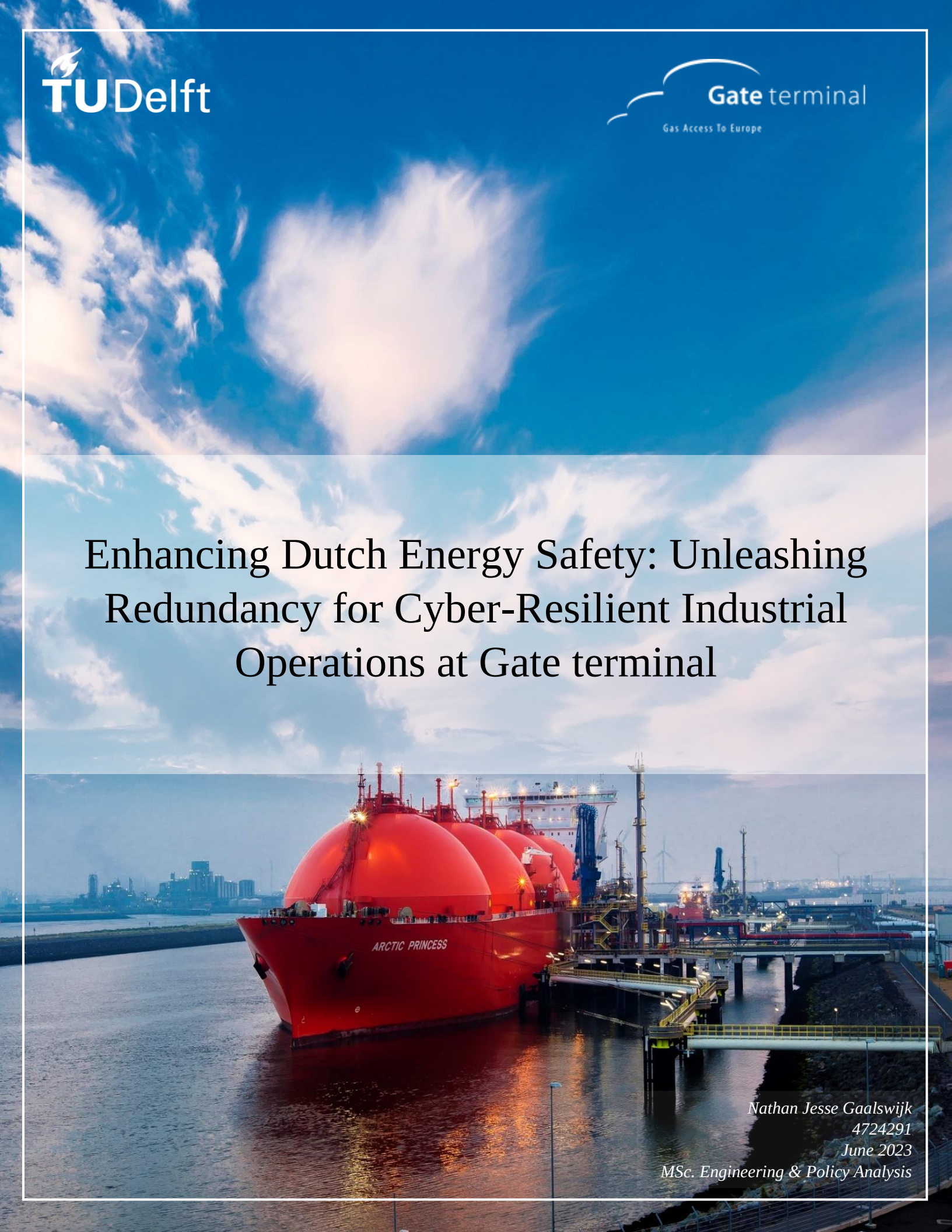
Enhancing Dutch Energy Safety: Unleashing Redundancy for Cyber-Resilient Industrial Operations at Gate terminal



Nathan Jesse Gaalswijk
4724291
June 2023
MSc. Engineering & Policy Analysis

Enhancing Dutch Energy Safety: Unleashing Redundancy for Cyber-Resilient Industrial Operations at Gate terminal

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Engineering & Policy Analysis**

Faculty of Technology, Policy and Management

by

Nathan Jesse Gaalswijk

Student number: 4724291

To be defended in public on September 11, 2023

Graduation committee

Chairperson	: Prof. Dr. M. Warnier	Multi-Actor Systems
First Supervisor:	: Prof. Dr. ir. P.H.A.J.M. van Gelder	Safety and Security Science
Second Supervisor	: Prof. Dr. M. Warnier	Multi-Actor Systems
External Supervisor	: M. Risse	Gate terminal B.V.
External Supervisor	: M.N. Noorlander	Applied Risk B.V.

Executive Summary

It is vital to recognize the importance of critical infrastructures such as the energy sector for the proper functioning of society. Since natural gas is used for the generation of electricity, large problems would occur in industrial sectors and households when this infrastructure is disrupted.

The rise of interconnected operational technology (OT) in these critical industries allows for automating, monitoring, and controlling the infrastructures effectively and in real-time, but also comes with a pitfall: the increase of convergence between the IT and OT domains exposes the traditionally isolated OT systems to cyber threats that were previously only applicable to the IT domain.

Gate terminal plays an increasingly large role in ensuring and maintaining energy safety for the Netherlands. A disruption in their operational processes caused by a cyberattack may deteriorate the country's energy supply, endangering public welfare. Therefore, it is key that Gate terminal is properly protected against (and resilient to) cyberattacks by malicious parties. Therefore, this thesis has investigated the impact of redundancy implementation on the operational performance of OT at Gate terminal. The following main research question has been investigated:

"To what extent does the implementation of redundancy enhance the operational performance of operational technology in the industrial processes of Gate terminal in the face of cyber threats, in order to maintain the availability of business services?"

To successfully answer this question, firstly, OT in the industrial processes at Gate terminal was highlighted, after which the impact of attacker and defender behaviors on the company's operational performance of the company was discussed. This information was used as a basis for an agent-based model (ABM), which allows for modelling the interactions between attackers, defenders, and implemented control loops. Ultimately, the operationalized ABM was used for experimenting with various redundancy strategies.

This thesis research shows that the operability of OT is affected by a variety of threats, including ransomware attacks, advanced persistent threats (APTs) and Denial of Service (DoS) attacks. These threats can impact the integrity and availability of services, which is vital in OT environments. As a result, the operational performance of the plant can be deteriorated. In order to be able to adequately prevent and deal with these threats, it is vital for the system operator to implement and optimize their incident response cycle.

In an effort to increase the operational performance of OT at Gate terminal in the face of cyber threats, a redundancy strategy can be implemented by the system operator. While this may come with numerous advantages, redundancy inevitably increases the attack surface of the system, thus increasing the likelihood of a successful attack. Due to this trade-off, redundancy must be implemented with caution to ensure that its benefits outweigh its drawbacks.

The main factors that play a role in the effectiveness of the implemented redundancy strategy, are the criticality of the redundantly implemented control loop, and the degree of diversity that is applied. Application of redundancy in high criticality control loops could prove effective, while redundancy in low criticality control loops may have unwanted effects on the operational performance of the company.

It is crucial to recognize that a redundancy strategy can only be as effective as the incident response procedure implemented by the system operator: if redundancy is implemented, but the system operator is incapable of dealing with occurring incidents, redundancy by itself is no lifesaver for the operational performance of Gate terminal in the face of cyber threats.

Based on the outcomes of the research, several recommendations can be done for Gate terminal:

Firstly, the company should iteratively improve all steps in the incident response cycle, while focusing on improving the quality of intrusion prevention and efficiency of incident containment. These two factors have the most impact on system performance.

Furthermore, the company should implement redundancy with careful consideration, after performing an extensive cost-benefit analysis. Random redundancy implementation can prove to be counterproductive for the operational performance of the company.

Finally, the company should collaborate with other parties present in the energy sector and other critical infrastructures when it comes to sharing cyber-related information. This enables Gate terminal to be more aware of vulnerabilities, and better prepared for handling incidents.

As future research recommendations, it is advisable to experiment with a wider range of redundancy strategies, using exploratory modelling packages such as EMA Workbench, which will allow for a more precise, Gate terminal-specific redundancy strategy formulation. Furthermore, specific types of attacks, as well as strategic defense systems could be implemented in the model, increasing the link of the model with reality. Finally, analyzing and optimizing the trade-off between the increased attack surface and the advantages of redundancy, and the trade-off between increased costs versus diverse redundancy, could yield interesting results. These future research recommendations can aid in resolving several main limitations of this thesis.

Acknowledgements

This master thesis is a milestone that marks the end of my Master's degree in Engineering and Policy Analysis at Delft University of Technology. The thesis was written between February and July 2023. Simultaneously, this thesis concludes my time as a student in Delft. I would like to use this section to thank everyone that has supported me during the modeling and writing required for this thesis.

First of all, I would like to thank my first supervisor, Pieter van Gelder. His supervision throughout the entire thesis process, starting with the selection of the topic, has been extremely helpful. Mr. van Gelder has guided me through any major difficulties that came with writing this thesis.

Additionally, without the expertise and insights in the field of agent-based modeling of my second supervisor and graduation committee chairman, Martijn Warnier, this research would not have been possible. I would like to thank Mr. Warnier for his constructive and honest feedback, which contributed significantly to increasing the final quality of this thesis.

Furthermore, I would like to show my gratitude to my supervisors from Gate terminal, Michael Noorlander and Michael Risse. These gentlemen acted as sparring partners, thinking along with me during several parts of this research. Furthermore, they have dedicated their time and energy to provide me with invaluable feedback and insights, for which I would like to thank them.

In addition, I would like to thank Gate terminal for providing me with an internship position. The increased applicability of the thesis proved to be a huge motivator throughout the process of writing this thesis. I thoroughly enjoyed my time as an intern at the company: I met very interesting people during the internship, all of whom immediately made me feel welcome and appreciated, for which I am thankful.

On top of that, I would like to show appreciation to my direct colleagues at Gate terminal. I thoroughly enjoyed the good times at the office! A special thanks to all of the employees of the company that dedicated a part of their time to provide me with useful insights through expert interviews.

Finally, I would like to thank my girlfriend, friends, and family. They have provided me with unconditional support throughout the entire thesis process. I much appreciate your genuine interest, questions, and encouragement during the past semester.

Now that my time as a student in Delft is over, I can look back on six years of developing myself and my interests, meeting new people, and making life-long friends. I'm looking forward to seeing what is next!

Enjoy reading my thesis!

Jonathan Gaalswijk
Delft, July 2023

Table of Contents

List of Figures and Tables

List of Abbreviations

Abbreviation	Meaning
ABM	Agent-Based Modelling
APT	Advanced Persistent Threat
BCMA	Billion Cubic Meters per Annum
BOG	Boil-Off Gas
CCR	Cargo Control Room
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CPS	Cyber-Physical System
DCS	Distributed Control System
DMZ	Demilitarized Zone
DOS	Denial of Service
ESD	Emergency Shutdown
FGS	Fire and Gas System
ICS	Industrial Control System
IDS	Intrusion Detection System
IIOT	Industrial Internet of Things
IOT	Internet of Things
IPS	Intrusion Preventions System
IT	Information Technology
KDE	Kernal Density Estimation
KPI	Key Performance Indicator
KVM	Acronym for Keyboard, Video, Monitor
LHS	Latin Hypercube Sample
LNG	Liquefied Natural Gas
MTBF	Mean Time between Failure
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NG	Natural Gas
ORV	Open Rack Vaporizer
OT	Operational Technology
PERA	Purdue Enterprise Reference Architecture
PDCA	Plan-Do-Check-Act
PLC	Programmable Logic Controller
RAMSSHEEP	Acronym for Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economics and Politics
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
TVC	Acronym for Threat, Vulnerability, Consequence
UML	Unified Modelling Language

1. Introduction

A country's energy supply is crucial for having a properly functioning industry and society. Electricity and gas supply are so-called 'critical infrastructures', due to their interconnectivity and their vital importance for public welfare (Pursainen, 2009). Due to the criticality of energy for having a functioning society, it is absolutely necessary for a country to ensure its energy safety, maintaining a steady supply and availability of energy for industry and society.

Historically, the EU has been highly dependent on gas, imported from Russia for their energy supply (Arınç, 2007). In recent years, the amount of gas imported from Russia to the Netherlands is declining (CBS, 2022), reducing the dependency on Russia and its gas. Moreover, about a year after Russia invaded Ukraine, the import of Russian gas has been greatly reduced (Rijksoverheid, 2023). This decreased dependency also reduces the country's energy security, since the total potential supply of gas is reduced.

Gate terminal, located at the second Maasvlakte in the Port of Rotterdam offers an alternative to the gas imported from Russia (Rijksoverheid, 2023), enabling the imports of liquefied natural gas (LNG) from all over the globe (Gate terminal, n.d.a.). Industrial processes at the plant are controlled using operational technology (OT)

OT has become increasingly interconnected with information technology (IT) in critical infrastructures, such as the gas industry (Alqudhaibi et al., 2022). The increased IT/OT convergence and 'smart energy' trend come with multiple advantages, including increased safety- and operational performance, increased efficiency, automation, and cost reduction (Denisova, 2019). However, due to an increase in IT/OT convergence, cybersecurity risks that were once only present in the IT domain are now transferred to the OT domain, negatively affecting security in these systems (Murray et al., 2017).

Since Gate terminal plays an increasingly large role in ensuring and maintaining energy safety for the Netherlands, a disruption in their operational processes, may endanger the energy supply of the country, ultimately endangering public welfare. These disruptions could be caused by a successful cyberattack on the OT of the company. Due to the criticality of a stable gas supply for a properly functioning society, it is crucial that Gate terminal is properly protected against the impact of cyberattacks by malicious parties. The implementation of redundancy in the company's OT might prove to be a worthwhile measure to achieve this goal.

The geopolitical aspect of energy safety results in a complex problem, with multiple stakeholders that have diametrically opposing viewpoints and interests. Furthermore, the outcome of the energy safety & cybersecurity issue may have a big impact on society. Therefore, the issue can be viewed as a complex, socio-technical problem in an open system with geopolitical aspects. Therefore, the issue at hand can be referred to as an international grand challenge in the fields of energy safety and cybersecurity.

As highlighted in Chapter 2 of this thesis, there is a lack of research when it comes to improving cybersecurity in OT in order to increase operational performance in LNG infrastructure in the Netherlands, specifically when it comes to increasing redundancy in the system. The identified knowledge gap can be filled by creating an agent-based model, based on attacker-defender interactions in the OT of Gate terminal. Various redundancy-related strategies can be tested using this model, in an attempt to partially fill the identified knowledge gap.

1.1. Problem Statement and Research Questions

Due to the criticality of Gate terminal for the energy safety of the Netherlands, as well as the increased cybersecurity risks resulting from increased IT/OT convergence as discussed in Chapter 2, it is important to safeguard the terminal against cyberattacks that could affect the availability of its industrial processes. The aim of this research is therefore to explore and analyze the effect of different redundancy-related

strategies on the operational performance of the OT at Gate terminal in case of a cyberattack. In order to achieve this goal, the following main research question has been formulated, providing the direction of this study.

Main research question:
"To what extent does the implementation of redundancy enhance the operational performance of operational technology in the industrial processes of Gate terminal in the face of cyber threats, in order to maintain the availability of business services?"

The main research question has been decomposed into multiple sub-questions, providing structure to the thesis.

Sub-question 1:

"What is the role of OT in the industrial processes of Gate terminal?"

The goal of this sub-question is to gain an insight regarding the system that is to be modelled using ABM. The main results of this sub-question will include a description of the industrial processes at Gate terminal, as well as an overview of the different process control loops at the plant.

Sub-question 2:

"How do different attacker and defender behaviors impact the availability of industrial processes of Gate terminal?"

The behavior of the attacking and defending model entities on the operational performance of the system as defined through the first sub-question is explored in this sub-question. Combined with the results of the first sub-question, the results of this sub-question will form the input for the ABM.

Sub-question 3:

"What behavior can be observed in the operational technology in the industrial processes of Gate terminal when simulating cyberattacks?"

Answering the third sub-question involves operationalization of the ABM. The behavior of the model will be explored and analyzed using multiple analyses. The result of the third sub-question will constitute a baseline performance for comparing the effectiveness of different redundancy strategies.

Sub-question 4:

"What redundancy-related cyber-strategies are effective for increasing availability of the industrial processes of Gate terminal?"

For answering the fourth and final sub-question, different redundancy-related strategies will be generated. These strategies will be used for model experimentation, comparing the operational performance of the modelled system when the various strategies are implemented.

1.2. Thesis Structure

This section elaborates on the structure of the thesis. Firstly, in Chapter 2, the current state of the art with regard to modelling security systems is described, in the form of a literature review. Subsequently, Chapter 3 is focused on the research approach and methods, used to answer all previously mentioned sub-questions successfully.

After highlighting the research methodology, OT in industrial processes in general, as well as OT implementations at Gate terminal are discussed in Chapter 4, forming the basis of the system that is to be modelled using the agent-based model. Chapter 5 highlights various attacker and defender behaviors and the impact these behaviors have on the operational performance of the system.

Now that there is a clear overview of the system that is to be modelled, a conceptual model is designed, and system key performance indicators (KPIs) are defined in Chapter 6. This conceptual model is operationalized and implemented into a full-fledged ABM. This process, as well as the verification and validation of the model, is described in Chapter 7. Consequently, in Chapter 8 redundancy strategies are formulated and used for experimentation. The results of this experimentation are also presented in this chapter. The results are discussed in Chapter 9, after which Chapter 10 presents answers to the research questions, and reflects on the scientific and societal relevance of the overall thesis.

2. State of the Art: Modelling Security Systems

In the following section, a literature review is performed on existing research about security concepts, and modelling (cyber)security systems. Several subjects, including modelled entities, model inputs and performance indicators, security of OT systems, as well as critical infrastructure modelling are discussed. Literature on (cyber)security modelling will be briefly summarized, and a new knowledge gap will be identified.

2.1. Modelling Security Systems

This section will open with a brief description of physical and digital security, and other concepts that are applicable in the security and safety science domain. Afterwards, modelling methods applied for both types of security systems will be described and compared.

Security can be measured as 'the degree to which malicious harm is prevented, detected, and reacted to' (Firesmith, 2003). In security systems, there exist two main different fields: physical security and logical (digital) security (Kinslow, 2006). Traditionally, physical security systems are aimed at protecting and controlling physical access to an organization and its assets, maintaining the integrity of the system (Kinslow, 2006; Karanikas, 2018).

Safety is a concept that is closely related to security. Similar to security, safety is aimed at preventing, detecting and reacting to harm. The main difference is the origin of this hard: while harm in a security context is caused by malicious intent, this is not the case in safety context (Firesmith, 2003).

Safety and security are unified by a third term: survivability. Survivability is focused on maintaining availability and continuation of an organizations' mission critical services. A system has to maintain a minimal (acceptable) level of performance at a given instant, even during partial unavailability of a part of this system (Yurcik & Doss, 2002). Firesmith (2003) states that survivability can be decomposed into three main quality subfactors: prevention, detection and reaction.

The relation between survivability and robustness is tight-knit, as both aspects are focused on maintaining operability of a system when it is under stress. The main distinction between the two aspects is in the duration of the stress/disruption in the system. Survivable systems 'recover' to the original state, while robust systems fully adapt to the new situation (Richards et al., 2007). Furthermore, Richards et al (2007) divide the prevention, detection and reaction quality subsystems as identified by Firesmith (2003) into active (through reaction/adaptation) and passive (by design) survivability.

2.1.1. Modelling Physical Security Systems

Physical security systems have been modelled with a wide variety of techniques. Relatively static approaches, like the Threat-Vulnerability-Consequence (TVC) framework have been used to investigate security risks in a wide variety of areas. One purpose of the TVC framework is to structure and explore a security/risk context. For this purpose, Linacre et al (2005) performed a security analysis for agroterrorism: the TVC framework proved to be applicable for the exploration of a security scenario.

Furthermore, Linacre et al (2008) applied TVC in a homeland security context, attempting to solve a resource allocation problem. Linacre et al (2008) conclude that TVC is able to offer a solution to these resource allocation problems. This statement is, however, contradicted by Cox (2008), stating that there is a lack of applicability of the TVC framework due to a lack of interaction with an adversary: attacker resource allocation has to be taken into account in order to assess and model security risk, especially when attempting to solve a resource allocation problem. This cannot be done using the TVC method (Baybutt, 2017; Brown & Cox, 2010; Cox, 2008)

Other methods to model security, such as a game-theoretical approach, are more dynamic. They can (partly) solve shortcomings of the TVC: they allow for the adversary to interact with the defender of a system (Fielder et al., 2014; Ibidunmoye et al., 2013). In the game-theoretical approach, the defender takes

measures and allocates resources to prevent damage to a potential target. The attacker, in turn, performs an attack on a specific target (Cox, 2009). In game-theory, the decisions of the players are made based on the expected value (or, expected loss) of a decision, as well as a specific player strategy, such as loss minimization, regret minimization, et cetera (Nochenson & Heimann, 2012).

An important, generally applicable finding of Nochenson and Heimann (2012) is that the defender shouldn't focus all of its resources at protecting a single, high value, asset. Main limitations of the long existent game-theoretical approach include bounded rationality and difficulties in estimation of player payoffs introduced by the lack of complete information (Samuelson, 1996).

2.1.2. Modelling Logical Security Systems

Kinslow (2006) states that Logical (IT) security focusses on controlling access to an organizations' information, as well as controlling access to devices on which this data is stored and processed. The main goal of IT security is to ensure the confidentiality, integrity and availability (also known as the CIA-triad) of the data as mentioned by Kinslow (Aminzade, 2018; Yee & Zolkipli, 2021).

Firstly, confidentiality is aimed at protecting data from becoming accessible to unauthorized parties. (Digital) access control and data encryption are mainstream basic security measures for safeguarding confidentiality. Secondly, the integrity aspect focusses on the accuracy and trustworthiness of the data. It is focused on 'knowing' that the data that is visible for the end host and user is not tampered with. Control measures such as version control and data hashing can be implemented for increasing the integrity of data. The final aspect, availability, is focused on 'reachability' of data, ensuring that the technical infrastructure is functioning properly. In IT security, measures like hardware and software updating, implementing monitoring systems, and ensuring redundancy can be applied to increase data availability (Chai, 2023). The CIA triad has to be balanced, as a higher focus on one of the three aspects could negatively impact one (or more) of the other two aspects (Aminzade, 2018).

Both physical and digital security systems have been modelled in various manners. Network security is an important topic in IT security and is successfully modelled using game-theoretical models (Zhao, 2020; Zhu & Rass, 2018). Furthermore, the game-theoretical approach has been implemented to successfully create a routing model, used for distinguishing normal user behavior and malicious adversary behavior in a network of nodes (Kiran et al., 2020).

2.1.3. System Interactivity

The methods that have been discussed in section 2.1 (TVC, attack tree, game theory) each have a different level of interactivity within the method. Whereas TVC has proven to be very static, attack tree and game-theoretical analysis allow for modelling more interaction between the attacker and defender.

Modelling systems with game-theoretical and/or attack-tree techniques does, however, have its shortcomings. Game-theory suffers from a lack of scalability of the models, due to the limited number of system states and struggling in capturing system behavior when multiple attackers/defenders are modelled (Bommannavar, 2011; Chen & Leneutre, 2009). Furthermore, the approach remains relatively static, decreasing its applicability when the interaction between defenders and attackers has multiple stages (Liang & Xiao, 2013). Attack trees have been found to be similar to 'two player binary zero-sum' game-theoretical games (Kordy et al., 2011). They come with similar issues: lack of scalability, applicability and limited scenarios are also present when modelling security systems using attack trees (Lippmann & Ingols, 2005; Nagaraju et al., 2017).

Agent-based modelling (ABM) is a modelling technique that simulates the behavior of different model agents based on their surroundings, and set interaction rules. The ABM method can alleviate some of the limitations that are present in the aforementioned modelling techniques. In ABM it is possible for

agents to engage in complex interactions not only with other agents, but with the system environment as well (Janssen, 2005).

The ABM modelling technique has been applied in multiple researches for modelling various physical and logical security problems. Physical airport security systems have been analyzed using ABM, modelling malicious parties with explosive devices attempting to achieve as many fatalities in the airport as possible (Janssen et al., 2015; Janssen & Sharpanskykh, 2017). Using the model, the researchers successfully found measures that could be taken to reduce this risk, with a model being able to investigate the trade-off between security and airport efficiency. Another research on physical security with regard to crime in a city implemented an agent-based model able to predict areas in a city that have a heightened burglary risk (Malleson, 2012).

Logical and cyber-physical security have also been modelled using the agent-based modelling technique. An ABM has been designed in order to design a situation-aware system integrity protection (SIP) system in a 'smart' power grid, in order to better detect system anomalies and adapt (load-shred) when under attack (Wang & Govindarasu, 2020). They model entire substations as a singular node, as intra-node communication is not required for anomaly detection. Wang & Govindarasu (2020) successfully managed to develop an adaptive SIP that performs better on anomaly detection than a non-adaptive SIP.

Furthermore, ABM's have been used for performing a business model risk assessment with regard to cybersecurity (Ashiku & Dagli, 2020). In the model, an attacker attempts to capture a cyber-environment (existing of workstations, users, data volume, etc.) of a company, using various types of attacks. The research shows that the organisations' size plays a sizable role in increasing cyber-risk. Furthermore, more working hours increase the risk of identity fraud of users.

2.2. Modelling Security of Operational Technology in Critical Infrastructures

Critical infrastructures, like the gas industry, have become increasingly digitized over the past years (Alqudhaibi et al., 2022). This trend comes with multiple advantages, like increased safety- and operational performance, increased efficiency, automation and cost reduction (Denisova, 2019).

Due to the convergence of OT and IT systems, the physical and logical security fields are becoming increasingly interconnected. The cyber-attack surface of the system has increased, due to the large number of internet-enabled Industrial Internet of Things (IIoT) devices, sensors, actuators and programmable logic controllers (PLCs) in the process control system (Buzdugan & Căpățână, 2020; Kebande, 2022).

Traditionally, OT systems are designed for isolated use. The major objective of these systems was to "guard the asset base and its associated production". The lack of connectivity of the systems resulted in a deficiency in OT cybersecurity when compared to IT cybersecurity (Murray, Johnstone & Valli, 2017). The convergence of IT and OT results in co-called cyber-physical systems, integrating aspects of the IT domain with the OT domain. As a result of this increased IT/OT convergence, OT systems are now exposed to the risks that were previously only applicable in the IT domain (Christopher, 2023; Pospisil et al., 2021).

Mitigating the newly introduced risks for the OT domain is however not as straightforward as implementing 'IT-measures'. While measures such as proper firewall implementation significantly reduces some of the risks, applying IT security measures in an OT environment still creates a mismatch (Conklin, 2016). To solve this problem, Conklin (2016) suggests adding resilience to the CIA triad, which could help in enhancing the alignment of OT security measures and system control objectives. The CIA triad can also be applied 'as-is' to the domain of OT and cyber-physical systems. There is, however, a shift in balance between the three pillars: in OT, the availability and integrity of the services in the system are absolutely vital, whereas in IT there is an increased focus on confidentiality and integrity (Department of Energy, n.d.; Dhirani et al., 2021). This is due to the criticality of these systems for the functioning of society: it is more important that OT in critical infrastructures is reliably usable than having an unreliable system that keeps data confidential.

Another IT measure that has quite some potential to increase operational performance is adding redundancy and diversity to the system (Laszka et al., 2020; Soikkeli et al., 2022). Adding extra OT elements, which are slightly different from existing OT elements, while fulfilling the same purpose, combines two strategies. This could realize a reduction in monetary costs arising from cyberattacks, while increasing the operational performance of the system (Soikkeli et al., 2022). This could prove an interesting field of research when it comes to increasing cybersecurity in critical infrastructures.

In existing scientific research, a variety of critical infrastructures systems have been modelled using multiple modelling techniques. This research varies from a vulnerability analysis of a critical railway system (Johansson, Hassel & Cedergren, 2012), to the transition to an LNG-based energy supply (Chapping & Dijkema, 2010). Cybersecurity strategies in critical infrastructures have also been researched with several modelling methods, including system dynamics (Tweneboah-Koduah & Buchanan, 2018), game theory & network analysis (Paté-Cornell et al., 2018), and agent-based modelling (Rybnicek, Tjoa & Poisel, 2014). The studies from 2018 have a main focus on the security in energy and electricity grids, while the 2014 research is focused on general importance and interconnectedness of different types of critical infrastructures in relation to cybersecurity. None of these researches however, are aimed at improving cybersecurity in OT systems through redundancy.

There is quite some scientific research stating the necessity of adding redundancies in order to safeguard critical infrastructures (Berkeley & Wallace, 2010; Laszka et al., 2020; Sotirios, 2022; Tranchita et al., 2010). Very little research, however, implements modelling techniques to implement and test different redundancy strategies, especially when it comes to LNG infrastructures. Research that is focused on modelling redundancy in critical infrastructure systems is presented by Horowitz & Pierce (2013) combining the system dynamics modelling technique with redundancy in the security of cyber-physical systems, aiming to improve the system operators displays. This research is, however, not related to a specific infrastructure.

3. Methodology

In this section, the research approach for answering the research question and the sub-questions as described in section 1.1 is addressed. Furthermore, in line with the suggested approach, the methods required to successfully answer the research questions will be discussed, as well as the tools and data required for successfully implementing these methods. Finally, the limitations of the research design are described.

3.1. Research Approach

An important dichotomy can be highlighted when it comes to the nature of the formulated sub-questions. The first two sub-questions are relatively descriptive: they describe OT in general and in Gate terminal, as well as the role attackers and defenders have when it comes to OT in the industrial processes of Gate terminal. The third and fourth sub-question are, however, more explorative. Answering these sub-questions involves designing a suitable model of the system, as well as experimenting with different redundancy strategies.

As a result of the dichotomy present in the four sub-questions, multiple modes of inquiry are required in order to successfully answer all sub-questions. Because of the need for multiple modes of inquiry, a 'mixed methods' research design is required (Creswell & Creswell, 2018). For answering the first two sub-questions, a combination of the qualitative observational approach and the evidence synthesis modes of inquiry are used. This allows for identifying and researching of the role OT has in industrial processes, as well as the effect that cyber-attackers and system operators have on the performance of the system. As such, the combination of these approaches can successfully be used to answer the first two sub-questions.

Using the results acquired through the qualitative observational and evidence synthesis modes of inquiry, a quantitative simulation model can be made. The Agent-Based Modelling (ABM) technique is used to model the operational processes at Gate terminal, and simulate the performance of the system when faced with cyberattacks. These results will constitute an answer to the third sub-question. For answering the fourth sub-question, the quantitative simulation approach is once more applied. This time, the constructed ABM will be simulated when configured with different redundancy-related strategies.

3.2. Research Methods

The first sub-question, assessing the role of OT within Gate terminal, as well as investigating the importance of OT in industrial processes in general, can be answered using two main methods. Firstly, the role of OT in industrial processes in general can be researched through a literature synthesis, providing insights into IT/OT convergence, control loops, et cetera. OT within Gate terminal can be identified through expert interviews with OT specialists, as well as conversations with Gate terminal employees from various branches.

The second sub-question, identifying attacker and defender behavior, and analyzing the impact this behavior may have on the operational performance of the system, will be answered through a literature synthesis. The synthesis will result in an overview of different actions an attacker and defender can perform, the type of attack(s) that the adversary attempts to launch, as well as the expected impact the actions of the attacker and defender have on the system.

The insights and information retrieved through the literature synthesis and the case study on OT within Gate terminal, combined with the knowledge retrieved about different attacker and defender behaviors will form the basis of the ABM. A conceptual model of the OT within Gate terminal will be constructed, after which the model will be operationalized and implemented in a full-fledged ABM. For the implementation of the model, a software package called NetLogo will be used. The modelling process, including conceptualization, operationalization, implementation, verification and validation is to be seen as

an incremental, iterative process. After the sensitivity of model outputs to deviations in model inputs is analyzed, various redundancy strategies will be constructed. These will be used as model inputs for experiments. The behavior of the ABM and the performance of the system when experimenting with various redundancy strategies provide the results for the third and fourth sub-questions, respectively.
In Figure 1, a schematic research flow diagram for the research is presented.

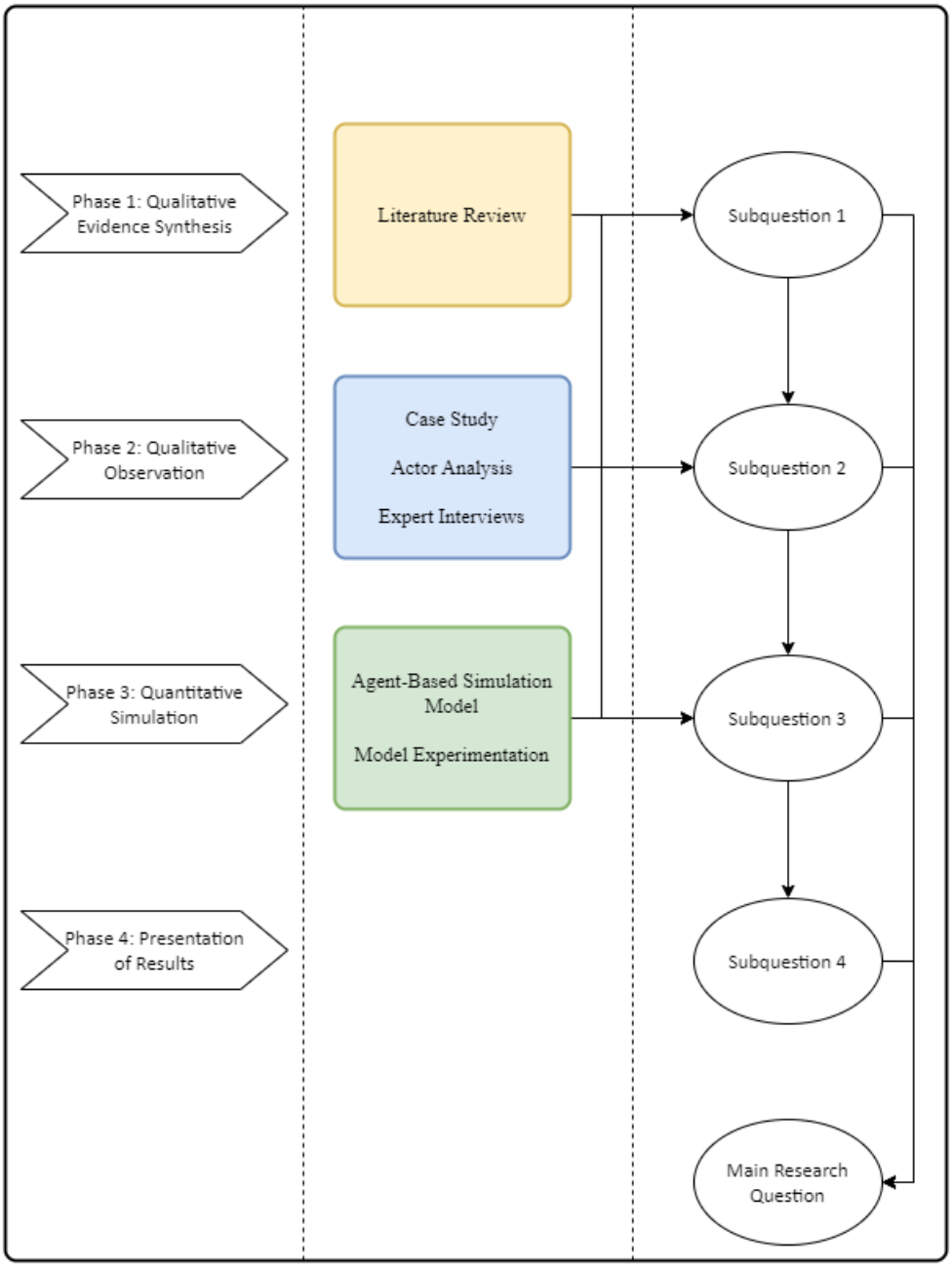


Figure 1: Research Flow Diagram

3.3. Data Requirements

In order to successfully be able to formulate answers to all research questions, several types of data have to be collected. For answering the first research question, aside from data retrieved from synthesizing scientific literature, reliable expert interviews have to be performed. The interviewees will be accessed through an internship position at Gate terminal.

Aside from data provided by the interviewees, internal company documents can be synthesized, allowing for a good insight into the industrial processes at Gate terminal, as well as the OT and control loops that are present in these processes.

Finally, data about attacker and defender behaviors has to be collected through literature synthesis. Measures taken to defend a system from cyberattacks, as well as data on steps for recovering a system after a successful attack has to be collected. Furthermore, information on attacker behavior has to be collected, for example about types of applicable cyberattacks and the spread of a disruption through a network.

4. Operational Technology in Industrial Processes

This chapter aims to describe the role that OT plays in industrial processes, as well as the impact that the ever-increasing convergence of the IT and the OT domain has on these industrial processes. Furthermore, the industrial processes at Gate terminal, as well as accompanying OT and control loops in the processes of the plant are identified and described. Using these findings, an answer to the first sub-question *"What is the role of OT in the industrial processes of Gate terminal?"* can be formulated.

4.1. Background

Processes in critical infrastructures, such as the Dutch LNG industry, have become increasingly digitized over the past years (Alqudhaibi et al., 2022). The industrial equipment and operational processes that are implemented throughout the critical infrastructures are monitored by hardware and software. These monitoring and controlling elements are called OT (Gartner, 2015). Digitization of industrial processes and OT comes with multiple advantages, including increased safety- and operational performance, increased efficiency, automation and cost reduction (Denisova, 2019).

The digitization and automation of operational processes is a part of what has become known as the fourth industrial revolution, or "industry 4.0". In industry 4.0, industrial processes are driven, controlled, monitored and improved by implementing technological developments, such as Internet of Things (IoT), cloud computing, big data and blockchain (Frank et al., 2019; Kumar & Nayyar, 2020). Successful implementation of these technological developments results in connected production chains, and allows for 'smart manufacturing', and overall 'smart supply chains' (Dornelles et al., 2022). In industrial applications, enabling this smart industry, Industrial Internet of Things (IIoT) devices are used in order to complement monitoring and control systems in OT in the industry (Agrawal & Kumar, 2022).

OT mostly consists of Industrial Control Systems (ICS). These systems include all (sub)systems that are used to monitor and control industrial processes (Williamson, 2015). The monitoring and controlling of industrial processes is organized as follows:

Using data provided by the IIoT devices, Cyber-Physical Systems (CPS) are used to perform computational and physical operations to the monitored systems (Al-Salman & Salih, 2019). CPS implement programmable logic controllers (PLC) in order to manage process control variables. These PLCs can alter the state of a monitored system using an actuator, based on the perceived state of the system (DeGuglielmo et al., 2020). A visualization of this process is presented in Figure 2. The PLCs, in turn, are monitored by a supervisory control system, such as a Supervisory Control and Data Acquisition system (SCADA) or Distributed Control Systems (Ali et al., 2018). The main differences between SCADA and DCS systems, are the scale of implementation. SCADA systems are typically implemented for large-scale industrial systems, such as entire power grids, centralizing their control. DCS systems, on the other hand, are used for smaller-scale industrial processes, providing faster control than SCADA due to their operation in higher bandwidth networks (Finnan & Nakagawa, 2021).

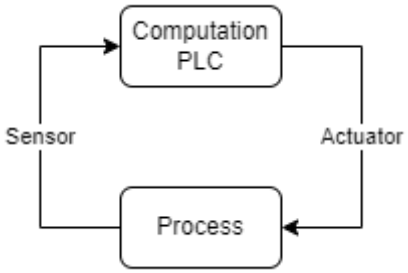


Figure 2: Cyber-Physical System / Process Control Loop

In order to further explain the implementation of OT systems, as well as IT/OT convergence, a typical IT/OT network is shown in Figure 3 (Colbert et al., 2017). The figure is based on the Purdue Enterprise Reference Architecture (PERA) model (Williams, 1994). The PERA model provides a framework for designing ICS networks in the context of OT in critical infrastructures, and introduces six different network levels in the environment (Mathezer, 2021):

Level 5: Enterprise Networks, providing corporate-level services such as email
Level 4: Business Networks, an IT network for business users
----------IT/OT Boundary----------
Level 3: Site-Wide Supervisory: providing monitoring & supervisory for a site or region
Level 2: Local Supervisory: providing monitoring & supervisory for a single process, line, or DCS
Level 1: Local Controllers: providing devices & systems for automated control, such as PLCs
Level 0: Field devices: providing sensors & actuators for local controllers

When analyzing the figure from top to bottom, first we find a demilitarized zone (DMZ), delineating an organization's network from the internet through a firewall, in which the enterprise network is located. Next, the business networks, including corporate servers and workstations are located. Then, another DMZ is implemented, with the goal of creating a boundary between the organizations' IT and OT.

When passing the second firewall located in the industrial operations DMZ, OT territory is entered, presenting us with levels 3 and 2 of the PERA framework. At this level, SCADA and/or DCS systems are present, having the highest level of control in OT. These systems control basic/logical controllers, illustrated as PLCs. These, as previously shown in Figure 2, form control loops using the sensors, actuators and equipment on site.

In Figure 3, several key design decisions are depicted. First off, it is important to note that the Safety Instrumented System (SIS) is separated from process control at level 1. The SIS has its own network and, as a result, can execute safety features such as a controlled shutdown, even while the PLCs are in an inoperable state. The second key design decision is the separation of IT and OT with a DMZ. This increases the difficulty for attackers to reach OT systems when IT is compromised, as well as ensures that OT can be functional when failures occur in the organizations' IT environment.

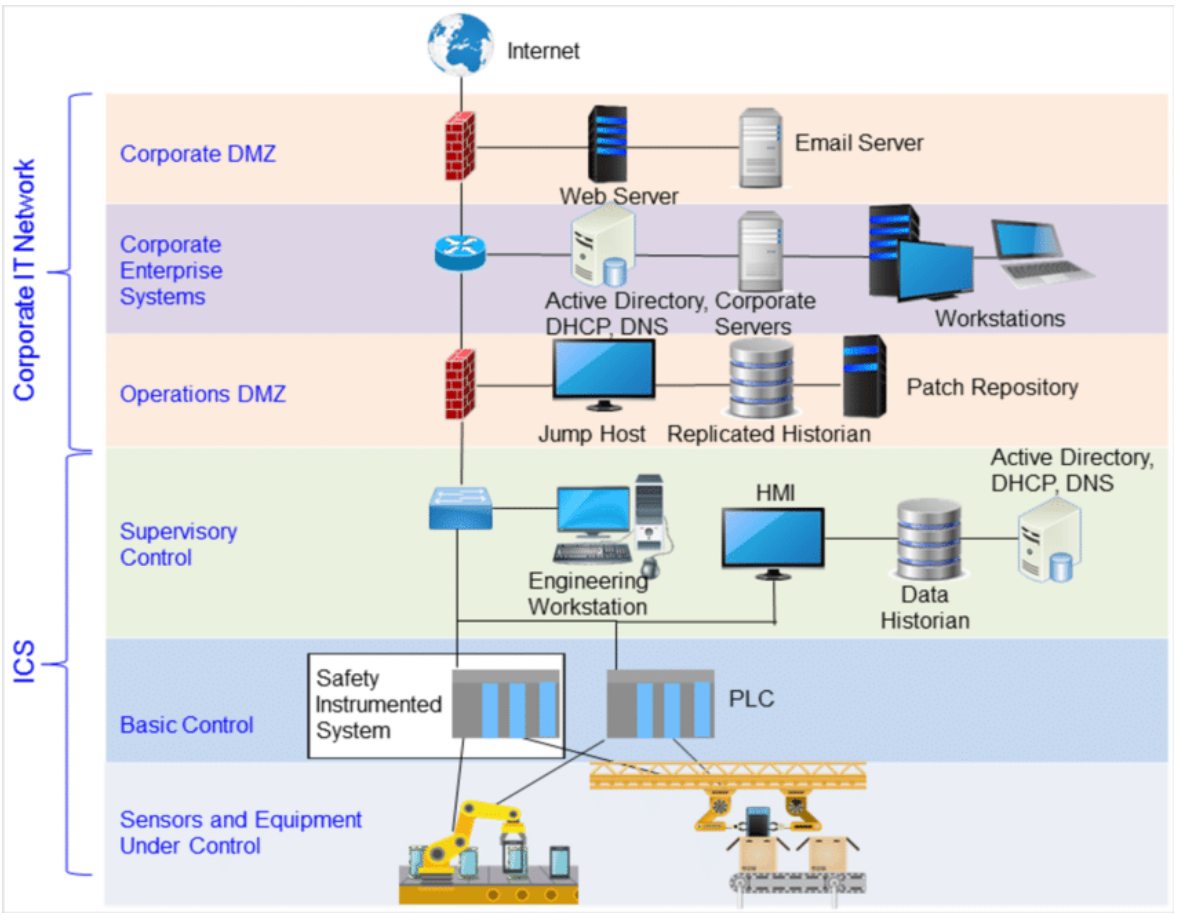


Figure 3: Network Architecture IT OT (Colbert et al., 2017)

While industry 4.0 offers a vast set of advantages in the form of smart manufacturing, the increased digitization of industrial processes does have some pitfalls that may have a significant impact on industry functionality. The cyber-attack surface of the system is increased, due to the large number of internet-enabled IIoT devices, sensors, actuators and PLCs in the system (Buzdugan & Căpățână, 2020; Kebande, 2022). Traditionally, OT systems are designed for isolated use. The major objective of these systems was to "guard the asset base and its associated production". The lack of connectivity of the systems resulted in a deficiency in OT cybersecurity (Murray, Johnstone & Valli, 2017). Now that OT systems have become increasingly connected, OT systems are now exposed to the risks that were once only applicable in the IT domain (Christopher, 2023).

4.2. Gate Terminal

Gate terminal B.V., founded in 2011, is one of the largest LNG terminals in Europe, and the main importer of LNG in the Netherlands. Located at the port of Rotterdam, the company is responsible for processing more than 1/3rd of the Dutch natural gas consumption, while simultaneously supplying Northwestern Europe with natural gas (Gate terminal, n.d.a.). Furthermore, the industrial processes at Gate are certified for use with bio-LNG (Gate terminal, 2021). This reduces the environmental impact of the LNG, as it helps to reduce CO_2-emissions.

Gate terminal is a joint venture between N.V. Nederlandse Gasunie and Koninklijke Vopak N.V., both large companies in the gas infrastructure and storage industries, respectively (Port of Rotterdam, n.d.).

With a capacity of 12 billion cubic meters per year (BCMA) and plans for expansion, Gate terminal aims to play a pivotal role in achieving and maintaining security of supply in Northwestern Europe when it comes to LNG (Vopak, 2022).

4.2.1. Industrial Processes at Gate

In the following section, the industrial processes of Gate terminal are identified. In conjunction with these industrial processes, the process variables and control loops in the processes are identified and clarified. Information that is specific to Gate terminal is gathered through several conversations with experts from within the company.

The industrial processes at Gate terminal can be divided into five main tasks (Gate terminal, n.d.b.):

1. Unloading LNG carriers
2. Storing LNG
3. Regasification and distribution of LNG through the gas pipeline
4. Vessel- and truckloading
5. Reloading LNG carriers

In the following section, these five main tasks are further examined.

Unloading LNG carriers

One of the main processes at Gate terminal is the unloading of LNG. Large carriers with a capacity of up to 270.000 m^3 LNG can dock at one of Gate's three jetties (Gate terminal, n.d.c.). The carrier has to dock (and remain) in a specific range of the jetty, in order to be able to unload its LNG. The exact location of the ship is monitored using proximity sensors. When the carrier is in the required range, up to three hydraulic unloading arms may be attached to the ship. These unloading arms will detach whenever the carriers drift off out of the desired range, in order to prevent any damage to the unloading arms and LNG leaks. If the valves in the unloading arms and at the carrier are opened, LNG flows to the tanks on site, while boil-off gas (BOG) returns to the carrier, in order to keep the pressure in the carrier in the required specification. The main process variables that are monitored and controlled at the jetties are LNG flow and backflow, temperature, pressure, carrier location and carrier LNG level. Furthermore, in all of the industrial processes, electrical current is measured: the current needs to remain within equipment specifications to prevent a shutdown of the processes. All data on the process control variables is sent to the DCS, where the industrial processes are monitored, and from where the valves of the unloading arms can be controlled.

Storing LNG

After the liquid, which is currently ± -160 °C, is unloaded from the vessels, it is stored in the three LNG tanks that are on the plant. The tanks have a concrete outer layer, a layer of thick insulation, and a steel inner tank in which the LNG is stored (Gate terminal, n.d.c.). The tank pressure, LNG level, and temperature of the LNG are monitored using various control loops. To prevent the dense liquid from regasifying in the tanks, the LNG is kept around cryogenic temperatures. In order to avoid actively having to cool the tanks, a process called 'auto-refrigeration' is implemented. In this process, through the continuous draining of BOG from the upper portion of the tank, the pressure, and therefore the temperature in the tank, is kept constant (Dobrota et al., 2013). The BOG is then either compressed using BOG compressors (reliquefying the gas) and pumped back into the tanks, or distributed to the gas network. Aside from pressure, level and temperature, several other factors are measured at the three tanks. The mixture of the LNG in the tank is monitored and controlled, due to 'weathering' (altering composition) of the LNG. Furthermore, the outflow towards the gas network (see next section) is monitored in the tanks, as well as electrical current of components in the tank.

Regasification and distribution

The vast majority of the LNG that is processed at Gate terminal is regasified and pumped into the underground gas network. When LNG is regasified, 1 m^3 of LNG is equal to about 600 m^3 of regular natural gas. In order to quickly be able to heat up the LNG to above its boiling point, Gate uses seawater as a heat exchanger. Seawater pumps located at the facility pump seawater towards open-rack vaporizers (ORVs). LNG is pumped out of the storage tanks using a low-pressure pump located in the tank, and flows upwards through an ORV. The seawater flows downwards through the ORV, heating up the LNG. When the LNG is sufficiently heated, it vaporizes and turns into regular natural gas. Once the LNG is regasified, the energy content of the gas is measured, which may differ due to the mixture of LNG. Finally, the gas is pumped into the high-pressure underground gas network. This industrial process is responsible for the main portion of the annual send-out of Gate terminal. For the seawater pumps, only a few process control variables are monitored and controlled: the (output) water pressure of the pumps is monitored for assessing the operability of the group of pumps. Furthermore, pump vibrations are monitored, as well as the electrical current in the pumps. At the ORVs, flows of the seawater and LNG/NG are monitored, as well as the temperatures of the seawater and LNG/NG.

Vessel- and truckloading

As an alternative to regasification and distribution of LNG through the pipeline, LNG is also loaded in vessels and trucks. While jetty 1 and jetty 2 are mainly used for large LNG carriers, the smaller vessels dock at the third jetty, which is mainly used for loading smaller vessels with LNG. After the LNG is loaded in a vessel, the vessel ferns to a carrier further down the harbour and supplies it with LNG. The carrier, in turn, uses the LNG as fuel. In the truckloading area at the plant, LNG retrieved from one of the storage tanks is loaded into trucks at one of the truckloading bays. Using the trucks, LNG is transported to the hinterland. At the vessel- and truckloading bays, the following process control variables are measured: temperature, flow, level, pressure and electrical current.

Reloading LNG carriers

The final industrial process at the plant is the reloading of LNG carriers docket at one of the three jetties. Two different processes are in place to fulfill this task. Firstly, the LNG can be reloaded instantly after it is retrieved from a carrier docked at another jetty. When LNG is reloaded using this method, it does not have to be temporarily stored in one of the three tanks, as a pipeline connecting the different jetties can be used. The second method of reloading an LNG carrier is the most common method, retrieving LNG from one of the three tanks and reloading it in the docked carrier. In order to reload the LNG, the same arms as the arms used for unloading LNG can be utilized. During this process, the same process control variables as used in the unloading of LNG are measured and controlled.

4.2.2. OT at Gate terminal

At Gate terminal, in the supervisory control layer denoted in section 4.1, a DCS is implemented, which is controlled from a Cargo Control Room (CCR). The decision for implementing a DCS instead of a SCADA system, is based on several factors. SCADA systems are usually implemented for high-level monitoring of industrial processes at a larger scale, which are often located at multiple remote locations. DCS systems, on the other hand, are mainly used for monitoring and controlling local, smaller processes, but with a greater level of detail. This allows for a higher level of control over the monitored system. As a result, process operators that use a DCS system are able to precisely manage industrial processes, such as those taking place at Gate terminal. The higher bandwidth resulting from the use of a decentralized system enables real-

time control of the industrial processes, which is vital for managing and enforcing various conditions on the plant.

At Gate terminal, multiple PLCs, sensors and actuators provided by a variety of different vendors are connected to the DCS. In each of the processes as described in section 4.2.1 multiple control loops are in place, which control and maintain various process variables (pressure, temperature, flow, etc) at the plant. These process control variables are monitored and controlled via the DCS. So-called KVM (keyboard, video, monitor) switches are implemented to supply the data provided by the various control loops to the DCS, as well as to display the data on the various monitors in the CCR.

There are two main SIS implementations at the terminal, an Emergency Shutdown system (ESD) and a Fire and Gas System (FGS). Whereas the DCS is used for controlling 'regular' operations, the ESD and FGS systems are failsafe systems. When sensor values (i.e. pressure) become extreme, the ESD can shut down operations in order to avoid unsafe situations, independently of implemented PLCs. The FGS system is used to monitor gas leaks and monitor and prevent any sort of fire on the plant.

4.3. Findings

In this chapter, the rise of OT in industrial applications, OT concepts and the network architectural structure behind OT have been discussed. Furthermore, the different industrial processes at Gate terminal and relevant OT in these processes have been discussed.

OT consists mainly of ICS, which implements a DCS or SCADA system to control process variables at an industrial plant. To this end, control loops that are operated through the DCS or SCADA systems are implemented, managing various process variables through sensors, actuators and PLCs.

While the rise of OT comes with numerous advantages, including automation, efficiency, and improved operational performance, the increased attack surface of the system and increased interconnectivity makes Industry 4.0 susceptible to cyber threats that were previously only applicable in the IT domain. A part of these threats is mitigated through the implementation of a layered network architecture, enhancing network segmentation and security.

Gate terminal is the largest LNG terminal in the Netherlands and is responsible for more than 1/3rd of the Dutch national gas supply. The company, located at the port of Rotterdam, has a sizable OT infrastructure that is used to manage the various industrial processes at the plant. The main industrial processes at the plant are the (un)loading of LNG carriers, vessels and trucks, storage of LNG, as well as regasification and distribution of the liquid. The company manages these processes using a DCS, which is used to control and monitor various process control variables, including pressure, temperature, flow and electrical current.

5. Attacker and Defender Behavior

Now that an overview is present of OT in industrial processes, such as the Dutch LNG infrastructure, it is important to examine the role attackers and defenders have in these systems. More precisely, the impact of attacker and defender behaviors on the operational performance of (critical) infrastructures is to be analyzed, with the goal of successfully answering sub-question 2: *"How do different attacker and defender behaviors impact the availability of industrial processes of Gate terminal?"*.

To this end, this chapter will first focus on different types of attackers, their incentives and the nature of possible attacks. Furthermore, the defender's incident response cycle is established, highlighting the different actions a system operator can perform in order to prevent or mitigate the effects of attackers on the system.

5.1. Attacker Behavior

In this section, the behavior of cyber attackers in the context of OT in critical infrastructures is described. Firstly, the incentives of these attackers are outlined, elaborating on various driving factors behind attacker behavior, ranging from bragging rights to the destruction of infrastructures. Furthermore, this chapter elaborates on different types of attacks that could play a role in the system, and the potential impacts these attacks may have.

5.1.1. Attacker Incentives

When it comes to the classification of types of cybersecurity threats, six different types of threats can be identified. The types are increasingly malicious and have an increasing impact on the system. Each of the classifications comes with its own incentives (Lehto, 2022):

1. Cyber vandalism

Cyber vandalism entails unorganized individuals hacking computer systems as they find it an 'enjoyable challenge'. The main incentives for these hackers are egoistic, such as bragging rights, reputational gains and showing off.

2. Cybercrime

Cybercrime is aimed at making money by committing crimes using a computer, for example through fraud or extortion. A ransomware attack is a good example of cybercrime that can be used in order to extort users for monetary gains. These monetary gains are the main incentive for cybercrime.

3. Cyber espionage

Cyber espionage is focused on gaining sensitive information from another party, such as governments or corporate organizations. This information is then used for multiple goals, such as knowledge, monetary gain, et cetera. The main incentives for cyber espionage are knowledge and power.

4. Cyber terrorism

Cyber terrorism occurs when terrorists launch cyberattacks, aiming to further their own goals by inducing terror among the public. This, for instance, could happen through temporarily disabling access to critical infrastructures, or tampering with control system setpoints (target process control variables). This could cause control processes to fail, resulting in physical damage.

5. Cyber sabotage

In the context of critical infrastructures, cyber sabotage occurs when a state, a state-sponsored group or hacktivists aims to sabotage the functionality of critical infrastructures. This could have a variety of incentives. The main goal, however, is to paralyze or destroy critical infrastructures through cyberattacks.

6. Cyber warfare

Cyber warfare is the occurrence of a cyber threat, in which state actors attack other states during a period of war between these states. The cyberattacks are a part of military operations, and (in critical infrastructure context) are aimed to destroy or disrupt the other state's critical infrastructures.

Traditionally, financial incentives have been the main driving force behind cyberattacks (Jaquet-Chifelle & Loi, 2022). This can easily be illustrated by the example of ransomware, a piece of malware that locks a victim's computer and/or data, attempting to extort a user in exchange for unlocking their data (O'Kane et al., 2018). When it comes to critical infrastructures, different incentives for attackers are at play.

Critical infrastructures are vital for a society, due to their interconnectivity and their importance for public welfare (Pursainen, 2009). This vitality is the main reason why these infrastructures form an attractive target for malicious parties to disrupt or destroy. To demonstrate this, the hack on the Ukrainian power grid in 2015 is considered. It is a popular example of attacks on critical power infrastructure, where Russian hackers managed to black-out the Ukrainian energy grid for multiple hours (Kshetri & Voas 2017). Among other things, energy outages like this can have a substantial impact on a country's production, military and population (Lewis, 2011). This is a substantial incentive for ill-willing parties to attempt to discover and exploit any vulnerability in the digital components of the system. Due to the critical nature of the LNG industry for the functioning of society and the incentives that are present, the threats to OT in this infrastructure are likely to fall into one of the later classifications as earlier identified, such as cyber terrorism, sabotage or warfare.

5.1.2. Threats

When falling back on the CIA triad, cybersecurity threats are typically targeted at one of the three pillars. In OT, as described in section 2.2, availability and integrity are the two most important pillars. Furthermore, availability and integrity are the most closely related to the RAMSSHEEP criteria (see section 6.3.2). Therefore, it is interesting to further investigate threats that impact the availability and integrity of OT.

A problem arises when attempting to investigate the threats that affect the operational performance of OT in industrial processes. Companies are hesitant to share data with regard to cyber-incidents, deteriorating the quality of available threat information (Solak & Zhuo, 2020). While threat intelligence data comes with its inaccuracies, the ICS focused cybersecurity company Dragos points out that main threats are ransomware attacks and exploitations of existing vulnerabilities (2023). Consequences of these threats are similar to those of a denial of service attack, affecting the operability of processes in industrial organizations.

A Denial of Service (DoS) attack is defined as 'the prevention of authorized access to resources of the delaying of time-critical operations' (NIST, n.d.b.). Such an attack has a major impact on the availability of a system: if access to the service is denied, it cannot be controlled and is therefore unavailable to the system operator. This may result in significant monetary and non-monetary losses for the system operator and other actors that are dependent on energy supply.

When discussing a DoS attack, the most common association is making systems inaccessible through a system overload: systems are overloaded by traffic, causing the legitimate user to not be able to

access the system. There are, however, other means of achieving these goals, such as the destruction of physical equipment, denying the ability to fix, account theft or interference (NCSC, n.d.a.).

The first of these three types is quite interesting, as it aims to physically destruct physical equipment through a digital hack. An example of this is the (relatively simple) overloading of circuit breakers in power grids, or the sophisticated Stuxnet worm. Stuxnet is a piece of malware, created jointly by the United States and Israel and discovered in 2010. Their goal was to disrupt the nuclear program of Iran by infecting their SCADA and PLCs, physically damaging centrifuges used in the nuclear program (Baezner & Robin, 2017). Stuxnet was one of the first of its kind in targeting ICS systems.

While the aforementioned threats are usually aimed at the short term, temporarily disrupting IT or OT systems, there are other important threats at play that are executed over a longer period of time. The advanced persistent threat (APT) is an example of this, and is used for infiltration of critical infrastructures and other systems over a prolonged period of time. Stuxnet, the earlier described worm, is an example of an APT, that has been used to destruct physical equipment. An APT is a highly sophisticated targeted cyberattack, that is strategically executed by a coordinated group of threat actors (NIST, n.d.a.). These threat actors are often nation-states or state-sponsored groups, and have access to high levels of knowledge and other resources to infiltrate IT and OT systems. The goal of an APT is to gain undetected longer-term access to a system using a variety of vulnerability exploits. The access can be used in order to exfiltrate information, or to impede critical aspects of a mission, program or organization, now or in the future (NIST, n.d.a.). In the case of critical infrastructures, APTs are most likely used for the goals of cyber espionage, -sabotage and -warfare, as described in section 5.1.1.

5.2. Defender Behavior

The main task of the defender in the system is to limit the damage that can be done to the system through successful cyberattacks, also referred to as incidents. In a company setting, the tasks of the defender (or system operator) are often performed by a chief information security officer (CISO) and their team. In order to limit the impact that can be done through incidents, it is vital for the defender to have implemented an incident response procedure or framework.

For incident response, there are two main frameworks that are commonly used (Voigt, 2018). The first framework, presented by the National Institute of Standards and Technology identifies four key steps that have to be executed properly in order for the defender to adequately handle cyber-incidents in their systems (Chiconski et al., 2012). The framework is shown in Figure 4. The first step in the framework is preparation for incidents, including actions such as personnel training and ensuring security protocols are in place to prevent incidents from happening altogether through prevention systems. Consequently, detection and analysis have to be performed, involving locating incidents and assessing the damage. After this knowledge is available, the next step is to contain and eradicate the incident, and to aptly recover the system in order to restore it to a fully operational state. Finally, after the incident is resolved, the defender is to perform post-incident activity, reviewing and incrementally improving the implemented incident response procedure with lessons learned from the handled incident.

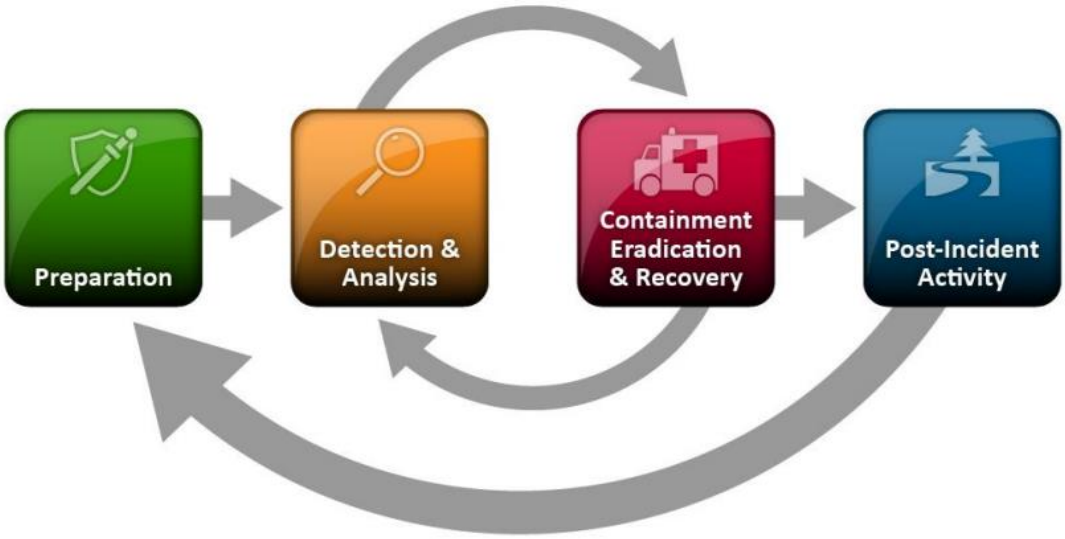


Figure 4: NIST Framework for Incident Response (Chiconski et al., 2012)

The second framework, provided by the SANS institute (Kral, 2021), is quite similar to the NIST framework. The main difference is to be found in the third step: instead of combining containment, eradication and recovery in one step, the SANS framework separates these actions into three different steps. The key difference between the framework is therefore the sequencing of the steps: whereas in the NIST framework the containment, eradication and recovery happen simultaneously, the steps can only be performed sequentially (Voigt, 2018).

In the following section, the steps of the NIST framework are further highlighted, and applied to the field of OT.

5.2.1. Preparation

The preparation phase is vital to the process of incident response. The main goal of this step is to increase the 'cyber preparedness' of the defender, which is essential for the mitigation of cybersecurity incidents (Maras, 2021). Cyber preparedness is crucial to having an effective cyber strategy (Kugler, 2009). An unprepared and/or poorly defended system is likely to have more difficulty in dealing with incidents. The preparation phase ensures that a trained, qualified incident response team is in place, which is sufficiently capable of fulfilling all next steps in the framework. Furthermore, in the preparation phase, all equipment that is required for handling incidents is to be gathered, inspected and tested.

Cyber preparedness does not end at organizational aspects, however: prevention of cyberattacks plays a large role in this step too. Through the implementation of so-called preventive controls, the defender is able to filter and block cyberattacks before they enter the system. The main preventive control that can be implemented by a defender is an intrusion prevention system (IPS). An IPS is a tool that is installed at hosts or around a network, which monitors incoming network activity, and blocks malicious traffic before it can enter the system. Hereby, an IPS protects the network and system in real-time, forming the first line of defense against malicious actions (li & Liu, 2010). Other measures, such as protecting systems through ensuring up-to-date firmware and increasing end-user awareness can also contribute to the companies cyber-preparedness, and are therefore also a part of the preparation phase.

5.2.2. Detection and Analysis

When the proper preparations have been made by the defender, and an attacker still manages to successfully attack a system, a cyber-incident occurs. It is important that the defender is capable of handling any incident, however, the defender should focus on the capability of handling attacks that are entered using commonly used attack vectors (Email, attrition, web, etc.). The first important step for the defender to be taken after an incident has occurred, is to become aware of the incident: if a defender isn't aware of an ongoing attack on its systems, it cannot be dealt with properly, potentially resulting in an increase in losses occurred from the attack.

The most commonly implemented system for becoming aware of ongoing cyber incidents is an intrusion detection system (IDS). The goal of IDS systems is to detect intrusions with the goal of catching attackers before they can damage a system in any way (Lutkevich, 2021). IDS systems implement two different detection methods for identifying potential cyber incidents (Einy et al., 2021):

1. Signature-based detection

Signature-based detection works by comparing behavior displayed by the system with a set of known attack patterns (also referred to as signatures). When the IDS finds a match between the behavior of the system and the database of known signatures, the IDS is triggered, raising a flag for a found intrusion.

2. Anomaly-based detection

Anomaly-based detection operates fundamentally different from the signature-based detection method. When anomaly-based detection is utilized, the IDS compares the current behavior of the system to known baseline system behavior using data-analytical techniques. If the current behavior of the system is considered 'abnormal', the IDS raises a flag.

The Problem of Intrusion Detection Systems

While signature-based detection is suitable for recognizing known signatures of an attack, attacks are often slightly different. Therefore, they are not always recognized through signature-based detection, as these altered signatures are not present in the reference database yet. Furthermore, while anomaly-based detection is theoretically capable of recognizing these new attacks due to anomalous behavior, this detection method comes with its own problems: the process of becoming aware of ongoing incidents is the most complex and problematic part of the incident response process. This is a result of three different factors (Chikaskia et al., 2012):

1. The multiplicity of means of identification, each with its own level of accuracy and detail.
2. The high volume of indicators of incidents.
3. The specific technical knowledge and experience required for identification and analysis.

Detection accuracy is a crippling factor for IDS systems. There is a large amount of traffic and activity that is to be monitored by the IDS. As a result, even an IDS that is > 95% accurate will still produce a large number of false positives, increasing the amount of manual labor for system operators. This problem often renders IDS systems impractical for real-world systems (Yahalom et al., 2019). This problem can be (slightly) alleviated using intelligent intrusion detection systems, and system operator training of the IDS (Shenfield et al., 2018; Halimaa & Sundarakantham, 2019).

IDS implemented for detection evolved to the IPS that are implemented in the first step of incident response. The main difference between the two is the fact that an IPS is implemented in-line with the flow of traffic

and can therefore immediately take action and block access, while IDS is mainly used out of band, for monitoring and raising the awareness of the system operator (Ashoor & Gore, 2011).

5.2.3. Containment, Eradication, Recovery and Post-Incident Activity

When a threat has been identified by the defender, he has to deal with the threat accordingly. The first action to be taken when an incident occurs, is containment. This will help in mitigating the impact that the incident will have on resources, system availability and overall attack damage (Chiconski et al., 2012). Containment strategies will differ, depending on the type of the incident: a full-blown ransomware attack requires a different containment strategy than a data leak or a man-in-the-middle attack. While the containment strategy may differ for different types of incidents, the main goal of containment strategies does align. The goal is to limit the amount of damage to the system that can be caused by the incident, by avoiding the spread of the incident throughout systems.

After the incident is contained, the defender has to take steps to remove the incident from the system. During this step, it is important to ensure that any and all components that are affected by the incident are cleared of any contamination. Ultimately, all access an attacker has to a system (if any) is to be denied. The combination of these two steps should ensure the removal of the incident from the affected system. Finally, only after the incident has been eradicated, the affected system has to be restored to its original operating condition. The steps taken to recover the system also vary per incident type. A key part of restoring the system is preventing it from being exploited from the same vulnerabilities again. This step includes actions like patching the exposed vulnerabilities, and tightening network perimeter security (Chiconski et al., 2012).

Finally, after the systems have been completely recovered, it is time for the system operator to perform post-incident activities, reflecting on the entire incident response cycle, including both organizational and technical aspects. This reflection is useful for increasing the capabilities of the system operator to improve the process of dealing with similar incidents. For instance, using information gathered about the incident the IPS and IDS systems can be improved, reducing the likelihood of a similar incident from happening in the future.

5.2.4. Redundancy and Attack Surface

One of the main goals of a system operator in a cybersecurity context is to avoid as many attacks as possible. Furthermore, the system operator aims to mitigate the impact of successful cyberattacks on the operational performance of a system. To achieve this goal, the defender can use various means. While hardening (strengthening individual system components) is a widely-used mean that can be used to partially achieve this goal, the importance of redundancy and diversity is not to be overlooked (Laszka et al., 2020; Soikkeli et al., 2022): combining these two strategies could realize a reduction in monetary costs arising from cyberattacks (Soikkeli et al., 2022). The integration of additional components, using multiple different implementation variants in the architecture of IIoT systems is therefore an interesting strategy to examine when it comes to Gate terminal.

When considering the implementation of redundancy and diversity, an interesting observation comes to light. A defender of a security system aims to avoid as many cyberattacks as possible. Reduction of the attack surface of the system has traditionally been an effective tool to reduce the likelihood of an attack on the system (Manadhata & Wing, 2004). Adding redundancy and diversity in a security system does exactly the opposite: it increases the attack surface of the system, through the addition of potential entry points for an adversary (Kebande, 2022). Therefore, there seems to be a trade-off between adding redundancy and reducing the attack surface of an OT system. One of the goals of the model is to explore

this trade-off, and to investigate what redundancy-related strategies are effective for increasing the operational performance of OT at Gate terminal.

5.3. Findings

In this chapter, possible behavior exhibited by attackers and defenders in cybersecurity context has been described.

There is a multitude of malicious parties that have a wide range of possible incentives to attempt to hack and disrupt cyber systems. These incentives range from smaller-scale cyber vandalism, where individuals are hacking to embrace the challenge, to full-out cyber warfare, where cyberattacks are part of military operations.

Availability and integrity of services and data are vital when it comes to OT. Ransomware attacks and vulnerability exploits are the most frequently occurring threats that affect these factors. These short-term threats have DoS-like consequences, impacting both availability and integrity of OT in critical infrastructures in the short-term. A long-term important threat that is present within the OT cybersecurity domain, is the advanced persistent threat (APT). APTs are highly sophisticated and coordinated cyberattacks, which are performed by states or state-sponsored groups that have access to a large amount of resources.

The system operator is tasked with the responsibility of defending their systems against cyberattacks, as well as the mitigation of losses resulting from incidents. This involves the execution of an incident response cycle. In this cycle, procedures are implemented to prepare for incidents, prevent them, as well as to detect and remove them from the system step by step.

To mitigate the impact of successful cyberattacks on the system, measures that are often implemented by defenders in their systems are hardening, redundancy and diversity. Simultaneously, redundancy increases the attack surface of the defender’s system, making it more prone to successful attacks. The extent to which an increase in redundancy works counterproductive for the operational performance of the system is a fascinating phenomenon to further explore with the envisioned ABM.

6. Model Conceptualization

In the following section, a conceptual model for modelling the industrial processes within Gate terminal is presented. Firstly, the different model agents and objects are discussed. Consequently, the interaction between the different agents is highlighted, after which system key performance indicators (KPIs) are proposed based on RAMSSHEEP operational performance metrics. The conceptual model will form the basis for the ABM that is ultimately operationalized and used for simulating cyberattacks on the OT at Gate terminal.

6.1. Abstraction Level and Scope

Before defining a conceptual model that can form the basis for a full-fledged ABM, it is vital to demarcate the boundaries of the system that is to be modelled. Furthermore, the desired level of abstraction is to be established in order to be able to successfully formulate a conceptual model.

The scope of the conceptual model has to be large enough to be able to make the envisioned model useful and applicable for answering the research questions by including essential elements. Simultaneously, the scope has to remain small enough to maintain clarity and interpretability, excluding overly complex or irrelevant elements from the scope.

The end goal of the model is to assess the impact of cyberattacks on the operational performance of OT at Gate terminal. To this end, only OT existent in the industrial processes of the company is included in the model scope, while all IT elements are excluded. Additionally, interactions of the company with other parties in their supply chain that are not required for executing the main industrial processes as described in section 4.2.1 are excluded from the model scope. Furthermore, modelling actual stocks and flows of LNG in the various industrial processes is not essential for assessing operational performance of OT at the plant, and is therefore left out of the model scope, reducing modelling simplicity later on.

The operational performance of OT at the company is impacted by two factors only. The first and main factor is the disruption through cyberattacks, launched by attackers. The second factor is the possibility of a node failing randomly, which increases the applicability of the model. All other factors that might have an impact on the operational performance of OT are excluded from the scope. Furthermore, user traffic is excluded from the scope of the model.

A final important demarcation is the inclusion of elements from the incident response cycle implemented by the system operator. Parts of the preparation and post-incident activity steps are excluded from the scope. More specifically, the organizational/managerial actions are excluded from the scope. The main cause for this, is that the inclusion of these actions would induce a high level of complexity in the model, deteriorating its final interpretability and usability. Furthermore, both attacker and defender resources are out of the scope of the model, in order to further reduce complexity.

Aside from demarcating the scope of the model, setting the correct abstraction level is vital for enabling a successful implementation of the model, ultimately allowing the investigation of system behavior. To this end, several important choices with regard to the level of abstraction of the envisioned model have been made.

Firstly, an important abstraction pertains to the OT implemented at Gate terminal. As shown in section 4.1, process control loops are used to manage process control variables. For reasons of interpretability and clarity, the decision has been made to not include the individual PLCs, sensors and actuators of these control loops in the model, but to integrate them into one node. This allows for avoiding electrotechnical complexities that would be involved in modelling the sensors, PLCs and actuators as standalone entities, while resulting in a clear and relatively complete overview of OT in the company.

However, the choice for this abstraction level does not allow for making intra-control loop communications explicit. The nodes representing the control loops will be categorized per location used in industrial processes at the plant, such as the tanks, jetties and ORVs.

Another decision with regard to the abstraction level is the selection of attacks that are executed by attacker entities. In the model, generic attacks are simulated. These attacks negatively affect the operability of a node. This will result in DoS-like behavior, as the 'service' of the control loops is disrupted. While this decision does somewhat decrease the applicability of model outcomes, as no specific threat is modelled, it significantly reduces the complexity that would have been caused by implementing specific and highly advanced threats, such as an APT.

6.2. Conceptual Model Definition

The envisioned ABM model, providing insight into the extent to which added redundancy can improve operational performance at Gate terminal, will consist of several different model agents. These agents will each have their own routine. For each timestep in the model, the agents will execute their own routine, interacting with other agents and their environment, based on their perception of the environment and state.

The ABM is based on the classic 'attacker-defender' model. Attacker-defender game theoretical models are widely used for modelling cybersecurity threats and vulnerabilities in a system (Hasan et al., 2020; Kam-Kung & Bell, 2021; Yamin et al., 2021). In attacker-defender models, the goal of the attacking entity is to enter and disrupt the defender's system/infrastructure, while the defender aims to protect their system from these attacks and disruptions. This approach to cybersecurity modelling allows for examining the system performance under various scenarios, enabling the assessment of the impact added redundancy may have on system availability.

The model will introduce multiple different types of agents. In this section, these agents, their attributes and their procedures will be described. A high-level conceptual overview of the different model agents and their interactions is depicted in Figure 5.

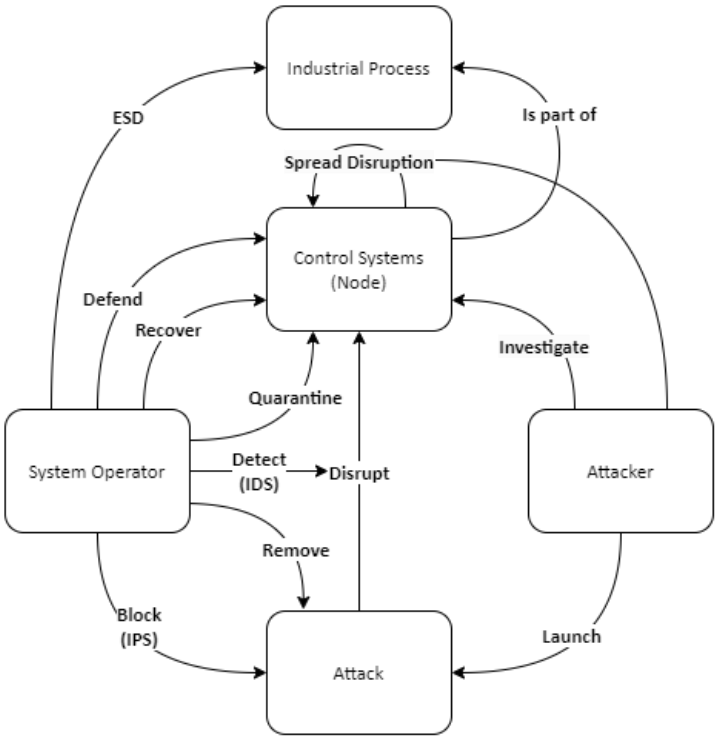


Figure 5: High-Level Conceptual Model of Attacker and Defender Interaction

In Figure 5, the interaction between the different model entities can be seen. In the conceptual model, it can be seen that the attacker investigates the control systems that are controlled and defended by the system operator (the defender). Every control system is part of an industrial process. When a target control system is selected, the attacker launches an attack on this control system, aiming to disrupt it, decreasing its operability. The system operator can block this attack before it arrives at a node through its IPS, detect an ongoing attack in the system using IDS, and quarantine the disrupted node. When the node is quarantined, the attack can be removed after which the node can be recovered by the system operator. If an attack goes unnoticed by the IDS, however, the attacker aims to spread the disruption to other control systems from the disrupted node. When nodes are disrupted to the point that the industrial process is no longer safely operable, the system operator can use the ESD to shut down the entire industrial process, containing the disruptions but rendering the system unavailable.

6.2.1. Attackers

In the model, the attacking agents are the malicious adversaries, attempting to disrupt the system by launching an attack at a node. Their main goal is to minimize the operationality of the nodes in the system, with the end goal of minimizing the availability of the industrial processes at Gate terminal. The internal state (investigating, attempting to attack, successful attack) of the attacker determines what actions the attacker performs during the given timestep.

When the attacker is investigating the system, the attacker decides what node he wants to attack. The selection of the target can be based on three different strategies. This is where the attacker's knowledge of the defender's system comes into play. If the attacker does not have any knowledge on the criticality (explained later in section 6.2.4) of the node, nor on the degree of node connectivity, the attacker randomly picks a target to attack. However, if the attacker does have knowledge on node criticality or connectivity, the target is selected based on one of these two criteria.

After the decision has been made by the attacker on which node to attack, the attacker relocates to the targeted node, and attempts to disrupt it by launching an attack on the node. The intrusion prevention system, as implemented by the system operator (explained in section 5.2.1) plays a pivotal role in 'deciding' whether or not the node is breached. If the hacking attempt fails, the hacker will reattempt a number of times, before retreating to their original location and re-investigating the system to select another target. If, however, the attack has been successful the node is disrupted to some degree. Furthermore, the attacker will attempt to spread the disruption to connected nodes in the system. When all attacks of an attacker are removed by the defender, the attacker will retreat to their original location, and will once again re-investigate the system for a new target.

Table 1: Attacker Attributes

Attribute of Attacker	Description
Attacker-strategy	Strategy for selecting target node: Random, Link-based or Criticality based.
Attack-state	0 = Investigate nodes, 1 = Attempting to hack target, 2 = Launched a successful attack
Breach-attempts	Counter for the number of attempted breaches
Original Location	Original coordinates for returning attacker to 'base'
Target	Selected node based on the strategy of the attacker

Table 2: Attacker Procedures

Action of Attacker	Description
Attempt-attack	Attempt to attack the targeted node
Disrupt-nodes	Reduce the operability of a node through an attack, based on its power
Give-up	Stop attacking and return to 'base'
Investigate-and-select	Investigate targets, and select a target using 'select-target'
Perform-attack	Launch an attack on a node
Select-target	Selecting a node to attack based on the strategy
Spread-infection	Attempt to hijack nodes connected to nodes that are successfully attacked

6.2.2. System Operator / Defender

The system operator aims to defend the system from disruptions caused by the attacker. To this end, the operator can monitor and control the nodes. Several steps from the incident response cycle as described in section 5.2 are implemented, including prevention of attacks, detection of attacks, containment and quarantine of the affected node, eradication of the attack and, finally, recovery of the affected node. The defender can implement IPS and IDS systems in order to defend the nodes. The IPS (prevention) is used by the defender to assess traffic that enters the nodes: if an attack goes unnoticed, it is more likely to spread further. User traffic is not part of the scope of the model: including user traffic would introduce differentiation between false positives, false negatives, true positives and true negatives in the research, however, the main user of the industrial processes at Gate terminal are the system operators themselves.

The IDS (detection) is also controlled by the defender: through the detection system, attacks that have successfully penetrated the IPS and are thus able to disrupt a node, can be detected by the defender. When it is known to the system operator that one or more of their controlled nodes are under attack, the operator can attempt to contain/quarantine the affected node, preventing the attacker from spreading the attack to other nodes. Once the node has been quarantined, the defender will attempt to remove the attack from the system. Only after the defender has succeeded in removing the attack, he can start recovering the node, in order to get it back to a fully operable state.

The final role of the defender is to completely shut down an industrial process if the extent to which the process is available is considered critical and dangerous. This role involves operating the ESD that is present at Gate terminal. Whenever the availability (the calculation of availability is provided in section 6.3.2) is lower than the ESD-threshold trigger value, all nodes in the industrial process are isolated and set to an inoperable state. This then allows the system operator to remove disruptions from the process and recover the system. Only when the industrial process is completely recovered, the emergency shutdown is released.

Table 3: Operator Attributes

Attribute of Operator	Description
Containment-successrate	Effectiveness of the operator in containing nodes that are disrupted through an attack
ESD-threshold	Trigger value for shutting down industrial processes through ESD
IDS-effectiveness	Effectiveness of the detection of attacks in the system
IPS-effectiveness	Effectiveness of the prevention of attacks in system

Table 4: Operator Procedures

Action of Operator	Description
Detect-ongoing-attacks	Use the IDS to detect ongoing attacks
Operate-esd	Trigger and release ESD based on the availability of industrial processes
Quarantine-attacked-nodes	Attempt to contain attacks by placing attacked nodes in quarantine
Recover-node	Recover operability of nodes that have been attacked
Remove-attacks	Remove attacks from quarantined nodes

6.2.3. Attacks

The attack that is launched by the attacker acts as its own model entity. This allows for keeping track of several important attributes of an attack, such as the power of the attack, providing the impact that the attack has on a control system. Tracking the state of an attack (detected/undetected) enables the model for the undetected spread of the disruption throughout control systems, which might majorly affect the impact an attacker has on the operational performance of the system.

The removal-time of the attack represents the degree of difficulty of removing the attack for the system operator. The more difficult an attack is to remove, the higher the removal time of the attack, increasing the number of time steps it takes for a defender to remove the attack. Finally, the duration of the attack, representing the total amount of time an attack is present in the system, is tracked for model performance purposes.

Table 5: Attack Attributes

Attribute of Attack	Description
Detected?	Flag for having detected and undetected attacks
Duration	Timing the total time the attack has been active in the system
Power	Impact an attack has on operability of a node. Lower is stronger.
Removal-time	Time it takes for a defender to remove the attack, indicative of difficulty to remove

6.2.4. Nodes and Industrial Processes

In the ABM, several industrial processes and operations at the Gate terminal plant are modelled:

- Tanks (1, 2, 3)
- Jetties (1, 2, 3)
- Seawater Pump
- ORV
- Truckloading

All of these locations are monitored and controlled using the DCS in the central control room of the plant. The DCS is also modelled as an industrial process. Each industrial process consists of various control loops, consisting of sensors, actuators and PLCs. These control loops are modelled as a node in the system.

The nodes have several states, representing the different levels of functionality of the node: normal, disrupted (known and unknown), contained/quarantined and recovering. Based on the state of the nodes in the system, the system operator is able to perform different actions (remove intrusion, recover, etc) on the respective node.

The criticality and the operability are the two most important attributes of the node, since these two attributes are used to calculate the availability of individual processes at the plant (see section 6.3.2). The operability of the node indicates how well the control loop itself is functioning. The operability of a node is affected by a successful cyberattack, and has a value between 1 (fully operable) and 0 (not operable). The criticality of a node represents the degree to which a node impacts the functionality of the industrial process to which the node belongs. For all nodes in a process, the criticalities are normalized, so that the sum of criticalities inside a process is equal to 1. This is required, as the availability of a process is calculated as the sumproduct of the operability and criticality of all nodes inside that process, and the availability of a process can never exceed 1, or 100%.

Whenever a node is successfully attacked, the attack can spread through the system by accessing nodes that are connected to the node that has been attacked. Unless the node is in quarantine, or part of an industrial process that is shut down through the ESD, an attacker can spread the disruption to the node.

Finally, the node has the capacity to fail randomly. A random failure, similar to a cyberattack, affects the operability of the node. This feature is incorporated to mimic random system failures, increasing the applicability of the model. A node can be attacked by an attacker while it is randomly failing.

Table 6: Node Attributes

Attribute of Node	Description
Criticality	Impact of the node on the functioning of its 'Node-process'
ESD	True if node is down through ESD, False otherwise
Identifier	Unique number allowing for creating links between specific nodes
Node-process	Indicative of the industrial process that the node is allocated to
Operability	Degree to which the node is functioning
State	0 = Functioning normally, 1 = Disrupted (unknown), 2 = Disrupted (known), 3 = Contained/Quarantined, 4 = Recovering
Vendor	Vendor of the node package, used for diversity purposes

Table 7: Node Actions

Action of Node	Description
Random-failure	A node can fail randomly, decreasing the operability of the node

Figure 6 shows a UML diagram of the interaction between the different model entities, their attributes, as well as their procedures.

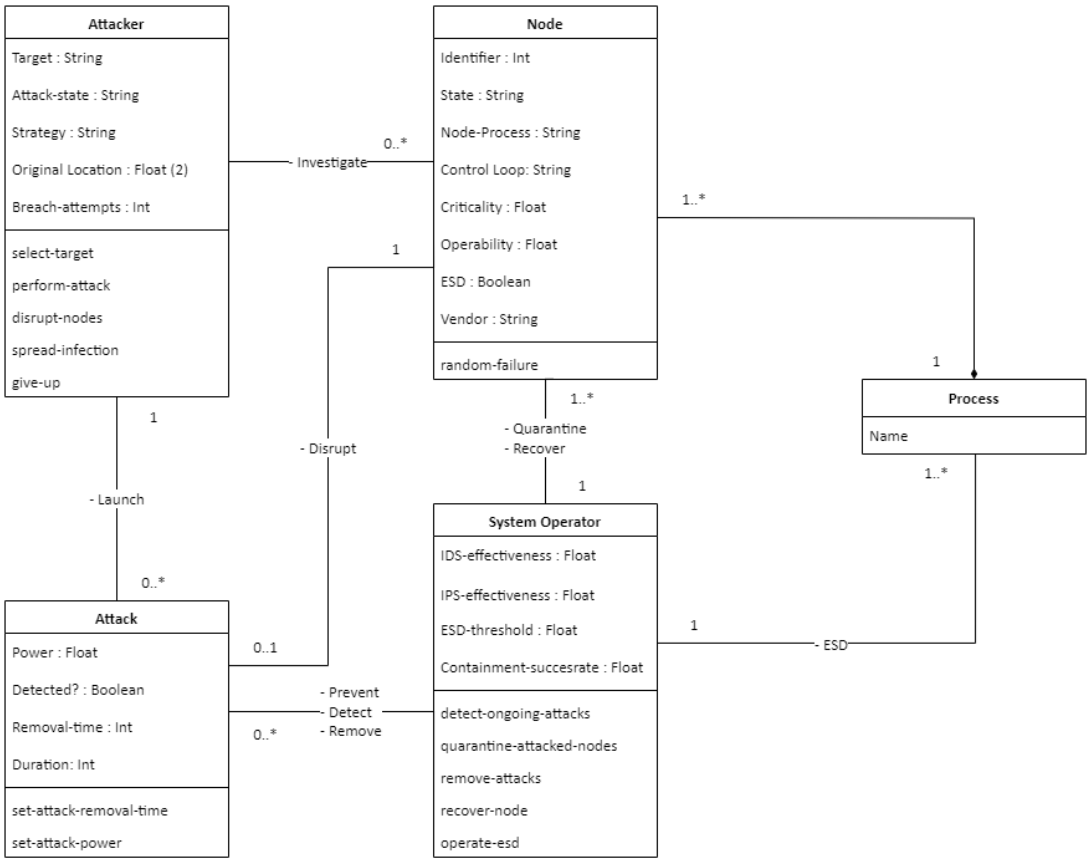


Figure 6: UML of ABM

6.3. System Key Performance Indicators

The described processes will form the basis for constructing the modelled system using ABM. The ABM will be used to simulate attackers and defenders in the system, attempting to disrupt and protect the systems and their control loops, respectively.

In order to quantify the performance of the system to enable comparison of different redundancy strategies, several key performance indicators (KPIs) have to be identified. In the following section, the RAMSSHEEP framework (Matos & Casas, 2018) will be used to identify these system KPIs.

6.3.1. The RAMSSHEEP Framework

The RAMSSHEEP framework is an extension on the earlier RAM (acronym for Reliability, Availability, Maintainability) framework. These RAM factors allow for quantifying and analyzing system failures and operational performance of a system (Corvaro et al., 2017). The RAMSSHEEP approach extends this framework, by including five other factors: safety, security, Health, Environment, Economics and Politics. In Table 8, definitions of the RAMSSHEEP criteria as presented by Wagner & Van Gelder (2014) are presented. Please note that some minor additions have been made to these definitions.

Table 8 - RAMSSHEEP Acronyms and Definitions

RAMSSHEEP Acronym	Definition
Reliability	Pertains to the failure probability of a system in which its intended functions cannot be fulfilled.
Availability	Pertains to the time duration in which the system is functional and its intended functions can be fulfilled.
Maintainability	Pertains to the ease in which the system can be maintained over time.
Safety	The absence of human injuries during using or maintaining the system. Addition: Pertains to hazards caused by natural forces or human errors (Nas, 2015).
Security	A safe system with respect to vandalism, terrorism and human errors. Addition: Pertains to hazards caused by deliberate intention of humans to cause harm (Nas, 2015).
Health	The objective argument of good health with respect to the physical, mental and societal views
Environment	Aspects pertaining to influence of the system on its direct physical environment.
Economics	A serious reflection in terms of costs versus benefits (as well as direct and indirect) to provide more insight for an economical responsible choice.
Politics	A rational decision on all previous aspects.

In these proposed definitions, reliability and availability are quite similar, differing only in timeframe. These definitions can however be refined and further separated through connecting them to performance metrics. While availability is focused on the 'uptime' of a system, reliability is aimed at how long a system can perform its intended function (Lanthier, n.d.).

6.3.2. Applying RAMSSHEEP on Gate terminal

For quantifying the impact on the performance of OT at Gate terminal in the case of a cyberattack, a selection of RAMSSHEEP aspects has been made. For the analysis, reliability, availability, maintainability, security, and economics aspects will be taken into account. The other aspects (safety, health, environment and politics) are out of scope for this research, since they are not as relevant for a system when it comes to measuring operational performance of a system under cyberattacks.

Cyberattacks are an intentional hazard caused by a malicious party and is therefore aimed at disrupting the security of the system. Human-related safety aspects are not included in the analysis: at Gate terminal, there is always a mechanical failsafe that can safely shut down (parts of the) system. The safety and health aspects are therefore not directly related to cybersecurity incidents and are thus out of scope of this research.

While there may be political driving forces incentivizing attackers and defenders, these are not (directly) related to operational performance of the system and are thus out of scope of this research. Environment-related aspects are less relevant to the operational performance of the system, as they aren't directly influenced by a successful cyberattack. Furthermore, actual gas flow and therefore potential gas leakages are not included in the model due to time and complexity constraints. The FGS system, which might have had the biggest impact on the environment. As a result, environment-related performance metrics are not included in the model.

A successful disruption will affect the reliability and availability of a system, as successful disruptions decrease the operability of nodes in the system, reducing its operational performance. Furthermore, a successful attack may lead to severe economic losses, as a result of the reduced system

availability. The maintainability aspect comes into play when modelling redundancy strategies: a system with added redundancy may be more complex to maintain. In certain systems, adding redundancy enables the maintenance of system parts while the system remains operational, since redundant elements can substitute for the element under maintenance (Sears, 2001). At Gate terminal, however, for larger maintenance tasks, entire system components (tanks, jetties, etc) are out of order while the maintenance is performed.

The aforementioned selected RAMSSHEEP categories can be quantified using various metrics. Per selected category, the performance metrics are described below.

Reliability

In order to enable the assessment of the operational performance in the system, it is crucial to first present a definition of a system failure. Defining a failure as a successful attack was a possibility, although it can hardly be stated that a single successful attack constitutes a system failure, due to the limited impact a single attack might have on the overall availability of the system. Therefore, a failure is defined as a dip in overall availability of 10 % or higher.

$$Failure = Dip\ overall\ availability \leq 90\%$$

Aside from failures occurring through malicious activity, failures can randomly occur in the system.

$$Random\ Failures\ (\#)$$

System will be measured using two often-used metrics (Low, 2015): the mean time between failure (MTBF) and the mean time to failure (MTTF). The MTBF measures the mean amount of failure-free time between two different system failures, while the MTTF measures the time until a first new failure occurs. The mean time to repair (MTTR) (as discussed in *Maintainability*) is the difference between the MTBF and the MTTF. In Figure 7, the differences between MTBF, MTTR and MTTF are visualized.

$$MTBF = \frac{Ticks\ (\#)}{Failures\ (\#)}$$

$$MTTF = MTBF - MTTR$$

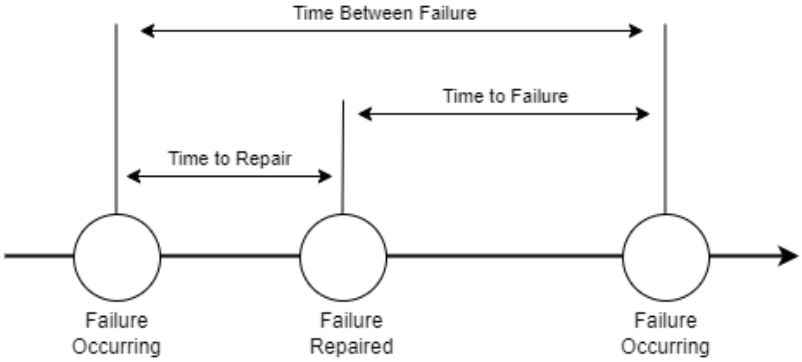


Figure 7: Visualization of Reliability Statistics

Availability

The availability of the system is a crucial part of measuring the performance of the system. A commonly used conceptual framework used to assess security incidents and their impact on availability are the complementary attack-, fault, and event trees (NCSC, n.d.b.). These trees show events required for a process to fail, and can be converted to combinations of parallel and series systems. In turn, these systems can be used to calculate failure probabilities, and the availability of a system ($1 - \mathrm{P(fail)}$). The application of this conceptual framework in ABM would result in a variety of problems. Using fault trees would result in static mathematical calculations, that requires knowledge on intra-process, non-changing dependencies, as well as on failure probabilities of individual components. Furthermore, application of this framework limits the number of system states: a process is either fully available, or not available at all. Finally, fault trees are based on the assumption that component failures are independent (Tolo & Andrews, 2023). This is not applicable when modelling attacks that can spread throughout the system.

ABM is a dynamic and exploratory modelling method by nature (Ding et al., 2018). The aforementioned limitations go against this dynamic nature: the intended model uses a multitude of possible system states and levels of availability per process, which are affected by emergent model behavior. Therefore, implementing static series and parallel systems with a limited number of states would significantly reduce the value of an ABM, as similar results can be found through a mathematical analysis. Therefore, this thesis uses another approach for calculating the availability of processes.

For quantifying the availability of the system, various metrics are calculated. The overall availability is an important outcome, as it plays a role in determining whether or not a failure has occurred in the system. The overall availability is defined as the mean of the availability of all subprocesses. All subprocesses in the intended model consist of nodes. Each of these nodes has a certain degree of criticality and a degree of operability. A node with a high degree of criticality for a process has a higher impact on the functionality of that process. The availability of a process is conceptualized as the sumproduct of these attributes of each node in the process. This approach allows for a more dynamic process availability when compared to event trees, with more possible values than 100% and 0% availability. The definitions for process- and overall availability are presented below. In these equations, P denotes the set of processes. Each process $p \in P$, and has a set of nodes corresponding to it: N_p.

$$Process\ Availability = \sum_{\mathrm{n} \in \mathrm{N_p}} \mathrm{Criticallity_n} \cdot Operability_{\mathrm{n}}$$

$$Overall\ Availability = \frac{1}{\#\mathrm{P}} \cdot \sum_{\mathrm{p} \in \mathrm{P}} \sum_{\mathrm{n} \in \mathrm{N_p}} \mathrm{Criticallity_n} \cdot Operability_{\mathrm{n}}$$

The MTBF and the MTTF as described in the *Reliability* section are used to calculate the availability of the system. In order to easily differentiate between the models ‘Overall Availability’ as described above, and the availability calculated by dividing the MTTF by the MTBF, this KPI is called ‘Availability 90’. The ‘90’ refers to the dip of 10% in overall availability, which is required in order for the dip to classify as a failure of the system, as described in the ‘Reliability’ section.

$$Availability\ 90\ (\%) = \frac{MTTF}{MTBF} \cdot\ 100$$

Finally, a KPI measuring the time that all nodes in the system are fully operational: 'Availability 100'.

$$Availability\ 100\ (\%) = \frac{Ticks\ full\ operability\ (\#)}{Ticks\ (\#)} \cdot 100$$

Maintainability

The maintainability of the system is measured using three different metrics. Two of these metrics are focused on the size of the system. A larger system size implies that the maintenance of the system will be more labor-intensive. The metrics used for measuring system size are the number of nodes in the system and the number of different vendors of nodes in the system. If a system has nodes of multiple different vendors, operators have to take more factors into account while performing maintenance due to the added complexity.

The number of nodes metric comes with an important note: not only does it provide an indication of the maintainability of the system, it presents a metric for the attack surface of the system too. The more nodes are present in the system, the more possible entry points for an attacker, and thus the bigger the attack surface of the system becomes.

$$Vendors\ (\#)$$

$$Nodes\ (\#)$$

The final metric used for analyzing the maintainability of the system is the mean time to repair (MTTR). The MTTR can be used to indicate the speed of system recovery after a failure, allowing for approaching the efficiency of maintenance. The MTTR is calculated by dividing the number of timesteps a system is failing by the number of failure occurrences. As presented in the *Reliability* and *Availability* sections, MTTR is closely related to MTBF, MTTF and Availability 90.

$$Mean\ Time\ To\ Repair\ (MTTR) = \frac{Ticks\ during\ failure\ (\#)}{Failures\ (\#)}$$

Security

In order to measure the impact of cyberattacks with regard to the security of the system, three different model output parameters have been selected. Firstly, the average attack duration provides an indication of the effectiveness and efficiency of the defender's incident recovery security measures in the system. The lower the average attack duration, the better the security of the system is performing, since the threat is contained and removed faster. In the equation, A denotes the set of attacks. Each attack $a \in A$, and has a duration.

Furthermore, the number of times the ESD is triggered is also included as a performance metric. The number of times the emergency shutdown system is triggered provides an insight in the amount of escalation that may occur after a security incident, indicating the capacity of the system operator to contain a threat in a timely fashion and limit damage.

$$\frac{1}{\#A} \cdot \sum_{a \in A} \text{Duration}_a$$

$$ESD\ Triggers\ (\#)$$

$$Succesful\ Attacks\ (\#)$$

Economics

The final selected RAMSSHEEP category, economics, is quantified using two mutually dependent metrics. The cumulative monetary losses metric is based on the total expected profit (a model input) and the overall availability of the system. Through division, the expected profit for a single timestep is calculated. Through multiplication of the expected profit per timestep with the overall availability of the system in that timestep, the expected profit is adjusted for the unavailability of the system, resulting in the actual profit. The expected losses can be calculated by subtracting the actual profit from the expected profit.

$$Expected\ Loss_{\ i} = \frac{Expected\ Profit}{365} - \frac{Expected\ Profit \cdot Overall\ Availiabity_{\ i}}{365}$$

$$Total\ Expected\ Loss = \sum_{i=0}^{t} Expected\ Loss_{\ i}$$

The total expected loss can be converted into a percentage by dividing it by the total expected profit, extrapolated to the number of timesteps that the model has run.

$$Expected\ Loss\ (\%) = \frac{Total\ Expected\ Loss}{\frac{Expected\ Profit \cdot Ticks\ (\#)}{365}}$$

7. Model Operationalization

In this chapter, the conceptualized model as presented in the previous chapter will be operationalized into a full-fledged ABM. When the model is implemented, the various features of the model are highlighted, after which the attacker and defender routines are described in the narrative of the model. Furthermore, multiple model assumptions that have been made in order to convert the conceptual model into an operational ABM are presented. Finally, the various steps taken for verifying the model and assessing its validity are subsequently discussed. The goal of this chapter is to aid in formulating an answer to the third sub-question: "*What behavior can be observed in the operational technology in the industrial processes of Gate terminal when simulating cyberattacks?"*

7.1. Agent-Based Modelling Implementation in NetLogo

For the implementation of the ABM, a software package called 'NetLogo' (version 6.3) is used. NetLogo provides a relatively user-friendly solution for creating a wide variety of ABMs. The aim of this section is to go through the implemented model in the NetLogo package, introducing the model overview, inputs of the model, as well as the implemented KPIs and monitors.

In Figure 8, the different model controls are presented. At the top, the model can be initialized, and run indefinitely, once, a year, or five years. For verification, validation and experimentation, a runtime of 5 years is used. Furthermore, the setup section allows for loading a setup of nodes from a .txt file (if 'load-from-txt' is enabled), as well as selecting a scenario from a loaded .csv file containing scenarios for sensitivity analysis and experimentation. Other model settings include hiding certain labels & links, usage of a seed, as well as initializing expected profits, failure rates, and other attacker and defender parameters. In order to imitate the increased difficulty for attackers to spread to nodes that are part of a different system, a vendor-multiplier is included in the model. When the attacker attempts to spread a disruption between two nodes that have different vendors, this factor is multiplied by the infection-spread-likelihood, ultimately decreasing the chance of spreading the disruption throughout the system.

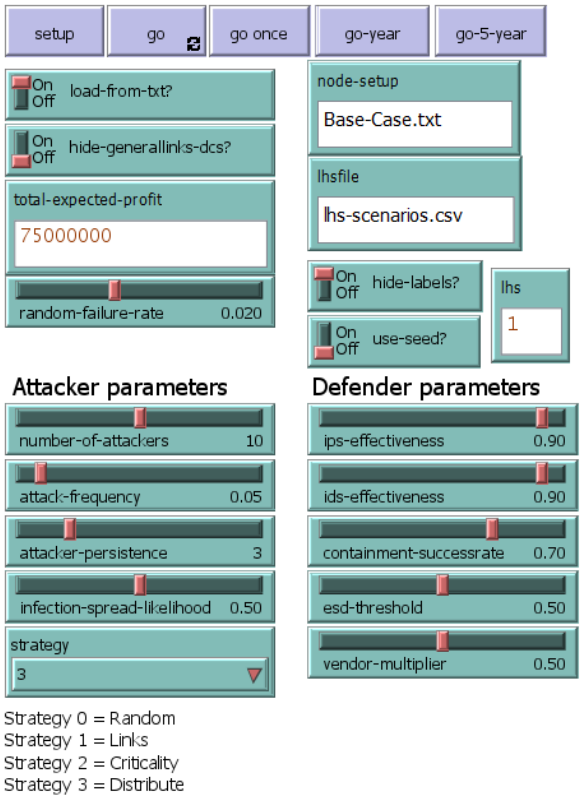


Figure 8: Model Setup

When the 'setup' button is clicked, the model is initialized, and the selected setup of nodes is loaded into the model. As shown in Figure 9, an abstract version of the various locations at Gate terminal is presented in the main model view. Each location/process contains various (blue) nodes, representing a fully operational control loop. The green nodes are interface nodes: each node in a process is connected to the interface node of that process, as well as to all other nodes in the process. The interface nodes, in turn, are connected to the DCS. The attackers are visualized in the top left corner of the main model view, and move to a node when they attempt to attack it.

When the state of a node changes during a model run (see Figure 10), the node changes colors:

- Red: Under attack, attack is not detected.
- Orange: Under attack, attack is detected
- Brown: Node is quarantined, still has incoming attacks
- Yellow: The node is quarantined and recovering

In the model, attacks are visualized using a directed link from the attacker to the attacked node. Similar to nodes, the attack link is colored red when the attack is undetected, and is colored orange when the attack is detected.

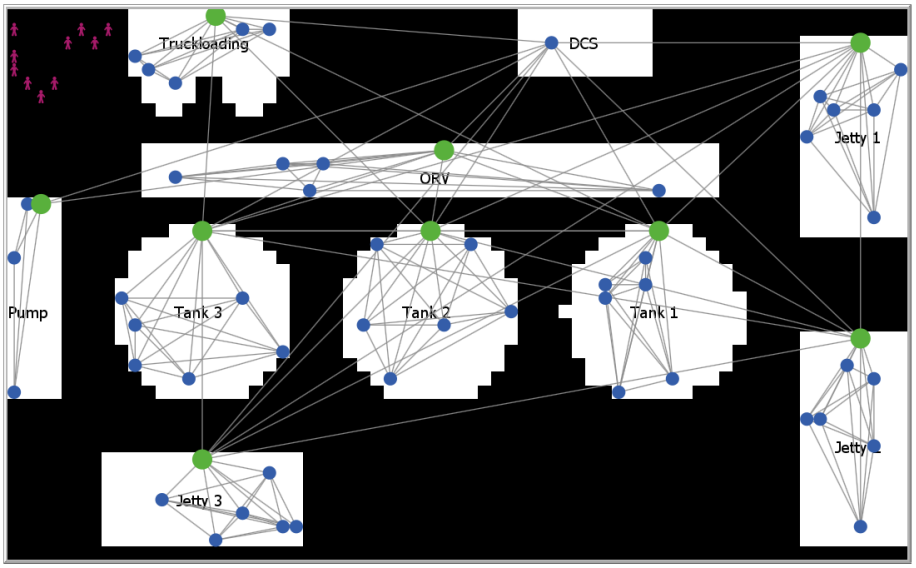


Figure 9: Main Model View

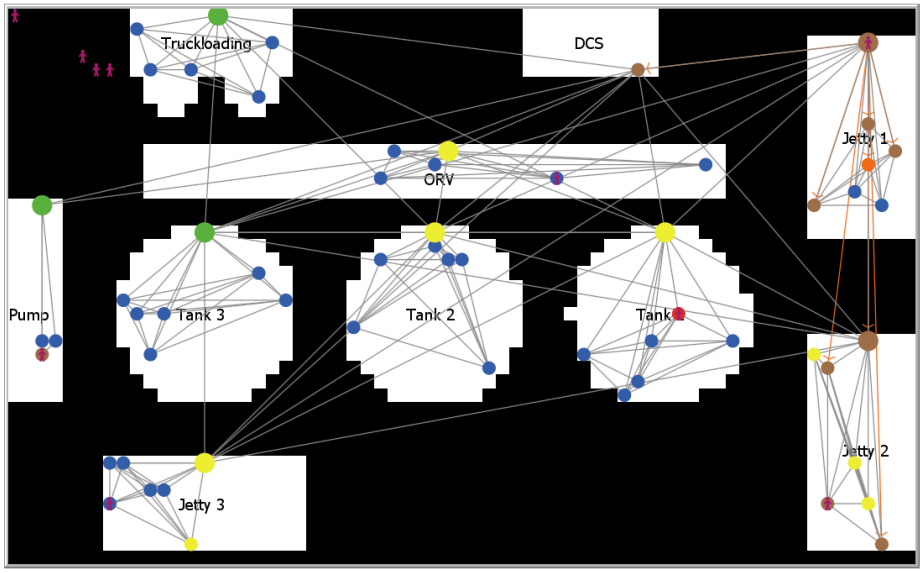


Figure 10: Main Model View (During Run)

The two final elements that are present in the NetLogo model are the selected RAMSSHEEP KPIs, as well as several plots of the development of component availability, monetary losses, etc. These elements are represented in Figure 11 and Figure 12, and have been extensively used throughout the implementation phase of the model for assessing the correctness of the implementation.

Reliability		Availability		Maintainability		Security		Economics	
System Failures	10	Availability >90 (%)	97.42	Amount of Nodes (#)	59	Successful Attacks (#)	673	Expected Losses (%)	1.19
Random Failures (#)	22	Availability 100 (%)	44.88	Amount of Vendors (#)	4	Avg. Attack Duration (Tick)	2.8	Expected Losses (€)	4478310.5
Mean Time Between Failure	182.5	Average Overall Availability	98.81	Mean Time to Repair	4.7	ESD Triggers (#)	8		
Mean Time to Failure	177.8								

Figure 11: RAMSSHEEP KPIs of the Model

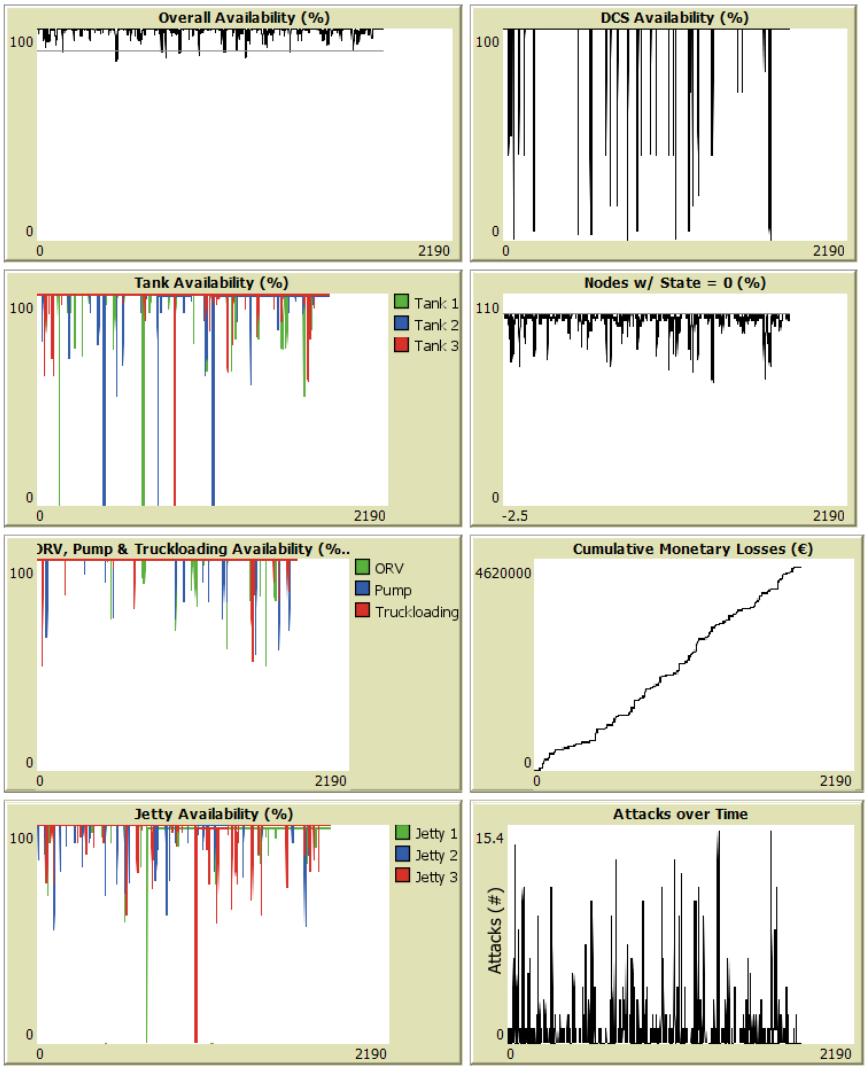


Figure 12: Plots of Model Run Behavior

7.2. Model Narrative

In Figure 13, a high-level overview of the actions in the model is represented using a flowchart. The red objects are part of the routine of the attacker, the green objects are part of the system operator's routine.

When a new time step in the model (tick) is instantiated, it is first the attacker's turn to execute their routine. Per attacker, this routine differs based on the state of the attacker: if the attacker does not have a target, it investigates and selects a new target (based on certain preconditions). If the attacker does have a target, but isn't currently attacking any nodes, the attacker attempts to attack its target. Else, if the attacker currently has ongoing attacks on the system, it attempts to disrupt the attacked nodes, reducing the operationality of the nodes. Furthermore, the attacker attempts to spread the infection, attempting to attack nodes that aren't under attack yet, but are connected to a node that is under attack by the attacker.

When the attackers are done executing their routine, it is the turn of the system operator. Their routine is based on the incident response procedure as described in section 5.2. The first step of the incident response procedure, prevention, is incorporated in the attacker's 'Attempt attack' action. Therefore, attack prevention is not an explicit defender procedure. In line with the incident response procedure, the next step after incident prevention is to detect ongoing attacks using an IDS system. This step is the first procedure incorporated in the system operator's routine. When an attack is detected, the defender attempts to quarantine the affected node. Hereby, the defender aims to prevent the spread of the attack through the disrupted node to other nodes. Once the attacked node is successfully quarantined, the defender can start removing the attack from the node, after which the node is recovered to a fully operational state. The final procedure of the system operator involves shutting down an industrial process through ESD if the process is no longer working sufficiently. The ESD is triggered when the availability of an industrial process is lower than the ESD threshold, which is set at 50%.

Finally, when both the attackers and the defender have completed all procedures in their routine, the model is designed to incorporate random node failures: this involves disrupting the operability of a node to a certain degree, mimicking the occurrence of failures in components without the involvement of an attacker. The defender is not immediately aware of a random failure. Therefore, a node can only be recovered using the defender's recover node routine once it is recognized as failed, which is done in the quarantine procedure.

In Appendix A, flowcharts of all different procedures implemented in the model, along with a short description are presented. Furthermore, the appendix contains an overview of the different implemented control loops in the model, as well as a formalization of the model concepts.

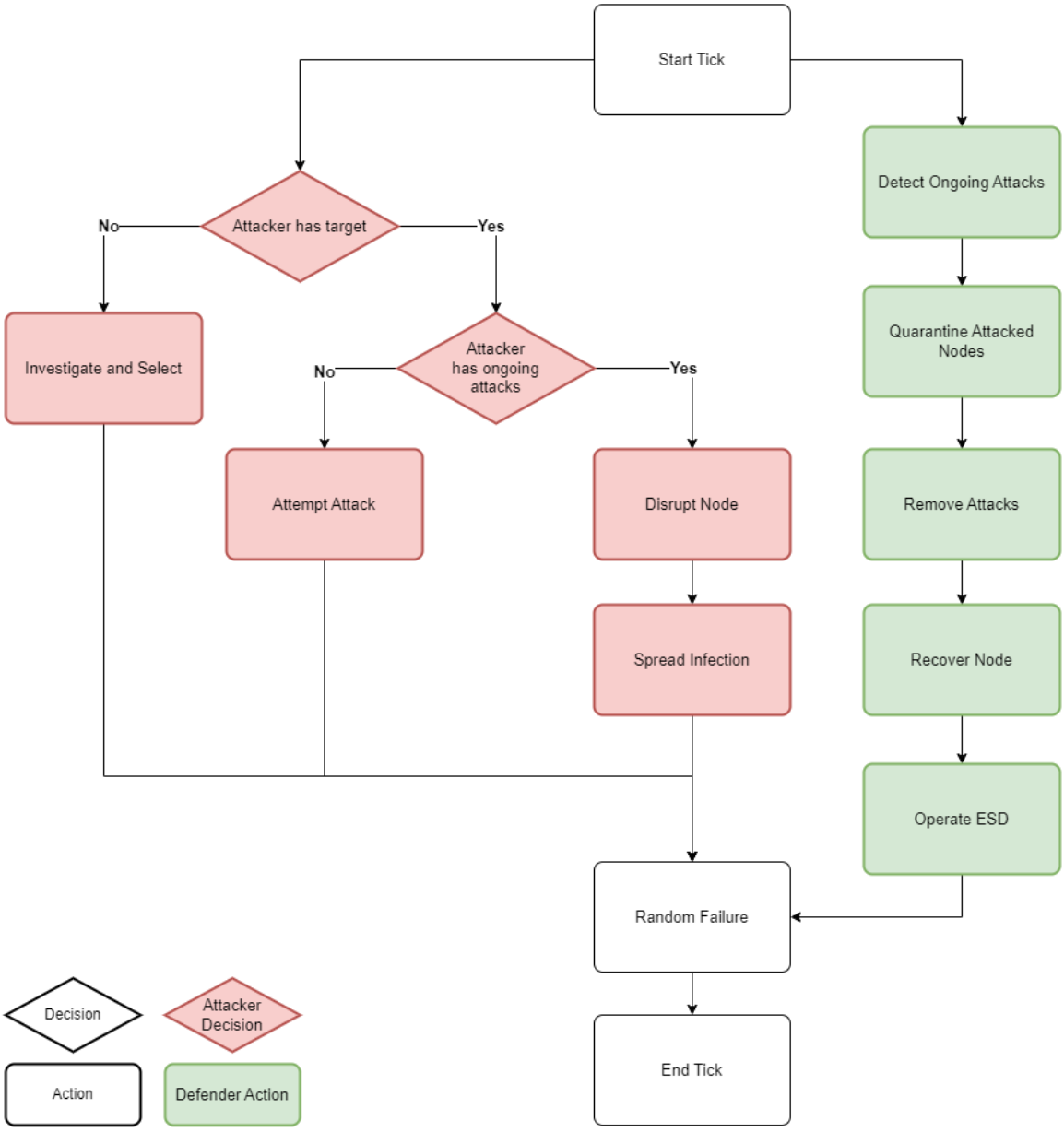


Figure 13: High-Level Flowchart of ABM Implementation

7.3. Model Assumptions

When modelling a complex system, one of the main tasks of the modeler is to make model assumptions in order to successfully be able to model a system. These assumptions can be made because of several reasons, including simplicity, feasibility, limited knowledge and interpretability of the model. This section aims to address the assumptions that have been made while modelling OT and attacker-defender interactions at Gate terminal in a structured manner.

Assumptions about attackers and attacks

1. A node can be attacked by one attacker at a time. An attack can only be launched at a node when the node is in operational state, or is randomly failed.
2. The attacker has multiple attempts to bypass the defender's IPS, before giving up and selecting another target.
3. Attacks are of a general, unspecified nature, and can only have a single target. An attack only affects the operability of a node, and has (aside from spreading) no immediate side effects on any other aspects in the system.
4. The power of an attack is distributed between 0 and 1, with values of 0.2, 0.4 and 0.8.
5. Attacks can spread from disrupted nodes to other nodes. The spread of a disruption to another node is modelled as a separate attack by the same attacker that infected the original node. As a result, while a node can only be attacked by one attacker, an attacker can attack several nodes simultaneously.
6. Depending on the vendor multiplier, spreading an infection to a node produced by the same vendor is easier than spreading to a node produced by a different vendor. This is representative of network segmentation caused by implementing multiple vendor systems.

Assumptions about defenders and nodes

1. Contrary to attackers and attacks, the defender is not modelled as a specific turtle breed. This is because the system operator is modelled as a single actor that has a holistic view of their system, which has the capacity to perform the incident response cycle for multiple occurring incidents simultaneously.
2. The defender has to detect an ongoing attack before he can quarantine the infected node. Attacks can only be removed from nodes if that node is quarantined.
3. A node can only recover after the incoming has been fully removed from the quarantined node.
4. When ESD is triggered for a process, the operability of all nodes is set to 0: each node will have to fully recover. This won't affect recovery times, as nodes in the ESD process that weren't attacked will always recover faster than those that are attacked.
5. Recovery of nodes happens equally fast for nodes that are equally disrupted by an attack or a random failure. While in reality, not all control systems recover equally fast due to their variations on complexity and intricacies, a somewhat static repair time enables a good assessment of the impact recovery strategies have on the availability of the system.
6. Nodes are prone to random failures.
7. There is a discrepancy between the locations of the control loops and the industrial processes. As flows of gas are out of the model scope, these control loops have been relocated to a location at the plant (tank, jetty, etc).

7.4. Verification

The process of verification is an important part of the modelling cycle, and is to be performed continuously while implementing the model, as well as once the entire model is operationalized. Model verification allows for investigating whether or not the conceptual model has been correctly implemented, assessing whether the operationalized model is consistent with the conceptual model (Wilensky & Rand, 2015). In other words, verification of the implemented model allows for assessing the correctness of the operationalization of the conceptual model.

In order to assess the correctness of the implemented model, various verification steps and methods have been applied.

Throughout model implementation, a wide variety of debugging methods have been continuously used to assess the operationality of the model, tracking single agent behavior and its interactions. This involved extensive use of integrated NetLogo features, such as the Command Center and Agent Monitors, as well as implementing best practices regarding the testing and debugging of code. During the model implementation phase, rigorous testing was continuously conducted on all of the operationalized model procedures and functionalities. These tests were performed to ensure proper code execution, while verifying that the implemented code had the intended impact on the various model agents and their interactions. During the implementation phase, a variety of bugs and other unexpected behavior were identified and resolved. Due to the iterative and complex nature of the implementation process of an ABM, not all of the performed verification checks have been documented.

In Appendix B, two other verification methods and their checks are presented. First, unit testing, an approach that involves writing small tests that check whether individual units are working correctly in the code (Rand & Rust, 2011), is performed. These unit tests have been extended to not only test individual units, but to verify whether the interaction between different agents works as intended as well.

The final executed verification tests involved attempting to break the model that has been created. One by one, all model outputs have been set to unrealistic model values, including extremely high, and extremely low values. The behavior of the system with these model values is observed. This allows for evaluating if the model can be 'broken' if unrealistic input values are used. Furthermore, unrealistic input values test the applied logic in the operationalization phase. All tests and outcomes have been presented in Appendix B.

7.5. Validation

Validation of the operationalized model is a vital part of the modelling cycle, and is to be performed before the model can be used for experimentation. The main question that can be answered through validation, is if "the right thing" is built by the modeler (Nikolic et al., 2013).

In order to validate the model that has been operationalized, two different validation methods are applied. First, a variability analysis is performed, providing an indication of the variability of the model outputs when multiple runs with identical model parameters are performed. Secondly, a univariate and multivariate sensitivity analysis is performed, supplying insights into the impact individual model parameters have on the outputs of the model.

7.5.1. Variability Analysis

As a starting point for the variability analysis, the model values as presented in Table 9 are used. During the operationalization phase, these parameter values have been found to result in sensible model outputs. For the variability analysis, the model is run 1000 times, tracking the performance of the model. Kernel Density Estimation (KDE) plots for all output variables are presented in Appendix C, visualizing probability

density curves for each of the model outputs. In Table 10, the mean, standard deviation and the relative variability of all output variables has been presented. The relative variability column represents the variability in the model output, and is calculated by dividing the standard deviation of the model output by its mean. A higher degree of relative variability indicates a wider range of distribution of data points around the mean, and provides an indication of the (in)consistency and randomness of the various model KPIs.

Table 9: Initial Model Values

Parameter	Value
attacker-persistence	3
attack-frequency	0.05
containment-successrate	0.7
esd-threshold	0.5
ids-effectiveness	0.9
infection-spread-likelihood	0.5
ips-effectiveness	0.9
number-of-attackers	10
random-failure-rate	0.02
Strategy	Distributed
vendor-multiplier	0.5

As can be seen in Table 10, there are quite big differences in variability when it comes to the model outputs. Some KPIs, like *overall availability* and *availability 90,* have little variability (< 5%) while other KPIs have a very large degree of variability. The *mean time between failure, mean time to failure, ESD triggers* and *failures* KPIs all have relatively large standard deviations, and thus a high degree of variability. This phenomenon can be attributed to the confluence of circumstances required for a change in these KPIs. This can be explained by system failures, for example. A failure is defined as a dip in overall availability below 90%. The combination of a high mean of *overall availability* and a low standard deviation, results in only a few dips below this 90% mark. A dip only occurs in relatively rare circumstances, in which multiple nodes have been significantly disrupted and/or processes are down through ESD. This only happens when multiple attacks (originating from one or more attackers) disrupt multiple nodes at the same time, and are not sufficiently handled by the system operator. This is unlikely to happen, as the system operator is quite efficient in defending their systems, with a high degree of IPS and IDS effectiveness and a good containment successrate. As a result, the variability of *failures* is quite high. Due to the dependency of the *mean time between failure* and the *mean time to failure* on the number of system failures, the variability within these KPIs is quite sizable as well.

Table 10: Mean and Standard Deviation of Model Outputs of Variability Analysis

Output	Mean	Standard Deviation	Relative Variability (%)
Attack Duration (Average)	2,84	0,07	2,61
Availability 100	47,36	2,76	5,83
Availability 90	96,85	1,11	1,14
Cumulative Monetary Losses	3922880	645305,6	16,45
DCS Availability 100	93,71	1,44	1,54
ESD Triggers	9,41	3,38	35,87
Failures	9,91	3,25	32,85
Mean Time Between Failure	211,81	115,15	54,36
Mean Time to Failure	206,02	115,15	55,89
Mean Time to Repair	5,8	0,71	12,27
Overall Availability	98,95	0,17	0,17
Random Failures	36,75	6,19	16,85
Successful Attacks	536,17	63,72	11,89

7.5.2. Sensitivity Analysis

A sensitivity analysis is a tool that is commonly used to perform model validation. The main principle of a sensitivity analysis is to assess how the model responds to a variety of model inputs. This allows for quantification of the amount of uncertainty in the model, and results in an estimation of the degree of sensitivity of model outputs to the different model parameters (Salciccioli et al., 2016).

The model inputs as presented in Table 9 have been used as a starting point for the sensitivity analysis. Two different sensitivity analyses have been performed. First, a univariate sensitivity analysis has been conducted. In a univariate sensitivity analysis, only one model input is altered at the same time, keeping other inputs constant. A full multivariate sensitivity analysis was conducted after the univariate analysis, and is able to give more insight into interactions between variations in different model inputs through altering multiple input variables at the same time (Lamboni, 2019).

For both analyses, model input values have been increased and decreased by 10% (in comparison to Table 9), in order to gain the minimum and the maximum value for the sensitivity analysis. The *random-failure-rate* and *vendor-multiplier* have been switched on and off for the analysis, instead of using low and high values. It is uncertain whether or not a *vendor-multiplier* exists, and, if so, how large this multiplier is. Therefore, it is more interesting to compare the existence of a vendor multiplier to a scenario where no vendor multiplier is implemented. The same goes for the *random-failure-rate*: it is more interesting to compare a system without random failures to one that is prone to a random component failure.

Table 11: Univariate Sensitivity Analysis Setup

Input	Min	Medium	Max
attacker-persistence	2	3	4
attack-frequency	0.045	0.05	0.55
containment-successrate	0.63	0.7	0.77
esd-threshold	0.45	0.5	0.55
ids-effectiveness	0.8	0.9	1,00
infection-spread-likelihood	0.45	0.5	0.55
ips-effectiveness	0.81	0.9	0,99
number-of-attackers	9	10	11
random-failure-rate (on-off)	0	0.02	-
Strategy (Distributed when performing analysis on other variables)	Links	Random	Criticality
vendor-multiplier (on-off)	-	0.5	1

In order to provide an uncluttered and more manageable overview of the univariate sensitivity analysis, the decision has been made to not include the sensitivity of all model outputs in the thesis. The following model outputs have been excluded from the univariate sensitivity analysis:

- Availability 100

  Excluded since the percentage of time that the entire system is fully up and running is not as important: a system failure is defined as a dip in performance below 90%. As *Availability 90*, *Failures* and *Overall Availability* are included, this should provide sufficient insight into the model performance.
- Cumulative Monetary Losses

  As shown in section 6.3.2, the *Cumulative Monetary Losses* output is highly dependent on the *Overall Availability*, as well as the *total-expected-profit.* Since *Overall Availability* is included in the analysis, and the *total-expected-profit* is kept constant, this model output is not as relevant in the sensitivity analysis.
- Mean time to repair

  Not included in the analysis as the MTTR = MTBF – MTTF (see section 6.3.2). As these two factors are included in the analysis, the MTTR is not as relevant.
- Random Failures

  The number of random failures is only dependent on the *random-failure-rate*. Only a change in this input will result in a change in this model output. Therefore, it has been excluded from the sensitivity analysis.

Several KDE plots of the univariate sensitivity analysis, as well as bar charts for the multivariate sensitivity analysis are presented in Appendix C. For reasons of clarity, only graphs yielding interesting results are presented, avoiding an excessive number of graphs in the appendix.

The KDE plots of the univariate sensitivity analysis show that the model is not sensitive when it comes to the number of attackers, while the model is more sensitive to other attacker parameters, such as persistence and frequency. When it comes to the strategy of the attackers, the analysis has shown that the ‘Criticality’ strategy results in slightly worse system performance, while the ‘Random’ and ‘Links’ strategies result in more similar system performance.

The model is quite sensitive to all of the different defender parameters. Of these parameters, the model outputs are the most sensitive to the IPS effectiveness. This can easily be explained, as a higher IPS effectiveness prevents the attacker from entering a node altogether, and therefore warrants the best possible system performance.

The introduction of random failures in the model only has a minor impact on the operational performance of the system. The model is, however, quite sensitive to the introduction of a vendor multiplier. The introduction of a vendor multiplier significantly impacts most model outputs, increasing the operational performance of the system.

The findings of the univariate sensitivity analysis are corroborated by the multivariate sensitivity analysis, which includes variations in multiple model inputs simultaneously. The multivariate sensitivity analysis has resulted in bar charts that are easier to interpret when compared to the KDE plots. The charts show not only the sensitivity of the model to changes in input levels of a single input variable in combination with multiple changes in other variables, but display the relative sensitivity of the model to different inputs, too. Overall, when assessing the model sensitivity using input deviations of 10%, the model outputs prove to be the most affected by the *IPS effectiveness* and the *Containment Successrate*. Meanwhile, the model is relatively insensitive to the *Number of Attackers*, as well as the introduction of *Random Failures*.

7.6. Findings

In this chapter, the operationalized ABM model is formalized and presented. The ABM is a translation of the conceptual model, as described in Chapter 6. The model includes a variety of behaviors of the attackers and defenders.

The main job of attacking entities in the model is to investigate and select targets to attack, in order to attempt to disrupt the operability of nodes (control loops) present in the system of the defender. In a system in which attacker behavior impacts the operability of nodes, of the various attacker behaviors, the frequency of attack attempts, as well as the persistence of those attempts have the largest impact on deteriorating the operational performance of the defender's system.

In turn, the main behavior displayed by the system operator is the execution of various steps in the incident response cycle. Of these steps, the effectiveness of the defender's intrusion prevention system appears to have the most impact on the overall model performance. Furthermore, the ability of the defender to effectively contain affected nodes, limiting the spread of disruptions throughout their systems, plays a key role in achieving the goal of maximizing operational system performance. It appears that the introduction of random system failures has very little impact on the overall system performance over the entire runtime.

After implementing the model, various verification and validation steps were performed, to assess whether the conceptual model has been correctly operationalized, and to assess whether the right thing has been modelled. While verification was mainly performed iteratively during model implementation, unit checks and attempting to break the model helped in removing final bugs. An interesting finding retrieved from the vulnerability analysis was that the more specific the circumstances required for a model output to change (successful attack, failure, ESD), the more variability can be observed in the output.

Now that the model is implemented, verified and validated, it can be used to assess the impact of different redundancy strategies on the operational performance of OT at Gate terminal. This will be discussed in the next chapter.

8. Experimental Design and Results

This chapter aims to explore the effect of different redundancy strategies on the operational performance of Gate terminal. Furthermore, it aims to further investigate a potential trade-off between the advantages of added redundancy and the risks the increased attack surface brings to the system. The main goal of this chapter is to formulate an answer on the fourth and final sub-question: *"What redundancy-related cyber-strategies are effective for increasing availability of the industrial processes of Gate terminal?"*

This chapter will first introduce different redundancy strategies, after which an experimental design is presented, which can be used to assess the impact of these different strategies on the system. Finally, the results of the exploratory analysis are presented.

8.1. Formulation of Redundancy Strategies

The aim of this section is to formulate and explain several redundancy strategies that can be used to explore and analyze the performance of the model when various forms of redundancy are implemented.

The formulated strategies for redundancy are two-dimensional, and based on the redundancy and diversity principles as described in section 2.2. When plotting the redundancy and diversity principles on the x and y axis of a coordinate system, respectively, a figure as shown in Figure 14 can be constructed. The redundancy principle is translated to the degree of criticality of the additionally implemented nodes, while the diversity principle relates to the vendors of these nodes.

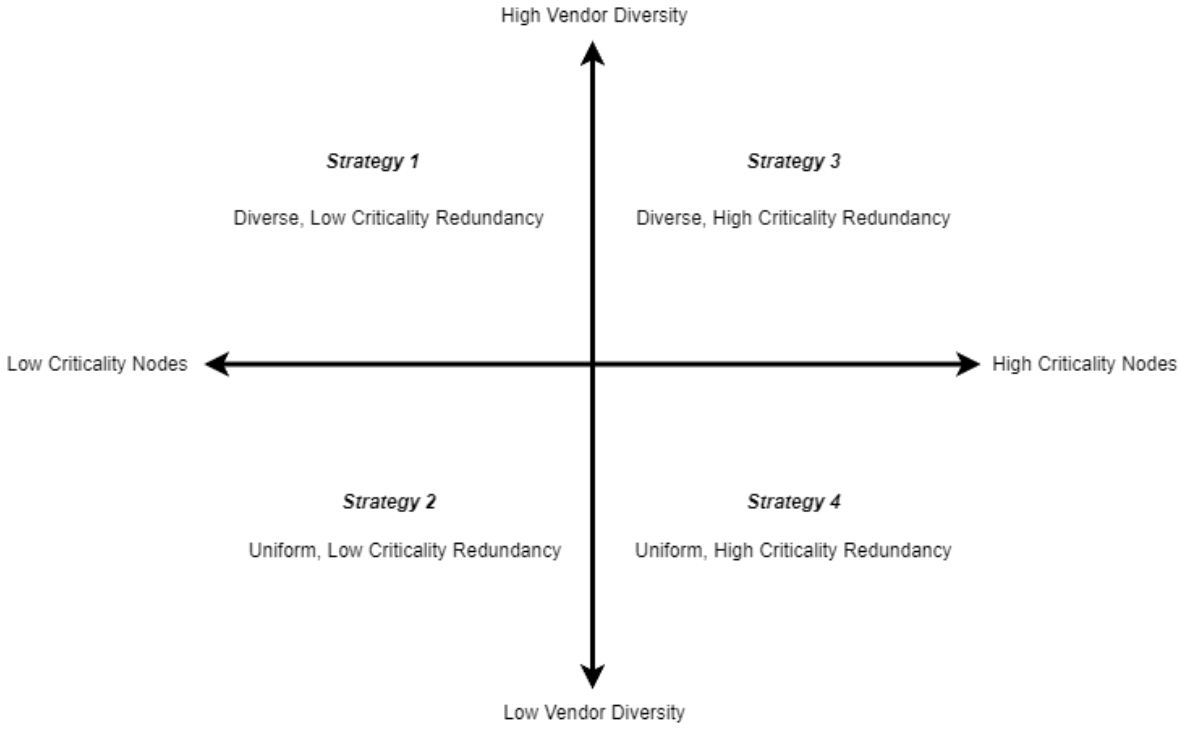


Figure 14: Construction of Redundancy Strategies

In the model, each redundancy strategy implements two additional nodes in each of the industrial processes at the plant. The decision for two nodes increases the impact of each strategy in comparison to only adding a single redundant node, amplifying the interpretability of final experimentation results. The choice is the middle ground between this interpretability/impact, and implementing an unrealistic degree of redundancy: adding more than two additional nodes results in implementing redundancy for more than half of the control loops in the model.

Based on these two axes, four main redundancy strategies can be formulated, based on criticality and different vendors. This results in four main strategies:

1. *Diverse, low criticality redundancy*
   When this strategy is implemented, for each industrial process, the two nodes with the lowest level of criticality are duplicated. For both the original nodes and the duplicates, the criticality is halved. The vendor of each duplicated node will be changed to a vendor that is not yet used in the model.

2. *Uniform, low criticality redundancy*
   When this strategy is implemented, for each industrial process, the two nodes with the lowest level of criticality are duplicated. For both the original nodes and the duplicates, the criticality is halved. The vendor of the duplicated nodes is equal to the vendor of the original nodes.

3. *Diverse, high criticality redundancy*
   When this strategy is implemented, for each industrial process, the nodes two with the highest level of criticality are duplicated. For both the original nodes and the duplicates, the criticality is halved. The vendor of each duplicated node will be changed to a vendor that is not yet used in the model.

4. *Uniform, high criticality redundancy*
   When this strategy is implemented, for each industrial process, the two nodes with the highest level of criticality are duplicated. For both the original nodes and the duplicates, the criticality is halved. The vendor of the duplicated nodes is equal to the vendor of the original nodes.

In order to avoid requiring 18 different vendors in the diverse redundancy strategies - as each process receives 2 extra nodes with different vendors - the same two vendors are implemented in the different processes.

The addition of an extra node in the DCS at the plant could also prove to be beneficial to the performance of the system. While adding an extra DCS may be quite an endeavor with its own pitfalls, it is interesting nevertheless to investigate the behavior of the system when this strategy is implemented, as the DCS appears to be a single point of failure in the system. This results in the fifth and final redundancy strategy.

5. *Addition of DCS node*

8.2. Experimental Setup

In order to gain an insight into the performance of the system when different redundancy strategies are implemented, this section aims to provide an overview of the experiments that are to be performed with the model.

For a proper assessment of the effectiveness of the various strategies, it is vital to simulate each strategy multiple times in a wide variety of scenarios. These scenarios are created by altering various model inputs simultaneously. The set of scenarios could have been constructed as a 'full factorial design', consisting of all possible combinations of input levels for all of the model inputs. This allows for investigating the effect of all the model inputs and their interaction (Das & Dewanjee, 2018), and when combined with the various redundancy strategies allows for the best assessment of the performance of each strategy.

There is, however, a large pitfall when it comes to using a full factorial design for the generation of scenarios: the number of levels and combinations required for a full factorial design would result in an immense number of scenarios and exceed computational restrictions. Therefore, Latin hypercube sampling is implemented to reduce the number of scenarios and simulations required when comparing the different strategies under uncertainty. Latin hypercube generates random samples, which are evenly distributed over the sample space (Loh, 1996). In Table 12 and Table 13, the levels and constants used for the generation of scenarios are presented.

For experimentation, a total of 200 different LHS scenarios have been combined with the 5 presented node-setups, as well as with the base case. For each scenario and strategy combination, the model is run for 50 repetitions. This experimental design has resulted in a total of 60000 model runs, executed using the integrated BehaviorSpace NetLogo feature.

Table 12: LHS Scenario Input Levels

Variable \ Level	0	1	2	3
attacker-persistence	2	3	4	-
attack-frequency	0.045	0.05	0.055	-
containment-successrate	0.63	0.7	0.77	-
ids-effectiveness	0.85	0.9	0.95	-
infection-spread-likelihood	0.45	0.5	0.55	-
ips-effectiveness	0.85	0.9	0.95	-
random-failure-rate	0	0.02	-	-
strategy	0	1	2	3
vendor-multiplier	1	0.5	-	-

Table 13: LHS Scenario Input Constants

Variable	Value
esd-threshold	0.5
number-of-attackers	10
total-expected-profit	75000000

8.3. Results

In this section, the processed results of the execution of the experimental design are presented. The impact of the various redundancy strategies when compared to each other and to the base case is discussed. An overview of all results is presented in Appendix D.

8.3.1. Successful attacks and attack surface

When comparing the different redundancy strategies, an interesting observation can be made with regard to the average number of successful attacks that occur during experimentation. Attackers manage to successfully launch more attacks on the systems with increased redundancy. This finding is illustrated in Figure 15.

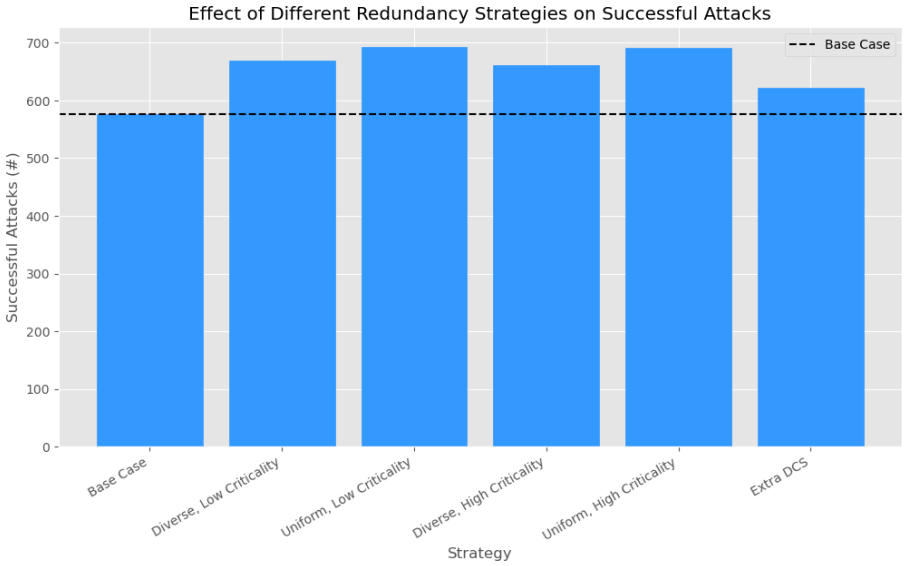


Figure 15: Effect of Different Redundancy Strategies on Successful Attacks

This phenomenon can be attributed to the increased attack surface that results from implementing redundancy in the system. In Table 14, the number of nodes in the system for each strategy is presented. This is indicative of the attack surface of the system, as each node is prone to an attack and presents a potential point of entry for an attacker.

Table 14: Number of Nodes and Vendors per Strategy

Strategy	Number of Nodes	Number of Vendors
Base Case	59	4
Diverse, Low Criticality	77	6
Uniform, Low Criticality	77	4
Diverse, High Criticality	77	6
Uniform, High Criticality	77	4
Extra DCS	60	4

The final interesting behavior that is presented by the model is the impact of diversity on the number of successful attacks. Redundancy strategies that implement diversity through adding nodes with different vendors perform better in the model, when compared to strategies that maintain uniformity in vendors when

adding extra nodes to the system. This phenomenon is shown in Figure 15, where strategies with an equal number of nodes and a higher number of vendors (Table 14) endure fewer successful attacks.

8.3.2. Availability and System Failures

Comparing the various availability metrics as well as system failures yield interesting results, too. When investigating the Availability 100 metric, the experiments show that the base case has the most timesteps with a fully operational system, without any attacks. This finding is in line with expectations, since the base case suffers the least number of successful attacks.

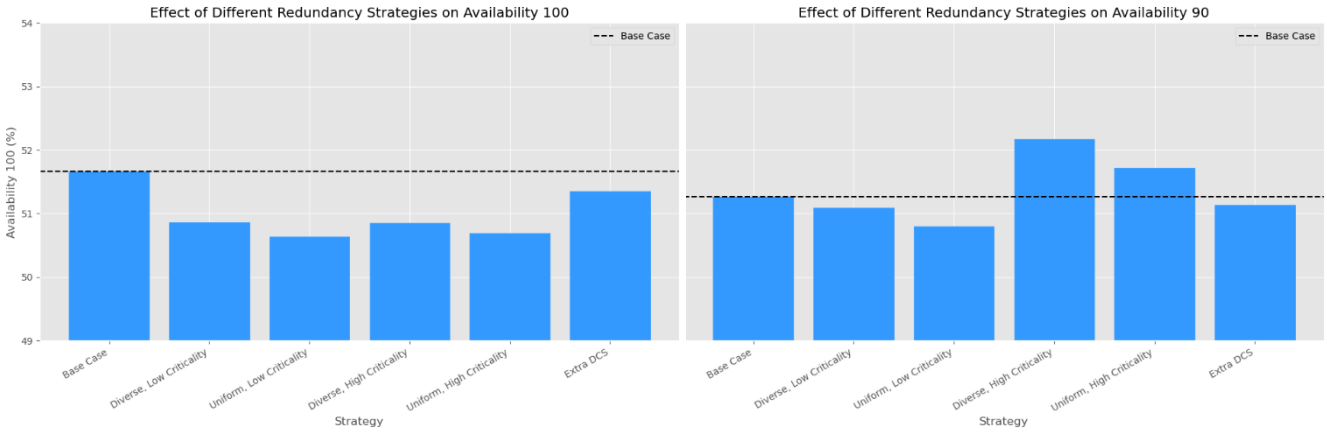


Figure 16: Availability Metrics for the Redundancy Strategies

When investigating the Availability 90 metric, however, the model seems to perform differently when implementing redundancy. When compared to the base case, Availability 90 is almost 1 percentage point higher for the strategy implementing diverse, high criticality redundancy. Likewise, the base case is outperformed by the other strategy that is aimed at implementing high criticality redundancy. The strategies focusing on low-criticality redundancy and the extra DCS strategy both perform worse in comparison to the base case. These findings can partly be explained through the overall availability, which is lower than the base case when experimenting with the low-criticality and the extra DCS strategies, while the high-criticality strategies have a higher overall availability.

Similar strategy performance can be observed when focusing on the number of failures and ESD triggers that occur during experimentation. For both KPIs, the model behaves quite similarly. Therefore, only the system failures metric is discussed. The effect of the redundancy strategies on the number of failures is shown in Figure 17. In the figure, similar to the Availability 90 metric, it can be observed that both of the high-criticality redundancy strategies perform better than the base case, reducing the number of failures by up to approximately 20%. Of these two strategies, the diverse redundancy strategy results in fewer system failures than the uniform redundancy strategy. The low-criticality strategies perform slightly better or slightly worse than the base case, depending on implementation of diverse or uniform redundancy, respectively. The strategy that implements an extra DCS node is slightly inferior to the base case when it comes to the number of failures that occur in the system.

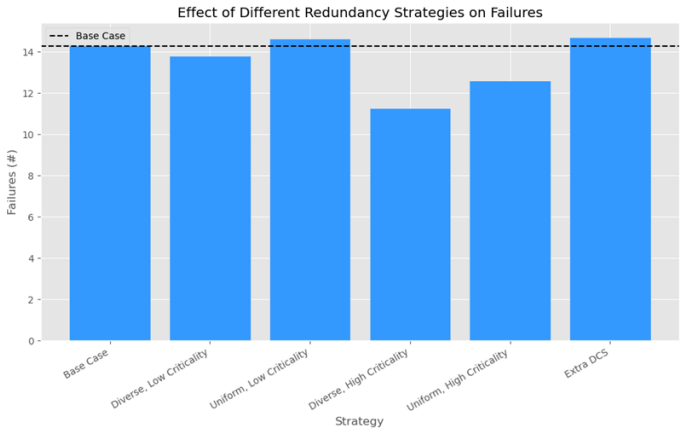


Figure 17: Number Failures for the Redundancy Strategies

The findings with regard to system failures are mostly consistent with the effect of different redundancy strategies when it comes to the MTBF, presented in Figure 18. The strategies that result in fewer failures have a significantly higher MTBF. This is conceptually consistent, since fewer failures over an equal runtime should result in a higher MTBF. It is interesting, however, that strategies that perform worse than the base case with regard to the number of failures have a similar MTBF to the base case, rather than a lower MTBF. This can be explained by the MTTR, which is higher when implementing these strategies. This indicates a longer average failure duration for these strategies.

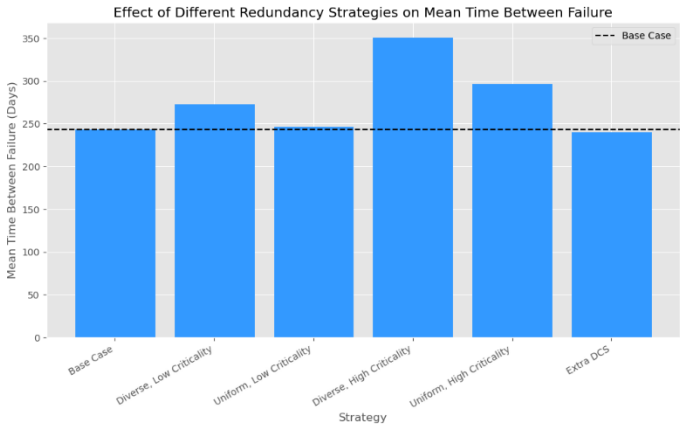


Figure 18: Mean Time Between Failure for the Redundancy Strategies

Overall, when it comes to system availability and the number of failures in the system, it can be concluded that the high-criticality redundancy strategies perform better than the low-criticality strategies. In addition, it appears that the strategies implementing diverse redundancy outperform their counterparts.

8.3.3. Monetary Implications

In the model, the cumulative monetary losses are highly dependent on the overall availability of the nodes in the model. The effect of different redundancy strategies on the cumulative monetary losses is presented in Figure 19. It can be observed that the cumulative monetary losses caused by reduced availability are higher (in comparison to the base case) when implementing one of the low-criticality strategies or the 'Extra DCS' strategy. When implementing a high-criticality redundancy strategy, the monetary losses are lower in comparison to the base case. Furthermore, it can be observed that (once again) the diverse redundancy strategies perform better than their counterparts, resulting in fewer monetary losses than the uniform redundancy strategies.

When investigating the monetary aspects of implementing redundancy, a trade-off that is not included in the model comes into play. Nevertheless, it is important to take this trade-off into account when deciding on the implementation of redundancy. While diverse redundancy, implementing different vendors, consistently outperforms uniform redundancy in all operational aspects, there are significant monetary costs involved with implementing diverse redundancy. These costs originate from an added network complexity, increased maintenance costs, etc. These costs have not been included in the model. Therefore, the actual costs of the different redundancy strategies will be higher than those shown in Figure 19. There will be a further discussion on this trade-off when assessing the limitations of the research in the next chapter.

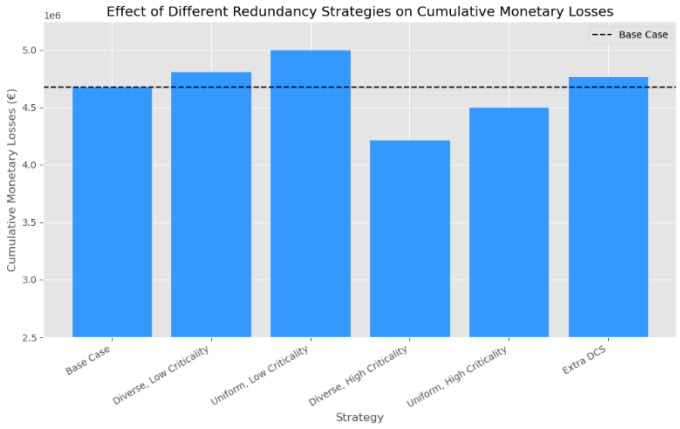


Figure 19: Cumulative Monetary Losses for the Redundancy Strategies

8.3.4. Trade-Off between Attack Surface and Availability

When analyzing the outcomes discussed in section 8.3.1 and 8.3.2, a trade-off between the up- and downsides of redundancy becomes apparent. The trade-off involves weighing the drawbacks of increasing the attack surface with the potential advantages of increased availability through increasing redundancy in the system.

When implementing redundancy in the model, an increase of successful cyberattacks on the system occurs. This increase in successful attacks can be attributed to the increased attack surface of the system, resulting from the addition of nodes and therefore the addition of entry points to the system. Furthermore, a decrease in full availability (Availability 100) can be observed when additional redundancy is implemented.

The advantages of redundancy become apparent when investigating Availability 90, the number of system failures and the number of ESD triggers. Some of the redundancy strategies manage to outperform

the base case on these performance metrics, while other strategies perform worse than the base case. These findings illustrate the trade-off between the increased attack surface and the potential increase in operational performance when implementing redundancy. On the one hand, when redundancy is implemented on system components with high criticality, while the full system uptime might decrease, the Availability 90 and thus system reliability increase. This is especially true when implementing diverse redundancy. On the other hand, when system components with low criticality are redundantly implemented, the disadvantages of the increased attack surface outweigh the advantages of adding redundancy to the system regarding operational performance.

9. Discussion

In this chapter, the model results as presented in Chapter 8 will be discussed. Limitations of the model are presented, as well as their impact on the model outcomes. Furthermore, the link between the outcomes and the reality is discussed, after which suggestions for future research are considered.

9.1. Limitations of the Research

One of the main limitations of the research pertains to the strategies that have been used for experimentation with the model. Since the .txt files used for loading the strategies had to be created manually, only a few strategies have been implemented and used for experimentation. This resulted in quite unspecific strategies, duplicating the two nodes with having the highest or lowest criticality. The use of non-specific strategies for experimentation has resulted in somewhat generic outcomes. While this allows for a better generalization of the implications of the model, the applicability of the model outcomes on Gate terminal is reduced.

A second limitation is introduced by the absence of distinct types of attacks that interrupt the system. Therefore, when interpreting simulation results, it is crucial to consider the implemented attacker model where attacks directly affect the operability of a control loop. The most common attack vectors on critical infrastructures are ransomware and vulnerability exploits. Furthermore, APT's are mainly targeted at critical infrastructures, and could have a significant impact on the performance of industrial processes (Yu et al., 2021). Therefore, the APT is an important threat to consider and investigate. These long-term threats are highly diverse and have an intricate structure. As a result of the intricate and diverse nature of APTs, modeling these threats using ABM is highly challenging. Therefore, the decision has been made to only include general, short-term, attacks with DoS-like consequences, temporarily impacting the operability of nodes. This decision not to include advanced threats like APTs partly limits the link of the research with reality, reducing the applicability of the model.

Another limitation in the model outcomes is related to the cumulative monetary losses that are incurred by cyberattacks. While some redundancy-related strategies prove to be capable of improving the overall availability, reducing the incurred monetary losses, several other costs caused by redundancy are not included in the model. For example, not only do the extra sensors, actuators and PLCs have to be bought and installed (incurring extra costs), they have to be maintained as well. Furthermore, increased OT increases network complexity, which could lead to higher costs as well. The exclusion of these factors necessitates caution when interpreting the monetary impact of different redundancy strategies.

A final limitation of the model is the absence of a key part of any LNG infrastructure: the LNG itself. Actual stocks and flows of LNG in and between the different parts of the plant are not included in the model. As a result, any impact a cyberattack may have on these stocks and flows of LNG is not included in the model. If this was included in the model, interesting results indicating the impact of cyberattacks on the actual send-out of the plant could have been included. However, modelling these stocks and flows is rather difficult using the ABM method. Other methods could have been used to model these LNG stocks and flows, such as system dynamics. While the implemented mode is limited due to the exclusion of LNG, it does give an insight into the operational performance of OT when implementing various redundancy strategies.

9.2. Linking Model Outcomes to Reality

The link of the model outcomes to reality is restricted by several limitations. When making policy recommendations and drawing conclusions from the research, it is important to keep these limitations in mind, as well as to have a deep understanding of the applicability of the model.

An important aspect to keep in mind when evaluating the effectiveness of different redundancy strategies on the operational performance of industrial processes at Gate terminal, is the degree to which an effective incident response cycle is implemented. As discussed in section 7.5.2, the model is quite sensitive to the effectiveness of the defenders IPS, as well as their effectiveness in containing incidents. These factors have a major impact on the overall operational performance. Therefore, it can be stated that the presence of an effective incident response procedure is a key prerequisite for reaping the rewards of implementing a redundancy strategy.

The first discrepancy between the model outcomes and reality appears in the number of successful attacks that occur in the system. The model outcome suggests up to 700 successful attacks over 5 years, which translates to ± 1 successful attack every 2.5 days. While most of the successful attacks are rapidly detected and quarantined by the system operator, this number is still quite large, especially when considering that APTs play a more prominent role in the critical infrastructure context. The model experimentation does allow for insights into the overall behavior and operational performance of the plant when different redundancy strategies are implemented. However, the model outcomes should be interpreted relative to each other, and not be directly translated to reality.

A second disparity between the model and reality is the accessibility of the control loops for outside parties. One of the main model assumptions is that the OT at the plant is relatively easily accessible to unauthorized parties. While there are defense mechanisms in place, the model fails to capture several technical intricacies, such as a layered network design as described in section 4.1, including demilitarized zones, firewalls, and other measures to decrease outside accessibility to the implemented OT at the company. This disparity has to be considered when interpreting model outcomes such as successful attacks, failures and ESD triggers: in reality, the values of these KPIs may very well be lower, due to implemented technical intricacies that hinder and prevent easy access to the OT systems.

Additionally, a break with reality is introduced through the function used for calculating the availability of the industrial processes in the model. While the calculation does allow for gaining insights into the impact of the redundancy strategies on system availability, it comes with a flaw, limiting the link with reality. In the model, even when an entire control loop is inoperable, the industrial process can remain available to a certain degree. In the model, an individual control loop only contributes partly to the availability of its process, and does not disrupt the entire process when it is inoperable, however, this is not realistic in all cases. Fault tree modelling mitigates this issue, but fails in several other ways, as mentioned in section 6.3.2.

Finally, as mentioned in the limitation section, actual stocks and flows of LNG are not included in the model. This has consequences for the placement of the various nodes in the system. In the model, all nodes are part of an industrial process. The different processes are relatively isolated. In reality, however, several process variables are measured ‘in between’ the various locations at the plant. LNG flow, for example, is per definition measured between two different locations, like the flow of LNG from a vessel to a tank. In the model, the nodes controlling these process variables are presented at both the origin and destination processes, creating a breach with reality.

9.3. Suggestions for Future Research

This research focused on the improvement of the operational performance of OT in LNG infrastructures through increasing redundancy, specifically in the context of cyberattacks. Based on the research, several recommendations and suggestions can be made for future scientific research on this (and adjacent) subjects. These recommendations are presented in this section.

The first recommendation for future research is aimed at formulating and experimenting with a wider variety of redundancy implementations. This allows for finding a highly specific redundancy strategy, catered to the OT at Gate terminal. To this end, the current model has to be altered to allow for easy process-specific redundancy configurations, acting as policy levers. Furthermore, exploratory modelling packages such as the EMA workbench can be implemented to experiment with large quantities of different combinations of policy levers and scenarios. These combinations can be used in order to find the most robust and reliable specific redundancy strategy for a large number of different model scenarios.

The second recommendation pertains to the modelling method that was used to model the OT in LNG infrastructures. In future research, it would be interesting to research a similar or identical main research question, using a different modelling method. As the model used in this research did not include the actual stocks and flows of LNG in the various plant locations, it would be interesting to include this using a modelling method that is more suitable for modelling these stocks and flows, such as system dynamics (Sterman, 2001). Furthermore, this method could be used to capture feedback loops, time delays, et cetera. If LNG stocks and flows are modelled, the actual send-out of the plant, as well as the impact of cyberattacks and other failures on the send-out of the plant can be analyzed. Finally, a threat modelling and analysis approach can provide a mathematical view into the workings of various cyberthreats, and their potential impact on the operational performance of Gate terminal.

Another recommendation for future research is modelling more specific types of attacks, as well as implementing strategic defense systems. Modelling a highly advanced type of attack, such as APTs, could provide useful insights in strategic attacker behavior. This can provide guidance for defenders to better defend against these types of threats. Modelling strategic defense systems, such as the implementation of honeypots in the network, can provide a more comprehensive insight into the interaction between attackers and defenders of a system. This knowledge can be used as well to optimize defensive systems for defenders of OT in critical infrastructures.

Furthermore, this research showed the existence of a trade-off between an increased attack surface and the advantages of redundancy. Moreover, a trade-off between the increased costs and the increased efficiency of diverse redundancy was exposed. The fist trade-off can be investigated in future research, aimed at optimizing redundancy using a numerical trade-off analysis. This involves maximizing the difference between advantages gained through redundancy and the disadvantages caused by increasing the attack surface. The optimum (if any) is most likely to be different for different types of systems. Therefore, it would be interesting to investigate this trade-off and its optimum in different types of IT and OT systems. The second trade-off can be analyzed using a cost-benefit analysis, exploring and optimizing the difference between the costs and benefits of diverse redundancy.

Finally, modelling the individual components of control loops may yield valuable insights when investigating a potential improvement in operational performance of OT through redundancy. If instead of modelling an entire control loop as a single entity, the different sensors, actuators and PLCs are separately modelled, different system behavior could be observed. For instance, the behavior of the system when it is affected by communication-based attacks can be observed. When a man-in-the-middle attack is used, which slightly alters communications between the sensor, PLC and actuator, an increase in redundancy might not be as effective in improving operational performance. Future research could focus on the effectiveness of implementing redundancy for different types of cyberattacks.

10. Conclusion and Reflection

In the final chapter of this thesis, answers to all of the research questions will be formulated. Moreover, suggestions are presented for policymakers in the field of OT security. Lastly, this chapter will reflect on the scientific and societal contributions of this thesis.

10.1. Answering Research Questions

In this section, after answering the four sub-questions, an answer to the main research question will be formulated.

Sub-question 1: "What is the role of OT in the industrial processes of Gate terminal?"

It is vital to recognize the importance of critical infrastructures – such as the energy sector – for the proper functioning of society. The rise of interconnected OT in these industries allows for automating, monitoring, and controlling the infrastructures effectively and in real-time, but also comes with pitfalls. The increase of convergence between the IT and OT domains exposes the traditionally isolated OT systems to cyber threats that were previously only applicable to the IT domain. These threats can negatively impact the operability of OT, and therefore deteriorate the operational performance of the plant.

Gate terminal, being responsible for more than 1/3rd of the Dutch national gas supply through the import of LNG, is a key service provider in ensuring gas access to the Netherlands and Northwestern Europe. The company carries out a variety of industrial processes, among which (un)loading LNG from vessels, storing the liquid, as well as regasifying the LNG to natural gas, and pumping it in the underground gas network.

The industrial processes at the company are measured using various process control variables, such as pressure, flow, etc. These variables are managed using various control loops, implemented PLCs, sensors, and actuators. Ultimately, all control loops are managed from the CCR, using a DCS. Without the proper functioning of the implemented OT, the industrial processes at the plant cannot be successfully and safely executed. Therefore, OT plays a vital role in the continuity of business operations at Gate terminal. Disruptions in the operation of OT can have far-reaching consequences to society, due to the critical nature of energy infrastructures.

Sub-question 2: "How do different attacker and defender behaviors impact the availability of industrial processes of Gate terminal?"

There is a multiplicity of malicious parties that have a wide range of incentives to disrupt OT. While these incentives range from shallow goals – such as bragging rights – to using cyberattacks for military reasons, it is important to note a trend in these incentives. Traditionally, financial motivations have been the main driving force behind cyberattacks. However, it has become increasingly interesting to disrupt or destruct the availability of OT at actors in the energy sector, due to the vitality of energy supply for public welfare, industry, and military purposes.

The main attack vectors for critical infrastructures are ransomware attacks and vulnerability exploits. These threats have the potential to decrease the operability of OT in these infrastructures. Another important threat that plays a role in the context of critical infrastructures is an APT. The goal of this threat is long-term, undetected access to the system, which can be used for a multiplicity of actions (monitoring, changing process variable targets, physical destruction, etc.). Hereby, an APT can deteriorate the two most important aspects of OT security – availability and integrity – as well as system confidentiality. There exists another applicable threat affecting these CIA aspects, which is a DoS attack. This type of attack aims to deny access to system services, and therefore has the potential to deteriorate the operational performance of industrial processes at Gate terminal.

The main behavior of the defender, or system operator, involves the execution of the incident response cycle. Hereby, the defender attempts to prevent attacks from happening altogether, mitigate impacts resulting from incidents, and perform a post-incident assessment to improve the execution of the cycle. Good implementation and execution of all steps of the incident response cycle at Gate terminal will improve its capability to prevent and handle incidents, ultimately increasing the availability and operational performance of OT at the company.

Sub-question 3: "What behavior can be observed in the operational technology in the industrial processes of Gate terminal when simulating cyberattacks?"

Answering this sub-question involved simulating with the operationalized model of OT at Gate terminal. In the model, attacks directly affect the degree of operability of a control loop, mimicking the effects of ransomware, DoS, et cetera. During the simulation, several emergent behaviors and interactions can be observed.

When looking at the different modelled attacker parameters, it seems that two main factors have a high negative impact on the overall performance of the defender's systems. When the frequency of attack attempts is relatively high, as well as when the attacker's persistence during attack attempts is increased, the attacker has the highest impact on the system. The number of attackers appears to be less relevant, although this could be attributed to model assumptions made with regard to target selection.

The defender has a large impact on the final model behavior through the implementation and execution of the incident response cycle. The effectiveness of the IPS is the most decisive step in the cycle, having the most impact on overall model outcomes. Furthermore, if the system operator is able to effectively contain detected incidents, the spread of disruptions throughout the system is limited significantly, reducing the impact that attackers have on the operational performance of OT at the company.

Sub-question 4: "What redundancy-related cyber-strategies are effective for increasing availability of the industrial processes of Gate terminal?"

When it comes to the effectiveness of implementing various redundancy strategies in the operationalized model of Gate terminal, two interesting trade-offs can be observed. Firstly, implementing redundancy inevitably expands the attack surface of the system, through an increase of possible entry points. Model simulation has shown that this added exposure increases the likelihood of a successful attack occurring. An increase in system availability is therefore not guaranteed when implementing redundancy: it might even deteriorate when implementing an improper strategy.

The second trade-off pertains to the costs of implementing diverse redundancy: while diverse redundancy strategies consistently outperform their uniform counterparts, this type of redundancy could be rather expensive due to overhead-costs. The increase in network complexity, vendor contracts, and maintenance costs may have a large impact on the cost-effectiveness of diverse redundancy.

The model has shown that the selection of control loops to be redundantly implemented is vital for the effectiveness of a redundancy strategy. When loops that are less critical for the functionality of industrial processes are redundantly implemented, the availability of the system deteriorates when compared to the original situation. On the other hand, implementing redundancy for process-critical control loops increases the availability of the system.

Aside from control loop selection, diversification is an important factor that impacts the effectiveness of redundancy strategies. Strategies that implement different vendors, increasing network segmentation, consistently increase system performance with regard to availability in comparison to their counterparts that implement uniform control loops.

Main research question: ***"To what extent does the implementation of redundancy enhance the operational performance of operational technology in the industrial processes of Gate terminal in the face of cyber threats, in order to maintain the availability of business services?"***

It is vital that suppliers of natural gas, such as Gate terminal, maintains availability and continuity of business services for the proper functioning of society. 1/3rd of the Dutch national supply of natural gas is provided by Gate terminal, which can be endangered by a variety of cyberattacks. These attacks, including ransomware, APTs and DoS attacks, have the potential to significantly impact the operational performance of the industrial processes of Gate terminal, through the disruption of their OT. The occurrence of these attacks has risen through the increased convergence between the IT and OT domains, exposing the historically isolated field of OT to threats that previously only existed in the IT domain. Implementation of security measures is therefore key in decreasing the risk of disruptions and system failures, which could result in a decrease in Dutch energy safety.

In an effort to increase the operational performance of OT at Gate terminal in the face of cyber threats, a redundancy strategy can be implemented. While this may come with numerous advantages, trade-offs are introduced by the inevitable increase in the attack surface of the system, and the increased costs resulting from diverse redundancy. Due to these trade-offs, redundancy is to be implemented with caution in order to ensure that its benefits outweigh the drawbacks.

To evaluate the effectiveness of redundancy strategies for increasing operational performance at Gate terminal, an ABM has been implemented. The model is used to simulate attacks with DoS-like effects, reducing the operability of various control loops in the industrial processes of the plant. After experimenting with different strategies, two main factors appear to affect the effectiveness of a strategy. The first factor is the degree of criticality of the redundantly implemented control loop. Application of redundancy in high criticality control loops could prove effective, while redundancy in low criticality control loops may have counterproductive effects on the operational performance of the company. These adverse effects can be attributed to the increased attack surface of the system.

Another factor that plays a role in the effectiveness of redundancy in increasing operational performance, is the degree of diversity applied. Diverse redundancy, while significantly increasing the overhead costs of redundancy, proves to be more effective in increasing operational performance than implementing uniform redundancy.

An important remark has to be made when it comes to the extent to which redundancy is capable of increasing operational performance. A redundancy strategy can only be as effective as the incident response procedure implemented by Gate terminal: if redundancy is implemented, but the system operator is incapable of dealing with occurring incidents, redundancy by itself cannot be a lifesaver for the company's operational performance in the face of cyber threats.

10.2. Policy recommendations

In order to ensure energy safety and gas for the Netherlands and Northwestern Europe, it is vital that the implemented OT at companies in this sector is well-protected against cyberattacks. To this end, using findings from this research, this chapter first presents policy recommendations for Gate terminal for improving its OT security. Furthermore, recommendations for governmental agencies are presented, which can be used to aid and incentivize companies in critical infrastructures in improving their capacity to deal with cyber threats.

The following possible policy recommendations for Gate terminal can be done:

- Iteratively improve all steps in the incident response cycle using a Plan Do Check Act procedure, with a focus on quality intrusion prevention and swift and efficient incident containment.
- Implement redundancy with careful consideration. Random implementation of OT can prove to be counterproductive.
- Collaborate with other parties present in the energy sector, using direct communications and alliances or through government initiatives.

Firstly, in order for Gate terminal to be protected against and prepared for cyberattacks, it is vital that all steps in the incident response cycle are implemented and continuously improved. To this end, the company could implement the Plan-Do-Check-Act (PDCA) model. This allows for iterative improvement of the incident response process, which could decrease the impact of cyberattacks on the operational performance of the company. Of the various steps in the incident response cycle, the company should specifically focus on the improvement of its intrusion prevention system and the ability to swiftly contain ongoing cyber threats: these two steps seem to have the largest impact on the operational performance of the system in the context of cyberattacks.

The second recommendation for Gate terminal pertains to the implementation of redundancy in their OT infrastructure. If the company chooses to implement extra redundancy with the goal of improving its operational performance in the face of cyberattacks, there should be a focus on the control loops that are most critical to the ability to execute various industrial processes. Before implementing redundancy, a comprehensive cost-benefit analysis (CBA) should be performed. A CBA can provide insights into the possible financial gains or costs resulting from implementing redundancy. Furthermore, it can be helpful in deciding whether the extra monetary investment required to implement diverse redundancy instead of uniform redundancy outweighs the potential benefits.

Finally, collaboration is key for Gate terminal to be more aware of vulnerabilities, and better prepared for incidents. Gate terminal should partner up with other (inter)national companies active in the energy sector. These companies face similar challenges when it comes to cyber threats. Collaboration can help in improving awareness of cyber risks, threats, vulnerabilities and incidents in the entire sector, which aids in increasing cyber preparedness and the ability to rapidly handle incidents. Sector-wide collaboration can be achieved through leveraging alliances of the company, or through tapping into governmental initiatives, such as the Dutch National Cyber Security Centre (NCSC).

Aside from policy recommendations for Gate terminal, some recommendations for governmental policymakers are presented that can aid in increasing OT security in critical infrastructures:

- Sharpening legislation and norms for securing critical infrastructures
- Providing knowledge, aid, and audits

One of the main goals of the government is to warrant public welfare. Ensuring stable and consistent access to energy is therefore a main concern of governmental agencies. To address this concern through increasing cybersecurity in the OT of critical infrastructures, two main policy recommendations are presented.

Firstly, it is vital for the Dutch government to sharpen legislation and provide and enforce cybersecurity norms for critical infrastructures. A first step to this end would be to speed up the conversion of the European NIS2 directive to the Dutch legal context, increasing enforceable cybersecurity requirements for companies in vital sectors. Whereas currently the NIS2 is expected to be applicable in September 2024 (PWC, n.d.), a more rapid implementation can help in increasing security standards more rapidly, increasing the overall level of cybersecurity of critical infrastructures.

Not only should the government sharpen legislation and norms for cybersecurity in critical infrastructures, it should also help companies affected by the legislation to the best of their ability to achieve compliance with these new regulations. By providing knowledge and offering a helping hand to companies affected by the new regulations, the government has the power to increase the level of OT security throughout various critical sectors, including the energy sector. Through security audits, the sharpened legislation can be enforced, compelling affected companies to comply with the heightened requirements for their security. Ultimately, these policy recommendations can increase the quality of incident response cycles throughout the entire energy sector, increasing energy security for the Netherlands.

10.3. Reflection

In the following section, a reflection will be made on the scientific and societal contributions of the findings of this thesis.

10.3.1. Scientific Contributions

In Chapter 2 of this thesis, a literature review highlighting the state of the art with regard to modelling security systems has been presented. The review showed that there is research modelling specific critical infrastructure systems, as well as other research modelling redundancy in critical infrastructures in general. There is, however, a gap in existing scientific research when it comes to modelling a specific LNG infrastructure using ABM, investigating the effect of redundancy on the operational performance of the infrastructure.

This thesis has provided an explorative agent-based model that can be used to contribute to filling the specified gap in existing scientific research. The application of ABM in the context of LNG infrastructures, simulating cyberattacks, offers a new perspective on the problem at hand. The model can aid in investigating emergent behavior patterns of attacker-defender models in critical infrastructures. For this thesis, the model was applied to test the effectiveness of various redundancy strategies on the operational performance of OT at Gate terminal. Hereby, this thesis aids in innovating redundancy modelling of OT in critical infrastructures, in the face of cyber threats.

The model provides increased insights in the functioning of the attacker-defender interaction in LNG infrastructures, the effectiveness of different redundancy strategies, and the prerequisites for reaping the rewards of redundancy. As a result, the model and the thesis provide communicative value, and can therefore be used to inform policy makers, private parties and researchers about attacker-defender behavior and the potential impact of cyberattacks on their operational performance. Moreover, the impact of occurring incidents and the effectiveness of various strategies for mitigating this impact can be communicated.

Furthermore, the model confirmed findings about the effectiveness of attack surface reduction on the likelihood of an attack on the system, as presented in section 5.2.4. Simultaneously, exploration and experimentation with the model exposed a trade-off between the advantages of redundancy, and the downsides of the increase in attack surface when implementing redundancy. While there does exist some scientific research on the potential downsides of redundancy in OT, for example by Ma et al. (2019), this flaw of redundancy is often disregarded by vendors of OT and ICS experts (Ma et al., 2019), and receives relatively little attention in existing scientific research, too. This thesis contributes to this area by further analyzing and exploring this drawback of redundancy, and highly encourages future research on optimizing this trade-off.

Finally, this thesis can form the basis for an advanced treat analysis and a numerical trade-off analysis. The thesis identified different threats, and investigated the potential impact these threats can have on the operational performance of a critical infrastructure using an exploratory model. These findings can be used by scientists as a basis for a more in-depth threat analysis, to be performed in future research. Moreover, the trade-off between an increased attack surface and redundancy advantages that was found in this thesis can be further investigated.

10.3.2. Societal Contributions

The importance of energy safety for a properly functioning society cannot be overemphasized. Due to the interconnectivity of critical infrastructures, without safety of supply of gas, other vital sectors will be crippled. Since natural gas is used for the generation of electricity, large problems would not only occur in other industrial sectors, but in civilian households, too. Without a steady supply of gas, the quality of life for civilians will deteriorate, as people do not have enough gas for home applications, such as cooking, access to hot water, and central heating during winter times.

This thesis aims to aid in enhancing energy safety in the Netherlands and Northwestern Europe, where Gate terminal is responsible for a part of the energy supply. Due to the attractiveness of Gate terminal to ill-willing parties, their cybersecurity practices and implementations are paramount for maintaining safety of supply in their target market. Therefore, this thesis has investigated the potential of redundancy strategies to increase the overall operational performance of OT in the industrial processes at Gate terminal. Based on the outcomes of the thesis, policy recommendations have been presented, for Gate terminal as well as governmental agencies. These recommendations could aid in increasing the operational performance of OT, at Gate terminal and other companies in the energy sector in the face of cyber threats. Hereby, the thesis aims to contribute to the enhancement of energy safety for the Netherlands and Northwestern Europe.

References

Agrawal, N., & Kumar, R. (2022). Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-wide Survey. *ISA Transactions*, *130*, 10–24. https://doi.org/10.1016/J.ISATRA.2022.03.018

Ali, S., al Balushi, T., Nadir, Z., & Hussain, O. K. (2018). ICS/SCADA System Security for CPS. *Cyber Security for Cyber Physical Systems*, 89–113. https://doi.org/10.1007/978-3-319-75880-0_5

Al-Salman, H. I., & Salih, M. H. (2019). A review Cyber of Industry 4.0 (Cyber-Physical Systems (CPS), the Internet of Things (IoT) and the Internet of Services (IoS)): Components, and Security Challenges. *Journal of Physics: Conference Series*, *1424*(1). https://doi.org/10.1088/1742-6596/1424/1/012029

Alqudhaibi, A., Aloseel, A., Jagtap, S., & Salonitis, K. (2022). Identifying and Predicting Cybersecurity Threats in Industry 4.0 Based on the Motivations Towards a Critical Infrastructure. *Advances in Manufacturing Technology XXXV*. https://doi.org/10.3233/ATDE220599

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, *2018*(5), 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Arınç, İ. S. (2007). The EU-Russian Gas Interdependence and Turkey. *Insight Turkey*, *9*(4), 23–36. https://www.jstor.org/stable/26328515

Ashiku, L., & Dagli, C. (2020). Agent Based Cybersecurity Model for Business Entity Risk Assessment. *IEEE International Symposium on Systems Engineering, Proceedings*, 1–6. https://doi.org/10.1109/ISSE49799.2020.9272234

Ashoor, A. S., & Gore, S. (2011). Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Communications in Computer and Information Science*, *196 CCIS*, 497–501. https://doi.org/10.1007/978-3-642-22540-6_48

Baezner, M., & Robin, P. (2017). Stuxnet. *CSS Cyberdefense Hotspot Analyses*, *4*. https://doi.org/10.3929/ETHZ-B-000200661

Baybutt, P. (2017). Issues for security risk assessment in the process industries. *Journal of Loss Prevention in the Process Industries*, *49*, 509–518. https://doi.org/10.1016/J.JLP.2017.05.023

Berkeley, A. R., & Wallace, M. (2010). A Framework for Establishing Critical Infrastructure Resilience Goals. *National Infrastructure Advisory Council*.

Bommannavar, P., Alpcan, T., & Bambos, N. (2011). Security risk management via dynamic games with learning. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2011.5963330

Brown, G. G., & Cox, L. A. T. (2010). How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Analysis*, *31*(2), 196–204. https://doi.org/10.1111/J.1539-6924.2010.01492.X

Buzdugan, A., & Căpățână, G. (2020). Factors for a Decision Support System in Critical Infrastructure Cyber Risk Management. *Romanian Cyber Security Journal*, *2*(2), 67–73.

CBS. (2022). *Waar komt ons gas vandaan?* https://www.cbs.nl/nl-nl/longread/diversen/2022/waar-komt-ons-gas-vandaan-?

Chai, W. (2023). *What is the CIA Triad? Definition, Explanation, Examples*. Techtarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Chappin, E. J. L., & Dijkema, G. P. J. (2010). Agent-based modelling of energy infrastructure transitions. *International Journal of Critical Infrastructures*, *6*(2), 106–130. https://doi.org/10.1504/IJCIS.2010.03107

Chen, L., & Leneutre, J. (2009). A game theoretical framework on intrusion detection in heterogeneous networks. *IEEE Transactions on Information Forensics and Security*, *4*(2), 165–178. https://doi.org/10.1109/TIFS.2009.2019154

Cheung, K. F., & Bell, M. G. H. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *European Journal of Operational Research*, *291*(2), 471–481. https://doi.org/10.1016/J.EJOR.2019.10.019

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-61r2

Colbert, E. J. M., Sullivan, D. T., & Kott, A. (2017). Cyber-Phisical War Gaming. *Journal of Information Warfare*, *16*(3), 119–133.

Conklin, W. A. (2016). IT vs. OT security: A time to consider a change in CIA to include Resilience. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2016*, 2642–2647. https://doi.org/10.1109/HICSS.2016.331

Cox, L. A. (2008). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, *28*(6), 1749–1761. https://doi.org/10.1111/J.1539-6924.2008.01142.X

Cox, L. A. (2009). Game Theory and Risk Analysis. *Risk Analysis*, *29*(8), 1062–1068. https://doi.org/10.1111/J.1539-6924.2009.01247.X

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Fifth edition ed.). SAGE Publications, Inc.

Cristopher, J. (2023). *Industrial Cyber Risk Management: Integrating IT And OT Security To Fully Address Business Risk*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/02/13/industrial-cyber-risk-management-integrating-it-and-ot-security-to-fully-address-business-risk/

Das, A. K., & Dewanjee, S. (2018). Optimization of Extraction Using Mathematical Models and Computation. *Computational Phytochemistry*, 75–106. https://doi.org/10.1016/B978-0-12-812364-5.00003-1

DeGuglielmo, N. P., Basnet, S. M. S., & Dow, D. E. (2020). Introduce Ladder Logic and Programmable Logic Controller (PLC). *2020 Annual Confnce Northeast Section (ASEE-NE)*, 1–5. https://doi.org/10.1109/ASEENE51624.2020.9292646

Denisova, S. (2019). Digitalization: Opportunity or challenge for energy industry? *Youth Technical Sessions Proceedings*, *1*(1), 11–17. https://doi.org/10.1201/9780429327070-2/

Department of Energy. (n.d.). *Operational Technology Cybersecurity for Energy Systems* . Retrieved April 12, 2023, from https://www.energy.gov/eere/femp/operational-technology-cybersecurity-energy-systems

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*, *21*(11), 3901. https://doi.org/10.3390/S21113901

Ding, Z., Gong, W., Li, S., & Wu, Z. (2018). System Dynamics versus Agent-Based Modeling: A Review of Complexity Simulation in Construction Waste Management. *Sustainability*, *10*(7), 2484. https://doi.org/10.3390/SU10072484

Dobrota, Đ., Lalić, B., & Komar, I. (2013). Problem of Boil-off in LNG Supply Chain. *Transactions on Maritime Science*, *2*, 91–100. https://doi.org/10.7225/toms.v02.n02.001

Dornelles, J. de A., Ayala, N. F., & Frank, A. G. (2022). Smart Working in Industry 4.0: How digital technologies enhance manufacturing workers' activities. *Computers and Industrial Engineering*, *163*. https://doi.org/10.1016/J.CIE.2021.107804

Dragos. (2023). *Everything You Need to Know to Defend Against ICS/OT Cyber Threats in 2023*. Dragos. https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Infographic-2022.pdf

Einy, S., Oz, C., & Navaei, Y. D. (2021). The Anomaly- And Signature-Based IDS for Network Security Using Hybrid Inference Systems. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/6639714

Ibidunmoye, E. O., Alese, B. K., & Ogundele, O. S. (2013). A Game-theoretic Scenario for Modelling the Attacker-Defender Interaction. *Journal of Computer Engineering & Information Technology*, *2*(1), 1. https://doi.org/10.4172/2324-9307.1000103

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2014). Game theory meets information security management. *IFIP Advances in Information and Communication Technology*, *428*, 15–29. https://doi.org/10.1007/978-3-642-55415-5_2

Finnan, K., & Nakagawa, W. (2021). *The Roles of DCS and SCADA in Digital Transformation*. Automation. https://www.automation.com/en-us/articles/september-2021/roles-dcs-scada-digital-transformation

Firesmith, D. G. (2003). Common Concepts Underlying Safety, Security, and Survivability Engineering. *Software Engineering Institute*.

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics*, *210*, 15–26. https://doi.org/10.1016/J.IJPE.2019.01.004

Gartner. (2015). *Definition of Operational Technology (OT)*. Gartner IT Glossary. https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Gate terminal. (2021). *Gate terminal has received ISCC certification*. https://www.gateterminal.com/en/nieuwsberichten-archive/gate-terminal-has-received-iscc-certification/

Gate terminal. (n.d.a.). *Gate terminal: access gateway for global supply of LNG*. Retrieved March 15, 2023, from https://www.gateterminal.com/gate-terminal/

Gate terminal. (n.d.b.). *Terminal Functions*. Retrieved March 15, 2023, from https://www.gateterminal.com/en/gate-terminal/functions/functions-terminal/

Gate terminal. (n.d.c.). *Facts & Figures*. Retrieved March 23, 2023, from https://www.gateterminal.com/en/gate-terminal/profiel/facts-figures/

Halimaa, A. A., & Sundarakantham, K. (2019). Machine learning based intrusion detection system. *Proceedings of the International Conference on Trends in Electronics and Informatics*, 916–920. https://doi.org/10.1109/ICOEI.2019.8862784

Hasan, S., Dubey, A., Karsai, G., & Koutsoukos, X. (2020). A game-theoretic approach for power systems defense against dynamic cyber-attacks. *International Journal of Electrical Power & Energy Systems*, *115*, 105432. https://doi.org/10.1016/J.IJEPES.2019.105432

Horowitz, B. M., & Pierce, K. M. (2013). The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems. *Systems and Information Engineering*, *16*(4), 401–412. https://doi.org/10.1002/SYS.21239

Janssen, M. A. (2005). Agent-Based Modelling. *Modelling in Ecological Economics*, *155*(1), 172–181. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=bad35e6993edf98f937735b8daf407e0c14977b8

Janssen, S., & Sharpanskykh, A. (2017). Agent-based modelling for security risk assessment. *Lecture Notes in Computer Science*, *10349*, 132–143. https://doi.org/10.1007/978-3-319-59930-4_11/

Janssen, S., Sharpanskykh, A., & Curran, R. (2019). Agent-based modelling and analysis of security and efficiency in airport terminals. *Transportation Research Part C: Emerging Technologies*, *100*, 142–160. https://doi.org/10.1016/J.TRC.2019.01.012

Jaquet-Chiffelle, D. O., & Loi, M. (2020). Ethical and unethical hacking. In *The ethics of cybersecurity* (pp. 179–204). Springer. http://www.springer.com/series/776

Karanikas, N. (2018). Revisiting the relationship between safety and security. *International Journal of Safety and Security Engineering*, *8*(4), 547–551. https://doi.org/10.2495/SAFE-V8-N4-547-551

Kebande, V. R. (2022). Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. *Forensic Science International: Reports*, *5*. https://doi.org/10.1016/J.FSIR.2022.100257

Kiran, V., Rani, S., & Singh, P. (2020). Towards a Light Weight Routing Security in IoT Using Non-cooperative Game Models and Dempster–Shaffer Theory. *Wireless Personal Communications*, *110*(4), 1729–1749. https://doi.org/10.1007/S11277-019-06809-W

Kinslow, J. (2006). Physical and IT security: The case for convergence. *Journal of Security Education*, *2*(1), 75–91. https://doi.org/10.1300/J460V02N01_06

Kordy, B., Mauw, S., Radomirović, S., & Schweitzer, P. (2011). Foundations of attack-defense trees. *Formal Aspects of Security and Trust*, 80–95. https://doi.org/10.1007/978-3-642-19751-2_6/

Kral, P. (2021). The Incident Handler's Handbook. *SANS Institute*. https://sansorg.egnyte.com/dl/6Btqoa63at

Kshetri, N., & Voas, J. (2017). Hacking Power Grids: A Current Problem. *Computer*, *50*(12), 91–95. https://doi.org/10.1109/MC.2017.4451203

Kugler, R. L. (2009). Deterrence of Cyber Attacks. *Cyberpower and National Security*, *320*, 309–340.

Kumar, A., & Nayyar, A. (2020). si3-Industry: A Sustainable, Intelligent, Innovative, Internet-of-Things Industry. *Advances in Science, Technology and Innovation*, 1–21. https://doi.org/10.1007/978-3-030-14544-6_1/

Lamboni, M. (2019). Multivariate sensitivity analysis: Minimum variance unbiased estimators of the first-order and total-effect covariance matrices. *Reliability Engineering & System Safety*, *187*, 67–92. https://doi.org/10.1016/J.RESS.2018.06.004

Lanthier, P. (n.d.). *Understanding the Difference Between Reliability and Availability*. Reliabiilty Web. Retrieved April 26, 2023, from https://reliabilityweb.com/tips/article/understanding_the_difference_between_reliability_and_availability

Laszka, A., Abbas, W., Vorobeychik, Y., & Koutsoukos, X. (2020). Integrating redundancy, diversity, and hardening to improve security of industrial internet of things. *Cyber-Physical Systems*, *6*(1), 1–32. https://doi.org/10.1080/23335777.2019.1624620

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. *Computational Methods in Applied Sciences*, *56*, 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Lewis, J. (2011). Cyberwar thresholds and effects. *IEEE Security and Privacy Magazine*, *9*(5), 23–29. https://doi.org/10.1109/MSP.2011.25

Li, H., & Liu, D. (2010). Research on intelligent intrusion prevention system based on Snort. *2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering*, *1*, 251–253. https://doi.org/10.1109/CMCE.2010.5610483

Liang, X., & Xiao, Y. (2013). Game theory for network security. *IEEE Communications Surveys and Tutorials*, *15*(1), 472–486. https://doi.org/10.1109/SURV.2012.062612.00056

Linacre, N. A., Cohen, M. J., Koo, B., & Birner, R. (2008). The Use of Threat, Vulnerability, and Consequence (TVC) Analysis for Decision Making on The Deployment of Limited Security Resources. *Wiley Handbook of Science and Technology for Homeland Security*, 1–9. https://doi.org/10.1002/9780470087923.HHS404

Linacre, N. A., Koo, B., Rosegrant, M. W., Msangi, S., Falck-Zepeda, J., Gaskell, J., Komen, J., Cohen, M. J., & Birner, R. (2005). Security Analysis for Agroterrorism: Applying the Threat,

Vulnerability, Consequence Framework to Developing Countries. *International Food Policy Research Institute*.

Lippmann, R. P., & Ingols, K. W. (2005). *An Annotated Review of Past Papers on Attack Graphs*. Defense Technical Information Center. https://apps.dtic.mil/sti/citations/ADA431826

Loh, W. L. (1996). On Latin hypercube sampling. *The Annals of Statistics*, *24*(5), 2058–2080. https://doi.org/10.1214/AOS/1069362310

Low, H. (2015). How to improve system availability and minimize down time with Hercules MCUs? *Texas Instruments*. https://www.ti.com/lit/wp/spny008/spny008.pdf?ts=1685524569578

Lutkevich, B. (2021). *What is an intrusion detection system (IDS)?* Techtarget. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

Ma, R., Cheng, P., Zhang, Z., Liu, W., Wang, Q., & Wei, Q. (2019). Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber-Physical System. *IEEE Internet of Things Journal*, *6*(6), 9783–9793. https://doi.org/10.1109/JIOT.2019.2931349

Malleson, N. (2012). Using agent-based models to simulate crime. *Agent-Based Models of Geographical Systems*, 411–434. https://doi.org/10.1007/978-90-481-8927-4_19/

Manadhata, P., & Wing, J. M. (2004). Measuring a System's Attack Surface. *School of Computer Science Carnegie Mellon University Pittsburgh*.

Mathezer, S. (2021). *Introduction to ICS Security Part 2*. SANS Institute. https://www.sans.org/blog/introduction-to-ics-security-part-2/

Matos, J. C., & Casas, J. R. (2018). An Overview of the European Situation on Quality Control of Existing Bridges-COST Action TU1406 Assessment of bridge condition and safety based on measured vibration level View project An Overview of the European Situation on Quality Control of Existing Bridges-COST Action TU1406. *Proceedings of the 40th IABSE Symposium*, 19–21. https://doi.org/10.2749/nantes.2018.s27-59

Maras, M.-H. (2021). Cybersecurity: Preparedness. *Encyclopedia of Security and Emergency Management*, 217–221. https://doi.org/10.1007/978-3-319-70488-3_302

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. *Australian Information Security Management Conference*, 149–155. https://doi.org/10.4225/75/5a84f7b595b4e

Nagaraju, V., Fiondella, L., & Wandji, T. (2017). A survey of fault and attack tree modeling and analysis for cyber risk management. *IEEE International Symposium on Technologies for Homeland Security*. https://doi.org/10.1109/THS.2017.7943455

Nas, S. (2015). The Definitions of Safety and Security. *Journal of ETA Maritime Science*, *3*(2), 53–54. https://doi.org/10.5505/JEMS.2015.42713

NCSC. (n.d.a.). *Denial of Service (DoS) guidance*. Retrieved May 30, 2023, from https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

NCSC. (n.d.b.) *Risk management – Using attack trees to understand cyber security risk.* Retrieved July 11, 2023, from https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk

Nikolic, I., Van Dam, K. H., & Kasmire, J. (2013). Practice. In K. H. Van Dam, I. Nikolic, & Z. Lukszo (Eds.), Agent-based modelling of socio-technical systems (Vol. 9, pp. 73-137). Dordrecht: Springer Science & Business Media.

NIST. (n.d.a.). *Advanced Persistent Threat - Glossary*. National Institute of Standards and Technology. Retrieved May 31, 2023, from https://csrc.nist.gov/glossary/term/advanced_persistent_threat

NIST. (n.d.b.). *DoS - Glossary*. National Institute of Standards and Technology. Retrieved May 30, 2023, from https://csrc.nist.gov/glossary/term/DoS

Nochenson, A., & Heimann, C. F. L. (2012). Simulation and game-theoretic analysis of an attacker-defender game. *Lecture Notes in Computer Science*, *7638*, 138–151. https://doi.org/10.1007/978-3-642-34266-0_8/

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/IET-NET.2017.0207

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/RISA.12844

Port of Rotterdam. (n.d.). *LNG terminal*. Retrieved March 15, 2023, from https://www.portofrotterdam.com/en/logistics/cargo/lng/lng-terminal

Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R., & Misurec, J. (2021). Application perspective on cybersecurity testbed for industrial control systems. *Sensors*, *21*(23). https://doi.org/10.3390/S21238119

Pursiainen, C. (2009). The Challenges for European Critical Infrastructure Protection. *Journal of European Integration*, *31*(6), 721–739. https://doi.org/10.1080/07036330903199846

PWC. (n.d.). *Nieuwe Europese richtlijn NIS2: strengere eisen cybersecurity*. Retrieved June 23, 2023, from https://www.pwc.nl/nl/actueel-en-publicaties/themas/risk-regulation/nieuwe-europese-richtlijn-nis2-strengere-eisen-cybersecurity.html

Rand, W., & Rust, R. T. (2011). Agent-Based Modeling in Marketing: Guidelines for Rigor. *International Journal of Research in Marketing*, *28*(3), 181–193. https://doi.org/10.1037//0033-2909.103.3.411

Richards, M. G., Hastings, D. E., Rhodes, D. H., & Weigel, A. L. (2007). Defining Survivability for Engineering Systems. *Conference on Systems Engineering Research*, 1–22.

Rijksoverheid. (2023). *Nederland niet meer afhankelijk van energie uit Rusland*. Rijksoverheid. https://www.rijksoverheid.nl/actueel/nieuws/2023/02/10/nederland-niet-meer-afhankelijk-van-energie-uit-rusland

Rybnicek, M., Tjoa, S., & Poisel, R. (2014). Simulation-Based Cyber-Attack Assessment of Critical Infrastructures. *Enterprise and Organizational Modeling and Simulation*, *191*, 135–150. https://doi.org/10.1007/978-3-662-44860-1_8

Salciccioli, J. D., Crutain, Y., Komorowski, M., & Marshall, D. C. (2016). Sensitivity analysis and model validation. *Secondary Analysis of Electronic Health Records*, 263–271. https://doi.org/10.1007/978-3-319-43742-2_17/FIGURES/4

Samuelson, L. (1996). Bounded rationality and game theory. *The Quarterly Review of Economics and Finance*, *36*(2), 17–35. https://doi.org/10.1016/S1062-9769(96)90006-X

Sears, J. R. (2001). Maintainability: The missing piece of the availability puzzle. *Twenty-Third International Telecommunications Energy Conference INTELEC 2001*, 399–405. https://doi.org/10.1049/CP:20010628

Soikkeli, J., Casale, G., Munoz-Gonzalez, L., & Lupu, E. C. (2022). Redundancy Planning for Cost Efficient Resilience to Cyber Attacks. *IEEE Transactions on Dependable and Secure Computing*, *20*(2). https://doi.org/10.1109/TDSC.2022.3151462

Solak, S., & Zhuo, Y. (2020). Optimal policies for information sharing in information system security. *European Journal of Operational Research*, *284*(3), 934–950. https://doi.org/10.1016/J.EJOR.2019.12.016

Sterman, J. D. (2001). System Dynamics Modeling: Tools for Learning in a Complex World. *California Management Review*, *43*(4).

Tolo, S., & Andrews, J. (2023). Fault Tree Analysis Including Component Dependencies. *IEEE Transactions on Reliability*. https://doi.org/10.1109/TR.2023.3264943

Tranchita, C., Hadjsaid, N., Viziteu, M., Rozel, B., & Caire, R. (2010). ICT and powers systems: An integrated approach. *Securing Electricity Supply in the Cyber Age*, *15*, 71–109. https://doi.org/10.1007/978-90-481-3594-3_5

Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *The Computer Journal*, *61*(9), 1389–1406. https://doi.org/10.1093/COMJNL/BXY002

Voigt, L. (2018). *6 Incident Response Steps to Take After a Security Event*. Exabeam. https://www.exabeam.com/incident-response/steps/

Vopak. (2022). *NEWS - LNG - Gate terminal expand its capabilities*. https://www.vopak.com/newsroom/news/news-lng-gate-terminal-expand-its-capabilities

Wagner, W., & van Gelder, P. H. A. J. M. (2013). Applying RAMSSHEEP analysis for risk-driven maintenance. *Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, ESREL 2013*, 703–713. https://doi.org/10.1201/B15938-109

Wang, P., & Govindarasu, M. (2020). Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid. *IEEE Transactions on Smart Grid*, *11*(4), 3447–3456. https://doi.org/10.1109/TSG.2020.2970755

Wilensky, U., & Rand, W. (2015). *An introduction to agent-based modeling : modeling natural, social, and engineered complex systems with NetLogo*. The MIT Press.

Williams, T. J. (1994). The Purdue enterprise reference architecture. *Computers in Industry*, *24*(2–3), 141–158. https://doi.org/10.1016/0166-3615(94)90017-5

Williamson, G. (2015). *What''s the difference between OT, ICS, and SCADA?* KuppingerCole Analysts. https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

Yahalom, R., Steren, A., Nameri, Y., Roytman, M., Porgador, A., & Elovici, Y. (2019). Improving the effectiveness of intrusion detection systems for hierarchical data. *Knowledge-Based Systems*, *168*, 59–69. https://doi.org/10.1016/J.KNOSYS.2019.01.002

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers & Security*, *110*, 102450. https://doi.org/10.1016/J.COSE.2021.102450

Yee, C. K., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT in Education*, *8*(2), 34–42. https://doi.org/10.37134/JICTIE.VOL8.2.4.2021

Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A. K., & Khan, F. A. (2021). Securing Critical Infrastructures: Deep-Learning-Based Threat Detection in IIoT. *IEEE Communications Magazine*, *59*(10), 76–82. https://doi.org/10.1109/MCOM.101.2001126

Yurcik, W., & Doss, D. (2002). A Survivability-Over-Security (SOS) Approach to Holistic Cyber-Ecosystem Assurance Log Anonymization and Information Management (LAIM) View project Security Incident Fusion Tools (SIFT) View project. *IEE Workshop on Information Assurance*.

Zhao, X. (2020). Attack-Defense Game Model: Research on Dynamic Defense Mechanism of Network Security. *International Journal of Network Security*, *22*(6), 1037–1042. https://doi.org/10.6633/IJNS.202011_22(6).19

Zhu, Q., & Rass, S. (2018). Game Theory Meets Network Security A Tutorial. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, *18*(4), 2163–2165. https://doi.org/10.1145/3243734

Appendices

Appendix A: Model Operationalization

In this appendix, flowcharts of all main model procedures are presented, and briefly explained.

Flowcharts of Attacker Procedures

Investigate and select

The investigate and select procedure is performed by attackers that do not yet have a target to attack. If a random float below 1 is smaller than the attack frequency, a new target will be set for the attacker, based on its attack strategy. When a target is selected, the attacker moves to the target, where it ultimately will attempt to perform an attack on the target.

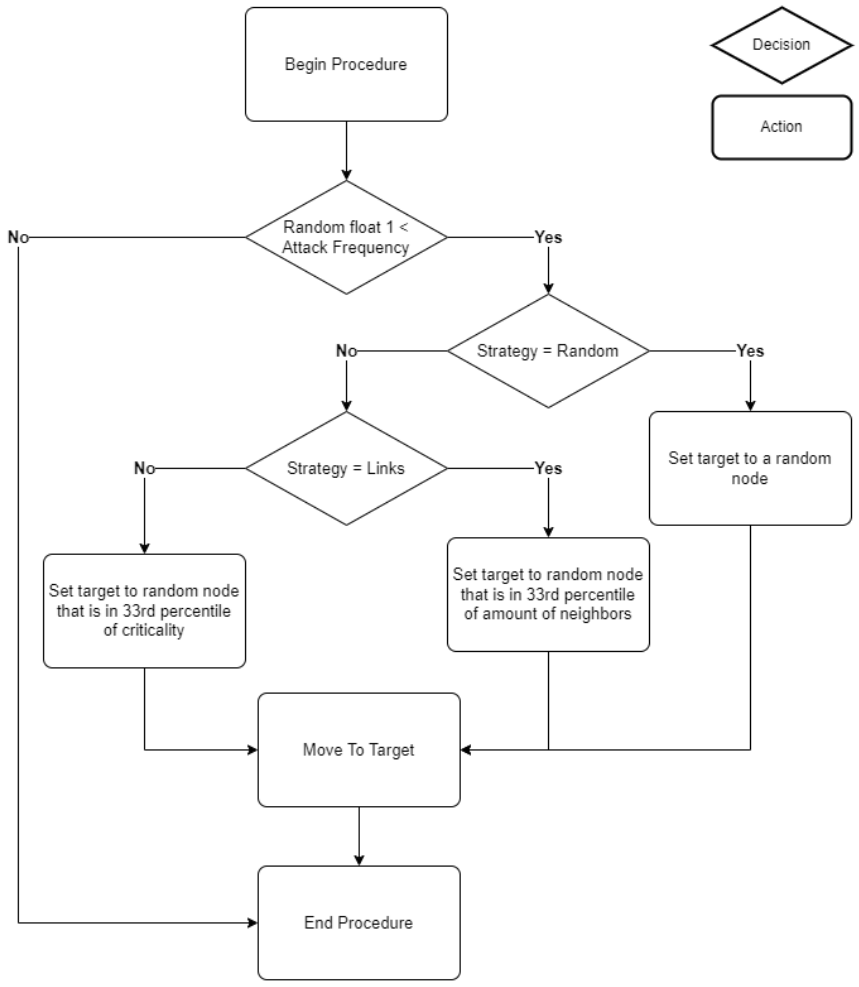


Figure 20: Investigate and Select Procedure

Attempt and perform attack

This procedure is called when an attacker that doesn't have ongoing attacks is located at its selected target, and attempts to perform an attack on the respective node. When a random float below 1 is greater than the IPS effectiveness, the defenders IPS is successfully bypassed by the attacker. The attacker can then perform an attack on its target, which is visualized using a directed link.

If the IPS is not successfully bypassed, the number of breach attempts of the attacker is increased by 1. If the number of breach attempts is higher than the attacker-persistence, the attacker gives up, returning to its original location and removing the initially targeted node as its target.

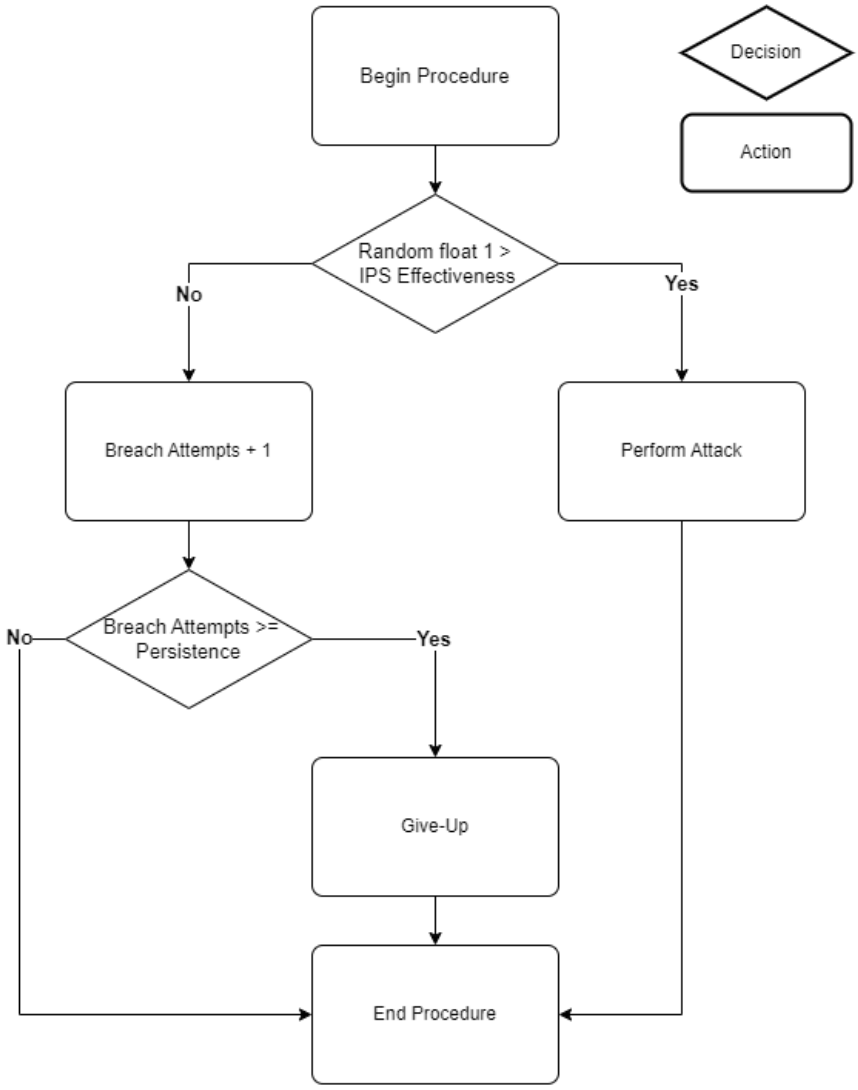


Figure 21: Attempt and Perform Attack Procedure

Disrupt node

When an attacker has any ongoing attacks on a node, it will attempt to disrupt this node. Nodes cannot be disrupted when they are part of an industrial process that is shut down through ESD. The attacker can disrupt nodes through multiplying its attack power (< 1) with the operability ($0 \leq Operability \leq 1$) of the node.

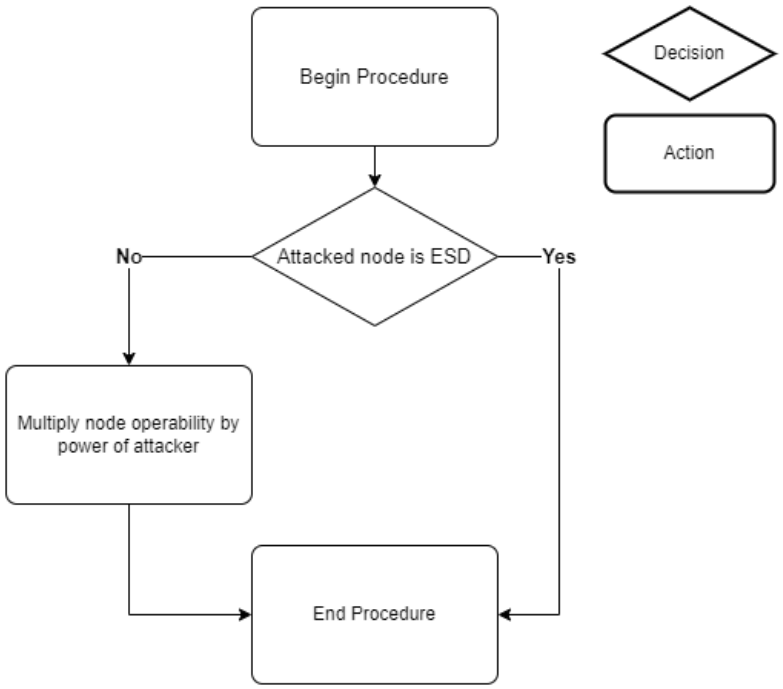


Figure 22: Disrupt Node Procedure

Spread Infection

The final procedure of an attacker involves spreading through the defender's nodes. There are some constraints on spreading, that are checked before new attacks are instigated. First, if the entry point of the attacker (= 'Target') is shut down through ESD, the attacker cannot spread its infection throughout the system. Furthermore, nodes to which the attacker can potentially spread its infection cannot be shut down through ESD, and have to be normally functioning (or failed randomly). A random number of the nodes eligible for being spread to are selected, and attack-attempts are initiated.

To incorporate the likelihood of spreading the infection throughout the system, for each of the potential targets, a comparison is made between the vendor of the origin of the spread and vendor of the potential target. When the vendors of these nodes are equal, the infection will spread with a likelihood of 'infection-spread-likelihood'. When the nodes have different vendors, the spread of the infection is more difficult, multiplying the 'infection-spread-likelihood' with the 'vendor-multiplier'.

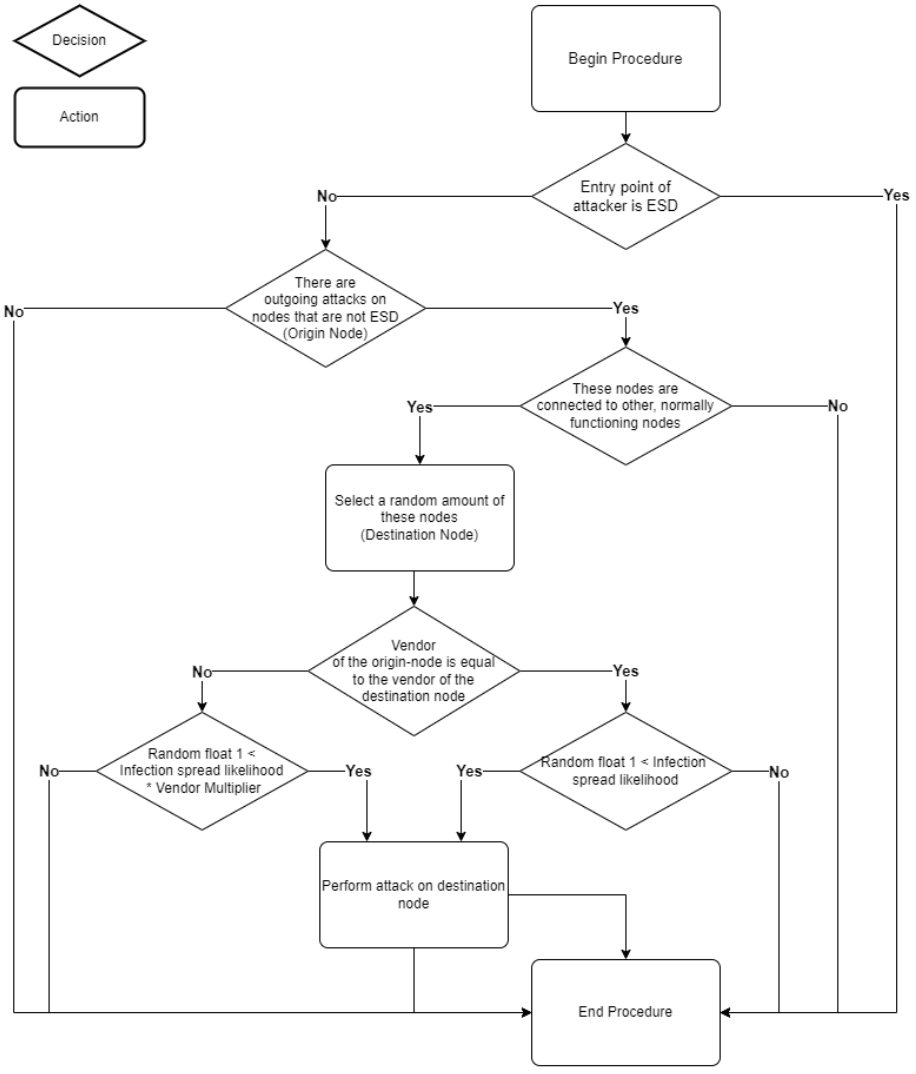


Figure 23: Spread Infection Procedure

Flowcharts of Defender Procedures

Detect ongoing attacks

The defender's first routine is detecting ongoing attacks in the system. Only when attacks are detected, they can ultimately be removed from the system. Detection happens using the defender's IDS system. If there is an ongoing attack that is not yet detected, the defender will recognize this attack if a random float below 1 is smaller than the IDS effectiveness.

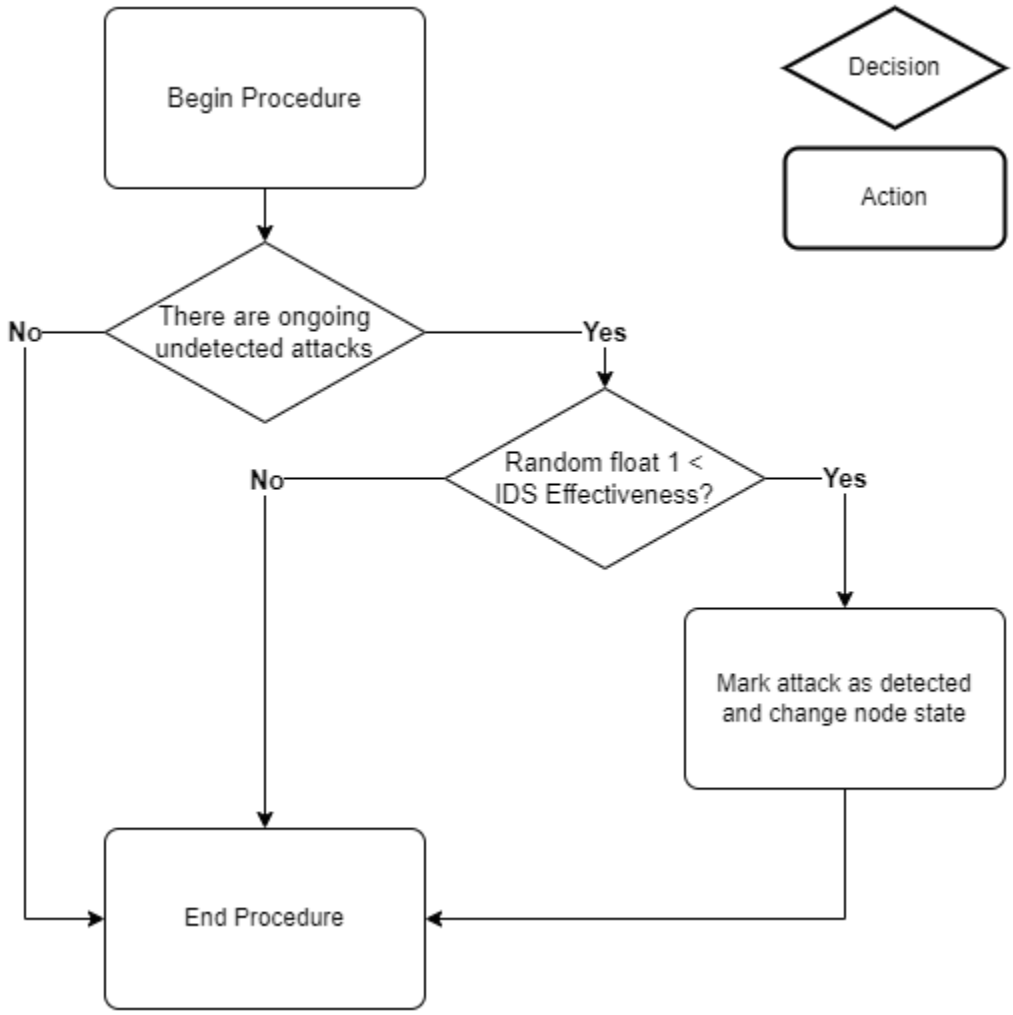


Figure 24: Detect Ongoing Attacks Procedure

Quarantine attacked nodes

This procedure is aimed at placing nodes that have been affected by an attack or by a random component failure in quarantine. This involves assessing whether nodes are being disrupted by attacks that have been detected by the IDS, as investigating nodes that have randomly failed. Depending on the containment success rate, attacks nodes affected by one of these two factors are quarantined, after which the attacks can be removed, and the nodes can start recovering.

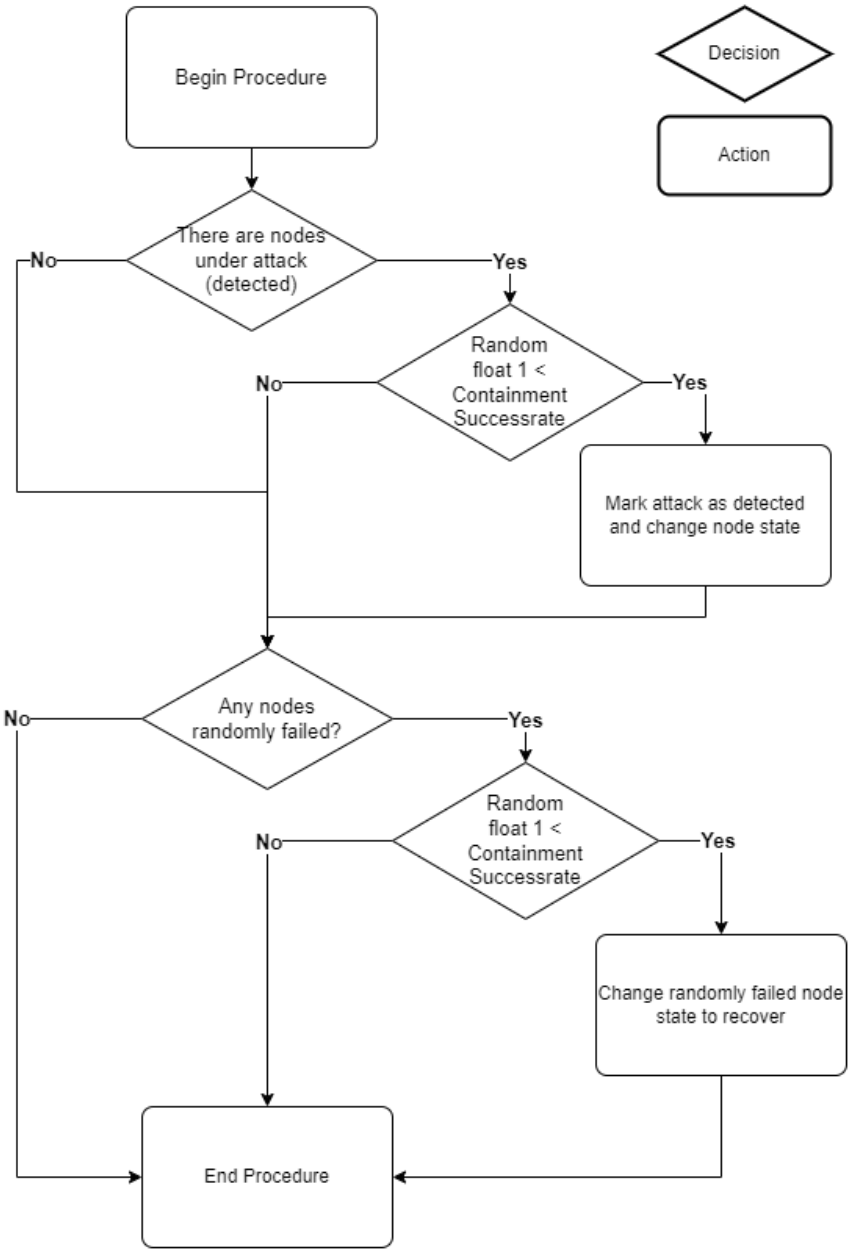


Figure 25: Quarantine Attacked Nodes Procedure

Remove attacks

The ‘remove attacks’ procedure allows the defender in the system to remove the attack from quarantined nodes. Each attack has a removal time, which is reduced by 1 in each time step. When the removal time of the attack has reached zero, the attack is removed from the attacked node. When that happens, based on other outgoing attacks of the attacker, the attacker either relocates to another node that has been infected by the attacker, or the attacker gives up, and goes back to investigate and select another target node to attack.

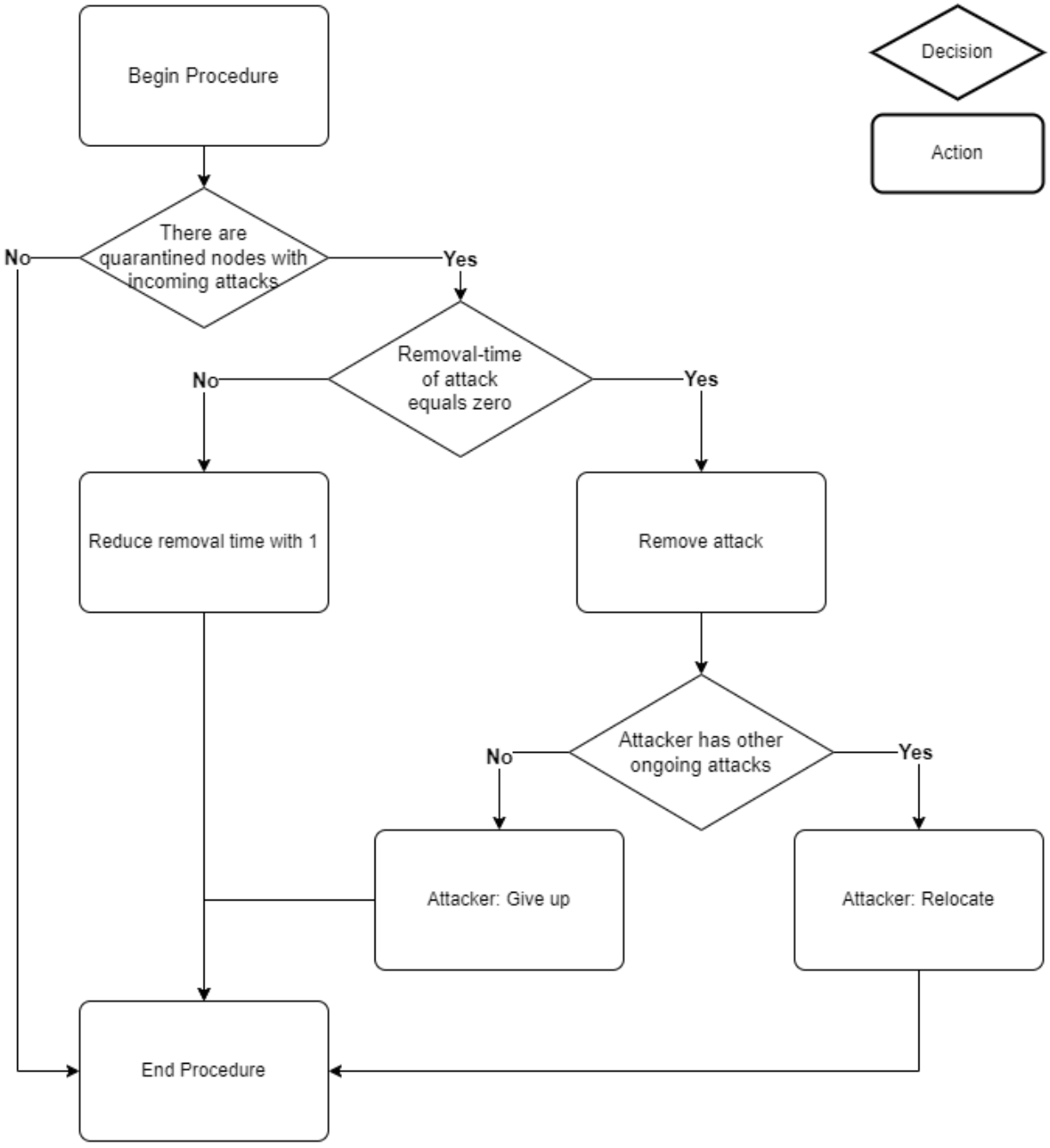


Figure 26: Remove Attacks Procedure

Recover node

When a node is in quarantine, and is successfully relieved of all incoming attacks, the system operator can start recovering the node with this procedure. Recovering a node happens gradually: when the node is severely damaged, the increase in operability is bigger than a node that is not as severely disrupted. Furthermore, when a node is fully recovered, the state of the node is set to normal operation. Not only quarantined nodes are recovered using this procedure: nodes that have been shut down through ESD are also recovered by the defender through this procedure. When all nodes in a process shut down through ESD, including the interface node, have fully recovered, the state of these nodes is changed to operational mode. The ESD itself will be lifted in the 'operate-esd' procedure.

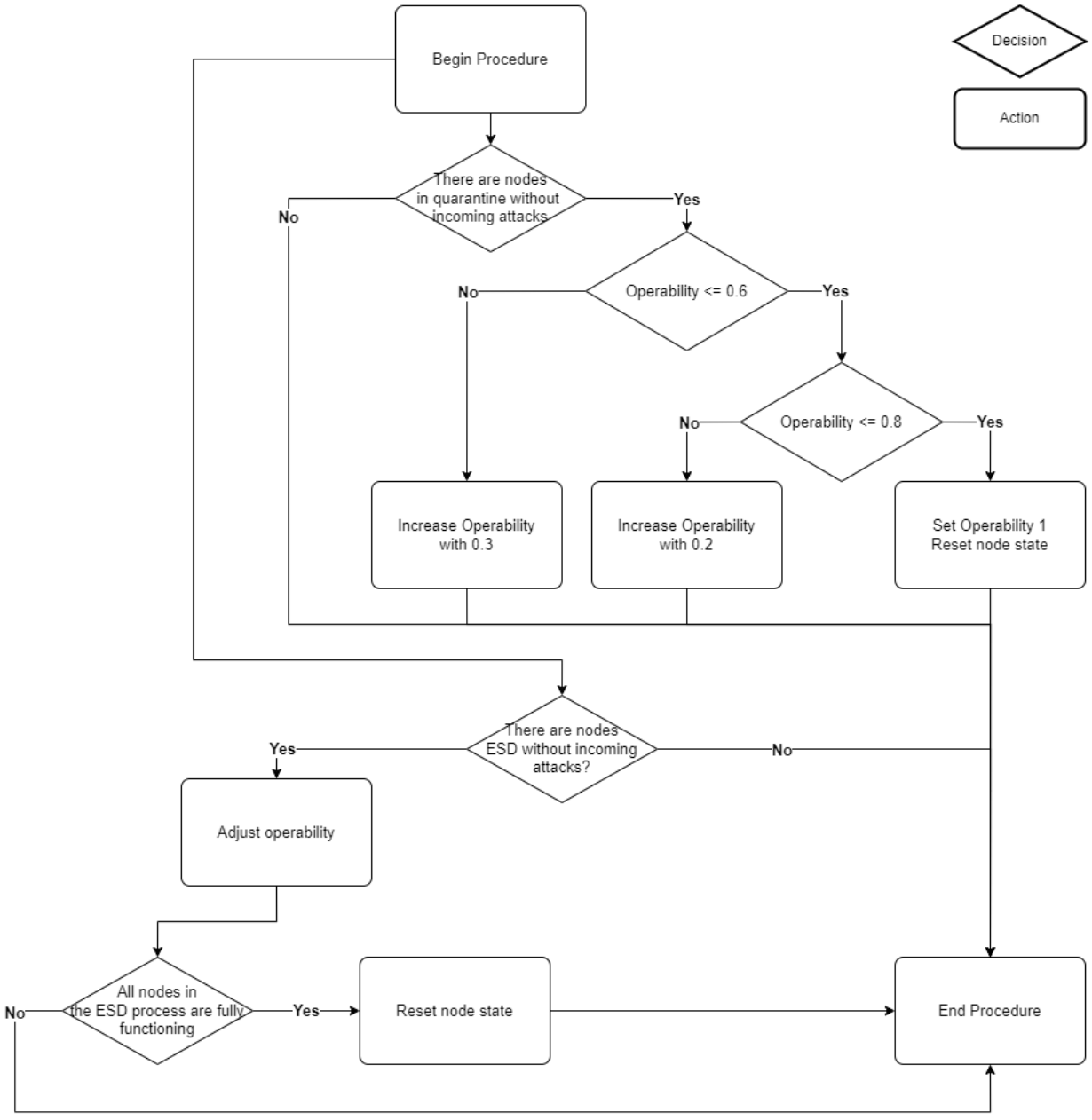


Figure 27: Recover Node Procedure

Operate ESD

This procedure is used to trigger and release the emergency shutdown system (ESD) on one of more of the industrial processes in the plant. Each timestep, the procedure triggers ESD for each node in a process if the overall availability is below the ESD threshold (of 50%). When ESD is triggered, the operability of all of the nodes in that process are set to 0, as the process is completely shut down. ESD can be released for the nodes in a process, if all attacks have been removed from the nodes in that process, and if all nodes are fully recovered.

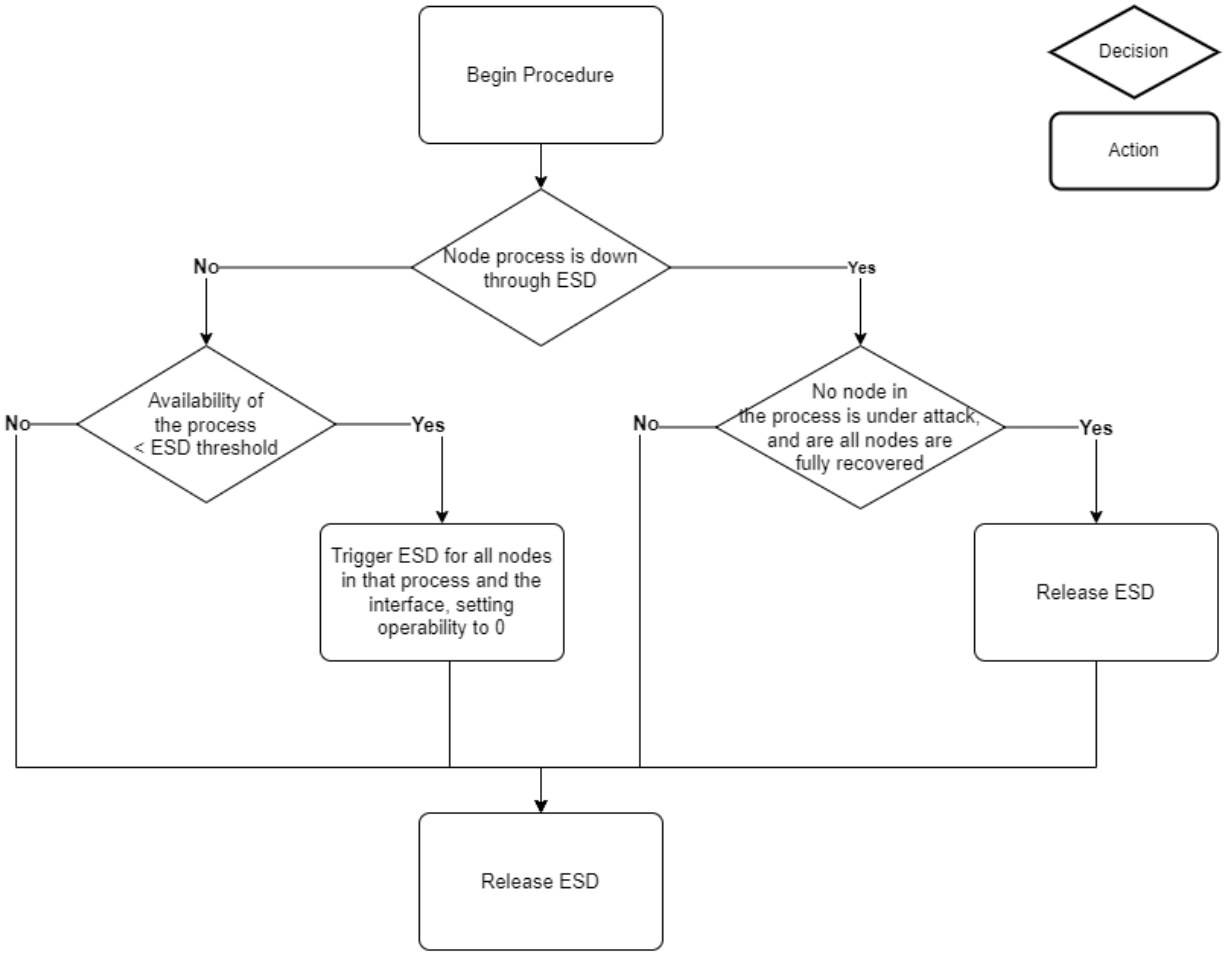


Figure 28: Operate ESD Procedure

Random Failure

This procedure is responsible for incurring random failures on nodes in the system. If a random float below 1 is smaller than the random failure rate, the procedure assesses if any nodes are eligible for a random failure. If so, one of these eligible nodes is chosen to fail. When this happens, the operability of the failing node is multiplied by a random float under 1, and the state of the node is altered.

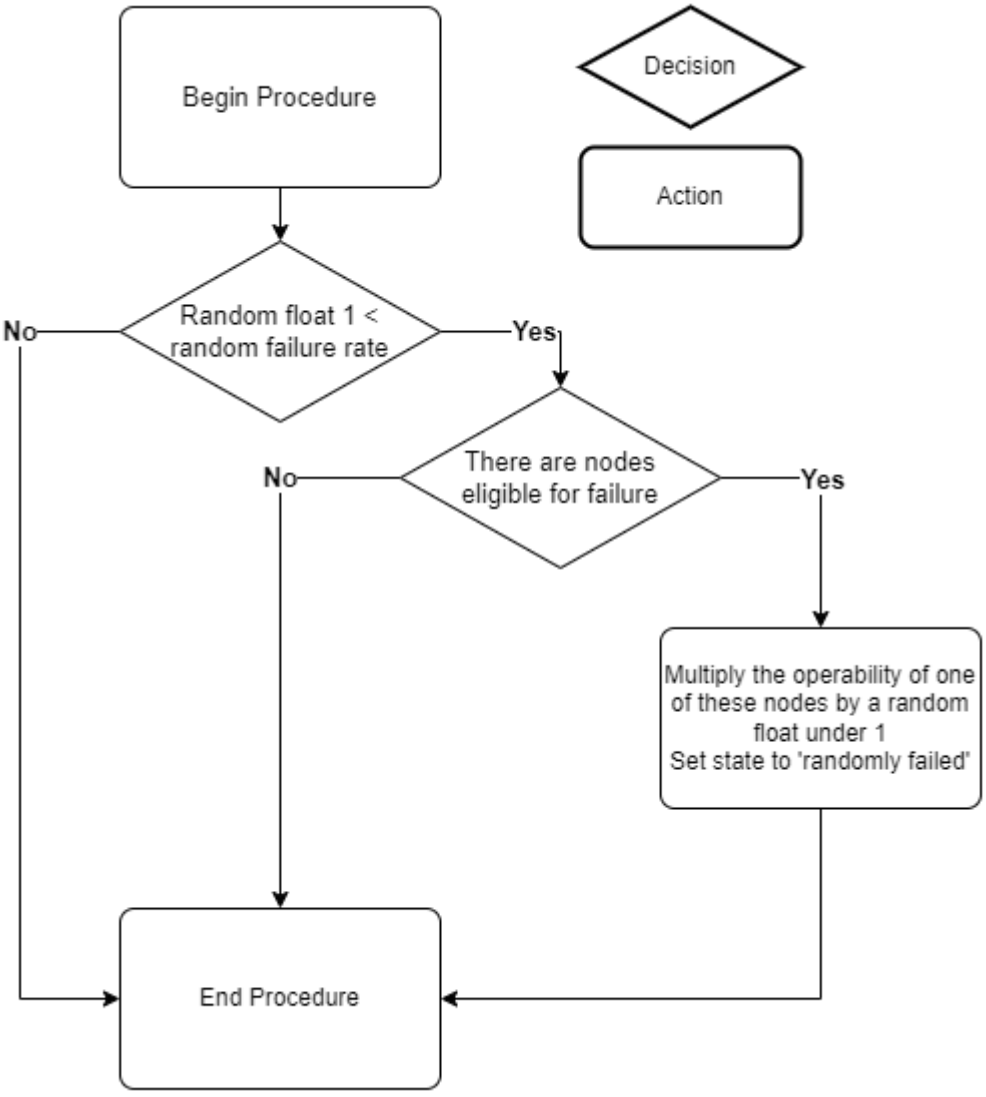


Figure 29: Random Failure Procedure

Overview of Control Loops

In Table 15: Overview of Control Loops, the control loops implemented in the model for the various process locations, together with their relative criticality is presented. The relative importance (Node Criticality, Interval) is based on a discussion with an expert within Gate terminal. The normalized criticality scores which sum up to 1 have been applied in the model.

Table 15: Overview of Control Loops

Location / Industrial Process	**Control Loop**	**Node Criticality (interval)**	**Node Criticality (Normalized)**	**Vendor**	**Explanation of criticality**
Tank	Current	1	0,26	Main	Crucial to remain within appropriate specifications
	Pressure	1	0,26	Main	Pressure is the main regulator of the processes
	Flow (LP)	0,8	0,21	Sub1	Flow to LP pumps in tank, crucial for having send-out
	Mixture	0,5	0,13	Sub3	Mixture of the LNG, mixing to prevent weathering
	Level	0,3	0,08	Sub1	Crucial to remain within appropriate equipment specifications
	Temperature	0,3	0,08	Main	Dependent on pressure, pressure is the main regulator of the processes
Jetty	(Back)Flow	1	0,26	Sub1	Pivotal for the usability of the jetties
	Current	1	0,26	Main	Crucial to remain within appropriate equipment specifications

	Location	0,5	0,13	Sub3	If the ship's location is out of bounds, LNG cannot be transferred to the tanks (or the other way around)
	Pressure	0,5	0,13	Main	Regulating pressure in a jetty is important, but limited connection to OT of Gate
	Temperature	0,5	0,13	Main	In order for LNG to transfer, the correct temperature in the piping has to be achieved
	Level	0,3	0,08	Sub1	
ORV	Current	1	0,28	Main	Crucial to remain within appropriate equipment specifications
	Gas Temperature	0,8	0,22	Sub1	Crucial for final output specifications and used materials send-out pipeline. Mutually dependent on gas temperature
	Water Temperature	0,8	0,22	Sub2	Crucial for final output specifications. Mutually dependent on gas temperature
	Water Flow	0,6	0,17	Sub2	Dependent on water and gas temperature, but supply not measured by SW pumps
	Gas Flow	0,4	0,11	Sub1	Dependent on water and gas temperature. Supply measured in tank (HP and LP Pumps)
Pump	Current	1	0,33	Main	Crucial to remain within appropriate equipment specifications
	Pressure	1	0,33	Sub2	Only measurement from pump providing an indication of amount of water pumped

	Vibrations	1	0,33	Sub2	Crucial to remain within appropriate specifications to prevent shutdown
Truckloading	Current	1	0,31	Main	Crucial to remain within appropriate equipment specifications
	Temperature	1	0,31	Main	Crucial for threshold to start loading truck
	Flow	0,5	0,16	Sub1	Only controlled/required after temperature is within specification
	Level	0,5	0,16	Sub1	Only controlled/required after temperature is within specification
	Pressure	0,2	0,06	Main	Has to remain within truck equipment specification
DCS	CCR	1	1,00	Main	

Formalization of Model Concepts

In table Table 16, the different model inputs and attributes are presented, together with their data type and value range

Table 16: Overview of Model Concepts

Name	Datatype	Value Range
Model inputs	Integer	
number-of-attackers	Float	$0 \leq X \leq 20$
attacker-persistence	Float	$0 \leq X \leq 10$
attack-frequency	Integer	$0 \leq X \leq 0.50$
containment-successrate	Float	$0 \leq X \leq 1$
esd-threshold	Float	$0 \leq X \leq 1$
ids-effectiveness	Float	$0 \leq X \leq 1$
infection-spread-likelihood	Float	$0 \leq X \leq 1$
ips-effectiveness	Float	$0 \leq X \leq 1$
random-failure-rate	Float	$0 \leq X \leq 0.050$
Strategy	Integer	0, 1, 2, 3
vendor-multiplier	Float	$0 \leq X \leq 1$
Attacker attributes		
Attacker-strategy	Integer	0, 1, 2, 3
Attack-state	Integer	0, 1, 2
Breach-attempts	Integer	$X \geq 0$
Original Location	Floats	$-33 \leq pxcor \leq -25$ $13 < pycor \leq 20$
Target	Node	Nobody, One of existing nodes
Attack Attributes		
Detected?	Boolean	True, False
Duration	Integer	$X > 0$
Power	Float	$0 \leq X \leq 1$
Removal-time	Integer	$X > 0$
Node Attributes		
Criticality	Float	$0 \leq X \leq 1$
ESD	Boolean	True, False
Identifier	Integer	$X \geq 0$
Node-process	String	tank1, tank2, tank3, jetty1, jetty2, jetty3, pump, orv, Truckloading, dcs, None
Operability	Float	$0 \leq X \leq 1$
State	Integer	0, 1, 2, 3, 4, 5
Vendor	String	Including, but not limited to: Main, Sub1, Sub2, Sub3

Appendix B: Model Verification

Unit Testing

In order to verify the behavior of the different model entities, checking whether or not the different entities go through all procedures in the correct order based on the preconditions required for that specific procedure, unit testing is applied. Firstly, tests on attackers and their attacks are performed, after which tests on the operator and the system nodes are performed.

Table 17: Attacker and Attack Unit Testing

#	Test	Method	Outcome
1	An attacker (with state 0) can only attack targets that aren't under attack and/or shut down by ESD. If a target is selected, the state of the attacker is set to 1.	Changing state of all nodes to anything other than 0 / triggering ESD, and checking whether or not it is targeted by an attacker.	Pass
2	A target is selected based on the strategy of the attacker.	Printing the different potential targets, their links/criticality to the command line, verifying that the potential targets are indeed those with high criticality/links, and that one of the potential targets is selected.	Pass
3	When the attacker strategies are distributed over de different attackers, on average, each strategy is applied by 1/3rd of the attackers.	Averaging over multiple model runs.	Pass
4	Distributions of attacker persistence and attack power are distributed correctly.	Create a temporary monitors with counts of the different persistence and power ocurrences, verifying output over multiple (long) model runs.	Pass
5	When an attacker has selected a target, it moves to the location of that target and attempts to disrupt it.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass
6	If an attacker cannot breach its target and avoid the IPS before his 'persistence' runs out, the attacker goes back to original state and location, and finds another target.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass
7	If an attacker succeeds in breaching the target, its state is changed, and it attempts to disrupt the availability of its target through multiplication of the operability with the attack power.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass
8	An attacker is able to launch attacks (through spreading) only via a node that is already under attack by that attacker, that isn't quarantined or down through ESD.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line, printing all nodes that are attacked by an attacker and their state, their connected nodes, as well as the node to which the infection is spread.	Pass
9	Attacks can only spread to nodes that are fully functioning, so not under ESD or	Visual inspection using the NetLogo 'inspect' feature in combination with the	Pass

	disrupted through an attacker, or to nodes that are disrupted through a system malfunction/random failure.	command line, printing all nodes that are attacked by an attacker, their connected nodes and their state, as well as the node to which the infection is spread.	
10	Spreading attacks to nodes with a different vendor than the origin node is more difficult than spreading between equal vendor systems.	Creating network with different vendors only, comparing the number of occurrences of spreading to a network with only equal venors.	Pass
11	When an attacker no longer has any outgoing attacks, the attacker goes back to original state and location, and finds another target.	Visual inspection using the NetLogo 'inspect' feature	Pass – After bugfix
12	All attributes have been properly allocated for all entities	Inspection through the NetLogo command line	Pass

Table 18: Operator and Node Unit Testing

#	Test	Method	Outcome
1	The network is set up properly: Nodes in a process are only connected to other nodes in the process. Connection to different processes has to go through interface nodes.	Visual inspection.	Pass
2	All attributes have been properly allocated for all entities	Inspection through the NetLogo command line	Pass
3	When an attack is detected through the IDS, the state and color of attacks and nodes are updated.	Visual inspection using the NetLogo 'inspect' feature.	Pass
4	Nodes can only be quarantined after the attack on the node has been detected, or when the node is disrupted through a random failure.	Inspection through the NetLogo command line.	Pass
5	Attacks can only be removed from a node when the node is quarantined or down through ESD.	Inspection through the NetLogo command line.	Pass
6	A node can start recovering only after the attack on the node has successfully been removed by the attacker.	Inspection through the NetLogo command line.	Pass
7	All nodes in an industrial process, as well as its interface node, are automatically shut down through ESD when the availability of the process is lower than the ESD threshold.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass
8	All nodes in an industrial process are released from ESD at the same time, only when all nodes, including the interface node, are back at state 0, have 100%	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass

	operability, and are not under attack by an attacker.		
9	A node cannot be disrupted when it is shut down through ESD.	Inspection through the NetLogo command line.	Pass
10	When a node is down through ESD, its operability is 0, as the node cannot be used.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass – After bugfix
11	A node can be disrupted through (and recover from) a random failure.	Visual inspection using the NetLogo 'inspect' feature in combination with the command line.	Pass

Breaking the model

For these verification tests, unrealistic input values for the model are used. This allows for evaluating if the model can be 'broken' if unrealistic input values are used. Furthermore, unrealistic input values test the applied logic in the operationalization phase. If the model behavior matches the expected model behavior (logically), the test is seen as a pass.

Table 19: Breaking the Model with Unrealistic Inputs

#	Test	Outcome
1	Amount of attackers < 0 and > 100	< 0: No attacks occur. > 100: No unexpected behavior. **Pass**
2	Attack power > 1 and < 0	> 1: Operability of a node exceeds 1. < 0: Operability of a node can become lower than 0. This behavior is expected based on the implementation, but not consistent with conceptual model. **Fail** Solution: Attack powers and probabilities are kept internal, and can only be changed by the modeler. Other solution could be to perform checks on attack power when allocating them to an attack, changing them automatically if they are out of bounds using 'ifelse' statements.
3	Attacker persistence < 0	If the first attempt does not succeed, attacker immediately backs off. **Pass**
4	Containment successrate > 1 and < 0	> 1: All nodes that have a detected attack are immediately quarantined. < 0: Nodes are never quarantined, allowing for free spread of the infection. **Pass**
5	ESD Threshold > 1 and < 0	> 1: System immediately goes into ESD. After recovering, system immediately goes in ESD again. < 0: ESD is never triggered. Even when no defensive measures are taken, the operability of a node can never go below zero. **Pass**
6	Failure rate > 1 and < 0	> 1: A random failure occurs every tick. < 0: No random failures occur. **Pass**

7	Infection spread likelihood > 1 and < 0	> 1: If potential spread is eligible for attacks (due to state, esd, etc), the attack will always spread. < 0: Attack never spreads. **Pass**
8	IPS and IDS effectiveness > 1 and < 0	> 1: All attacks are prevented (IPS) or instantly detected (IDS) < 0: No attack is prevented (IPS) or detected (IDS) **Pass**
9	Node Setup: entering an nonexistent file.	Presents user with a warning **Pass**
10	Removal times > 100 and < 0	> 1: Attack duration increases to > 100. < 0: As soon as the disrupted nodes is contained, the attack is removed. **Pass**
11	Total expected profit <= 0	0: Cumulative Monetary Losses remains equal to zero. <0: Cumulative Monetary Losses will go negative. **Fail:** Negative losses is equal to profit. Solution: Input check for total-expected-profit. This solution has been implemented. **Pass**
12	Vendor Multiplier > 1 and < 0	> 1: Spreads occur easier between different vendor nodes compared to equal vendor nodes. < 0: Spread cannot occur between different vendors. **Pass**

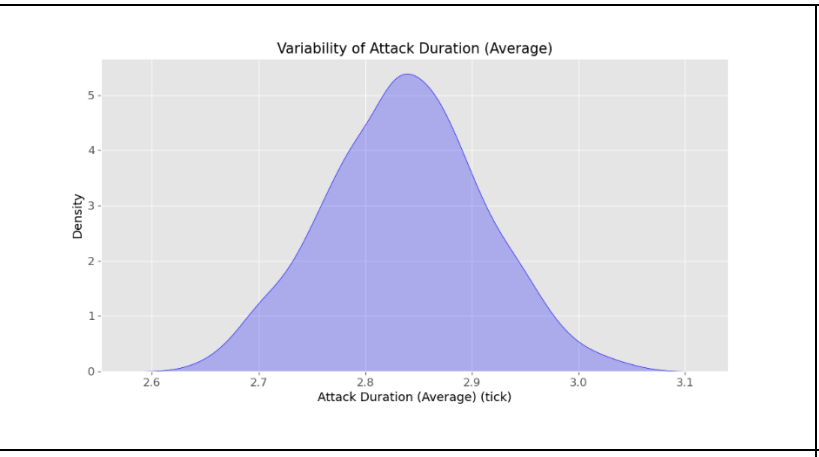
Appendix C: Model Validation

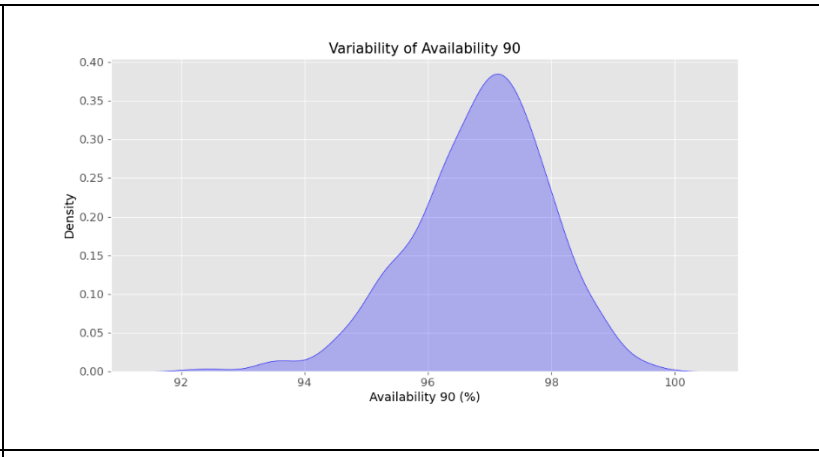
This appendix contains the results of the main validations steps that have been taken in order to assess the validity of the model. Firstly, the appendix presents KDE plots of the outcomes of the variability analysis, after which KDE plots and bar plots of the univariate and multivariate sensitivity analysis, respectively, are presented.

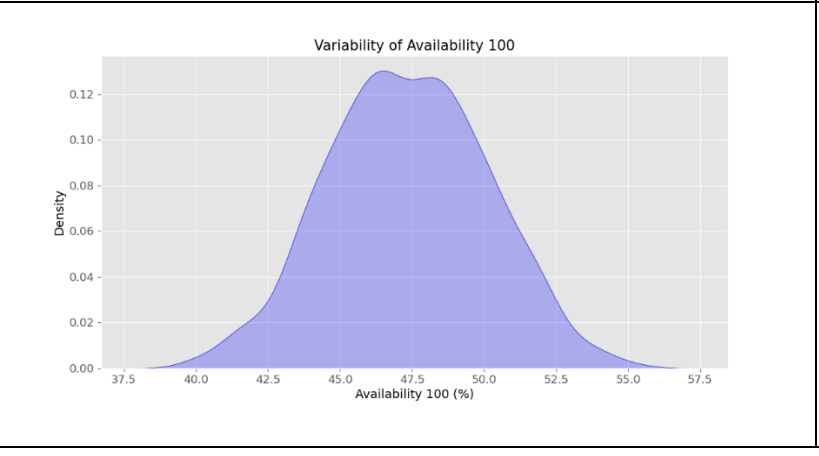
Variability Analysis

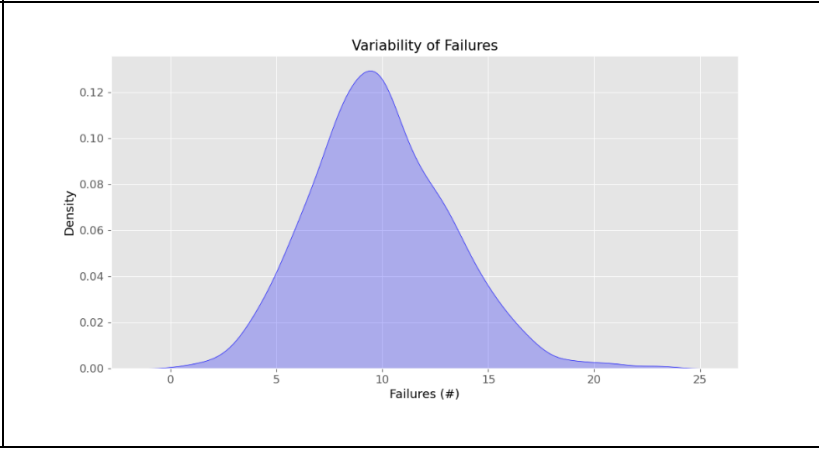
This section contains KDE plots of the variability analysis, presented in Table 20. The KDE plots result from 1000 model runs with the inputs presented in Table 9. Aside from certain skewed KDE plots, mainly for MTBF and MTTF, the majority of plots appear to follow a normal distribution. An interesting observation on the KDE plots that validate model behavior, is the widening of the 95% confidence intervals when more specific and unlikely circumstances are required for a change in model output (such as changes in ESD triggers, Failures, etc.).

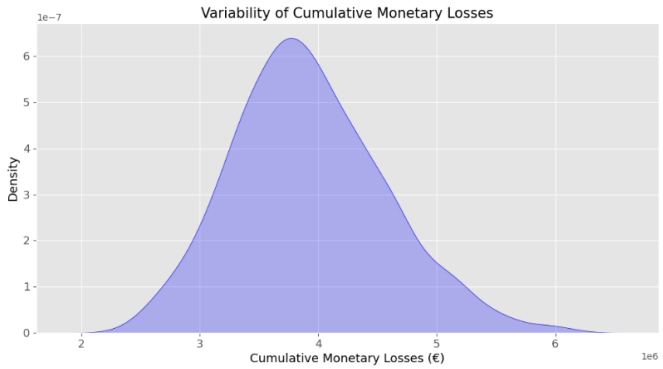
Table 20: Overview of Variability Analysis Outcomes

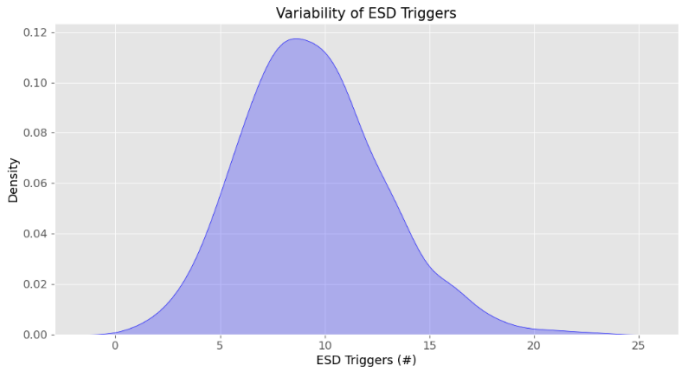


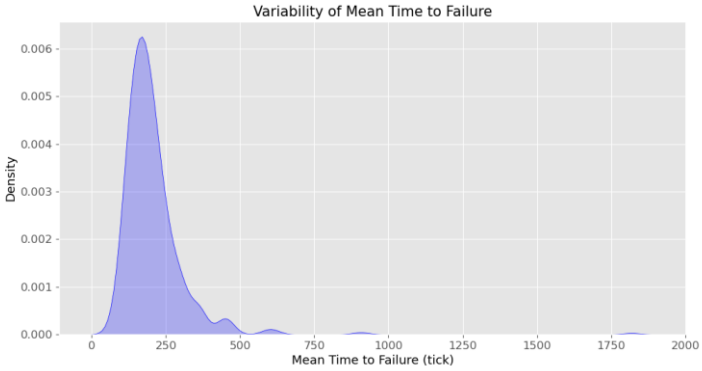


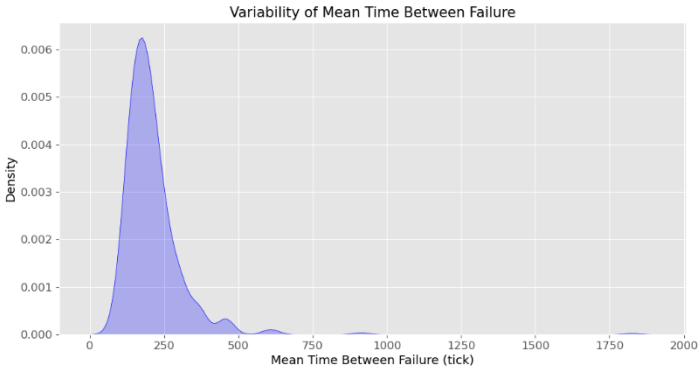


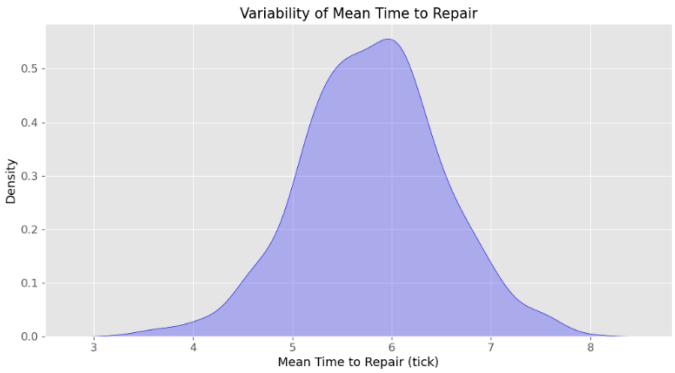


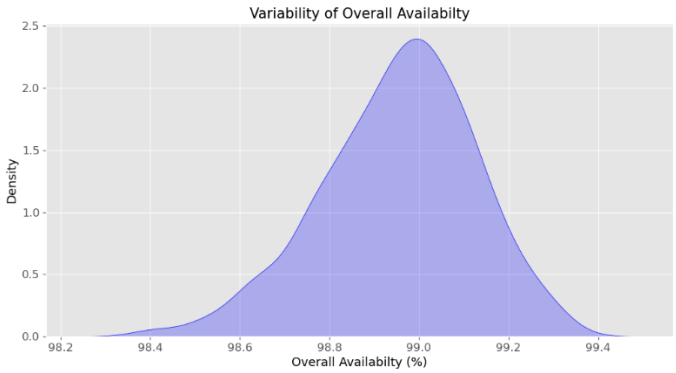

Variability of Cumulative Monetary Losses
1e−7
Density
Cumulative Monetary Losses (€)
1e6

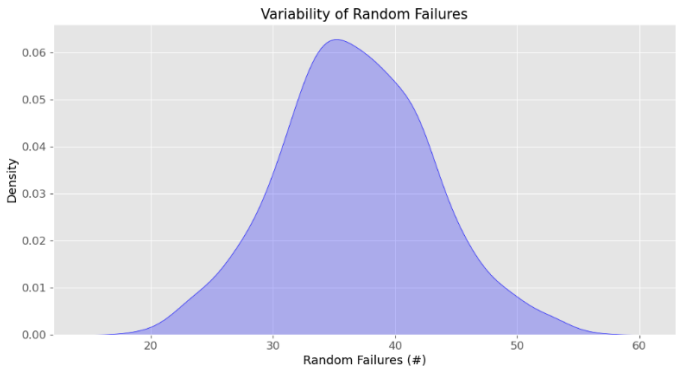

Variability of ESD Triggers
Density
ESD Triggers (#)

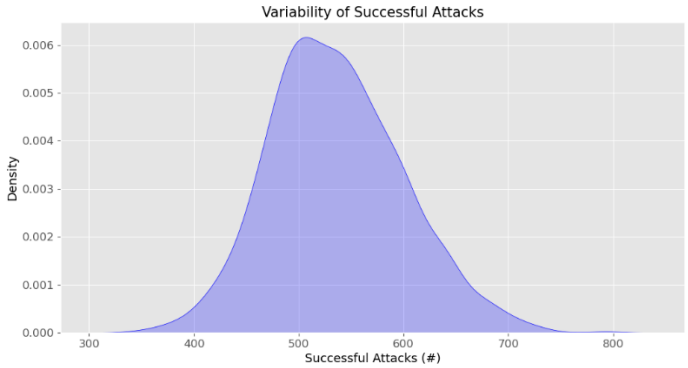

Variability of Mean Time to Failure
Density
Mean Time to Failure (tick)


Variability of Mean Time Between Failure
Density
Mean Time Between Failure (tick)


Variability of Mean Time to Repair
Density
Mean Time to Repair (tick)


Variability of Overall Availabilty
Density
Overall Availabilty (%)


Variability of Random Failures
Density
0.06
0.05
0.04
0.03
0.02
0.01
0.00
20
30
40
50
60
Random Failures (#)


Variability of Successful Attacks
Density
0.006
0.005
0.004
0.003
0.002
0.001
0.000
300
400
500
600
700
800
Successful Attacks (#)

Sensitivity Analysis

In this section, figures yielding interesting findings regarding the univariate or multivariate sensitivity analysis are presented.

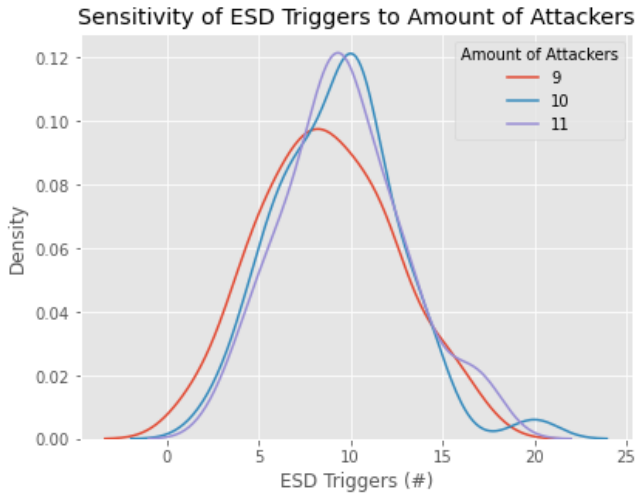
Univariate Sensitivity Analysis

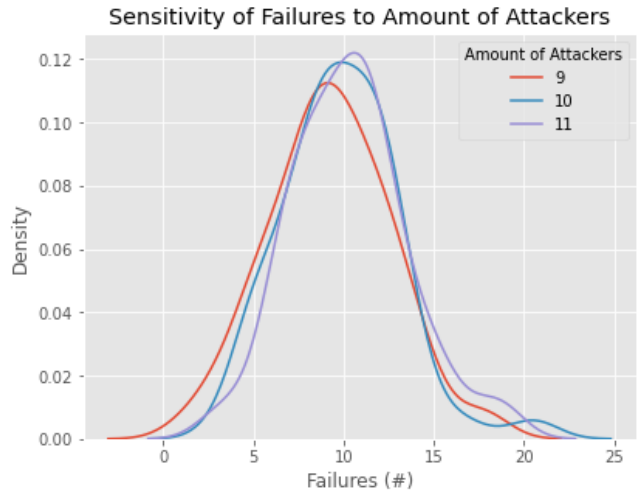
This section presents an overview of interesting KDE plots of the univariate model sensitivity of both the attacker and defender model parameters, presented in Table 21 and Table 22, respectively.

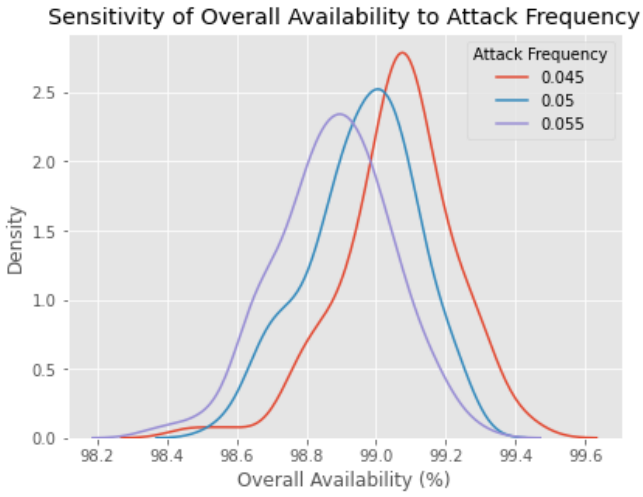
Plots for the attacker parameters show that deviating the attacker persistence has the most impact on the model outcomes. While the model is somewhat sensitive to deviations in the attack frequency and the infection spread likelihood, the model seems insensitive to the number of attackers in the system. When it comes to the strategy of the attackers, attackers seem to succeed slightly better in disrupting the system when they focus on attacking nodes with a high degree of criticality, while the 'links' and 'random' attack strategies perform quite similar.

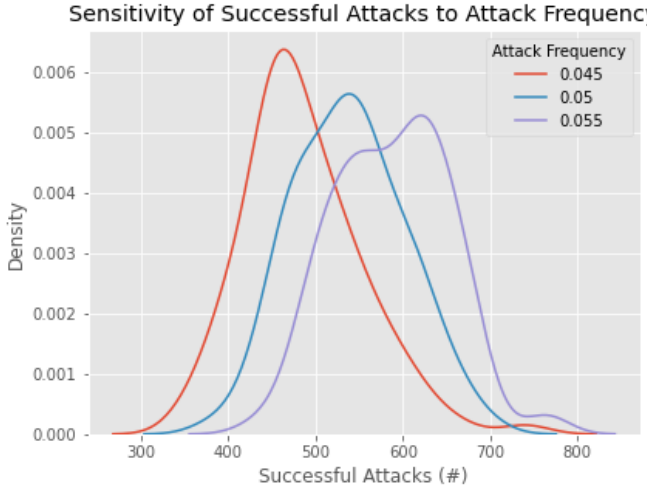
Table 22 shows an overview of the sensitivity of the model to deviations in singular defender parameters. It is clear that the model is rather sensitive to all of these inputs, as unmistakable differences between the plotted KDE curves can be observed. Of the defender parameters, the model seems to be the most sensitive for the IPS effectiveness, having the smallest overlap in density. The high level of sensitivity of the model to the IPS effectiveness can be attributed to the IPS being the first layer of defense: when the defender is capable of preventing attacks from happening altogether, other measures aren't required for securing the system. This implicates that other defense measures are relatively less critical in securing the system.

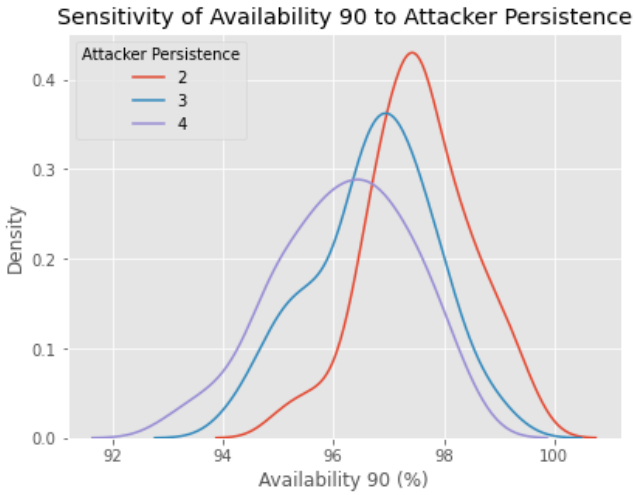
Table 21: Overview of Univariate Sensitivity of Attacker Parameters

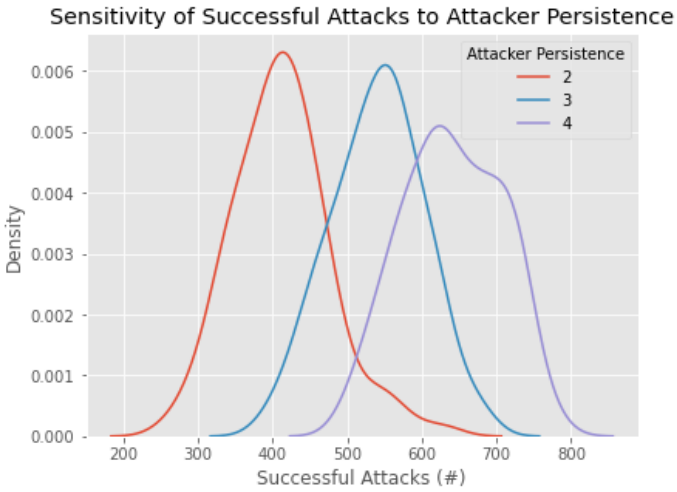


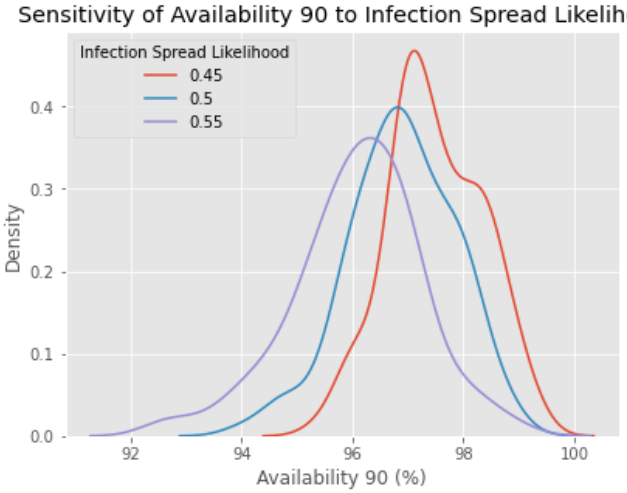


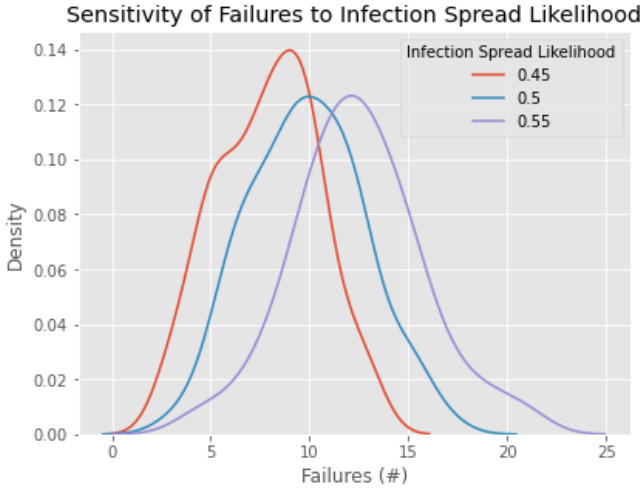

Sensitivity of Overall Availability to Attack Frequency
Attack Frequency
0.045
0.05
0.055
Density
Overall Availability (%)

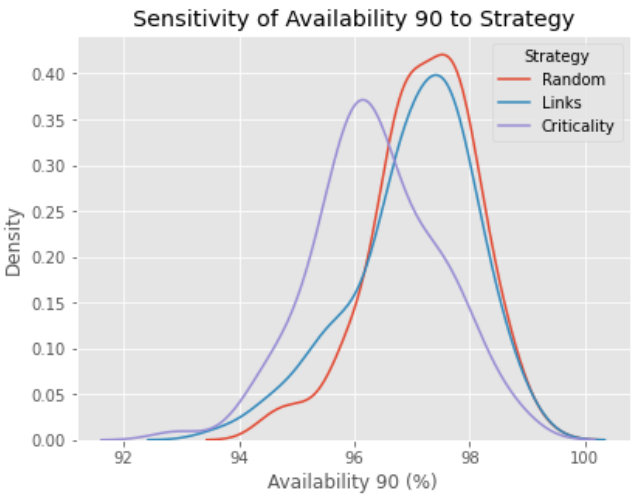

Sensitivity of Successful Attacks to Attack Frequency
Attack Frequency
0.045
0.05
0.055
Density
Successful Attacks (#)


Sensitivity of Availability 90 to Attacker Persistence
Attacker Persistence
2
3
4
Density
Availability 90 (%)


Sensitivity of Successful Attacks to Attacker Persistence
Attacker Persistence
2
3
4
Density
Successful Attacks (#)

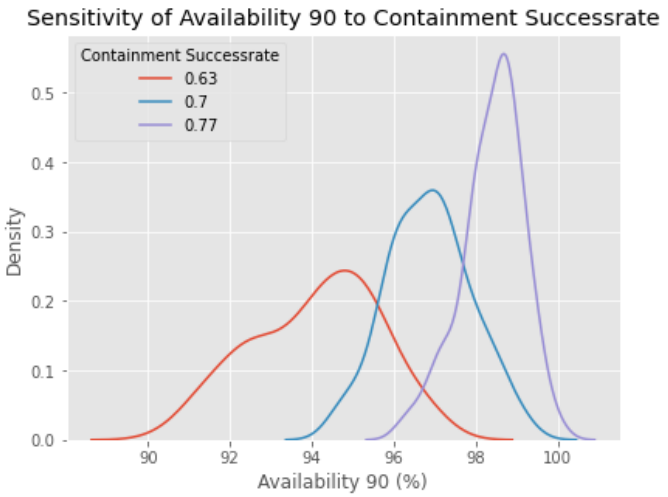

Sensitivity of Availability 90 to Infection Spread Likelihood
Infection Spread Likelihood
0.45
0.5
0.55
Density
Availability 90 (%)

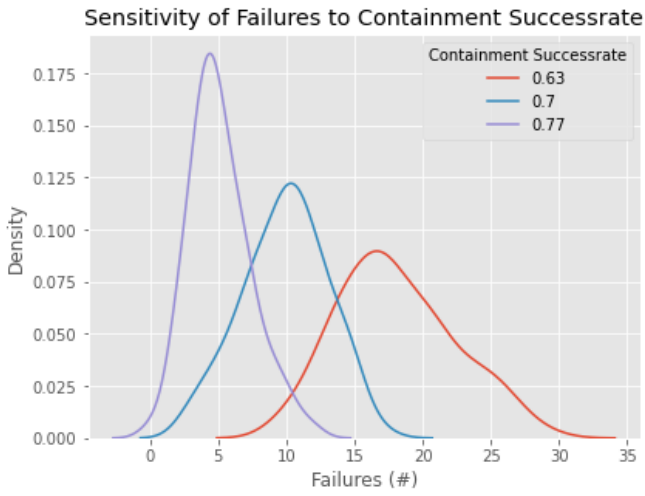

Sensitivity of Failures to Infection Spread Likelihood
Infection Spread Likelihood
0.45
0.5
0.55
Density
Failures (#)

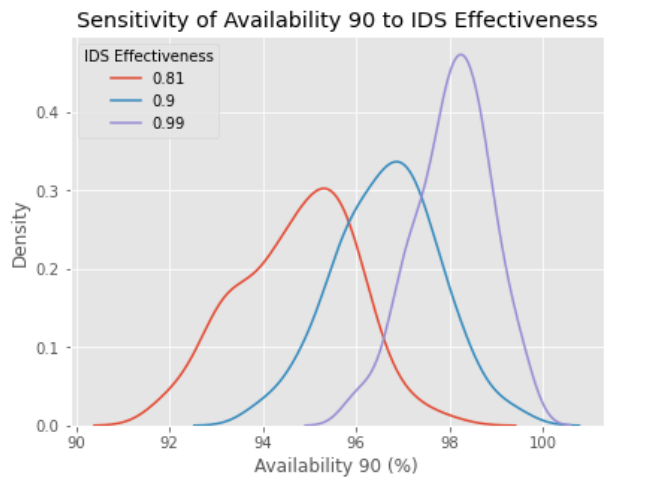

Sensitivity of Availability 90 to Strategy
Strategy
Random
Links
Criticality
Density
Availability 90 (%)

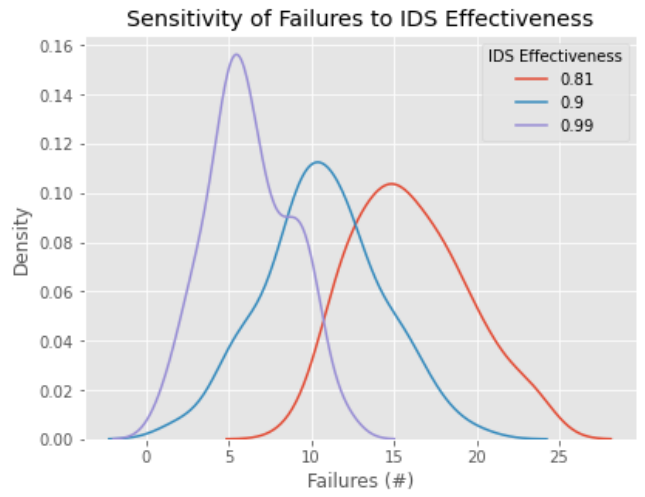

Sensitivity of Failures to Strategy
Strategy
Random
Links
Criticality
Density
Failures (#)

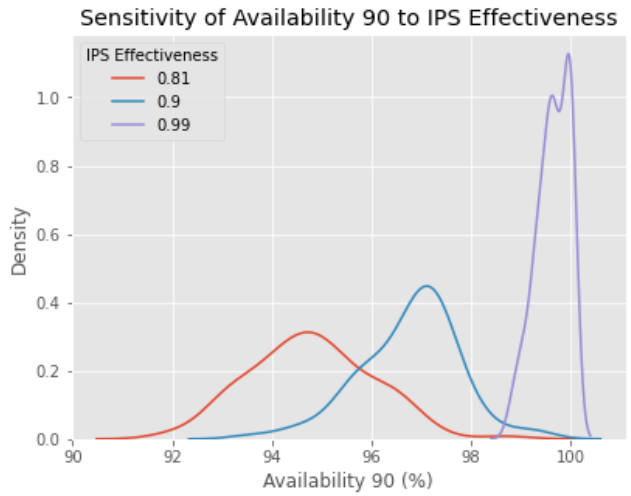
Table 22: Overview of Univariate Sensitivity of Defender Parameters

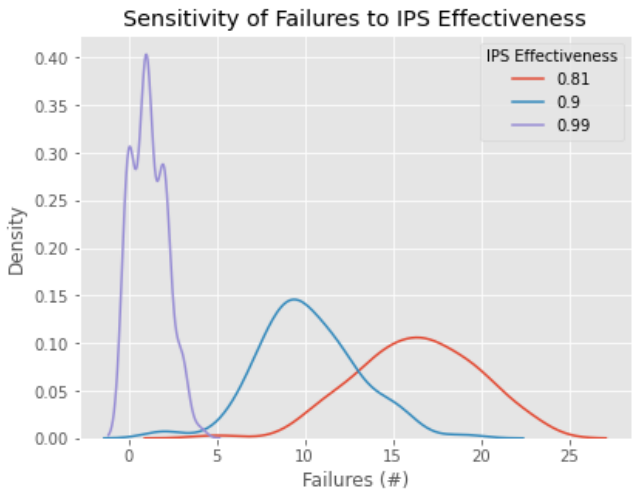


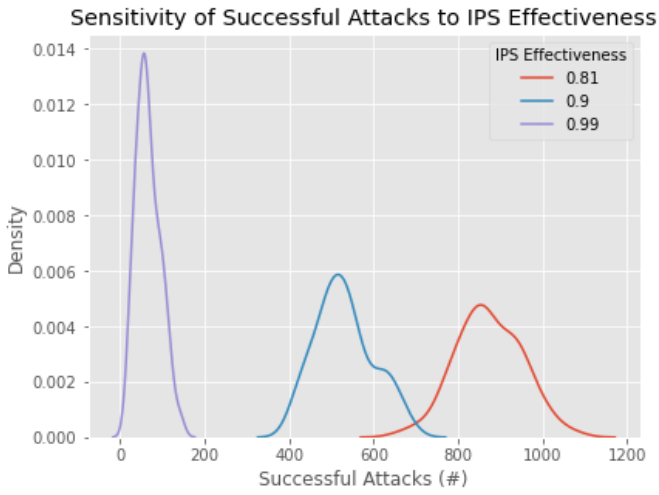


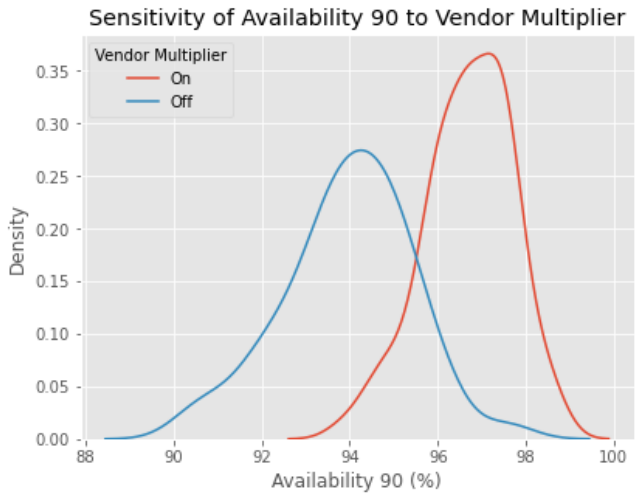


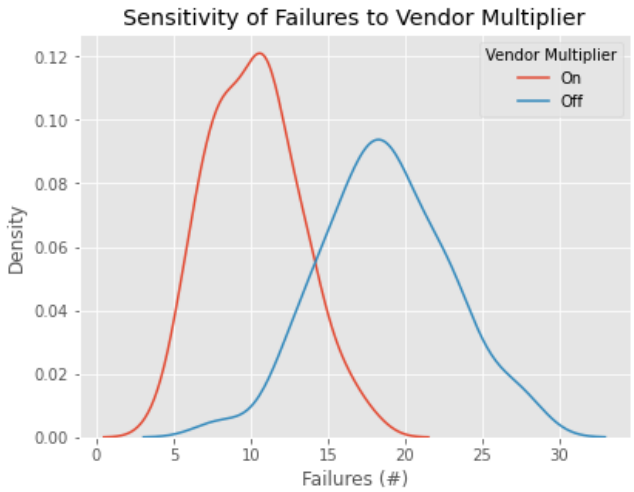



Sensitivity of Availability 90 to IPS Effectiveness
IPS Effectiveness
0.81
0.9
0.99
Density
Availability 90 (%)


Sensitivity of Failures to IPS Effectiveness
IPS Effectiveness
0.81
0.9
0.99
Density
Failures (#)


Sensitivity of Successful Attacks to IPS Effectiveness
IPS Effectiveness
0.81
0.9
0.99
Density
Successful Attacks (#)


Sensitivity of Availability 90 to Vendor Multiplier
Vendor Multiplier
On
Off
Density
Availability 90 (%)



Multivariate Sensitivity Analysis

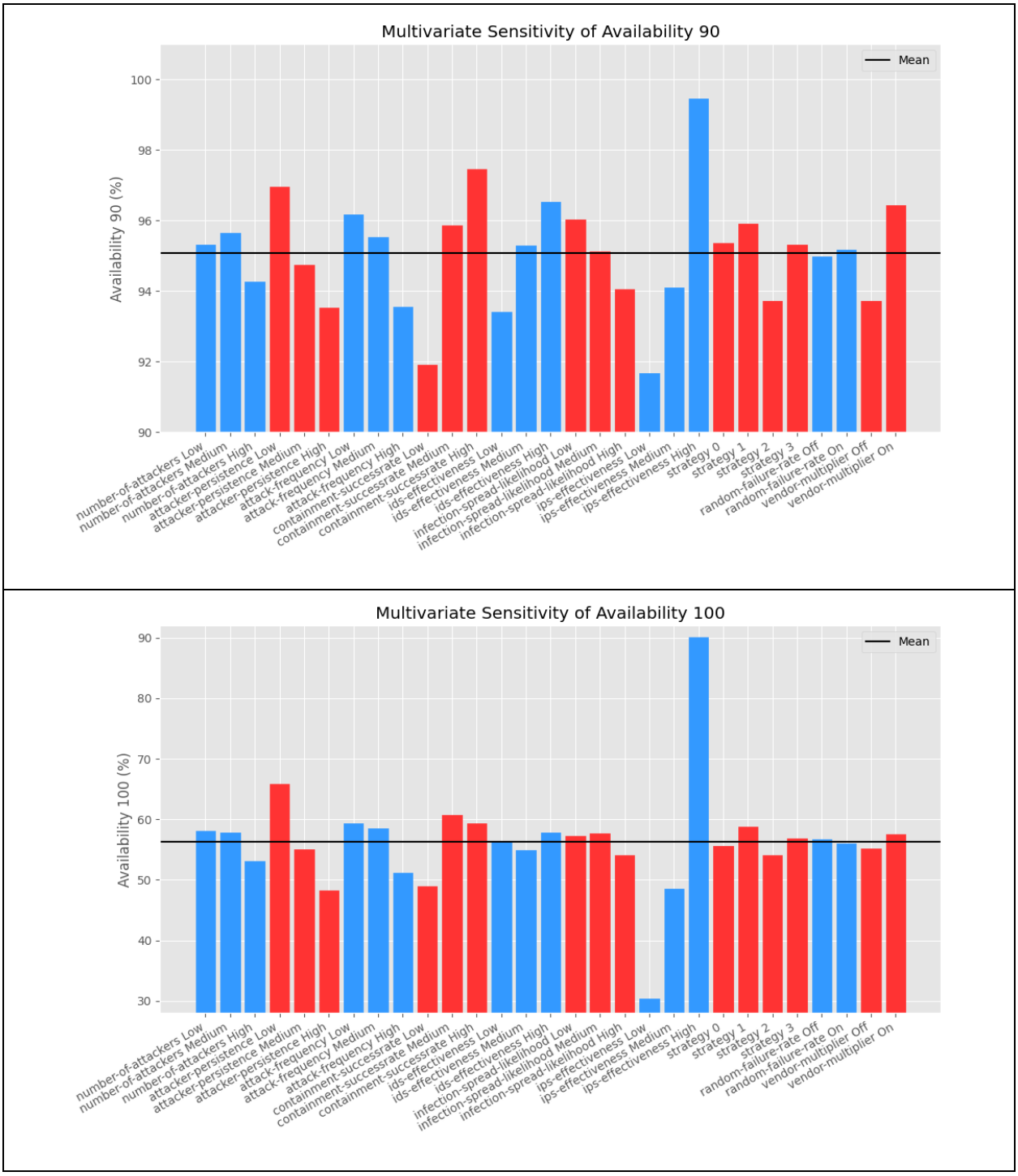
Similar to the univariate sensitivity analysis, some graphs showing the model sensitivity have been excluded in order to avoid an overabundance of graphs in the appendix. The following outputs have been excluded of this appendix:

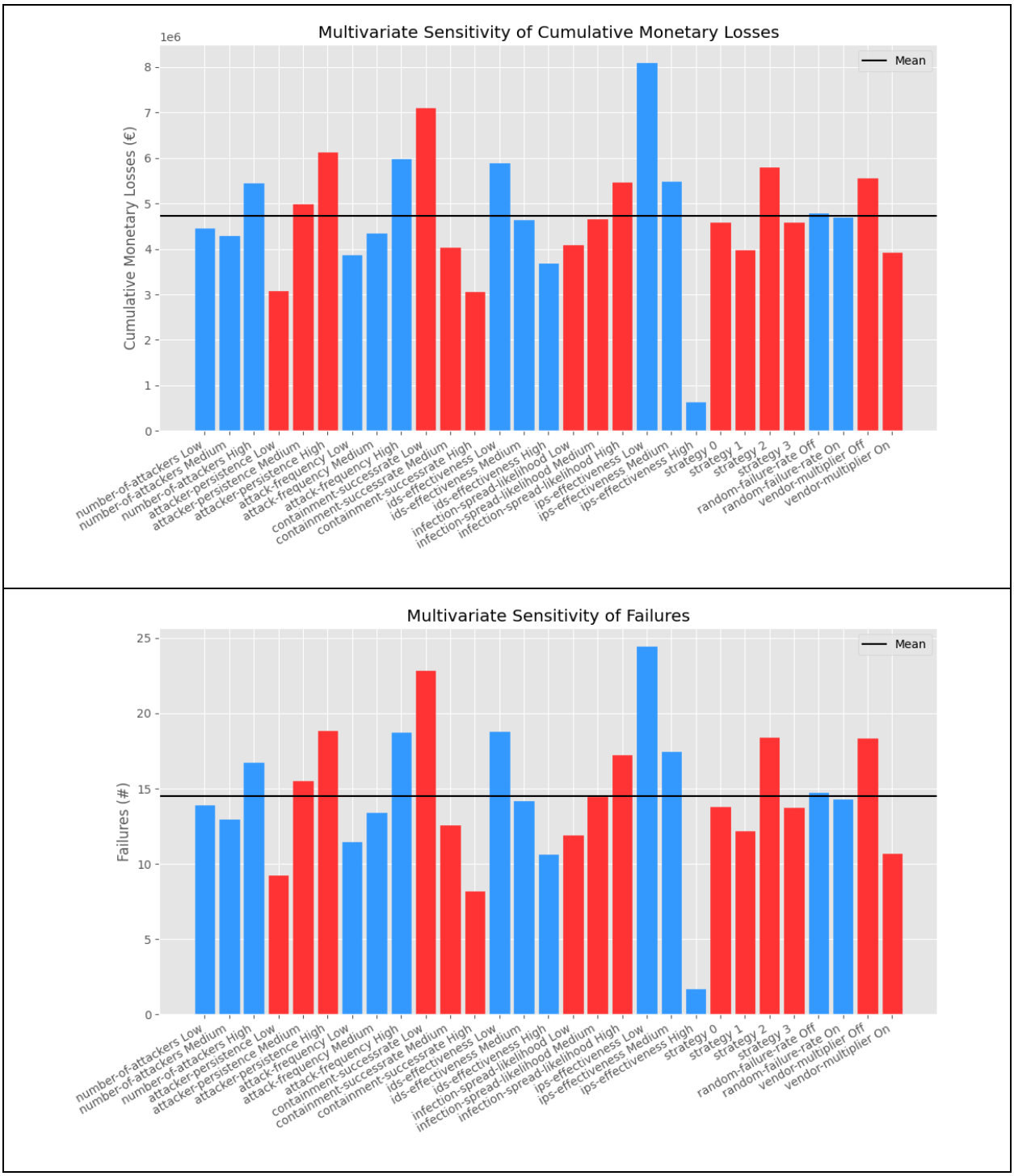
- *Average attack duration*: Little to no sensitivity
- *Mean time to repair*: Little to no sensitivity
- *Mean time to failure*: Similarity to *MTBF*
- *ESD Triggers*: Similar to *Failures*
- *Random Failures*: Only sensitive to Random Failure Rate

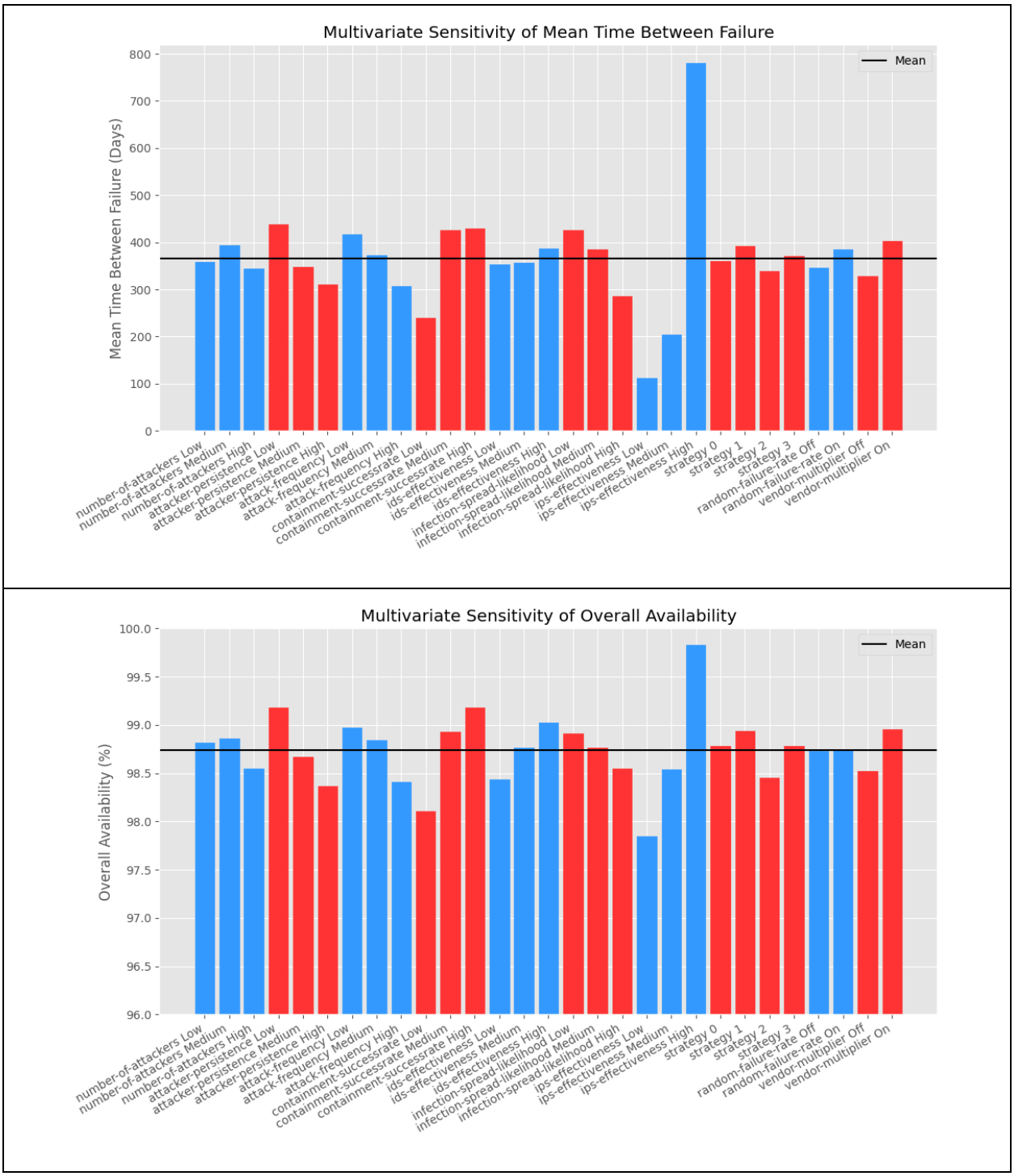
The findings of the univariate analysis are mostly corroborated by the multivariate sensitivity analysis. When it comes to the attacker parameters, the multivariate analysis once again shows that the model is the most sensitive to the *attacker persistence*, moderately sensitive to the attack frequency and *infection spread likelihood* and the least sensitive to the *number of attackers*. When it comes to the strategy of the attackers, the multivariate sensitivity analysis shows that criticality-based attacks (strategy 3) result in slightly worse system performance when compared to other strategies.

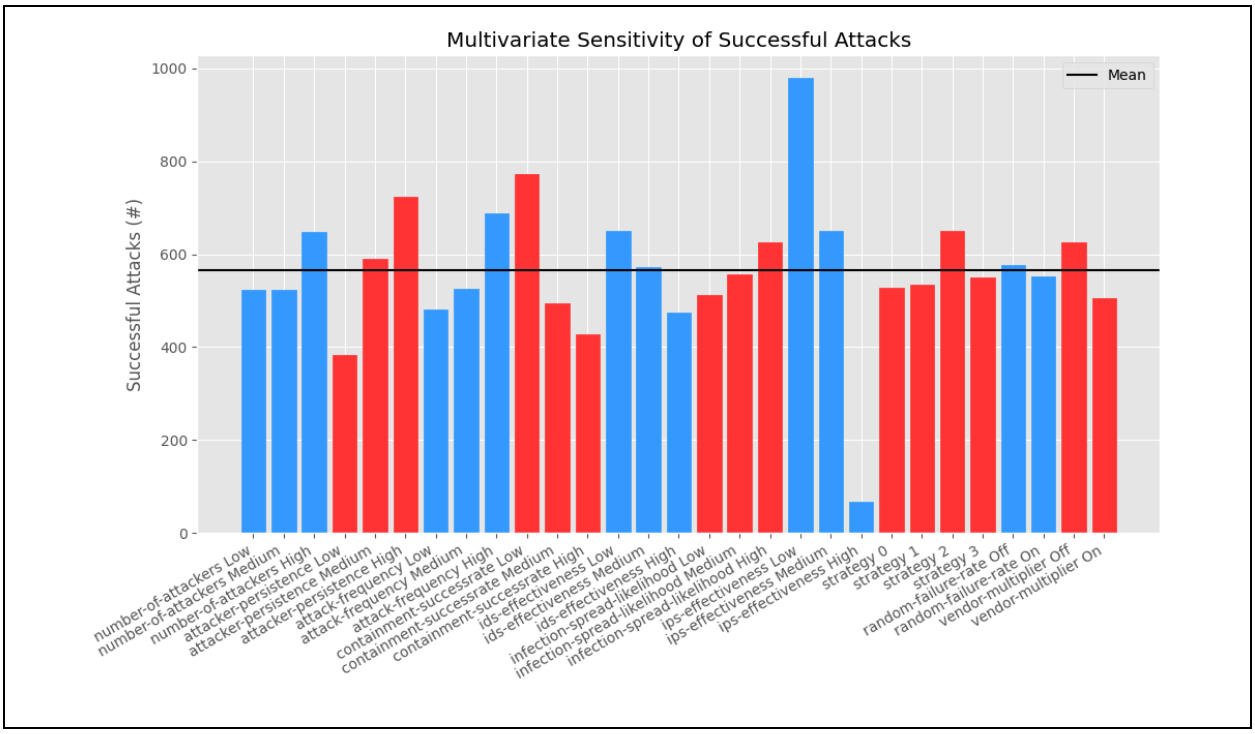
The multivariate sensitivity of the model to defender input parameters also match the findings of the univariate analysis. The model is the most sensitive to deviations in the IPS effectiveness: the variations in bar height are the largest for all of the output variables. Furthermore, the bar charts show that the model is sensitive to both *IDS effectiveness* and *Containment Successrate* (slightly higher sensitivity to the latter). While enabling *random failures* in the model has little impact on the actual operational performance of the system, *the* operational performance is rather sensitive to the presence of a *vendor-multiplier*. This is an easily explainable phenomenon, as the presence of a *vendor-multiplier* significantly reduces the likelihood of the spread of infections throughout the system, decreasing operational performance.

Table 23: Overview of Multivariate Sensitivity Analysis




Multivariate Sensitivity of Cumulative Monetary Losses
1e6
Cumulative Monetary Losses (€)
Mean
number-of-attackers Low
number-of-attackers Medium
number-of-attackers High
attacker-persistence Low
attacker-persistence Medium
attacker-persistence High
attack-frequency Low
attack-frequency Medium
attack-frequency High
containment-successrate Low
containment-successrate Medium
containment-successrate High
ids-effectiveness Low
ids-effectiveness Medium
ids-effectiveness High
infection-spread-likelihood Low
infection-spread-likelihood Medium
infection-spread-likelihood High
ips-effectiveness Low
ips-effectiveness Medium
ips-effectiveness High
strategy 0
strategy 1
strategy 2
strategy 3
random-failure-rate Off
random-failure-rate On
vendor-multiplier Off
vendor-multiplier On
Multivariate Sensitivity of Failures
Failures (#)
Mean


Multivariate Sensitivity of Mean Time Between Failure
Mean Time Between Failure (Days)
Mean
0
100
200
300
400
500
600
700
800
number-of-attackers Low
number-of-attackers Medium
number-of-attackers High
attacker-persistence Low
attacker-persistence Medium
attacker-persistence High
attack-frequency Low
attack-frequency Medium
attack-frequency High
containment-successrate Low
containment-successrate Medium
containment-successrate High
ids-effectiveness Low
ids-effectiveness Medium
ids-effectiveness High
infection-spread-likelihood Low
infection-spread-likelihood Medium
infection-spread-likelihood High
ips-effectiveness Low
ips-effectiveness Medium
ips-effectiveness High
strategy 0
strategy 1
strategy 2
strategy 3
random-failure-rate Off
random-failure-rate On
vendor-multiplier Off
vendor-multiplier On
Multivariate Sensitivity of Overall Availability
Overall Availability (%)
Mean
96.0
96.5
97.0
97.5
98.0
98.5
99.0
99.5
100.0
number-of-attackers Low
number-of-attackers Medium
number-of-attackers High
attacker-persistence Low
attacker-persistence Medium
attacker-persistence High
attack-frequency Low
attack-frequency Medium
attack-frequency High
containment-successrate Low
containment-successrate Medium
containment-successrate High
ids-effectiveness Low
ids-effectiveness Medium
ids-effectiveness High
infection-spread-likelihood Low
infection-spread-likelihood Medium
infection-spread-likelihood High
ips-effectiveness Low
ips-effectiveness Medium
ips-effectiveness High
strategy 0
strategy 1
strategy 2
strategy 3
random-failure-rate Off
random-failure-rate On
vendor-multiplier Off
vendor-multiplier On


Multivariate Sensitivity of Successful Attacks
Successful Attacks (#)
1000
800
600
400
200
0
Mean
number-of-attackers Low
number-of-attackers Medium
number-of-attackers High
attacker-persistence Low
attacker-persistence Medium
attacker-persistence High
attack-frequency Low
attack-frequency Medium
attack-frequency High
containment-successrate Low
containment-successrate Medium
containment-successrate High
ids-effectiveness Low
ids-effectiveness Medium
ids-effectiveness High
infection-spread-likelihood Low
infection-spread-likelihood Medium
infection-spread-likelihood High
ips-effectiveness Low
ips-effectiveness Medium
ips-effectiveness High
strategy 0
strategy 1
strategy 2
strategy 3
random-failure-rate Off
random-failure-rate On
vendor-multiplier Off
vendor-multiplier On

Appendix D: Results

This appendix aims to present the results retrieved while performing experiments with the constructed model. To this end, two different types of bar charts have been created. The first type of bar chart presented all of the model outcomes for each strategy, and used a logarithmic scale in order to properly visualize all of the bars due to differences in scale. As a result of this, there were barely any identifiable differences between the different strategies. Therefore, these bar charts have not been included in the thesis. The second type of bar charts is included, and presents a single model outcome, comparing the average value of that outcome per implemented strategy.

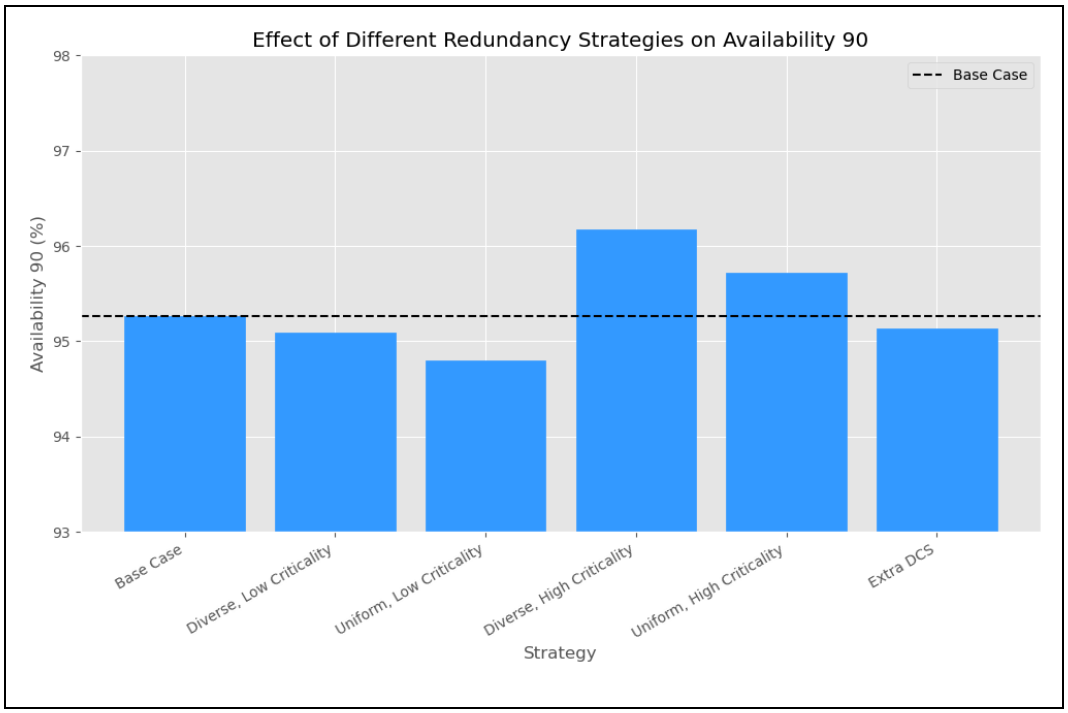
Effect of strategy on model outcomes

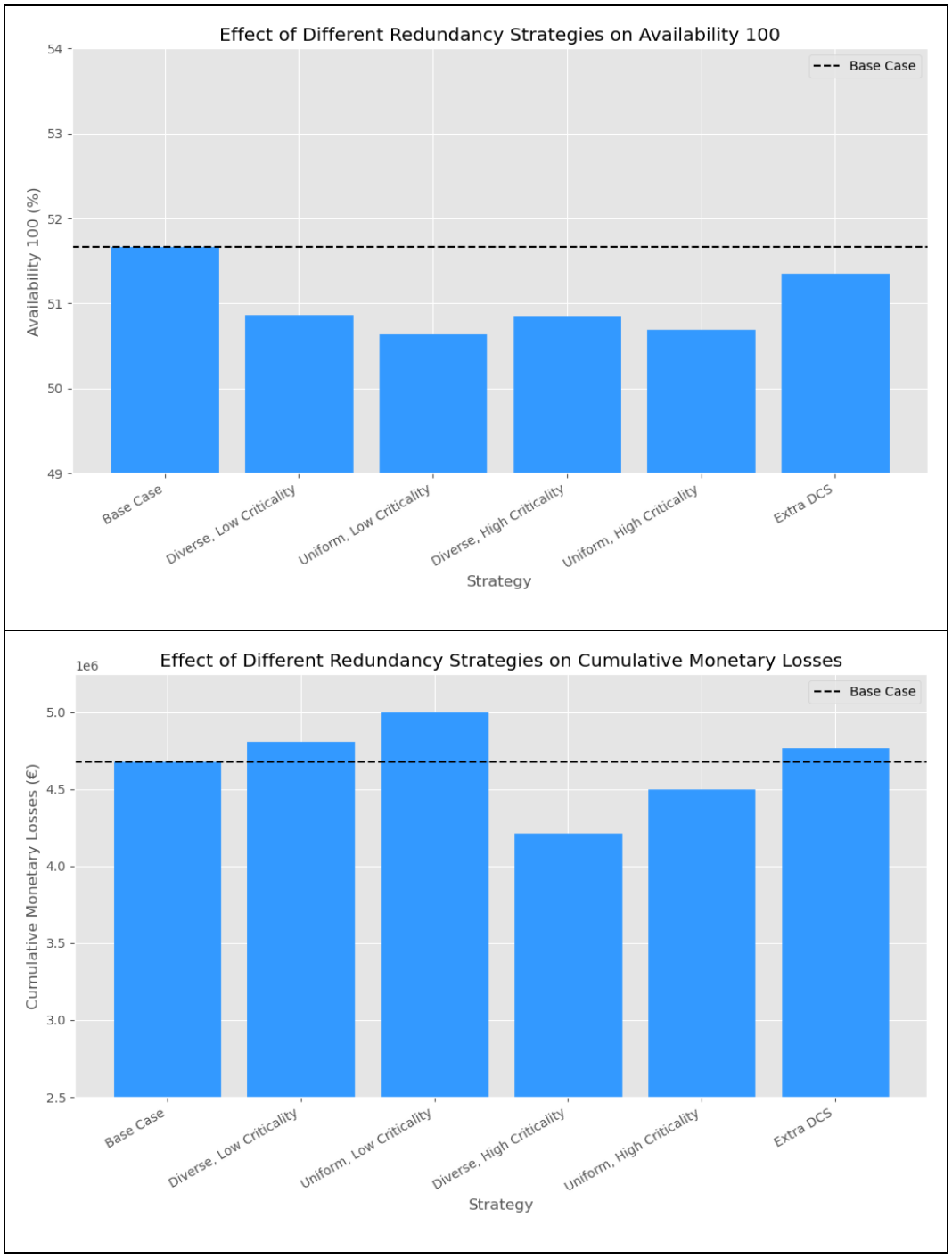
Not all performance indicators have been included in order to avoid an overabundance of charts: only charts yielding interesting results have been included in the appendix.

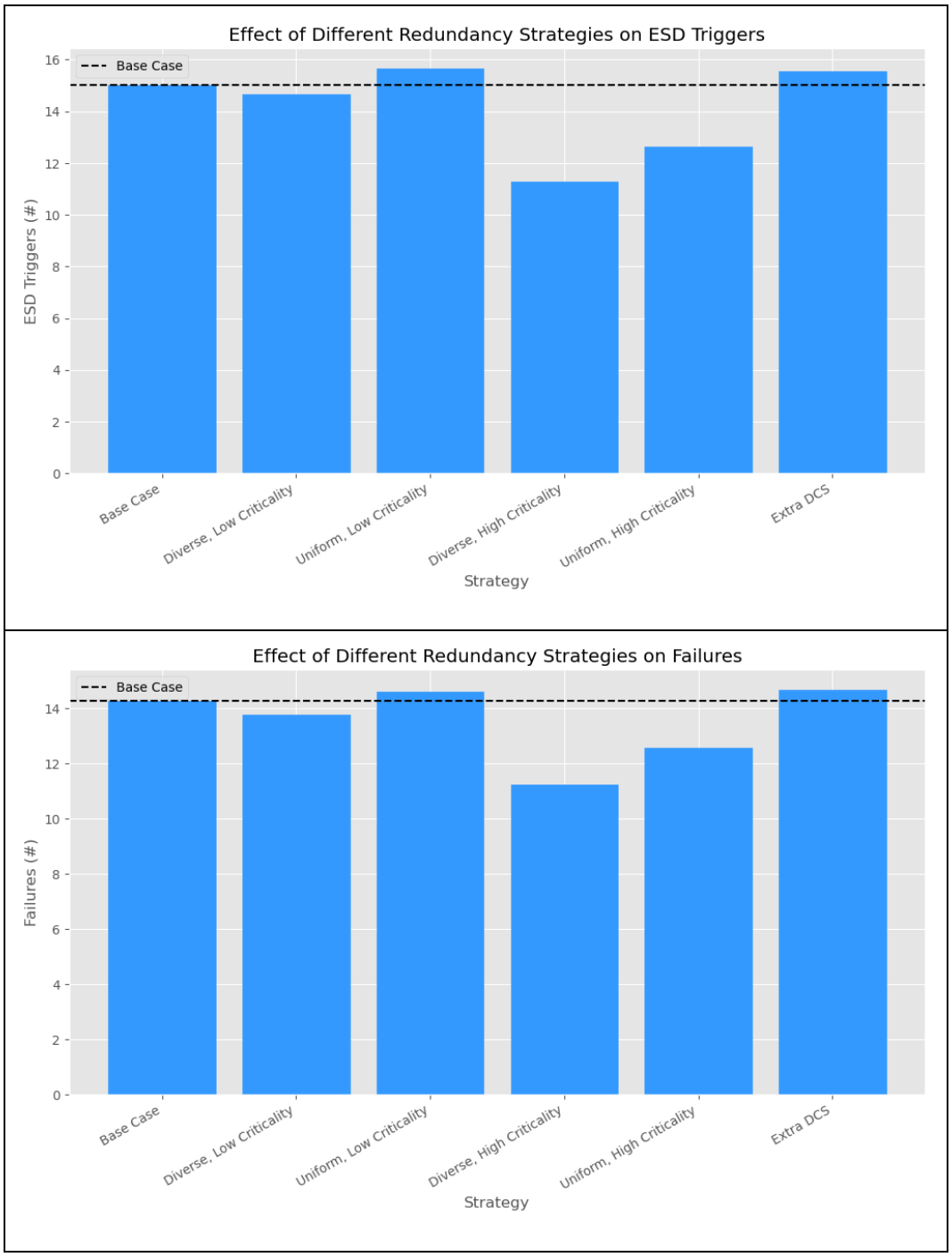
- Average Attack Duration: Little to no variation between strategies
- *Mean time to failure*: Similarity to *MTBF*
- *Random failures: Not affected by redundancy strategy*

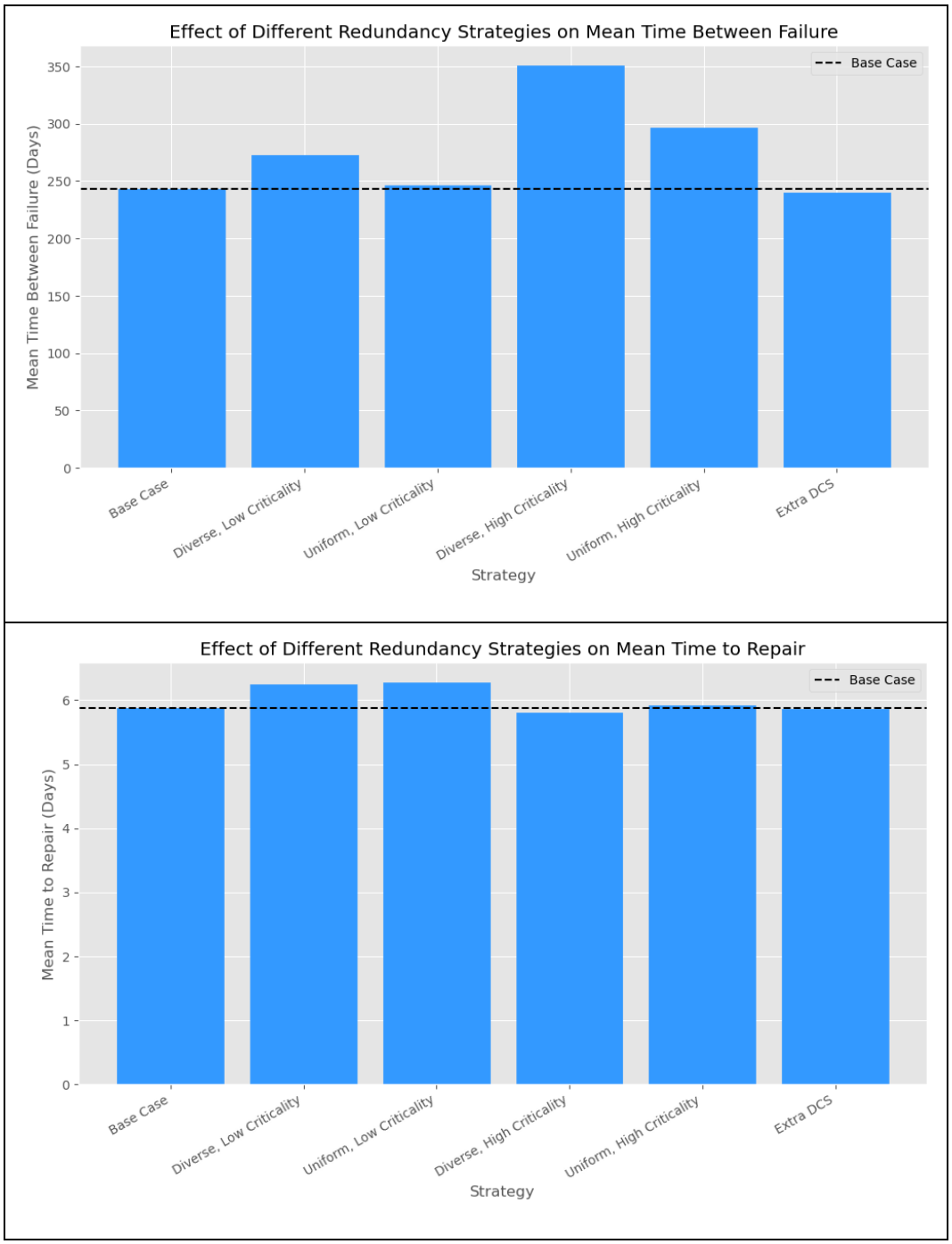
The findings resulting from these figures have been presented in Chapter 8 of this thesis.

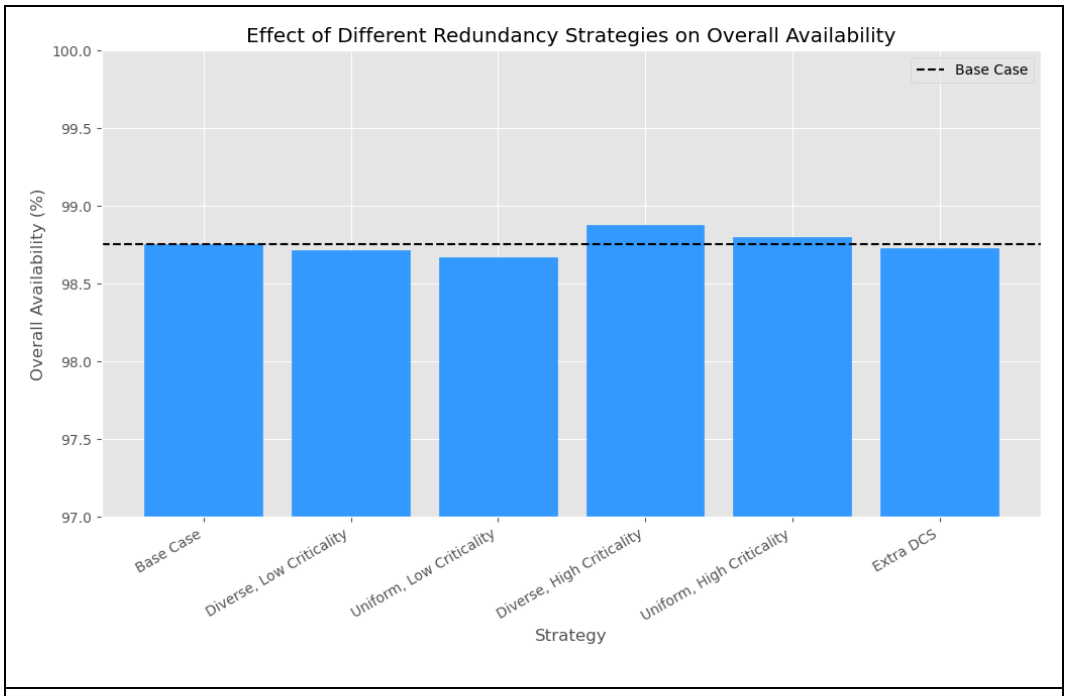
Table 24: Overview of the Effect of Strategy on Various Model Outcomes

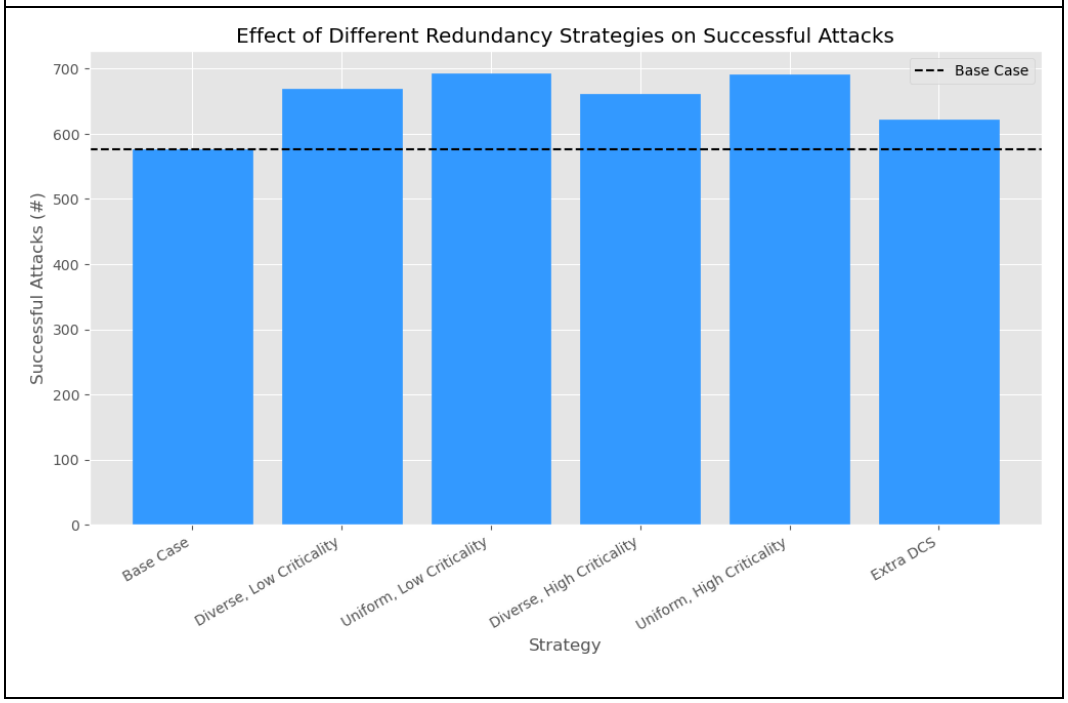



Effect of Different Redundancy Strategies on Availability 100
Availability 100 (%)
54
53
52
51
50
49
Base Case
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy
Effect of Different Redundancy Strategies on Cumulative Monetary Losses
1e6
Cumulative Monetary Losses (€)
5.0
4.5
4.0
3.5
3.0
2.5
Base Case
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy


Effect of Different Redundancy Strategies on ESD Triggers
Base Case
ESD Triggers (#)
0
2
4
6
8
10
12
14
16
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy
Effect of Different Redundancy Strategies on Failures
Base Case
Failures (#)
0
2
4
6
8
10
12
14
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy


Effect of Different Redundancy Strategies on Mean Time Between Failure
Base Case
Mean Time Between Failure (Days)
0
50
100
150
200
250
300
350
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy
Effect of Different Redundancy Strategies on Mean Time to Repair
Base Case
Mean Time to Repair (Days)
0
1
2
3
4
5
6
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy


Effect of Different Redundancy Strategies on Overall Availability
Base Case
Overall Availability (%)
100.0
99.5
99.0
98.5
98.0
97.5
97.0
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy


Effect of Different Redundancy Strategies on Successful Attacks
Base Case
Successful Attacks (#)
700
600
500
400
300
200
100
0
Base Case
Diverse, Low Criticality
Uniform, Low Criticality
Diverse, High Criticality
Uniform, High Criticality
Extra DCS
Strategy

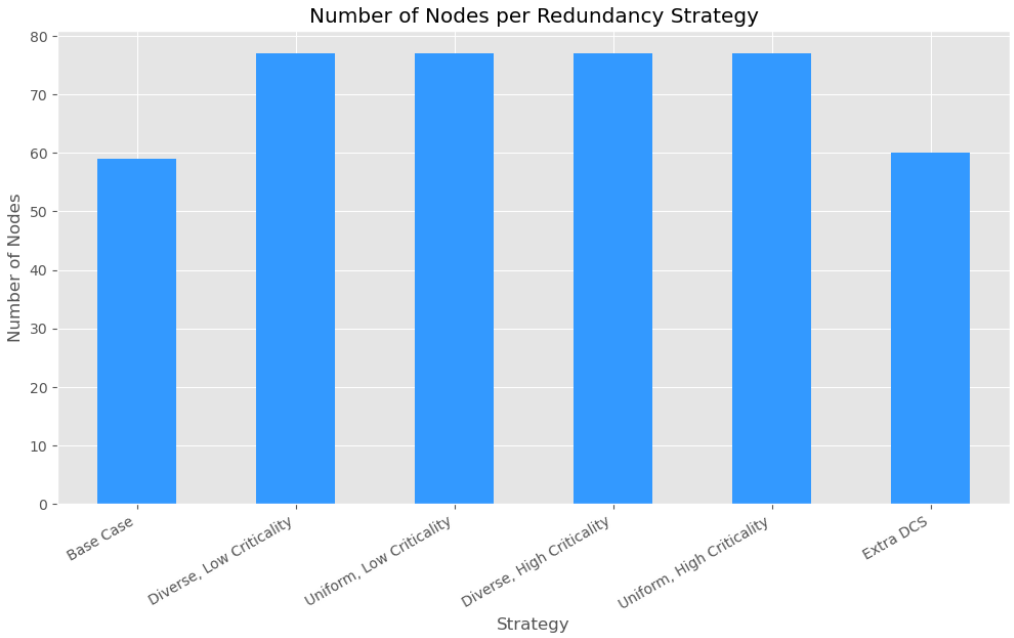


Figure 30: Number of Nodes per Redundancy Strategy

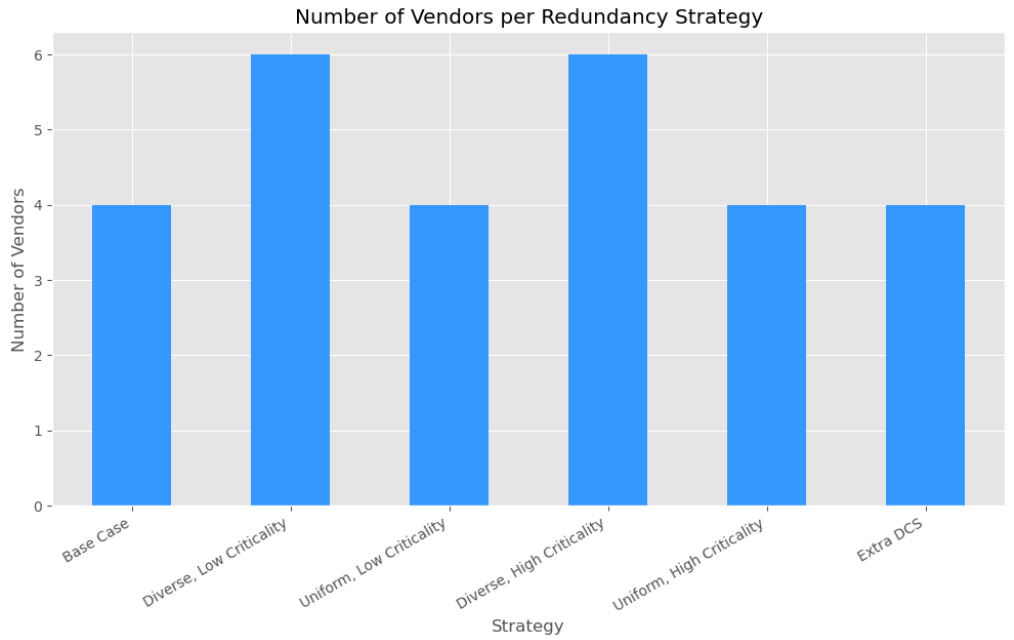


Figure 31: Number of Vendors per Redundancy Strategy