtual version exists.

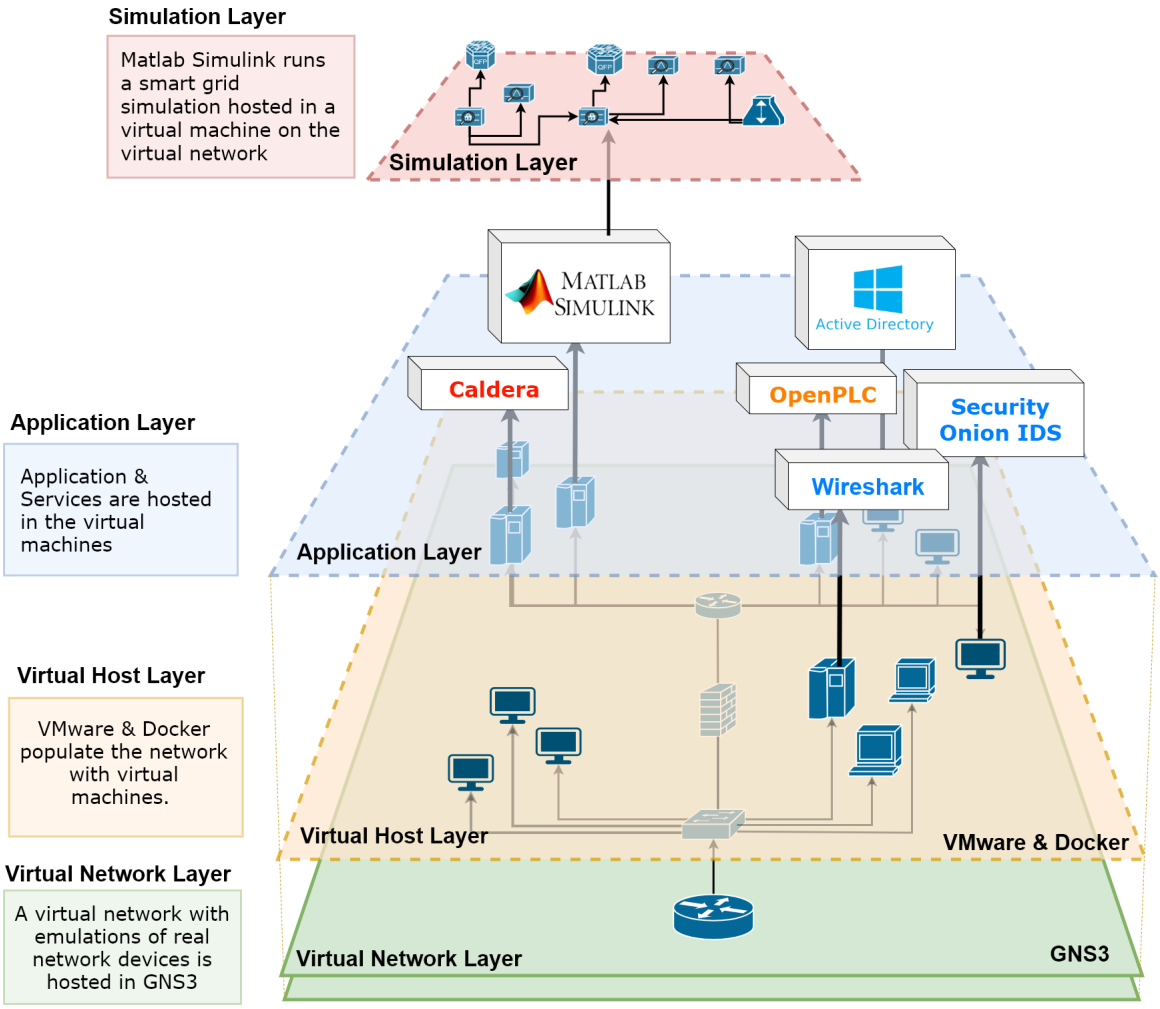


**Figure 7.2:** Logical structure of the virtual scenario environment component.

The next paragraph demonstrates an example environment that can be created and executed in the VSE.

### IT Enterprise Zone and DMZs

In the IT enterprise Zone, network equipment and routing protocols such as TCP/IP, OSPF, ethernet, etc, are hosted by and configured in GNS3. GNS3 supports most protocols in the OSI network model and can emulate all network devices that are compatible with the Qemu[1] emulation engine. It, therefore, allows the VSE module to be flexible and adaptable to a wide range network topologies and thus scenario types. The zone separation is also handled in GNS3 by dividing the zones into separate VLANS and passing traffic through firewalls located at zone borders. The firewalls

[1] https://www.qemu.org/

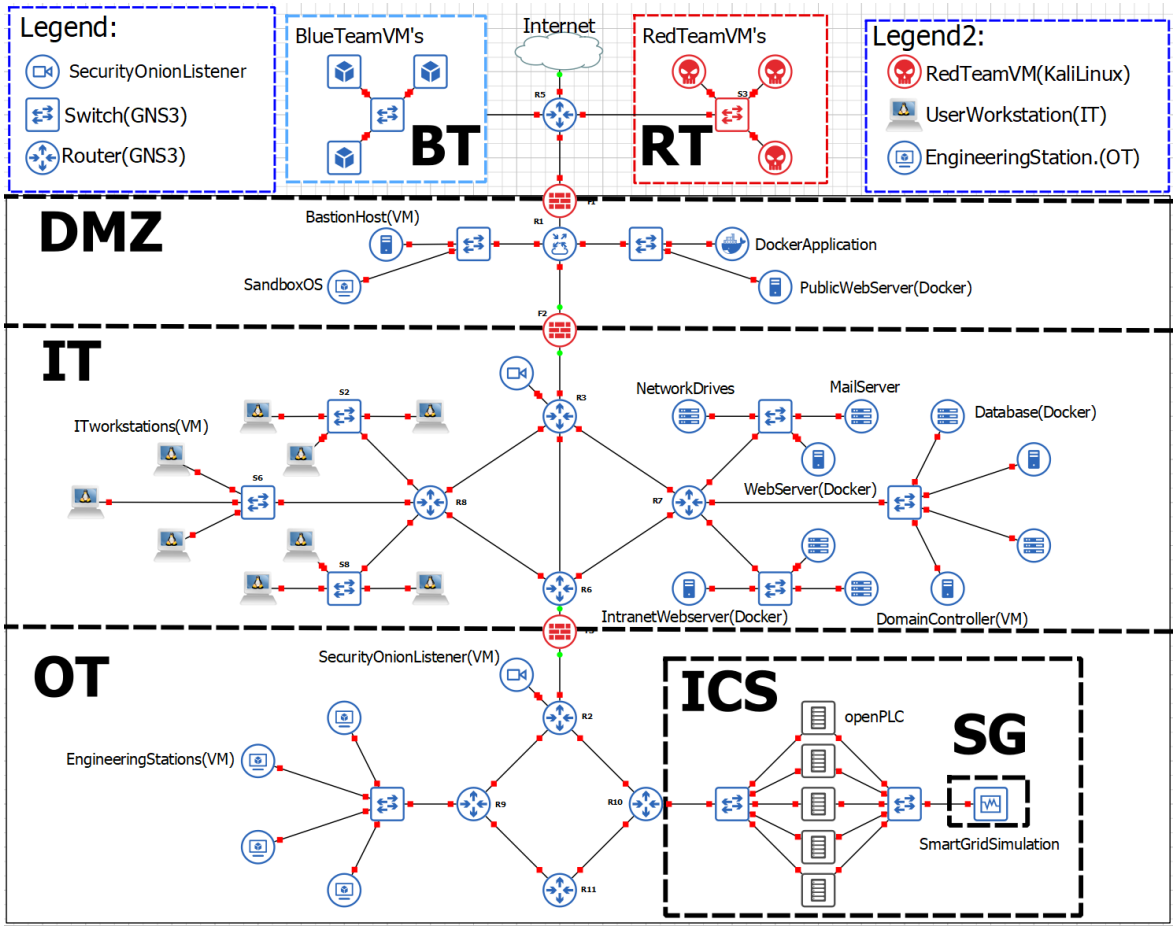


**Figure 7.3:** Example of how a virtual environment can be structured in SG3C.

can be implemented by using Qemu compatible emulations of physical devices, or by deploying software firewalls such as PFsense[2] or IPFire[3], hosted in a VM by VMware. IT hosts and services such as user workstations, domain controllers, and fileservers are similarly realized by installing the relevant operating system and software on virtual machines hosted in VMware. After integrating and configuring a VM in the environment, it can then be cloned and used as a template for new machines.

**OT Network: Area supervisory control and Basic control**

The OT zones are realized by the same principles. GNS3 hosts the network, and VMware virtual machines host the domain controller, data historian, and engineering workstations. The Purdue model suggests blocking internet traffic into the OT network; this can be achieved quite simply in GNS3 by only allowing LAN traffic on the southside of the gateway router separating the two zones. However, unique to the

[2]https://www.pfsense.org/
[3]https://www.ipfire.org/

OT layer are industry communication protocols and control systems. To replicate a SCADA system, we chose the open-source PLC emulator, aptly named, OpenPLC. OpenPLC is in compliance with the IEC-61131-3 standard, which is commonly used in ICS systems, and this makes it compatible with a wide range of existing PLC software [100]. OpenPLC was also found by Yamin, Katt, and Gkioulos in [84] to be the most popular choice of PLC emulators for research projects and cyber ranges targeting ICS systems. For HMI, we chose SCADAbr, which is a customizable open-source HMI that interfaces with openPLC. Communication between them is established by using DNP3, an old but still common industry protocol for control systems. The DNP3 emulation is handled by GNS3.

**OT Network: Process zone**

The process zone contains, in our design, the smart grid components. These are handled by Simulink, where realistic representations of various devices and components can be simulated. However, in order for the simulation to be of any value, the red team must be able to communicate with, and change the state of the simulation. This is done by using the open-source tool Simlink, designed to enable communication between OpenPLC and Simulink over DNP3, wrapped in UDP packets. The idea is that the HMI is controlled from engineering stations in the supervision and control zone, which sends control signals to OpenPLC and changes the state of the smart grid simulation in Simulink. This communication chain can then be attacked by the red team. Either by intercepting traffic or gaining control of an engineering station, the HMI or OpenPLC.

**IT Network: User Traffic Generation**

User traffic generation is an important element in order to ensure realism in the VSE component. This is achieved in the design by using a scripting language called AutoHotKey (AHK) and a user task automation tool called Macro recorder. The purpose of both is to generate traffic by automating user behaviors, such as surfing the web, accessing network drives, and downloading files. Macro recorder gives quick results by enabling us to record and playback mouse movements, clicks, and keyboard strokes. However, it is dependent on the GUI it is interacting with to be in the same position as when recorded. This makes it prone to malfunction if UI elements move or the resolution is changed. AHK is slower to implement but more reliable as it executes the user behavior in code. The idea of having both is to use macro recorder for prototyping new user behaviors in the environment, and then solidify final behavior patterns in AHK code. The AHK scripts are then stored and executed on hosts in the VSE network.

### 7.3.2 Range Management Center (RMC) Module

As stated in the high-level description, the RMC is the module that contains the functionalities needed to create, edit and deploy the training environments as well automated attack scenarios in the VSE. It also handles resource and traffic monitoring in ongoing training scenarios. These tasks are carried out by the green team (described in Section 7.2.2), which access the RMC either by connecting remotely with Teamviewer or by working directly on the machine hosting the cyber range.

**Logical separation of RMC and VSE**
This paragraph highlights the logical separation between the RMC and VSE, as it can be somewhat bewildering. The RMC is the combination of tools that hosts and manages all elements in the training environment (VSE). Whereas, the VSE is the sum of all the hosted devices, their relations (how they are connected), and the applications and services executed on them. As such, the VSE is the training environment, as seen from the perspective of the red and blue team, where the RMC tools are not visible nor reachable for the blue and red team.

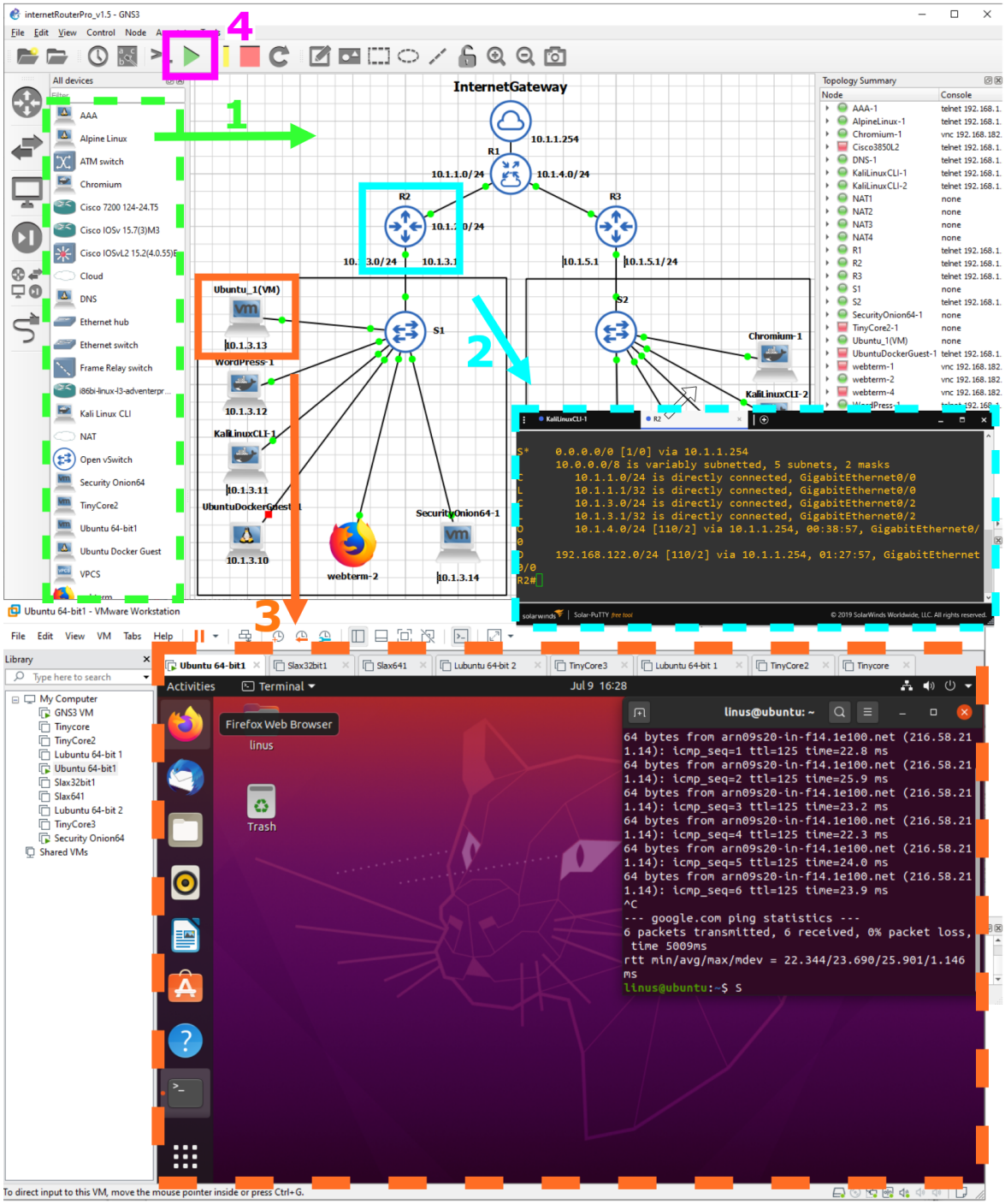


**Figure 7.4:** Screendump of the main control interfaces in the RMC. The arrows indicate the workflow when creating training environments.

**Creating Scenario Environments.**

Figure 7.4 shows the two main control interfaces used in the RMC, GNS3 and

VMware Workstation pro. The top half displays the GNS3 interface, whereas in the bottom half is VMware Workstation Pro. The green square highlights virtual devices imported into GNS3. These can either be network devices or VMs from VMware and Docker. After selecting a device, it can be dragged and dropped into the network topology, and then connected to a desired node. The device can then be configured by right-clicking, and either selecting remote terminal access or GUI access, depending on the device type. A remote terminal to a networking device with a command-line interface is marked by blue in the figure. Whereas graphical desktop access to a virtual machine is highlighted in orange. Deployment of the environment is done by simply pressing the green "start" button, which will instantiate all VMs in the environment. In summary, the workflow is as follows: 1) Import device into GNS3 2) drag, drop and connect 3) access and configure 4) Deploy.

These functions enable the green team to add and remove devices with relative ease, as well as configuring and installing new services in the native GUI of the device or OS. This implies that the green team can choose to implement devices, operating systems, and applications based on previous experience if it suits the training scenario. It also implies that lessons learned from managing the range translate into real-world implementations of the elements contained in the range.

**Creating Automated Attack Scenarios**

The green team can create and configure automated cyberattacks against the training environment. This reduces the reliance on having skilled red team participants available in order to execute a training scenario.

Attack automation is achieved by using the open-source adversarial emulation engine, Caldera, developed by MITRE ATT&CK (MA). Two other engines were investigated during the project. These were Red Team Automation (RTA) and Atomic Red Team. However, Caldera was chosen for the final design, as it was the only engine that allowed scheduling and automation of whole attack scenarios. Whereas, RTA and Atomic Red Team must be managed on a per attack basis. The next paragraph gives some more details about Caldera and how operations are created and customized by the green team.

The Caldera engine consists of two main components, a command and control server, executed from the RMC, and software agents deployed on hosts in the training environment. These agents receive and execute commands from the Caldera C2 server, and can be hidden by injecting the agents into running processes on their host. The hosts serve as initial attack vectors for the attack scenarios to develop. The C2 server also hosts a web dashboard that the green team utilizes to create and configure the attack scenarios, called operations. In Caldera, operations are defined as a collection of adversaries, which in turn are defined by their abilities. These

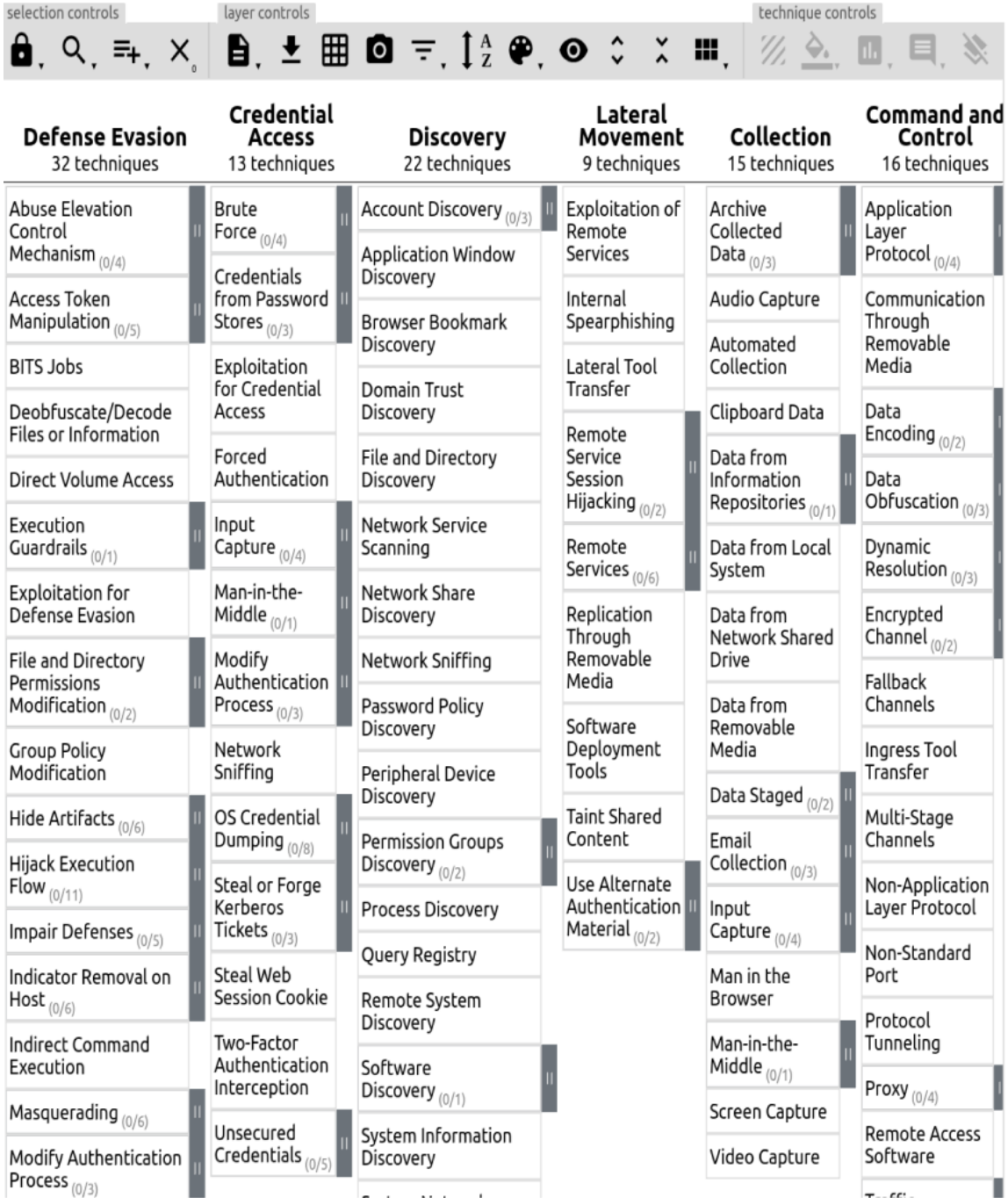


**Figure 7.5:** Some of the available adversary abilities in Caldera.

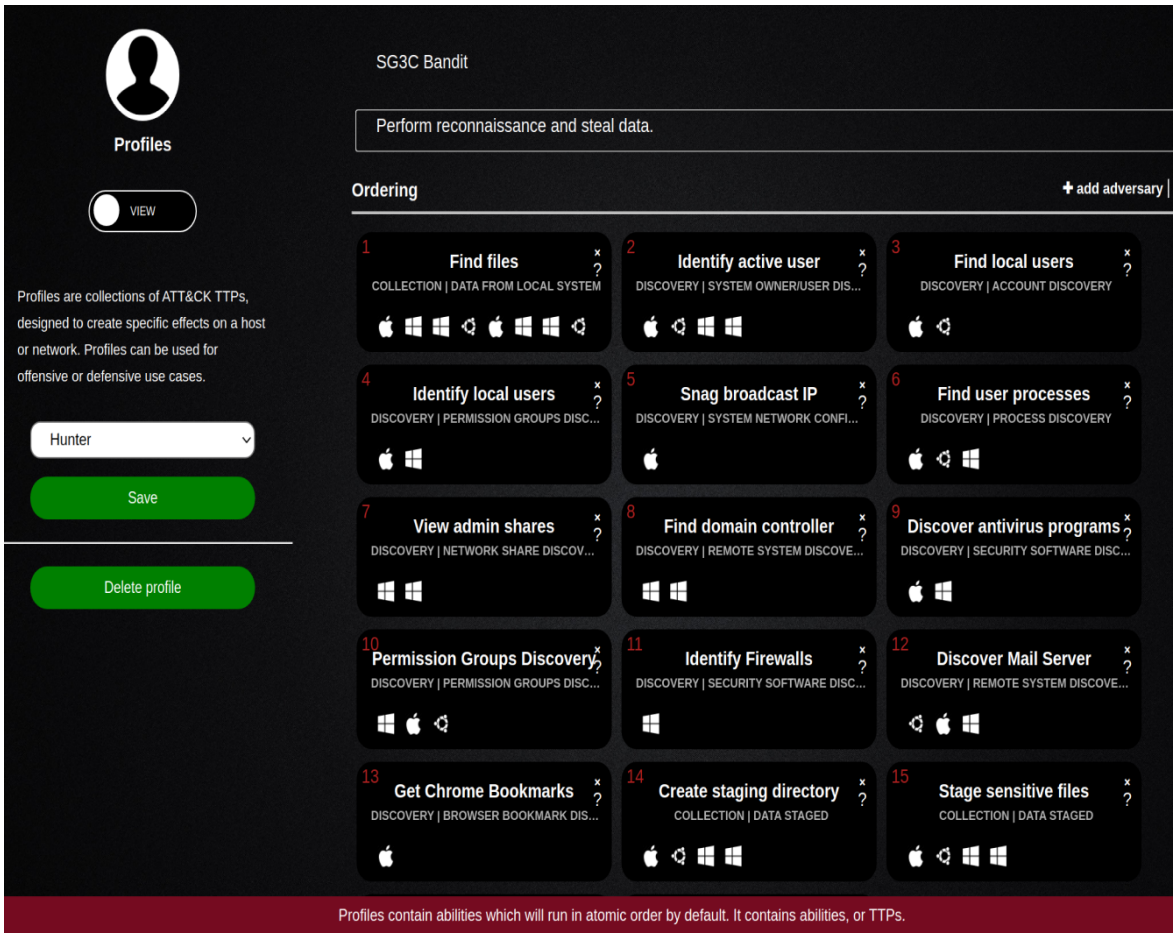


**Figure 7.6:** An automated adversary and its abilities in the Caldera dashboard.

abilities are based on the MITRE ATT&CK matrix, which is a set of behaviors and techniques extracted from observations of real-world cyber intrusions. In total, 155 such abilities are available in Caldera. Custom abilities can further be written and uploaded to the C2 server, if necessary. Figure 7.5 shows a sub-selection of the available abilities, which includes, among others, stealing Kerberos tickets, OS credential dumping, and sniffing network traffic. Adversaries are created in the web dashboard and further customized by assigning him of the available abilities and specifying their order of execution. A template adversary designed to perform reconnaissance and steal sensitive data can be seen in Figure 7.6.

The green team then constructs operations by selecting the desired adversaries and assigning them to the pre-installed agents in the environment. Additional settings, like time scheduling and obfuscation of communications, can also be specified. After launching the operation, the agents emulate their assigned adversaries by executing their abilities from the pre-compromised hosts. Any abilities involving network

communications, such as data exfiltration or port scanning, will generate malicious traffic in the environment that the blue team must try to detect.

Throughout the operation, the agents will report back to the C2 server about the status of their attacks. These status updates are shown in a timeline in the web dashboard, enabling the green team to monitor the progress.

**Monitor and control**
As described in the cyber range taxonomy from Section 5.2.4, range management should include functions that enable the green team to monitor traffic and resource usage, as well as to control elements of the training environment during scenario execution. Resource monitoring of the cyber range is achieved by using the built-in resource monitoring tools in the hosting OS as well as of the virtual machines. This was deemed as a "good enough" solution as resource monitoring was not a strict priority in this project. Traffic monitoring is described in the blue team section, as both the blue and green team uses the same tools and methods to monitor network traffic in ongoing scenarios. In order to control devices, applications and services in ongoing training scenarios, the green team again uses the GNS3 interface to access network devices and virtual machines.

### 7.3.3 Virtual Participant Environment (VPE) Module

**The Blue Team** The objective for the blue team is to monitor and defend the IT and OT networks, hosts and applications against the red team. The blue team can also be tasked to locate and resolve security vulnerabilities in the scenario environment. Expressed more formally, the blue team executes the technical phases of incident response frameworks such as ISO 27035, described in chapter 4 Information Security Incident Management. Detect, isolate, eradicate and recover. In order to perform monitoring and detection, the blue team machines have access to Security Onion, an open-source Unix distribution bundled with state of the art enterprise monitoring and log management tools. Some highlighted tools are:

- Snort, Zeek and Suricata, intrusion detection system (IDS)
- Elasticsearch, Logstash, Kibana (ELK stack), log and alert management systems.
- Cyberchef and Wireshark, packet and data analysis tools.

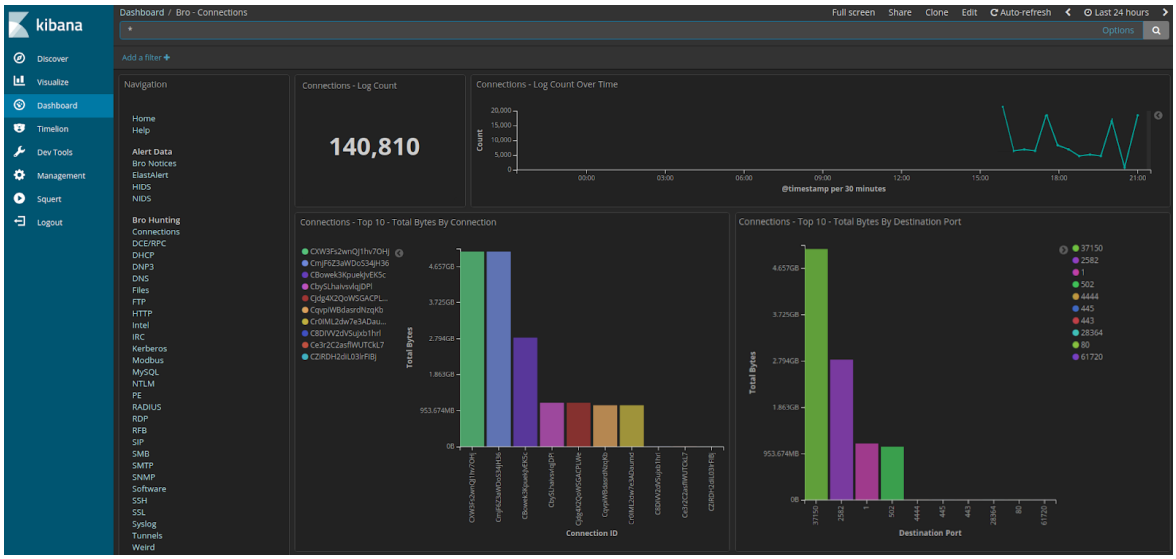


**Figure 7.7:** The Kibana dashboard in Security Onion. One of several monitoring dashboards available through the Security Onion web server.

Security Onion listeners are connected to mirroring ports on routers and switches throughout the VSE. These listeners feed traffic data back to a central SO controller, which processes the data and displays it in a web dashboard reachable for the blue team over LAN. The Kibana dashboard is shown in Figure 7.7, and lets the blue team get an overview of the network. If alerts are issued, by for instance, Snort, further inspection can be done by using available tools such as Wireshark or Cyberchef.

In order to isolate compromised hosts in the environment, the blue team is given administrator access to routers and switches in the network, which they can connect to with SSH. This enables the blue team members to shut down network interfaces and isolate compromised hosts. To eradicate malware and recover normal system operation, the blue team are also given remote desktop admin access, by use of Teamviewer, to hosts with graphical interfaces, such as Windows and Ubuntu machines.

**The Red Team** The main purpose of the red team is to plan, prepare, and execute an ICS cyber attack towards the simulated smart grid environment. In order to do this, they follow the ICS cyber kill chain (ICS-CKC), as described in detail in Section 3.2. Although, the ICS-CKC model is intended for defenders, we found it to be a good scenario framework for the red team. Depending on the training scenario, the red team choose an ICS-CKC stage and a corresponding phase to begin their assigned scenario tasks.

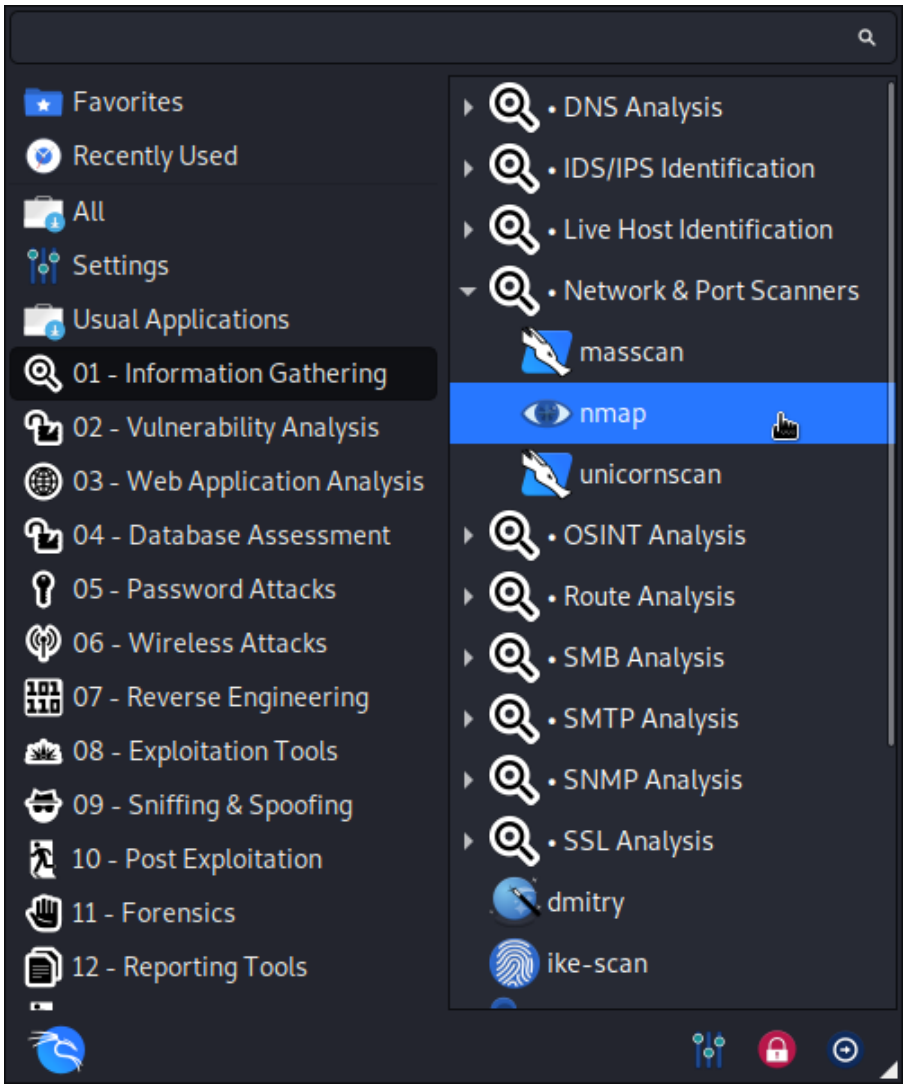


**Figure 7.8:** Showing the Kali Linux tools and folder hierarchy.

The SG3C artifact was primarily made with adversary emulation in mind, as described in Subsection 7.3.2 Range Management Center. However, SG3C also supports a human red team that potentially could use any desired operating system, as well as any network penetration tools, but we assigned Kali Linux for this purpose. Kali Linux is an open-source operating system that is meant for ethical hacking, digital forensics and advanced penetration testing. Accordingly, it comes with a wide range of software tools to the advantage of a red team. These tools are preinstalled and easy to access, and usually comes with a user manual. Metasploit, Cisco exploiter, Sqlmap, Nmap, and many others, are examples of such tools, but will not be further explained here. Moreover, these tools are also categorized into several folders, depicted in Figure 7.8. The folders include tools for information gathering, vulnerability analysis, web application analysis, password attacks, reverse

engineering, exploitation tools, sniffing & spoofing, etc. Meaning that a red team participant (RTP) could easily choose the right cyber weapons for the right purpose, and use the ICS-CKC framework as guidance to prepare a cyber attack campaign. For example, if an RTP were tasked to perform a cyber intrusion (i.e. Phase 3 in Stage-I in the ICS-CKC attack framework), the participant would be wise to begin with information gathering of the IT network. By choosing the "Information Gathering" folder, the participant would be provided with a wide range of tools for this exact purpose, as can be seen in Figure 7.8. The more familiar a participant is with the Kali Linux tools and folder hierarchy, the more prepared they are to perform a rapid and targeted cyber attack. This structure provides easy access for red team tools and demonstrates the benefit of using Kali Linux in our treatment artifact. Additionally, Kali Linux is also a well-known and customary operating system among security professionals. Making it easy for stakeholders to obtain qualified participants.

## 7.4 Prototype Validation

This section describes the protype developed and the testing conducted during this project. The tests were formulated as knowledge questions which were designed to give us better insight into the practicality of the design. The knowledge questions are listed below, followed by the prototype description and the results of the tests. Testing implications and limitations are further discussed in chapter 8 8.

- How well does VMware Workstation Pro and Docker integrate with GNS3?
- How is the network performance between nodes inside the emulated network?
- Can the emulated network route internet traffic with sufficient performance?
- How is the user experience when connecting to a VM in the emulated network, using remote desktop software?
- How feasible is it to control Simulink with OpenPLC through the SCADAbr HMI interface?
- Are the Simulink smart grid simulations available online, good enough?
- Is Macro Recorder a viable solution for Traffic generation by user behaviour automation?

### 7.4.1 The SG3C prototype

The prototype consists of three emulated Cisco routers and two emulated Cisco switches and an internet gateway. The routers were configured with OSPF routing and VLAN segregation, and a small selection of VMware and Docker VM's were

integrated into the topology. From VMware the following machines were used: Two Ubuntu VM's, one Kali Linux VM and one Security Onion distribution. The first Ubuntu machine served as a blue team host, Kali Linux as a red team host, and the final Ubuntu machine as an enterprise workstation. The Security Onion distribution was configured in evaluation mode, meaning it acted as a listener and a master node simultaneously, this was done to conserve resources. From Docker, we integrated a command-line-only Kali Linux container, as well as two containers, each serving a browser (i.e. Chromium and Firefox). The browser containers were integrated for traffic generation and some light stress-testing of the network. Some additional experimental VMs were also integrated, but as they are not crucial for the design we will not discuss them here. A short description of these VM's are given in Appendix A.1. Although small, the prototype proved somewhat helpful when investigating posterior knowledge questions about some basic properties of the design. The remaining part of this chapter describes this investigation.

### 7.4.2 VMware Pro, Docker and GNS3

**How well does VMware Workstation Pro and Docker integrate with GNS3?**
Both docker and VMware integrated quite seamlessly with GNS3. After creating a VM in either Docker or VMware it was just a matter of clicking through an import wizard, dragging the VM's into the topology, and configuring the network settings of the device. Premade Docker containers could also be imported and downloaded from repositories on the web from within GNS3, which eased the workflow. Interfacing with the imported devices to, either through a CLI or a graphical desktop, was also easily accomplished by right clicking and selecting the appropriate option. Although the machine hosting the prototype was not very powerful in terms of hardware, the graphical interfaces of the VM's were responsive and comfortable to work with. However, if CPU and memory capacity approached their respective limits on the main host, all interfaces related to the range would become sluggish, but this was to be expected.

### 7.4.3 GNS3 Network Performance

**How is the network performance between nodes in the emulated network?**
We wanted to check if the emulated routers added extra latency to network communications. This was important to check, because if every router hop added latency that could potentially cause issues for larger implementations. We checked latency by issuing pings between a selection of the internal hosts, from and to all four subnets. The resulting latency was quite low, with round trip times (RTTs) between 2 ms and 6 ms. The RTT was dependent on the number of hops in the route, where the

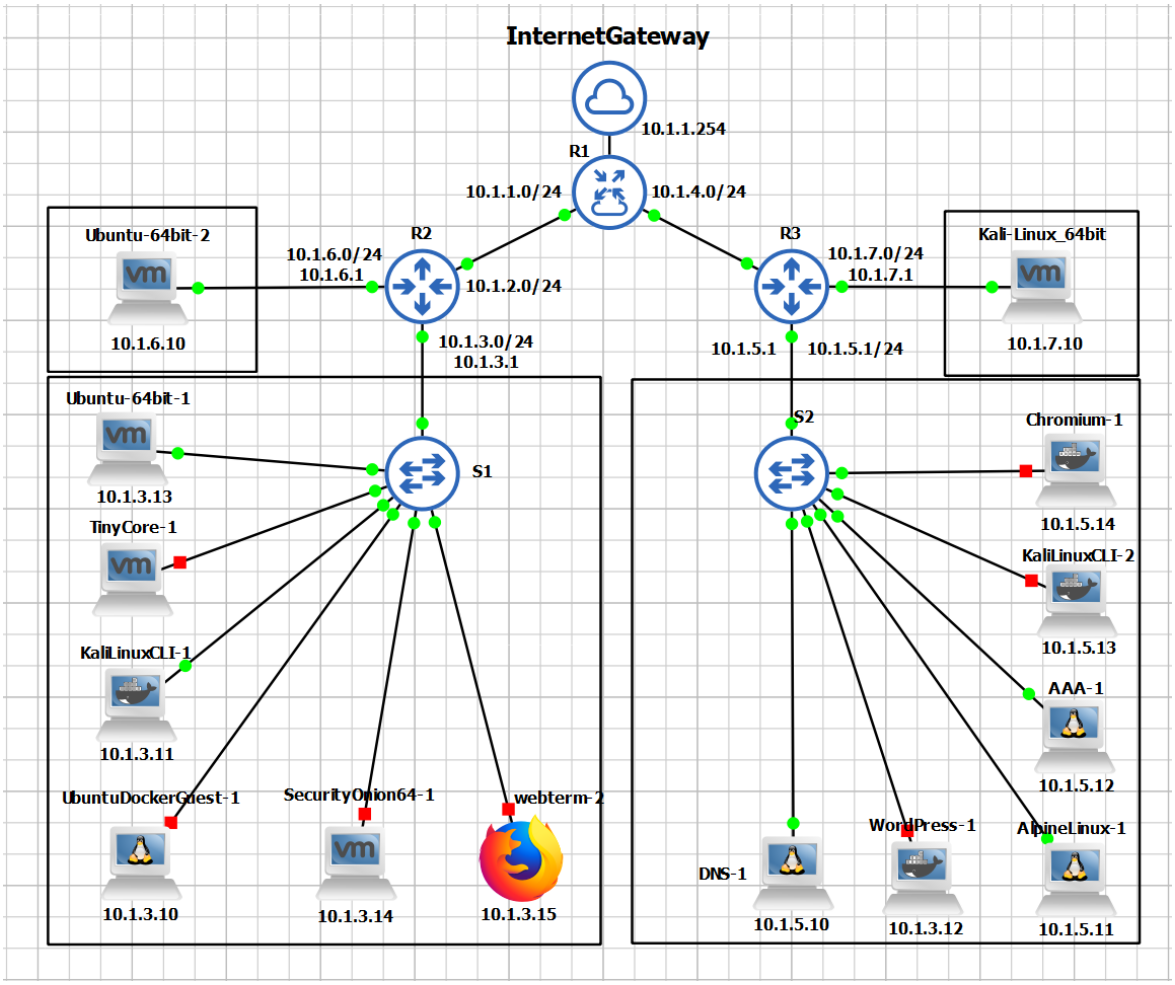


**Figure 7.9:** Prototype developed during the project.

shortest route (one router hop) produced the 2ms RTT, and the longest route (three hops) produced the 6 ms RTT. That is, an average of 2 ms latency per hop.

### 7.4.4 GNS3 Routing Network Traffic

**Can the emulated network route internet traffic with sufficient performance?**

We wanted to see if the emulated network would experience packet loss or increased latency when running larger amounts of data through the emulated network. We tested this by running online bandwidth tests from hosts in the emulated network, and compared the results with tests conducted directly to the testing site from the main host machine. We first ran the test on a single VM, and then at two VMs at the same time. When running the bandwidth test from one internal VM, we observed no impact on latency, upload or download speeds compared to the main host. In

the second test, the assumption was that speeds would be lower for the individual VMs but that the sum of both would add up the total available bandwidth. This was almost the case, except that the combined upload speeds were consistently lower in the emulated network compared to the main host ($\tilde{2}$00Mbps vs $\tilde{3}$00Mbps). Figure 7.10 displays a screenshot of one of the tests. We were not able to determine the cause of lost transmission rate, and the finding was a bit concerning, as it equates to a approx. 33% loss of upstream performance. On the other hand, the test also indicated that the emulated network could handle download rates of about 300 Mbps, which was the maximum rate available to the host machine. Thus indicating that download performance did not suffer any significant packet loss. The latency, in all tests, were about the same ($\pm 2ms$) for the machines in the emulated network and the main host.

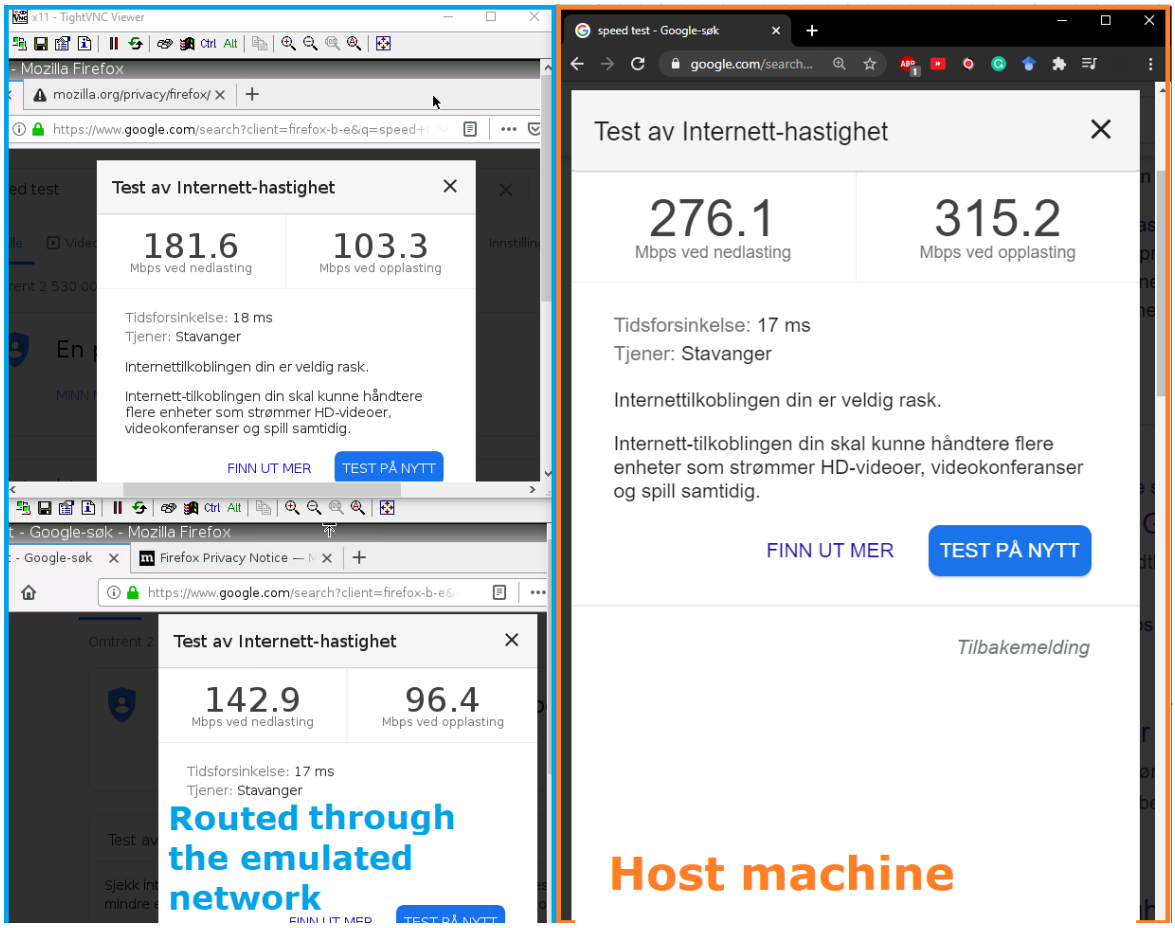


**Figure 7.10:** Test of performance when routing internet traffic trough the emulated network.

### 7.4.5 End User Experience in GNS3 and VMs

**How is the user experience when connecting to a VM in the emulated network, using remote desktop software?**
An important assumption in the design was that the blue, red and green team members could connect to virtual machines in the emulated network in order to remotely participate in a training scenario. However, this is only useful if the user experience is responsive. In order to test this, we installed Teamviewer on a Ubuntu machine inside the emulated network, and connected to it from an external machine over the internet. The connection was successful and the responsiveness was similar to a normal Teamviewer performance. Meaning it was workable, but not as fast as working directly on the machine.

### 7.4.6 Testing OpenPLC-SimLink-Simulink Communication

**How feasible is it to control Simulink with OpenPLC through the SCADAbr HMI interface?**
As seen from the prototype description, we did not have time to integrate Simulink, OpenPLC, SimLink and SCADAbr into the prototype. We did, however, test communication between OpenPLC and Simulink early in the project, before the prototype was developed. During those tests we were able to change the state of a lightbulb in Simulink from OpenPLC. This was all carried out locally on a single Ubuntu machine, so the network connectivity has not been properly tested, but at least for the simplest base case we did not face any issues.

### 7.4.7 Smart Grid Simulation in Simulink

**Are the Simulink smart grid simulations available online, good enough?**
When researching the availability of smart grid simulations online, we found that several academic papers had made their simulations available for download, royalty free. Therefore, it should not be too difficult to find a simulation suitable for our project. However, when trying to import these, most were either too old to be compatible with our version of Simulink (i.e. 2019a), or missing some essential dependency that prohibited the simulation to be executed. We did however manage to import and run a micro grid simulation used in a research paper on microgrid stability during blackouts [107]. This is a valid test scenario, as microgrids are thought to be frequently used in the coming smart grids. A screenshot depicting an overview of the microgrid is given in Figure 7.11. While not having any concrete data on what constitutes a large or small simulation, we were able to assess the resource usage of this particular simulation. After starting Simulink and running the simulation, total RAM usage stabilized around an increase of $1.0 - 1.2$GB and the CPU usage between 15 and 25%. We were also able to manipulate the inputs of the simulation, and track the corresponding changes in voltage and current, using a data

logger included in Simulink. However, as electrical engineering is outside our domain of expertise we could not say anything certain about the realism of the simulation itself. Zoomed in screenshots of the microgrid simulation can be seen in Appendix A.1.

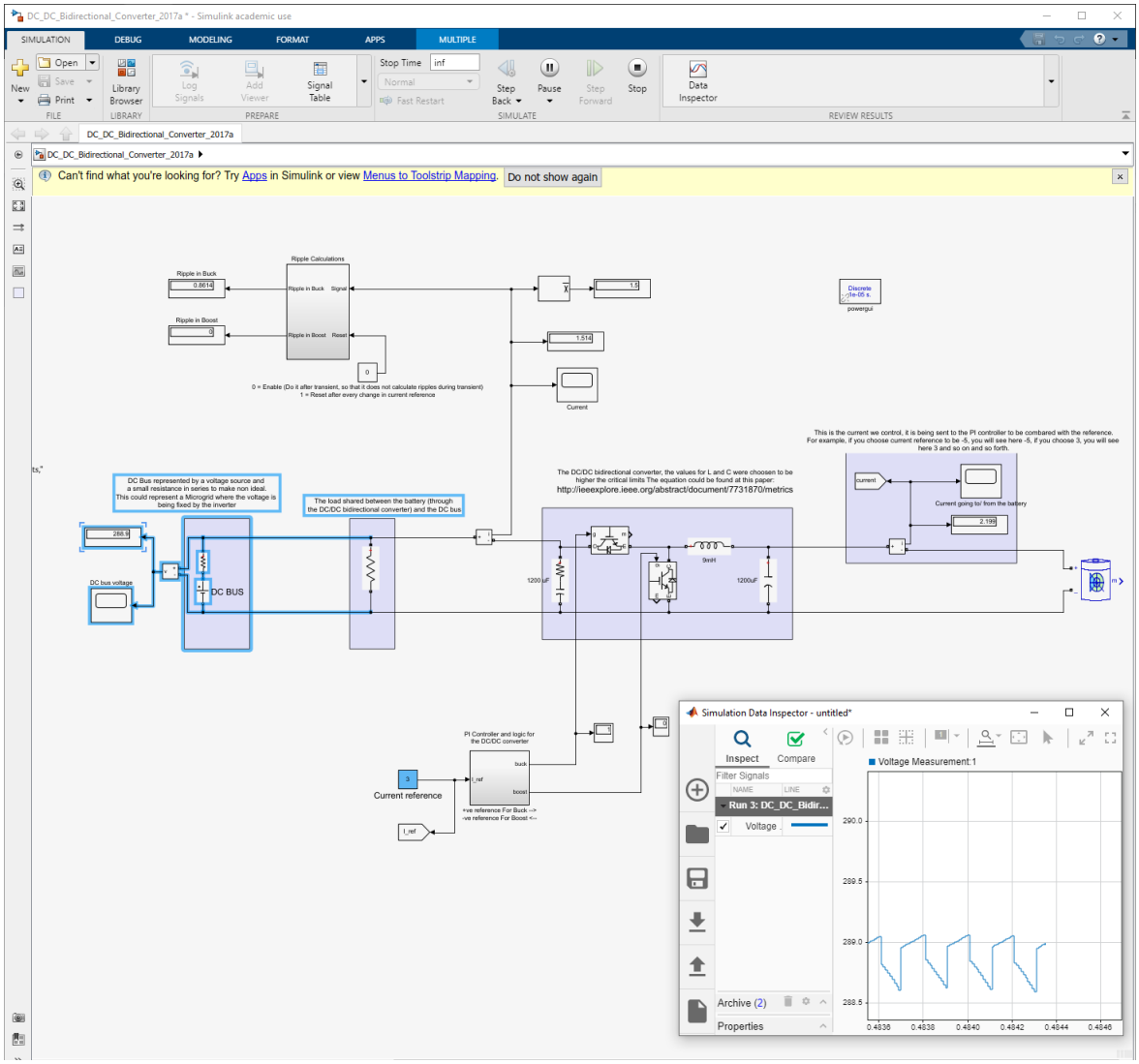


**Figure 7.11:** The Matlab Simulink microgrid simulation used in this project. Used with permission from [108].

### 7.4.8 Traffic Generation with Macro Recorder

**Is Macro Recorder a viable solution for traffic generation by user behaviour automation?**

As a minimal viable product (MVP) for user behavior automation, we created some scripts that surfed the internet. Using the Macro Recorder tool, we captured mouse

movements and clicks, while opening a web browser, navigating to a webpage called uroullete.com and clicking a roulette symbol. Clicking this symbol opened a new tab with a random website. After scrolling up and down for 3-4 seconds, we issued the ctrl+w keystroke combination, which closes the tab. This behavior was then looped, creating an infinite stream of random web page visits. The resulting script generates random traffic, but the pattern of opening and closing random sites does not mimic human behavior very well. On the other hand, due to its simplicity it was easily loopable and ran without issues for 2 hours in testing. In an attempt to create more human-like behaviour, we recorded 20 minutes of web surfing, and then looped this pattern. This generated more believable traffic, but as Macro Recorder relies on the X,Y coordinates of the element to be clicked, it was prone to breaking if the site contained dynamic content that had changed positions between the loops.

# Chapter 8
# Discussion

This chapter discusses to what degree the requirements are fulfilled by the design. The discussion is based on the design itself, results from the tests conducted in 7.4, and observations made during the development of the prototype. Limitations of the results are then discussed in section 8.2 followed by suggestions for future work in section 8.3.

## 8.1 Fulfillment of Requirements

**R1 Versatility**
*Requirement Description: SG3C must be versatile in order to represent different functions and systems across the IT, OT and smart grid domain, either by substitution or modification of individual components.*

From the prototype we found that this requirement is well covered in the IT domain, as the combination of GNS3, VMware and Docker enables the VSE module to host virtual versions of most IT software and systems. For the OT domain, the availability of virtual versions of real-world components is more limited. For instance, PLC emulation is dominated by OpenPLC and has no strong alternatives. The OT domain is however still versatile in our design, as it is based on the same virtualization concepts as the IT domain, and can host most OT systems as long as a virtual counterpart exists. The versatility of our smart grid domain was harder to assess. Modification and substitution of components is certainly a supported feature in Simulink. However, we were not able to perform any meaningful modification or substitution in the micro grid used in this project. This was due to our limited expertise in both electrical engineering and Simulink. Nevertheless, it is still our impression that smart grid versatility is sufficiently accounted for by using Simulink, but it requires the necessary skills.

**R2 Scalability**
*Requirement Description: SG3C must be scalable in terms of number of users,*

*components, and services represented in the training scenarios.*

The design was initially created with single machine hosting in mind, but during the prototype development it became evident that any complex scenario with several participants will likely demand more resources than any single machine can deliver. This is largely due to the red and blue team machines, which requires fully featured operating systems to accomplish their objectives. As these operating systems demand a lot of resources, our cyber range design does not scale well with large numbers of participants. Possible scalability improvements are discussed in subsection 8.3 Future Work.

**R3 Compatibility**
*Requirement Description: SG3C must support compatibility in terms of being able to interface with external systems*

Testing showed that GNS3 can route traffic from the internet to hosts within the emulated network. As such, SG3C can communicate with external systems given the communication is internet based. If any special tools are needed in order to interface with the particular system, given the versitility of the VSE, then these can likely be hosted inside the virtual environment as well. Although not tested directly, GNS3 should also be able to receive and route traffic transmitted over LAN. Communication with external systems by other standards are however not supported.

**R4 Open-Source**
*Requirement Description: SG3C should employ open-source solutions whenever possible, to keep costs down and maintain adaptability.*

Of the 15 tools employed in the design, three are closed source, commercial solutions. These are VMWare workstation Pro, Matlab Simulink and TeamViewer. Open source virtual machine hypervisors such as Virtualbox do indeed exist. However, during our research we found that VMware Workstation Pro would suit the solution best. This was due to the virtual machine functionalities built into GNS3 being designed around VMWare Worsktation Pro, and that stability and correctness could not be guaranteed with other hypervisors such as Virtualbox. The survey from Yamin et al [84] also indicated that VMware heavily outweighed other virtual machine hypervisors.

Open source alternatives to the Matlab Simulink, such as Scilab Xcos[1] and Modelica[2] were investigated. Both tools were deemed insufficient due to not being able to interface with OpenPLC and the rest of the virtual scenario environment. Similarly to VMware, the survey of Yamin et al. shows that Matlab Simulink outweighs its

[1] https://www.scilab.org/software/xcos
[2] https://www.modelica.org/

alternatives. This is likely due its robust simulation capabilities, frequent use in academia and large user base.

**R5 Monitoring**
*Requirement Description: SG3C must support real-time monitoring and after-action analysis of traffic data, packet capture and alert logs from the training environment.*

Security Onion lets the blue and green team members monitor network traffic, logs and alerts from the Splunk intrusion detection system, which is bundled into Security Onion. The data is displayed real time in the security onion dashboard. As the logs, alerts and events are stored on the Security Onion master node, these can also be inspected and analyzed post mortem (after a particular event, or the training scenario as a whole). Wireshark further assists both the blue and green team by enabling them to capture packets and inspect these as well as complete packet streams within the graphical GUI of Wireshark.

**R6 Customizability**
*Requirement Description: SG3C must have the ability to add, remove and modify applications and services represented in the training environment in order to support custom learning objectives.*

Similarly as for R1 Versatility, components, applications and services can be added, removed or modified within the Virtual Scenario Environment. In hindsight we see that these two requirements (R1 and R6) in essence are the same, and that they could have been merged for simplicity.

**R7 Reusability**
*Requirement Description: SG3C must support storage, re-use and customization of previous training scenario configurations.*

Storage, reuse and customization of previous training scenarios is partially supported in the design. Topology configurations can be saved and exported with built-in functions in GNS3. VMware and Docker images can be snapshotted after configuration, and then exported and imported to new scenarios. As all components in the range are contained within one of these tools, then all the configurations should be savable and exportable. Nevertheless, the configurations of the VMware and Docker images have to be compatible with the GNS3 topology that they are imported to. Therefore, it is likely that additional configuration must be performed regardless. Despite this, snapshotting should still reduce configuration and setup times, as template images can be made and reused. As such, the design partially fulfills this requirement.

**R8 ISIM**
*Requirement Description: SG3C must support practicing Cyber Security Incident*

*Response frameworks such as ISO 27035 and NIST SP 800. This implies the following; the blue team must be able to perform the technical steps in the information security incident management (ISIM) phases: detect, isolate, eradicate and recover.*

Detection is handled by the same functionalities as described above, in R5 monitoring. The isolate, eradicate and recover phases are covered in the design by including SSH and the remote desktop tool, TeamViewer. By use of SSH the blue team are given remote CLI admin access to network devices, which enables blue team participants to shut down interfaces and isolate network hosts. Eradication and recovery are handled by the blue team having remote admin desktop access to all hosts in the VSE by use of TeamViewer. This enables the blue team to conduct digital forensics on affected machines, run malware scans and removal in order to eradicate and recover affected systems.

**R9 ICS-CKC**
*Requirement Description: SG3C must support exercise scenarios that include one or more of the following ICS-CKC phases: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command Control, Action On Objectives*

Assuming the network and VM hosting works as intended in a full implementation, then this requirement should be fulfilled by the design. This conclusion stems from the fact that VSE module supports virtual network components and hosts that closely mimic a real world environment. Further, the tools needed to perform the necessary actions in each phase are included by the Kali Linux distribution made available to the red team participants.

**R10 Applicability**
*Requirement Description: The SG3C must reflect one or more core smart grid functions: Distributed management, Distributed power generation, Distributed power storage, V2G or G2V, Sensor networks, Actuator networks, Bidirectional power or communication, Computational intelligence*

During initial investigations regarding simulation of a smart grid environment in the cyber range, we found that several Matlab Simulink models used in previous research projects, were available for free online. Our assumption were that if these simulations were realistic enough to be used in peer reviewed and published research articles, then they should also be realistic enough to be used in our cyber range. However, during prototyping and testing, we found that the actual availability of suitable simulations were more restricted than initially thought. Although several was indeed available, through services such as Mathworks FileExchange [3], most would not execute properly, or at all. This was due to reasons such as the file

[3]https://se.mathworks.com/matlabcentral/fileexchange/

being developed on an outdated version of Simulink, requiring missing libraries or requiring input datasets not provided. However, after several attempts, we managed to successfully import and execute a micro grid simulation, previously used in [108]. From that particular simulation we were able to assess that resource demand was within tolerable ranges, and that the state of the grid could be changed, and its effects measured, in real time during execution. The results are further described in 7.4 prototype validation. Nevertheless, due to our limited expertise in both electrical engineering and Simulink, we could not accurately determine if the simulation was complex or large enough. During the project this was also the only simulation we were able to test, and such, the resource demand measurements are uncertain.

Despite this, we still believe that Simulink likely is an appropriate choice for replicating smart grid systems in cyber ranges. However, this assumes that one can access or acquire the necessary skills and knowledge to import, adapt and troubleshoot peer reviewed simulation models. This is further supported by our literature study indicating that Simulink is an overwhelmingly popular choice for simulation and testing of electrical systems.

## 8.2 Limitations

The following discuss limitations in regards to the methods applied during the project and how this may impact the acquired results.

Project limitations:

- Interview sample size
- Interview transcription
- Project Management and Scope
- Implementation Hardware
- Limited testing

**Interview sample size**
As the sample size of interviews conducted during the project only consisted of 4 candidates, it is reasonable to believe that this selection may not accurately represent the stakeholder group. Consequently, the validity of the resulting stakeholder goals may be uncertain. As the specified requirements for the artifact design is based on the goals, and the design in turn is created to fulfill the requirements, this uncertainty is carried throughout the entire design process.

**Interview transcription**
The project was not registered with the Norwegian Centre for Research Data (NSD). As a consequence, we were not allowed to use audio recordings during the interviews. This may have introduced transcriptions errors as they had to be manually transcribed during the interview.

**Project Management and Scope** We failed to narrow the scope of the project sufficiently, and too much of the available research time was spent on the first phases of the work. As a consequence, the prototype development, testing, and discussion of the results were affected. Restricting the scope of the prototype and tests, and the depth of the discussion.

**Implementation Hardware**
The project was initially granted access to a computer with strong virtualization capabilities, from The Department of Electric Power Engineering at NTNU. This machine was to be used for the prototype development. However, due to the lockdown caused by the Covid-19 pandemic, this machine became inaccessible roughly one month into the project. The prototype was instead developed on a consumer desktop not well suited for virtualization tasks. This hardware limitation further impacted prototype development, as only a handful of virtual devices could be ran simultaneously. The hardware specifications for both machines are given in Appendix C.1 and C.2, respectively.

**Limited testing**
The limited testing carried out in the validation phase can only be considered indicative of the results they produced. This is due to the small scale of the prototype and the lack of any proper methodology being applied to the testing. As such, the design is not robustly supported by first-hand evidence, and mostly relies on the research gathered from the literature study and the interviews.

## 8.3 Future work

This section gives suggestions for future work based on unresolved problems encountered during the project.

Future work includes:

- Implementation and testing of a larger prototype
- User traffic generation
- Multiple remote sessions
- Cluster- and cloud hosting

**Implementation and Testing of a Larger Prototype**
A larger-scale implementation should be attempted in order to acquire better insight into the validity of the design. Additional testing should also be conducted to see how the VSE performs under larger traffic loads with more complex topologies. The viability of having several active participants connecting with remote desktop access should also further be assessed through practical tests.

**User Traffic Generation**
During testing, we found that generating realistic user traffic was unfeasible to do with the Macro Recorder tool. Realistic user behaviour requires complex automation patterns, and as complexity increased, so did the likelihood of the automation script failing. Additionally, the hosts executing the user automation scripts were rendered unusable to other users. This came as a consequence of the scripts requiring interaction with the UI of the operating system it ran on. Further, the tool is only compatible with fully featured operating systems, such as Ubuntu and Windows. Thus, in order to achieve dense user traffic generation, several full scale operating systems would then have to be run in the VSE. This quickly demands unsustainable amounts of resources. We, therefore, advise against using the Macro Recorder tool for traffic generation. As future work, we suggest investigating other possible tools for user traffic generation.

**Multiple Remote Sessions**
If several team members from either the red, blue, or green team simultaneously connect to the same host via remote desktop, they will all share the same mouse and keyboard. This limits both the green team's ability to control hosts in running scenarios, as well as the blue team's ability to conduct their eradication and recovery steps. A possible workaround is for members to issue a request to access a particular machine, and then be given clearance by an administering green team member. Another alternative is to use the server edition Windows, as it supports multiple remote sessions. However, these licenses are expensive and only solves the multiple remote sessions problem for Windows-based hosts. We, therefore, suggest that investigating other methods and tools to enable multiple remote sessions should be conducted as future work.

**Cluster- and Cloud Hosting**
As mentioned in section 8.1 requirement fulfillment, the design was initially created to be executed on one single machine with powerful hardware. However, as a consequence of the participant machines being hosted within the virtual environment, this would not scale well with many participants. As future work, we suggest investigating the possibility of dividing the scenario hosting between several physical machines and connecting them through a high-speed LAN. This should theoretically be possible as GNS3 can communicate with external networks. Another strategy could be to

keep the VSE on one machine as described in the design and then host the red and blue team participant VMs on additional physical machines. If the interconnection of separate GNS topologies if found to be viable, then scalability should be increased for both strategies.

Another direction for future research is to forego the physical machines altogether and investigate whether the design can be implemented on a cloud hosting platform. As the design is based around software virtualization, it is reasonable to believe that a cloud implementation is feasible. Assuming the implementation is done on a platform that sells computing power as a service, scalability could then be improved by dynamic allocation of more resources as demand grows. Naturally, financial costs would then increase in accordance with the resources used. However, investing in physical hardware also incur financial costs, and an assessment of the tradeoff between local physical hosting and cloud computing should be made accordingly.

# Chapter 9
# Conclusion

In this thesis, we have presented our novel smart grid cyber range design, named SG3C. The design was constructed in order to improve stakeholders' ability to create and execute, cyber-security training scenarios targeting the smart grid domain. The design science methodology was applied to guide the research process, which included a literature study and a set of qualitative interviews conducted with stakeholders. Stakeholder goals were extracted from the interviews and combined with findings from the literature study to create the design requirements. The resulting stakeholder goals and requirements highlighted that realism, scalability, versatility, and relevance of training scenarios were important factors. To fulfill the requirements, the resulting design is based on two core concepts, virtualization and simulation. Where the idea is to host a virtual environment that training participants connect to via remote desktop access. The training environment supports emulation of realistic real-world systems and components from the IT, OT and smart grid domain. Virtualization is realized by combining VMware, Docker and GNS3, which enable us to virtualize all the layers in the OSI model, from the network to the application layer. Simulation is further realized by integrating Matlab Simulink, which supports realistic simulations of smart grid components and systems.

The cyber defense and monitoring capabilities included in the design are based on a review of the ISO 27035 standard for information security incident management (ISIM). This was done in order to ensure that the range could support all necessary actions performed in an incident response process. Similarly, the offensive capabilities made available to red team participants are based on the phases of the cyber kill chain (CKC) applied to industrial control systems (ICSs). The Unix distributions, Kali Linux and Security Onion, were included in the design to support the identified red and blue team capabilities. Both distributions comprise several state of the art tools for cyber offense and defense, respectively. The Caldera adversary emulation engine was further included to support automated red teams and attack scenarios.Additionally, a literature study of the conventional grid, the emerging smart grid, as well as critical infrastructures and industrial control systems, were conducted to determine which

systems and components were necessary to include in the virtual environment. Key findings were the Purdue model for industrial control systems, and components such as SCADA, HMI, PLC and the industry communication protocols Modbus and DNP3. Whereas for the smart grid domain, we found that the virtual environment should support one of the following smart grid functions: distributed management, power, storage and generation, sensor networks, actuator networks, bidirectional power or communication, and computational intelligence. OpenPLC, ScadaBR, Simulink and the SimLink interface were the main tools to realize these findings.

A small scale prototype was developed in order to test and validate selected parts of the design. Testing indicated that virtual machines from VMware and Docker integrated well with virtual networks hosted by GNS3. Further assessments were conducted in regards to network performance between integrated VMs, as well as routing of internet traffic through the virtual network. Results showed that internal network performance was good, with low latency between hosts. However, when routing internet traffic through the virtual network, upload performance was consistently reduced by 30%. Download performance and latency were not affected. The reason for the performance loss remains unknown. Remote desktop access to VMs inside the virtual network was tested from an external machine via the Internet. We found responsiveness and performance during this test to be acceptable and similar to remote desktop connections not routed through the virtual network. The design was initially planned to be hosted on a single powerful virtualization host, but experiences from the prototype development indicated that this would ultimately restrict participant count and training scenario sizes. As a response, two possible strategies to improve scalability has been proposed as future work.

Our results carry some uncertainty as both the prototype and the testing itself were limited. The practicality and performance of the design are still unknown for large-scale implementations. As such, our leading suggestion for future work is to implement and test larger parts of the design. Ultimately, working up to the full design and validating its functionality by executing a training scenario. If further testing shows that performance and reliability are maintained in larger scenarios, then a full implementation of the design should aid stakeholders in creating and executing realistic cyber-security training scenarios targeting the smart grid domain.

THIS PAGE IS INTENTIONALLY LEFT BLANK

# References


[1] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon 2015*, 2015, pp. 1–6.

[2] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2016.

[3] S. Karnouskos, "Cyber-physical systems in the smartgrid," *IEEE International Conference on Industrial Informatics (INDIN)*, pp. 20 – 23, Aug. 2011.

[4] M. Mikusz, "Towards an understanding of cyber-physical systems as industrial software-product-service systems," *Procedia CIRP*, vol. 16, pp. 385 – 389, 2014, product Services Systems and Value Creation. Proceedings of the 6th CIRP Conference on Industrial Product-Se rvice Systems.

[5] K. I.-K. W. Flavia C. Delicato, Adnan Al-Anbuky, "Editorial: Smart cyber–physical systems: Toward pervasive intelligence systems," *Future Generation Computer Systems*, vol. 107, pp. 1134 – 1139, 2020.

[6] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Towards a cyber-physical range," in *CPSS 2019 - Proceedings of the 5th ACM Cyber-Physical System Security Workshop, co-located with AsiaCCS 2019*, 2019, pp. 25–34.

[7] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, p. 40, Jul. 2016.

[8] J. Slowik, "Industrial control systems threats," Mar. 2018, [Online]. Retrieved 23.04.2020 from https://dragos.com/wp-content/uploads/2017-Review-Industrial-Control-System-Threats.pdf.

[9] K. Bernsmed, M. G. Jaatun, and C. Frøystad, "Risiko- og sårbarhetsanalyse for økt integrasjon av ams-dms-scada," The Norwegian Water Resources and Energy Directorate (NVE), , 2018.

[10] J. M. G. F. C. Bernsmed, Karin, "Is a smarter grid also riskier?" in *Security and Trust Management*, S. Mauw and M. Conti, Eds. Cham: Springer International Publishing, 2019, pp. 36–52.

[11] A. Cherepanov, "Industroyer: A new threat for industrial control systems," Tech. Rep., Jun. 2017. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[12] R. K. Knake, "A cyberattack on the U.S power grid," *Council on foreign relations*, p. 9, Apr. 2017.

[13] M. Myhre, "Deler ut 196 millioner til forskning på ikt-sikkerhet," 2018. [Online]. Available: https://www.forskningsradet.no/nyheter/2018/deler-ut-196-millioner-til-forskning-pa-ikt-sikkerhet-/

[14] M. Bartnes, "Understanding Information Security Incident Management Practices a case study in the electric power industry," Ph.D. dissertation, NTNU, Apr. 2015.

[15] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[16] V. K. Gran, Bjørn Axel, "Cybwin – cybersecurity platform for assessment and training for critical infrastructures," https://ife.no/en/project/cybwin-cybersecurity-platform, Mar. 2019.

[17] Norwegian Cyber Range, "NTNU – Norwegian Cyber Range (NCR)," 2019. [Online]. Available: https://www.ntnu.no/ncr

[18] R. Brunner, S. Oh, J. Ramirez, P. Houck, N. Stickney, and R. Blaine, "Design for an educational cyber range," Apr. 2019, pp. 1–2.

[19] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.

[20] J. Machowski, Z. Lubosny, J. W. Bialek, and J. R. Bumby, *Power system dynamics: stability and control*. John Wiley & Sons, 2020.

[21] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: A survey," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[22] "Open networks project dso definition and R&R," Energy Networks Association, 2017.

[23] "Directive 2012/27/eu of the european parliament," Official Journal, pp. 1–56, 2012.

[24] "Supporting document for the network code on operational security," ENTSO-E, Belgium, pp. 35,36, 2013.

[25] C.-H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 799–821, 2011.

[26] S. M. Nosratabadi, R.-A. Hooshmand, and E. Gholipour, "A comprehensive review on microgrid and virtual power plant concepts employed for distributed energy resources scheduling in power systems," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 341–363, 2017.

[27] N. Shaukat, S. Ali, C. Mehmood, B. Khan, M. Jawad, U. Farid, Z. Ullah, S. Anwar, and M. Majid, "A survey on consumers empowerment, communication technologies, and renewable generation penetration within smart grid," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 1453–1475, 2018.

[28] J. Rogelj, M. Den Elzen, N. Höhne, T. Fransen, H. Fekete, H. Winkler, R. Schaeffer, F. Sha, K. Riahi, and M. Meinshausen, "Paris agreement climate proposals need a boost to keep warming well below 2 c," *Nature*, vol. 534, no. 7609, pp. 631–639, 2016.

[29] M. Souryal, C. Gentile, D. Griffith, D. Cypher, and N. Golmie, "A methodology to evaluate wireless technologies for the smart grid," in *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 2010, pp. 356–361.

[30] D. Moongilan, "5G wireless communications (60 GHz band) from an smart grid EMC perspective," in *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*. IEEE, 2016, pp. 689–694.

[31] DSB, *Samfunnets kritiske funksjoner*. Directorate for Civil Protection (DSB), 2016, vol. 1.

[32] I. F. Mikhalevich and V. A. Trapeznikov, "Critical infrastructure security: Alignment of views," in *Systems of Signals Generating and Processing in the Field of on Board Communications*, 2019, pp. 1–5.

[33] S. Adepu, N. K. Kandasamy, and A. Mathur, "Epic: An electric power testbed for research and training in cyber physical systems security," Nov. 2018.

[34] NIST, *Cyber-Physical System (CPS)*, Jun. 2020. [Online]. Available: https://www.nist.gov/el/cyber-physical-systems

[35] ENISA, "Analysis of ICS-SCADA cyber security maturity levels in critical sectors," Sep. 2015. [Online]. Available: https://www.enisa.europa.eu/publications/maturity-levels

[36] E. ENISA, "Critical infrastructures and services," Jul. 2020, retrieved 21.03.2020 from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.

[37] ENISA, "Communication network dependencies for ICS/SCADA systems," Tech. Rep., Dec. 2016.

[38] P. N. Stockton, "Resilience for grid security emergencies: Opportunities for industry and government collaboration," 2018. [Online]. Available: https://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf

[39] E. ENISA, "Critical information infrastructures and services," 2019, retrieved 23.03.2020 from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada.

[40] T. Securion, *What's the Difference Between OT, ICS, SCADA and DCS*, May 2019. [Online]. Available: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

[41] G. Williamson, "OT, ICS, SCADA – what's the difference?" Jul. 2015, retrieved 13.04.2020 from https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

[42] CISA, "Control system engineering workstation," 2020, retrieved 20.04.2020 from https://www.us-cert.gov/ics/Control_System_Engineering_Workstation-Definition.html.

[43] M. Albahar, "Cyber attacks and terrorism: A twenty-first century conundrum," *Science and Engineering Ethics*, vol. 25, p. 993, Jan. 2017.

[44] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," May 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/paper/36297

[45] E. Cole, *Advanced persistent threat : understanding the danger and how to protect your organization*. Syngress, Apr. 2013.

[46] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*. Springer, 2019.

[47] F. Mandiant, "M-trends 2020 – fireeye mandiant services, special report," FireEye Mandiant, pp. 11, 20, 2020.

[48] L. Huang and Q. Zhu, "A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems," *Computers & Security*, vol. 89, p. 101660, 2020.

[49] FireEye, *Anatomy of Advanced Persistent Threats, Retrieved 20.03.2020 from https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html*, year 2020.

[50] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *International Symposium on Security in Computing and Communication*. Springer, 2015, pp. 438–452.

[51] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, "Kill chain for industrial control system," in *MATEC Web of Conferences*, vol. 173, Jan. 2018.

[52] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, vol. 1, 2015.

[53] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 747–748.

[54] M. Sikorski and A. Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, 1st ed. USA: No Starch Press, 2012.

[55] "ISO/IEC 27039:2018(E). information technology – security techniques – information security management systems – overview and vocabulary," Geneva, CH, Feb. 2015.

[56] J. Slowik, "Stuxnet to crashoverride to trisis," retrieved 05.04.2020 from https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html.

[57] G. Desarnaud, "Cyber attacks and energy infrastructures," IFRI Center for Energy, Jan. 2017.

[58] D. Kushner, "The real story of stuxnet," *ieee Spectrum*, vol. 3, no. 50, pp. 48–53, 2013.

[59] S. P. Rao, "Stuxnet, a new cyberwar weapon: Analysis from a technical point of view," pp. 1–2, May 2014.

[60] M. Dadashzadeh, "Choosing it platforms in the age of stuxnet," *Journal of Cybersecurity Research*, vol. 2, no. 1, 2017. [Online]. Available: https://clutejournals.com/index.php/JCR/article/view/10076/10178

[61] N. Nelson, "The impact of dragonfly malware on industrial control systems," SANS Institute, Jan. 2016.

[62] CISA, *ICS Focused Malware*, Jun. 2014. [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-14-178-01

[63] FireEye Inc, "Cyber attacks on the ukrainian grid: What you should know," FireEye, pp. 1–2, Feb. 2016. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf

[64] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," E-ISAC and SANS, Mar. 2016.

[65] D. Inc, "Crashoverride analysis of the threat to electric grid operations," Dragos Inc, p. 555, Jun. 2017. [Online]. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[66] J. Slowik, "Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack," Aug. 2019. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf

[67] ESET, *Industroyer: Biggest malware threat to critical infrastructure since Stuxnet*, Jun. 2017. [Online]. Available: https://www.eset.com/int/industroyer/

[68] J. Slowik, "Threat intelligence and the limits of malware analysis," Dragos Inc, Jan. 2020. [Online]. Available: https://www.dragos.com/wp-content/uploads/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

[69] D. Inc, *Robert M. Lee*, 2020. [Online]. Available: https://www.dragos.com/team/robert-m-lee/

[70] A. Cherepanov and R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since stuxnet," *WeLiveSecurity, ESET*, vol. 12, 2017.

[71] M. ATT&CK, *Sandworm Team*, May 2017. [Online]. Available: https://attack.mitre.org/groups/G0034/

[72] J. Slowik, "Anatomy of an attack: Detecting and defeating crashoverride," Dragos Inc, Oct. 2018. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf

[73] P. Shedden, A. Ahmad, and A. Ruighaver, "Organisational learning and incident response: promoting effective learning through the incident response process." Edith Cowan University, Perth, 2010.

[74] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST, NIST Special Publication 800-61, 2012.

[75] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams–challenges in supporting the organisational security function," *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[76] N. H. Ab Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *computers & security*, vol. 49, pp. 45–69, 2015.

[77] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, pp. 42–57, 2014.

[78] "Information technology — Security techniques — Information security incident management," International Organization for Standardization, Geneva, Switzerland, Standard, 2016.

[79] M. Jaatun and R. Koelle, "Cyber security incident management in the aviation domain," Aug. 2016.

[80] NIST, "Cyber ranges," National Initiative for Cybersecurity Education, Mar. 2018. [Online]. Available: https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

[81] Y. Chandra and P. K. Mishra, "Design of cyber warfare testbed," in *Software Engineering*. Springer, 2019, pp. 249–256.

[82] S. Adepu, N. K. Kandasamy, and A. Mathur, "Epic: An electric power testbed for research and training in cyber physical systems security," in *Computer Security*. Springer International Publishing, 2019, pp. 37–52.

[83] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[84] M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers and Security*, vol. 88, 2020.

[85] D. Haynes, *Metadata for Information Management and Retrieval: Understanding metadata and its use*. Facet Publishing, 2018.

[86] I. Priyadarshini, "Features and architecture of the modern cyber range: a qualitative analysis and survey," Master's thesis, University of Delaware, 2018.

[87] U. J. Staff, "Joint training manual for the armed forces of the united states (cjcsm 3500.03 d)," Washington, DC: Joint Chiefs of Staff, 2012.

[88] J. Vykopal, M. Vizváry, R. Oslejsek, P. Celeda, and D. Tovarnak, "Lessons learned from complex hands-on defence exercises in a cyber range," in *2017 IEEE Frontiers in Education Conference (FIE)*, 2017, pp. 1–8.

[89] G. Subaşu, L. Roşu, and I. Bădoi, "Modeling and simulation architecture for training in cyber defence education," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2017, pp. 1–4.

[90] G. Vigna, K. Borgolte, J. Corbetta, A. Doupe, Y. Fratantonio, L. Invernizzi, D. Kirat, and Y. Shoshitaishvili, "Ten years of ictf: The good, the bad, and the ugly," in *Summit on Gaming, Games, and Gamification in Security Education*, 2014.

[91] M. Ernits, J. Tammekänd, and O. Maennel, "i-tee: A fully automated cyber defense competition for students," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 113–114, 2015.

[92] J. Kim, K. Kim, and M. Jang, "Cyber-physical battlefield platform for large-scale cybersecurity exercises," in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, 2019, pp. 1–19.

[93] P. Čeleda, J. Čegan, J. Vykopal, and D. Tovarňák, "Kypo–a platform for cyber defence exercises," M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization, 2015.

[94] T. Jirsík, M. Husak, P. Čeleda, and Z. Eichler, "Cloud-based security research testbed: A DDoS use case," in *Network Operations and Management Symposium (NOMS)*. IEEE, 2014, pp. 1–2.

[95] C. Pham, D. Tang, K.-i. Chinen, and R. Beuran, "Cyris: A cyber range instantiation system for facilitating security training," in *Proceedings of the Seventh Symposium on Information and Communication Technology*, 2016, pp. 251–258.

[96] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (TASSCS)," in *ISGT 2011*, 2011, pp. 1–7.

[97] R. Beuran, D. Tang, C. Pham, K.-i. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: Cytrone," *Computers & Security*, vol. 78, pp. 43–59, 2018.

[98] R. Horvath, D. Nedbal, and M. Stieninger, "A literature review on challenges and effects of software defined networking," *Procedia Computer Science*, vol. 64, pp. 552–561, 2015.

[99] L. Ma, S. Yi, and Q. Li, "Efficient service handoff across edge servers via docker container migration," in *Proceedings of the Second ACM/IEEE Symposium on Edge Computing*, 2017, pp. 1–13.

[100] T. Morris, T. Alves, and R. Das, "Virtualization of industrial control system testbeds for cybersecurity," in *ACSAC ICSS 2016*, Dec. 2016.

[101] I. Somarakis, M. Smyrlis, K. Fysarakis, and G. Spanoudakis, "Model-driven cyber range training: A cyber security assurance perspective," in *Computer Security*. Springer, 2019, pp. 172–184.

[102] S. Braidley, "Extending our cyber-range cyran with social engineering capabilities," Master's thesis, De Montfort University, Sep. 2016.

[103] J. Iivari and J. R. Venable, "Action research and design science research-seemingly similar but decisively dissimilar," 2009.

[104] R. Wieringa, *Design science methodology for information systems and software engineering*. Springer, 2014, 10.1007/978-3-662-43839-8.

[105] W. Adams, *Conducting Semi-Structured Interviews*, Aug. 2015.

[106] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers & Security*, vol. 88, p. 101636, 2020.

[107] M. S. Saleh, A. Althaibani, Y. Esa, Y. Mhandi, and A. A. Mohamed, "Impact of clustering microgrids on their stability and resilience during blackouts," in *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*. IEEE, 2015, pp. 195–200.

[108] M. Saleh, Y. Esa, Y. Mhandi, W. Brandauer, and A. Mohamed, "Design and implementation of ccny dc microgrid testbed," in *Industry Applications Society Annual Meeting*. IEEE, 2016, pp. 1–7.

# List of Figures

THIS PAGE IS INTENTIONALLY LEFT BLANK

# List of Tables

THIS PAGE IS INTENTIONALLY LEFT BLANK

# Chapter A
# Results

## A.1 Prototype – Experimental VMs from VMWare

Tinycore, Slax and Lubuntu OS from VMware were tested as possible alternatives to Ubuntu workstation as they are all less resource demanding. Tinycore was found to be too limited in terms of functionality and supported applications, and Slax had consistent interface issues, so both of these were deemed unfitting. Lubuntu worked well for user tasks, such as browsing, sending emails and using office tools and it also supports a wide range of applications. As such, it might be useful when trying to keep resource demand down.

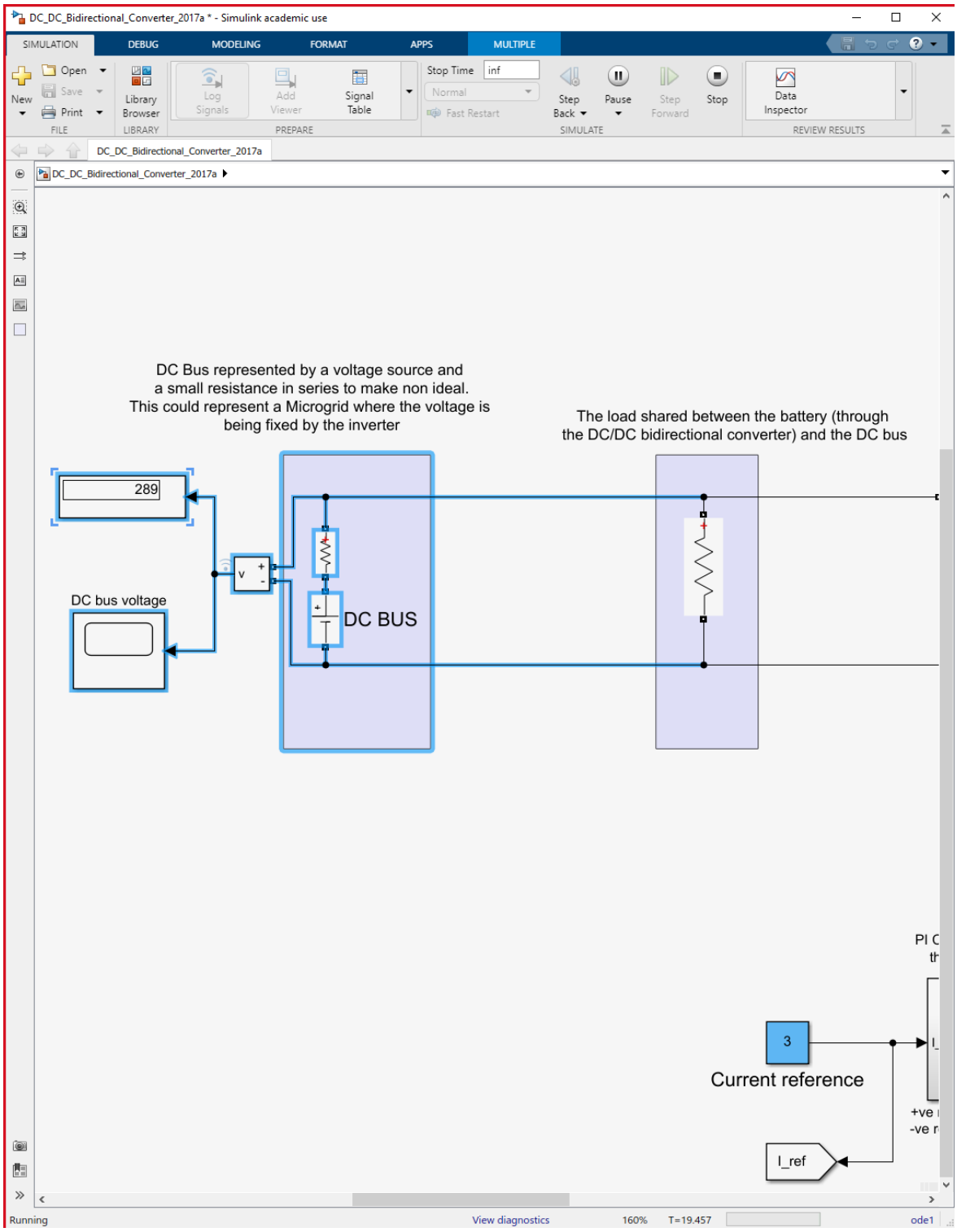


**Figure A.1:** Close up screenshot of the micro grid simulation used in the project. Part 1.

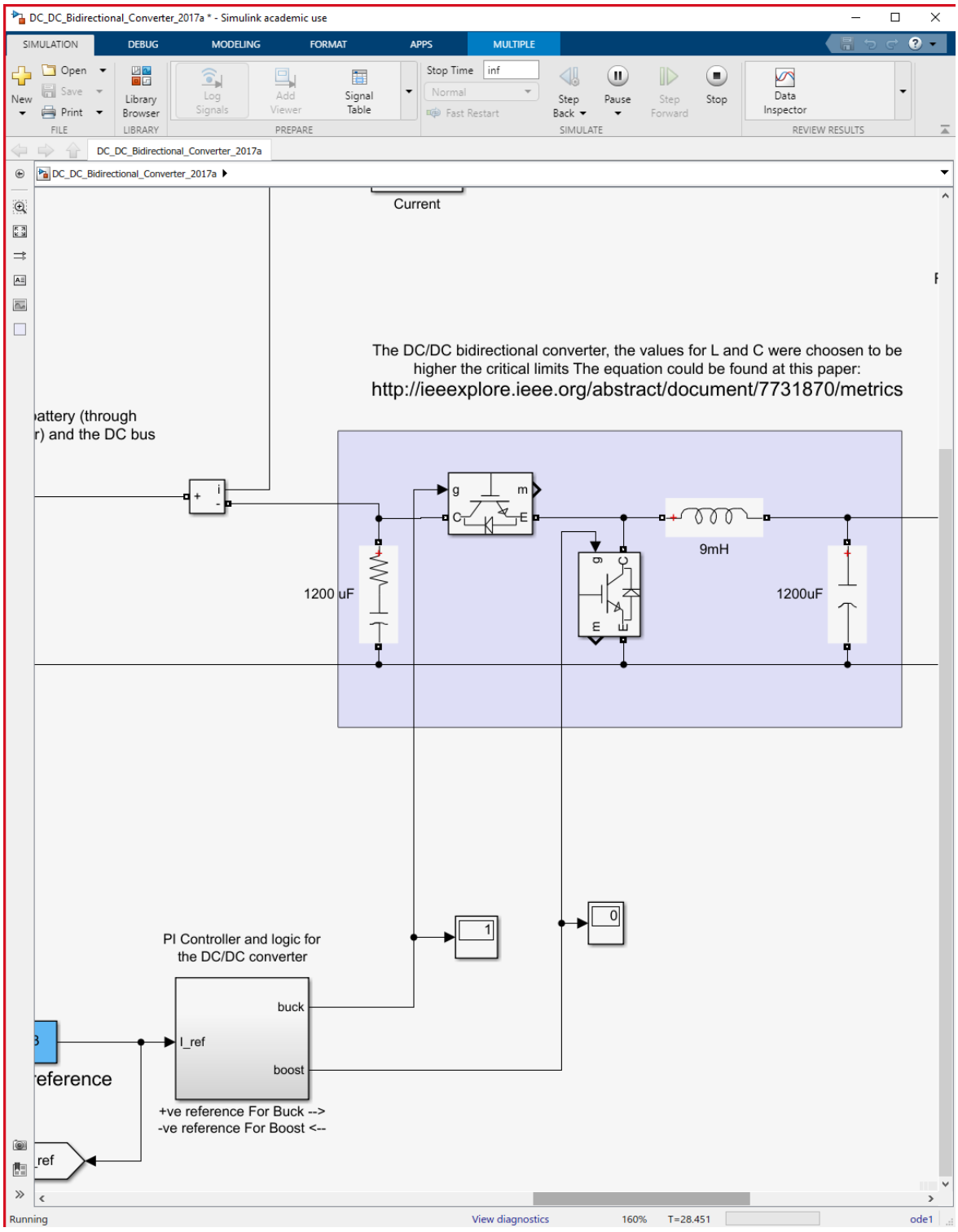


**Figure A.2:** Close up screenshot of the micro grid simulation used in the project. Part 2.

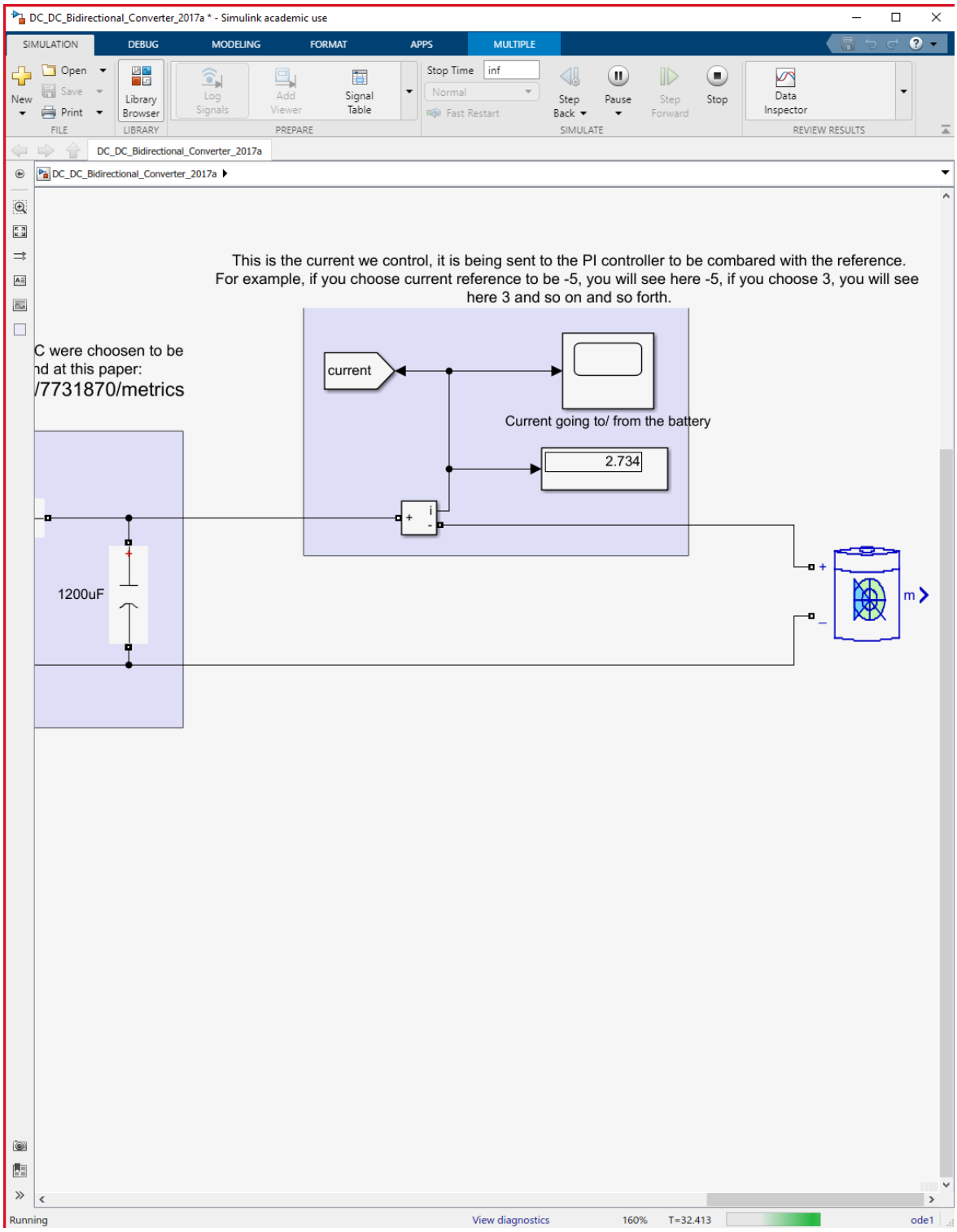


**Figure A.3:** Close up screenshot of the micro grid simulation used in the project. Part 3.

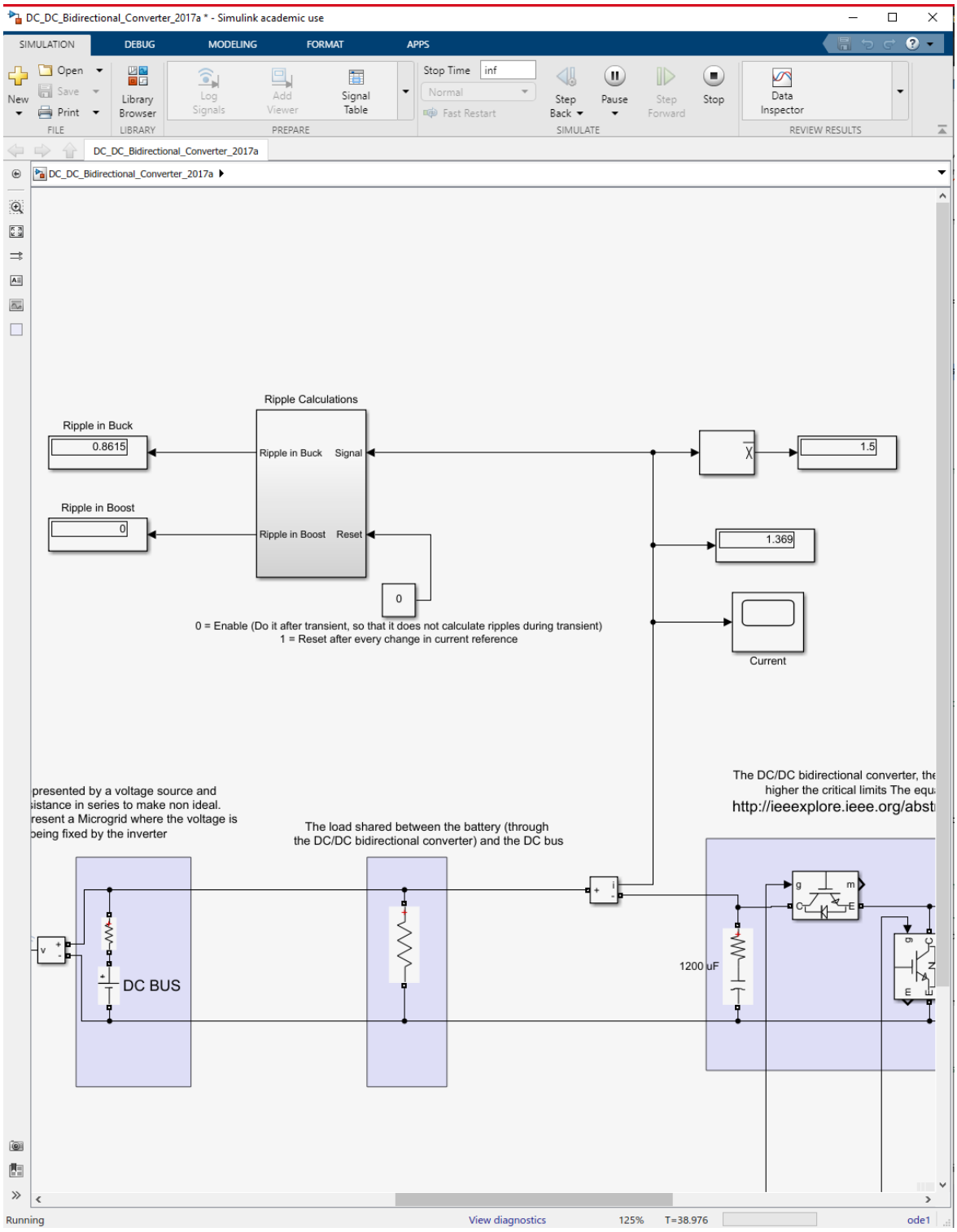


**Figure A.4:** Close up screenshot of the micro grid simulation used in the project. Part 4.

# Chapter B
# Semi-Structured Interviews

## B.1 The Interview Guide

**Part I: Introduction**

- Introduction of ourselves, give information about the interview structure and our topic of study
- Inform about laws and regulations

**Part II: Background**

- Can you briefly tell us about your background and expertise in IT security?
- Are you familiar with the term incident response?
- Have you participated in any training in terms of security incident response?
- Are you familiar with the concept of a smart grid? In what way?
- Are you familiar with the term cyber ranges? In what way?

**Part III: Incident Response and Cyber Ranges**

- Can you think of any particular skills that might come in handy when training in a cyber range?
- What kind of skills do you think will be useful to practice in a cyber range?
- Do you know of anybody in Norway that uses cyber ranges for training?
- In your experience, what type of components/systems do you find most important to include in a cyber range?

– Can you think of any examples of cyber attacks on the electric power infrastructure that could be interesting to include in a cyber range?

## B.2 Important Quotations

**Quote 1 – Can you please explain some of your experience with cyber ranges?**

> "Cyber ranges must be as seamless as possible for the users, and thus, automation is key! ... It's typical to speak about scenarios in a cyber range. A scenario is a textual description that "someone" has written on paper, but this again, must be transferred to simulations, emulators, machines, and so on. ...Monitoring is very important, both in terms of training scenarios, but also for cyber range management. ...In my experience, try to automate as much as possible. ...Another thing is that realism is very hard to achieve, but it should be easier if you define the Main Training Audience (MTA), which is the group of focus that you intend to train. For instance, is it a rookie blue team member? or a cyber security professional? And then, define the level of realism needed."

– Person 1: Technical lead and cyber range expert

**Quote 2 – How are cyber security training performed in your business?**

> "People are sporadically sent on training courses, but there is a lack of sufficient, realistic and good training. ...A simple thing like learning how to respond to alarms cannot be done in these courses. ...Many organizations don't take data logging and alarms seriously, but they really should, and some are really good at it. ...When it comes to my line of work (incident response), the cooperation between people is very important. ...and it is very common to experience communication failure between people."

– Person 4: Cyber security professional and incident responder.

**Quote 3 – Does control center operators need cyber security training in your opinion?**

> "They need to be trained in cyber security. In addition, to hardware failure and other kinds of communication errors. Because, with the current

situation, if an cyber attack should occur, they would say it was an error or fault or something."

– Person 3: Expert in cyber security and incident response in TSOs.

**Quote 4 – Is there anyone monitoring the network traffic within your organization in order to prevent cyber attacks?**

"Yes. A company, called (Redacted), is looking at network traffic in/out of Norway. They monitor, for instance, all the communication to and from Russia. In addtion, we have our own CERT, called (Redacted). ...However, it is still uncertain if the the DSOs have this, but anyway, this is a very new topic. So, I believe there are little to none monitoring in terms of cyber security in the control systems."

– Person 3: Expert in cyber security and incident response in TSOs.

**Quote 5 – Could a cyber attack lead to a power loss?**

"Yes! One interesting angle is that such attacks used against a smart grid could trigger islanding. Meaning that a section of the grid is cut off from the rest, where prosumers and consumers are "islanded" inside their own loop. If you could trigger this in several parts of the network, it could affect transmission and generation. ...You should focus on replay, delay and DoS attacks."

– Person 2: Researcher and cyber range expert

# Chapter C
# Hardware Specifications

## C.1 Granted Virtualization Host

- **CPU:** Double Intel Xeon Gold 5118 (12 cores, 24 threads, 16M Cache)
- **Memory:** 64GB, 2666 MHz DDR4
- **Storage:** 2TB HDD + 512GB SDD


**Figure C.1:** The virtualization host granted to the project by the Department of Electric Power Engineering at NTNU.

## C.2 Consumer Desktop Specifications

- CPU: Intel i7 6700K (2015 release)
- Memory: 16GB, DDR4, 1072MHz
- Storage: 2TB HDD Seagate, 7200RPM

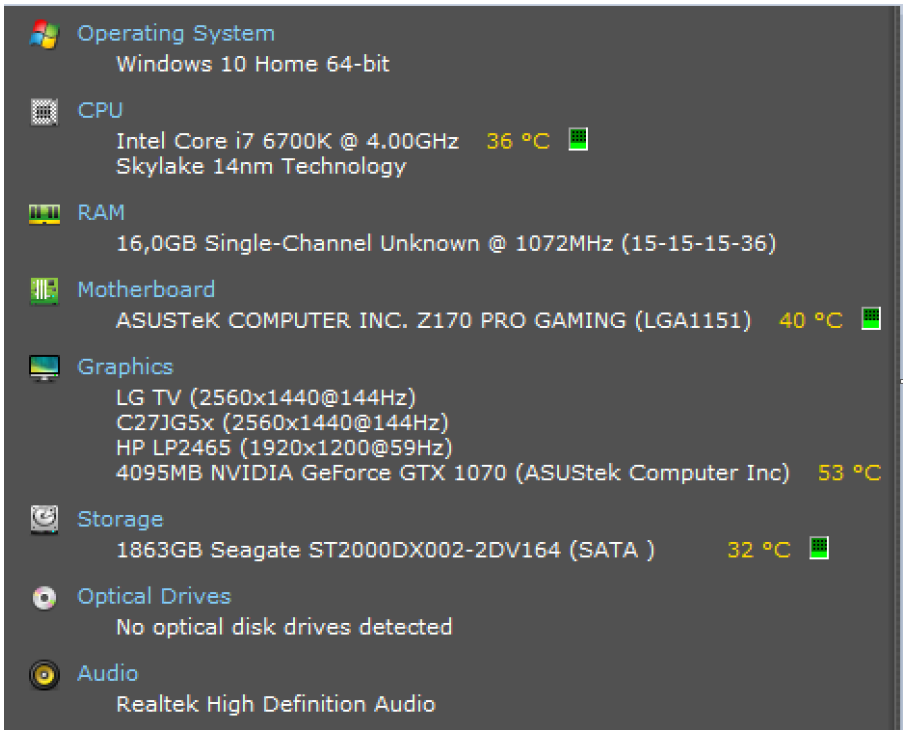


**Figure C.2:** Hardware used for prototype implementation.

# Chapter D
# Miscellaneous

## D.1 The National Smart Grid Laboratory


**Figure D.1:** Picture from a visit to the Norwegian National Smart Grid Laboratory. The picture shows an electrical power generator.

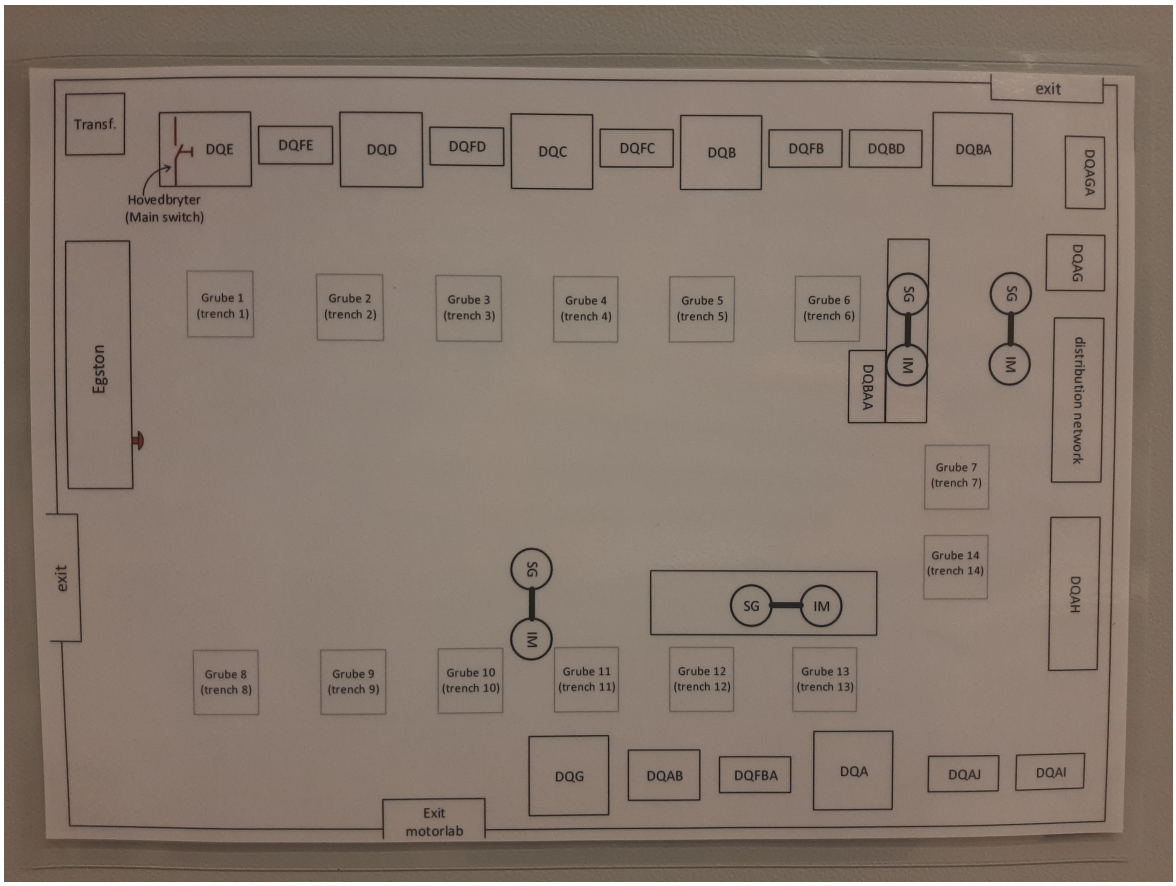


**Figure D.2:** High-level overview of the National Smart Grid Laboratory.

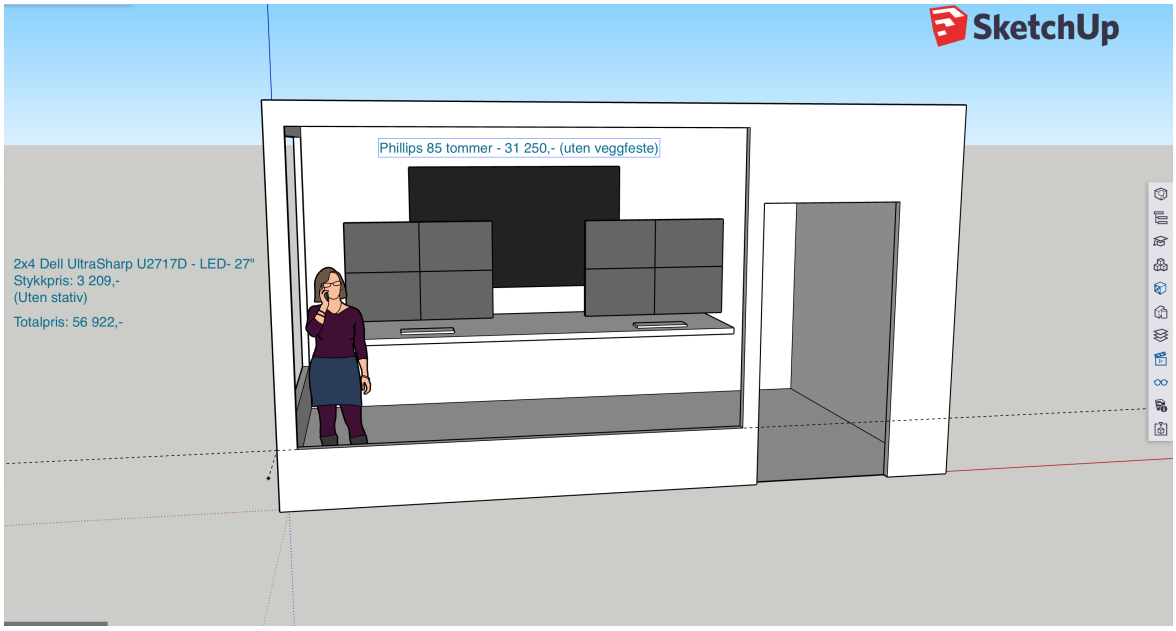


**Figure D.3:** 3D model of a potential blue team control room made in early stages of the project.

## D.2 Miscellaneous


**Figure D.4:** Digital meeting with a stakeholder. From left to right; Alexander Bakken, Supervisor Thomas Haugan, Bjørn Olav and Associate Professor Marie Moe.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Bjørn Olav Gjørven, Alexander H. Bakken

NTNU
Norwegian University of
Science and Technology

CINELDI
Centre for intelligent electricity distribution
- to empower the future Smart Grid