Cardiff University

School of Computer Science and Informatics

CMT400 – MSc Dissertation

Rules Formation for Cyber Resiliency Metrics

This thesis is submitted in partial fulfilment of the requirements for the qualification of Master of Science in Cyber Security

Supervisor: Dr Neetesh Saxeena

Moderator: Dr Tingting Li

Author: Saleh Mohamed

Module Code: CMT400

Date of Submission: September 2023

Declaration of Originality

I declare that this thesis is based on the original work that I have produced, apart from citations which have been acknowledged. I also declare that the thesis has not been submitted previously for any other award or degree at Cardiff University or any other University.

Acknowledgement

Firstly, I would like to acknowledge my family for their support in helping me through the completion of this dissertation. In addition, I would like to formally acknowledge my supervisor for the project, Dr Neetesh Saxena, for his support and guidance throughout the project.

Abstract

With the advancements in modern-day cyber-attacks on industrial control systems, the need for sufficient cyber resiliency metrics that govern recovery methods has never been more important. Especially with the rise in Denial of Service (DoS) and ransomware attacks. Due to the fact that infrastructure that is critical is constantly being targeted by cyber-attacks, it is essential that vital industries have effective rules formation in place to guide them in initiating various forms of recovery/ mitigation in the event of a cyber-attack. This thesis demonstrates the given attacks on a Chemical Plant through the use of a tool and describes a rules formation that can enable recovery/ mitigation methods against the attacks. The rules formation explains how to best defend against the attacks and the methods that can be put in place to mitigate the damage caused by the attacks.

Contents

Chapter 1 Introduction

The growing importance of Industrial Control Systems (ICS) has led to an increase in cyber-attacks targeting these systems. Industrial Control Systems are responsible for shaping the working conditions in various industries such as manufacturing, energy, healthcare, and transportation, among others. Cybersecurity has emerged as one of the most significant challenges to Industrial Control Systems. Over the years, many organisations have focused on developing cybersecurity strategies that include the application of cyber controls and technologies that prevent cyber threats. Organisations have developed several techniques to assess and gauge their cyber-resiliency.

Cyber resiliency metrics can be used to determine the level of an organisation's ability to respond and recover from various cyber threats. It is imperative to measure cyber resiliency as it helps organisations remain proactive in identifying vulnerabilities, developing cyber resiliency metrics as well as developing an action plan to enhance their security posture. In this chapter, the concept of cyber resiliency metrics will be defined. The importance of implementing cyber resiliency metrics for industrial control systems will then be evaluated. Additionally, the various ways of assessing cyber resiliency will be examined.

1.1 Defining Cyber Resiliency Metrics

Cyber resiliency metrics refer to the set of measures and procedures developed by an organisation to determine its ability to respond, recover and adapt to cyber-attacks or disruptions. These metrics measure the organisation's level of preparedness in addressing cyber threats and vulnerabilities.

1.2 The Importance of Implementing Cyber Resiliency Metrics for Industrial Control Systems

The importance of implementing cyber resiliency metrics for Industrial Control Systems cannot be overstated. ICS is an essential component of industrial infrastructure that significantly impacts various sectors, including transportation, energy, water and wastewater, among others. Cyber threats on ICS have increased in the past few years, leading to considerable damage to the industrial infrastructure and disruption of essential services.

Implementing cyber resiliency metrics for ICS is crucial to assess the level of cybersecurity maturity of an organisation. These metrics can assist organisations in identifying their critical assets and vulnerabilities that need protection. They ensure the effective detection of cyber-attacks and provide an organisation's IT personnel with a response plan to reduce the impact of an attack.

The significance of industrial control systems significantly contributes to the growth of various sectors. However, the rapid growth of cyber-attacks on ICS exposes them to various vulnerabilities.

Cyber resiliency metrics provide an effective method of assessing an organisation's cybersecurity posture. By identifying vulnerabilities and developing a response plan, organisations can effectively address cyber threats and protect their critical assets.

The implementation of cyber resiliency metrics is crucial to safeguarding Industrial Control Systems. This chapter has proposed that effective cyber resiliency metrics programs should address business impact analysis, threat assessment and risk management, incident response testing, recovery capability assessment and continuous improvement. By implementing robust cyber resiliency metrics programs, organisations can enhance their security posture and mitigate potential cyber risks.

In addition, the metrics can also enable organisations to gauge their cyber resilience maturity, identify vulnerabilities and areas of improvement, allocate resources effectively, and prioritise cybersecurity investments. Through the use of cyber resiliency metrics, various organisations are able to lower an attack’s impact and make sure that they are able to successfully operate efficiently after the attack.

Cyber resiliency metrics are increasingly important due to the fact that various businesses are often concerned about a system’s ability to be able to withstand, recover and adapt from different types of attacks. When a system is being considered by these stakeholders, they tend to look at several factors including, which cyber resiliency aspects are the most important, what way the given system enforces the aspects and how successfully does it do it as well as what risks are present (D. J. Bodeau et al., 2018).

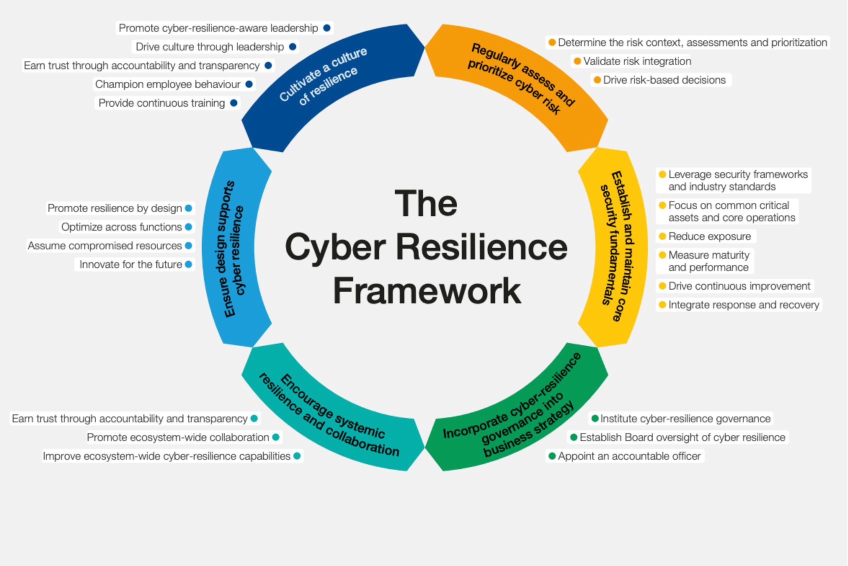

The Cyber Resilience Framework
Cultivate a culture of resilience
Promote cyber-resilience-aware leadership
Drive culture through leadership
Earn trust through accountability and transparency
Champion employee behaviour
Provide continuous training
Regularly assess and prioritize cyber risk
Determine the risk context, assessments and prioritization
Validate risk integration
Drive risk-based decisions
Establish and maintain core security fundamentals
Leverage security frameworks and industry standards
Focus on common critical assets and core operations
Reduce exposure
Measure maturity and performance
Drive continuous improvement
Integrate response and recovery
Incorporate cyber-resilience governance into business strategy
Institute cyber-resilience governance
Establish Board oversight of cyber resilience
Appoint an accountable officer
Encourage systemic resilience and collaboration
Earn trust through accountability and transparency
Promote ecosystem-wide collaboration
Improve ecosystem-wide cyber-resilience capabilities
Ensure design supports cyber resilience
Promote resilience by design
Optimize across functions
Assume compromised resources
Innovate for the future

Figure 1 The Cyber Resilience Framework (NOPSEC et al., 2022)

Moreover, cyber resiliency metrics continue to become more and more essential in the cyber security world as various hackers and malicious users attempt to launch attacks on computer systems. In these instances, it is pivotal that computer systems have been prepared in advance for attacks such as Denial of Service or phishing and have the necessary features and functionalities to be able to recover from these attacks.

Furthermore, for cyber resilience metrics to be created, the systems performance concept is crucial and must retain a degree of desirable efficiency after a performance degradation has occurred (Linkov & Kott, 2019).

1.3 Aim and Objectives

The aim of this project is to produce a rules formation that will be used to govern cyber resiliency metrics, examples in this report will primarily focus on Industrial Control Systems. The objectives can be broken down into the following:

- Analysing state-of-the-art attacks
- Develop use cases and test cases
- Creating rules formation for test cases
- Validate the rules formation

1.4 Scope

Critical infrastructure-based industries such as Industrial Control Systems are often targets for cyber-attacks. In such scenarios, these attacks can have a significant impact not only on the victim organisation but also on the region in which the critical infrastructure is operating. For example, a power plant which provides energy/lighting within a specific region. A successful attack could significantly impact thousands of people's daily lives. An example is the 2017 cyber-attack directed at a petrochemical plant in Saudi Arabia which resulted in a disruption in the operations of the plant (Alshammari et al., n.d.)

Due to this, it is important to have a concrete understanding of cyber-related industries as well as cyber resiliency metrics which can be applied to these industries. This will be essential in understanding how these industries work and the way in which they can recover from a successful attack, as well as which parts are the most vulnerable to being attacked. It is important to know the way in which they operate as well as how attackers can carry out attacks against them. It will also be crucial to understand how cyber resiliency metrics can be applied to different industries as well as how rules formation will be able to be produced in order to detail the given procedures whereby various industries are able to both, recover from and adapt to attacks that are launched against them.

Finally, the main purpose of this project will be to detail and produce a set of rules formation related to cyber resiliency metrics that can be applied to numerous cyber-related industries. This will be acquired through undertaking extensive research into cyber resiliency metrics as well as producing various forms of use cases that put the rules into practice.

1.5 Problem Statement

Cybersecurity attacks are on the rise and despite attempts to mitigate attack vectors, often these attacks are successful and cause considerable harm to their intended target. According to research conducted by Cloudflare (who specialises in cyber security) the number of distributed denial of services attacks increased by 109% over the previous year. This is a significant concern to all industries but in particular, the industrial control industry as a successful attack could cause havoc and render critical infrastructure inoperable (Law, n.d.)

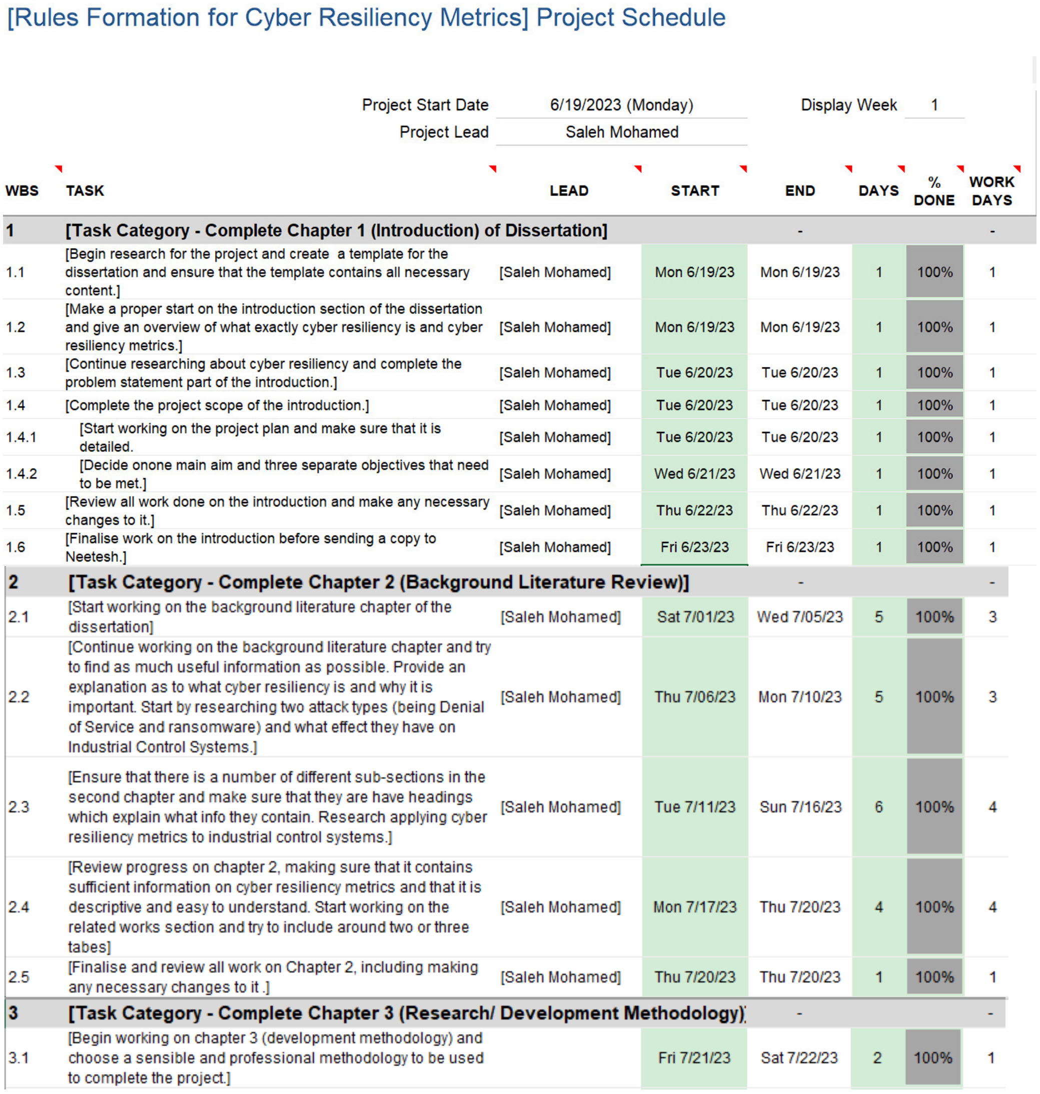
The challenge, therefore, is to assess the potential attack vectors as well as a potential victim's readiness to remain in service or to recover quickly in the event of a successful attack. To that end, a formal rules formation is vital.

As a result, the primary issue here will be to improve the overall resilience of various industries by setting forth cyber resiliency metrics in the form of a rules formation. This will enable industries to be able to plan ahead in case of a potential cyber-attack and act accordingly to minimise the damage as much as possible.

The completed project details an efficient rules formation, backed up by test cases to indicate the procedures of cyber resiliency metrics. It will imply the way the rules are formed and how they are used in cyber resiliency metrics when it comes to Industrial Control Systems.

1.6 Project Plan

Throughout the course of the project, as a means of conducting time management efficiently, as well as successfully completing each task by specific timeframes, a plan for the project was produced both, on the website Trello and on MS Excel. This allowed for different tasks to be completed smoothly and sufficiently, as it signified exactly what requirements needed to be met to complete each task as well as the deadline for completing each task.

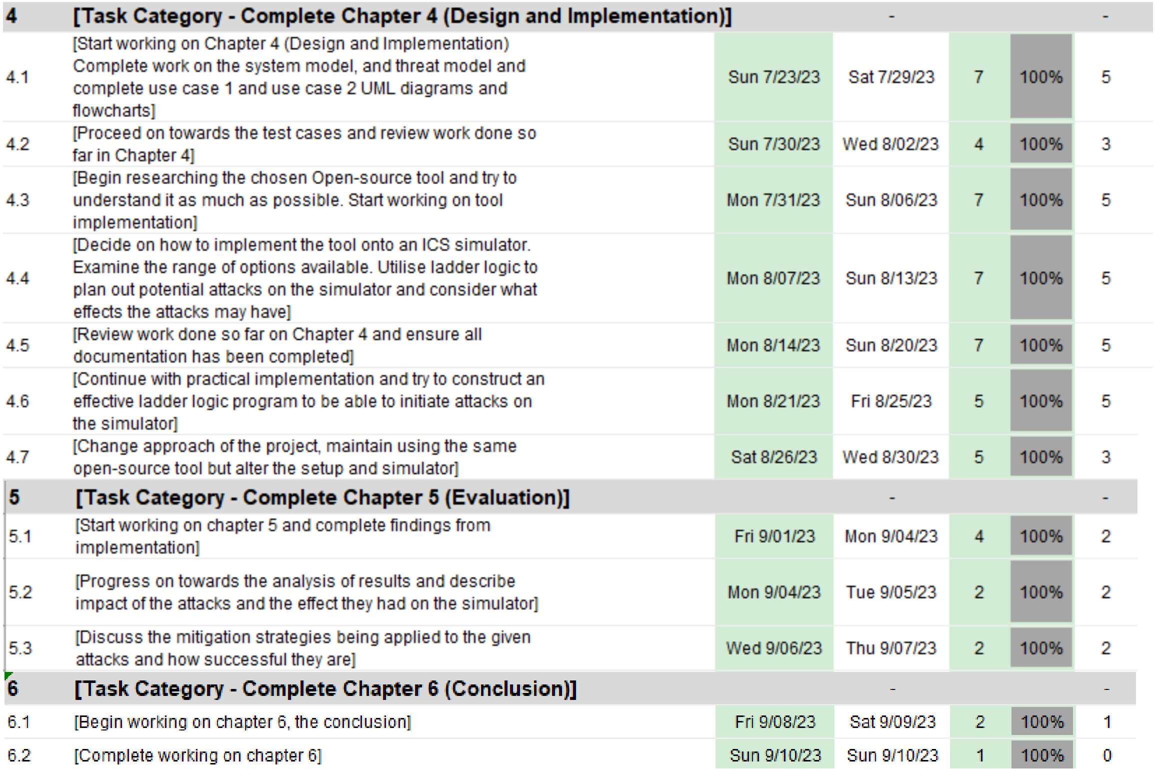


[Rules Formation for Cyber Resiliency Metrics] Project Schedule

Project Start Date	6/19/2023 (Monday)
Project Lead	Saleh Mohamed
Display Week	1

WBS	TASK	LEAD	START	END	DAYS	% DONE	WORK DAYS
1	[Task Category - Complete Chapter 1 (Introduction) of Dissertation]			-			-
1.1	[Begin research for the project and create a template for the dissertation and ensure that the template contains all necessary content.]	[Saleh Mohamed]	Mon 6/19/23	Mon 6/19/23	1	100%	1
1.2	[Make a proper start on the introduction section of the dissertation and give an overview of what exactly cyber resiliency is and cyber resiliency metrics.]	[Saleh Mohamed]	Mon 6/19/23	Mon 6/19/23	1	100%	1
1.3	[Continue researching about cyber resiliency and complete the problem statement part of the introduction.]	[Saleh Mohamed]	Tue 6/20/23	Tue 6/20/23	1	100%	1
1.4	[Complete the project scope of the introduction.]	[Saleh Mohamed]	Tue 6/20/23	Tue 6/20/23	1	100%	1
1.4.1	[Start working on the project plan and make sure that it is detailed.	[Saleh Mohamed]	Tue 6/20/23	Tue 6/20/23	1	100%	1
1.4.2	[Decide onone main aim and three separate objectives that need to be met.]	[Saleh Mohamed]	Wed 6/21/23	Wed 6/21/23	1	100%	1
1.5	[Review all work done on the introduction and make any necessary changes to it.]	[Saleh Mohamed]	Thu 6/22/23	Thu 6/22/23	1	100%	1
1.6	[Finalise work on the introduction before sending a copy to Neetesh.]	[Saleh Mohamed]	Fri 6/23/23	Fri 6/23/23	1	100%	1
2	[Task Category - Complete Chapter 2 (Background Literature Review)]			-			-
2.1	[Start working on the background literature chapter of the dissertation]	[Saleh Mohamed]	Sat 7/01/23	Wed 7/05/23	5	100%	3
2.2	[Continue working on the background literature chapter and try to find as much useful information as possible. Provide an explanation as to what cyber resiliency is and why it is important. Start by researching two attack types (being Denial of Service and ransomware) and what effect they have on Industrial Control Systems.]	[Saleh Mohamed]	Thu 7/06/23	Mon 7/10/23	5	100%	3
2.3	[Ensure that there is a number of different sub-sections in the second chapter and make sure that they are have headings which explain what info they contain. Research applying cyber resiliency metrics to industrial control systems.]	[Saleh Mohamed]	Tue 7/11/23	Sun 7/16/23	6	100%	4
2.4	[Review progress on chapter 2, making sure that it contains sufficient information on cyber resiliency metrics and that it is descriptive and easy to understand. Start working on the related works section and try to include around two or three tabes]	[Saleh Mohamed]	Mon 7/17/23	Thu 7/20/23	4	100%	4
2.5	[Finalise and review all work on Chapter 2, including making any necessary changes to it .]	[Saleh Mohamed]	Thu 7/20/23	Thu 7/20/23	1	100%	1
3	[Task Category - Complete Chapter 3 (Research/ Development Methodology)			-			-
3.1	[Begin working on chapter 3 (development methodology) and choose a sensible and professional methodology to be used to complete the project.]		Fri 7/21/23	Sat 7/22/23	2	100%	1

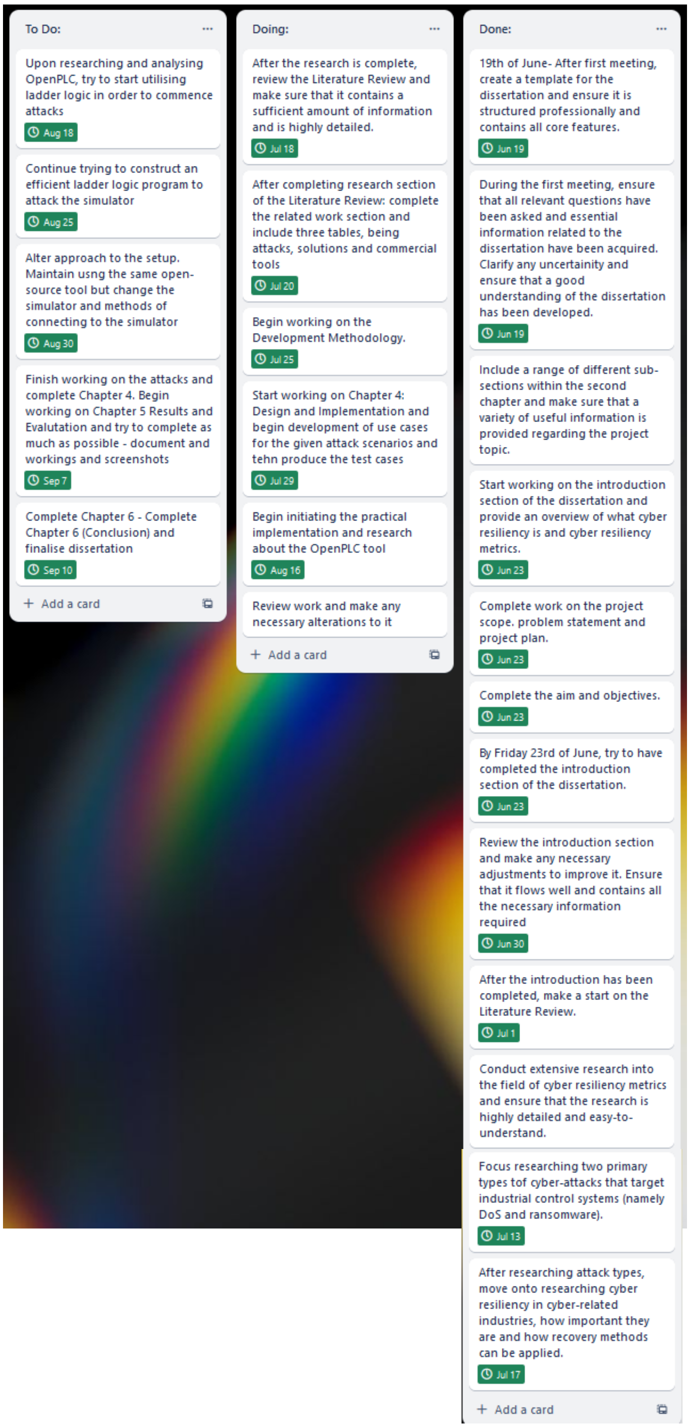
Figure 2 Project Plan



4	**[Task Category - Complete Chapter 4 (Design and Implementation)]**		-			-
4.1	[Start working on Chapter 4 (Design and Implementation) Complete work on the system model, and threat model and complete use case 1 and use case 2 UML diagrams and flowcharts]	Sun 7/23/23	Sat 7/29/23	7	100%	5
4.2	[Proceed on towards the test cases and review work done so far in Chapter 4]	Sun 7/30/23	Wed 8/02/23	4	100%	3
4.3	[Begin researching the chosen Open-source tool and try to understand it as much as possible. Start working on tool implementation]	Mon 7/31/23	Sun 8/06/23	7	100%	5
4.4	[Decide on how to implement the tool onto an ICS simulator. Examine the range of options available. Utilise ladder logic to plan out potential attacks on the simulator and consider what effects the attacks may have]	Mon 8/07/23	Sun 8/13/23	7	100%	5
4.5	[Review work done so far on Chapter 4 and ensure all documentation has been completed]	Mon 8/14/23	Sun 8/20/23	7	100%	5
4.6	[Continue with practical implementation and try to construct an effective ladder logic program to be able to initiate attacks on the simulator]	Mon 8/21/23	Fri 8/25/23	5	100%	5
4.7	[Change approach of the project, maintain using the same open-source tool but alter the setup and simulator]	Sat 8/26/23	Wed 8/30/23	5	100%	3
5	**[Task Category - Complete Chapter 5 (Evaluation)]**		-			-
5.1	[Start working on chapter 5 and complete findings from implementation]	Fri 9/01/23	Mon 9/04/23	4	100%	2
5.2	[Progress on towards the analysis of results and describe impact of the attacks and the effect they had on the simulator]	Mon 9/04/23	Tue 9/05/23	2	100%	2
5.3	[Discuss the mitigation strategies being applied to the given attacks and how successful they are]	Wed 9/06/23	Thu 9/07/23	2	100%	2
6	**[Task Category - Complete Chapter 6 (Conclusion)]**		-			-
6.1	[Begin working on chapter 6, the conclusion]	Fri 9/08/23	Sat 9/09/23	2	100%	1
6.2	[Complete working on chapter 6]	Sun 9/10/23	Sun 9/10/23	1	100%	0

Figure 3 Project Plan Continued

The Excel spreadsheet provides a detailed overview with regard to each task which has been completed, in each chapter of the dissertation as well as the length of time it took to complete each task.



Upon researching and analysing OpenPLC, try to start utilising ladder logic in order to commence attacks
Aug 18

Continue trying to construct an efficient ladder logic program to attack the simulator
Aug 25

Alter approach to the setup. Maintain usng the same open-source tool but change the simulator and methods of connecting to the simulator
Aug 30

Finish working on the attacks and complete Chapter 4. Begin working on Chapter 5 Results and Evalutation and try to complete as much as possible - document and workings and screenshots
Sep 7

Complete Chapter 6 - Complete Chapter 6 (Conclusion) and finalise dissertation
Sep 10

After the research is complete, review the Literature Review and make sure that it contains a sufficient amount of information and is highly detailed.
Jul 18

After completing research section of the Literature Review: complete the related work section and include three tables, being attacks, solutions and commercial tools
Jul 20

Begin working on the Development Methodology.
Jul 25

Start working on Chapter 4: Design and Implementation and begin development of use cases for the given attack scenarios and tehn produce the test cases
Jul 29

Begin initiating the practical implementation and research about the OpenPLC tool
Aug 16

Review work and make any necessary alterations to it

19th of June- After first meeting, create a template for the dissertation and ensure it is structured professionally and contains all core features.
Jun 19

During the first meeting, ensure that all relevant questions have been asked and essential information related to the dissertation have been acquired. Clarify any uncertainity and ensure that a good understanding of the dissertation has been developed.
Jun 19

Include a range of different sub-sections within the second chapter and make sure that a variety of useful information is provided regarding the project topic.

Start working on the introduction section of the dissertation and provide an overview of what cyber resiliency is and cyber resiliency metrics.
Jun 23

Complete work on the project scope. problem statement and project plan.
Jun 23

Complete the aim and objectives.
Jun 23

By Friday 23rd of June, try to have completed the introduction section of the dissertation.
Jun 23

Review the introduction section and make any necessary adjustments to improve it. Ensure that it flows well and contains all the necessary information required
Jun 30

After the introduction has been completed, make a start on the Literature Review.
Jul 1

Conduct extensive research into the field of cyber resiliency metrics and ensure that the research is highly detailed and easy-to-understand.

Focus researching two primary types tof cyber-attacks that target industrial control systems (namely DoS and ransomware).
Jul 13

After researching attack types, move onto researching cyber resiliency in cyber-related industries, how important they are and how recovery methods can be applied.
Jul 17

Figure 4 Project Plan 2

As well as the Excel spreadsheet the Trello board which was utilised during the course of the project duration was highly useful as it enforced a different kind of view than that of the spreadsheet created on Excel.

Chapter 2 Literature Review

This chapter will explain aspects of cyber resiliency metrics in relation to industrial control systems and various threats that can target them. It will detail attacks including DoS and crypto malware/ ransomware that target ICS systems such as smart grids, chemical plants and nuclear power plants, while also detailing how ICS systems can initiate a recovery in the aftermath of an attack and apply cyber resiliency metrics.

2.1 State-of-the-art Attack Analysis of Industrial Control Systems

2.1.1 Analysis of Cyber Resilience Metrics in Nuclear Power Plants

Due to power plants ageing and goals for efficiency, nuclear power plants are becoming increasingly digitalised. This resulted in an increase in cyber-attack occurrences, an example being in the year 2019, malware was located on computer systems within the Nuclear Power Plant Kudankulam in India. Furthermore, other attacks such as the STUXNET attack at an Iranian plant for enrichment as well as recent attacks on a power grid in Ukraine indicate the level of significance posed by cyber-attacks against industrial control system operations.

As cyber-attacks are becoming more and more advanced, it has become clear that ensuring total security for nuclear power plants is an impossibility and as a result, the need for sufficient cyber resiliency metrics has become ever more apparent. Cyber resiliency metrics focus on minimising damage taken, and maintaining system operations in the event of a cyber-attack.

Despite, the importance and usefulness of cyber resiliency metrics in nuclear power plants, they face several challenges. One such challenge is an insufficient amount of capabilities which can be used in order to inform the evaluation of resilience. In order to solve this issue, a platform for modelling cyber resilience which enables support for resilience analysis that is quantitative was produced by researchers at Sandia National Laboratories. The platform contains two main components, the first being testbeds that are virtual and undertake simulation integration as well as produce an accurate estimation of the attack's consequences on the given components. The second is Resilience VeRification Unit (RevRun) whereby RevRun undertakes data extraction and utilises them to produce metrics for cyber resiliency.

The topic of metrics for resilience can be seen as one that is open and Sandia National Laboratories have various researchers who have produced numerous types of metrics that conduct an analysis of a systems resilience to a cyber-attack through the use of conducting measurements of the negative repercussions related to the given attack as well as the resources needed to withstand and recover from the effects of the attack. The given metrics have already been enforced in infrastructure such as bulk power systems and supply chains and recently have been utilised as a means of classifying a power systems level of resilience to various cyber-attacks.

The platform overall generates resilience metrics that are quantitative and can be utilised across different types of Industrial Control Systems. RevRun is able to report all scores for the resilience metrics. The scores of resilience provide a score for particular devices and make use of a structure that is hierarchical in order to generate scores to different fidelity levels. The hierarchy begins at the bottom, splitting into three distinct groups; network, physical process and host (Galiardi et al., 2020).

2.1.2 Cyber-attacks on Smart Grid Control Systems

Smart grids have become increasingly prone to cyber-attacks with the primary issues being the identification and detection of vulnerabilities. This includes being able to identify potential vulnerabilities within smart grid components and understanding how to detect certain vulnerabilities and threats. Smart grids often contain components such as operators, sensors and programmable logic controllers (PLCs) (Talaei Khoei et al., 2022). Some significant vulnerabilities in smart grids include field equipment, network communication and local controllers including PLCs.

In addition, personnel who are unauthorised are potentially able to acquire access to the system's internal layers which is another significant vulnerability in smart grids as unauthorised access can result in changes that can have detrimental effects on the smart grid.

The first phase in ensuring smart grid systems are secure is by conducting vulnerability identification as well as access points (whereby an attacker will be able to gain access to the smart grid through certain points). These can be split into two primary areas including protocols and equipment for communication. Numerous protocols are created with the intention of being designed to improve reliability and efficiency, however, the majority of the given protocols do not take into account certain features of security including cryptography and authentication. In recent years, due to these protocols becoming integrated, attackers have been able to acquire highly important information regarding their structure and their function. With this, attackers have been able to identify packets of data and make modifications to them by finding vulnerabilities within the protocols.

A particular protocol which suffers from a lack of encryption and authentication is Modbus. One issue with this protocol is that it enables an individual to program controllers which various protocols of smart grids utilise with Modbus. Because of this, an attacker would be able to utilise it as a means of conducting malware injection into Programmable Logic Controllers.

However, in order to improve the cyber resiliency of smart grids in industrial control systems as well as utilise adequate strategies for security, there needs to be sufficient management of security such as strategies, and policies for security (Ghiasi et al., n.d.).

2.1.3 DoS Attack Analysis in Industrial Control Systems

Industrial Control Systems are critical infrastructure and smart grids of different countries, despite the advantages that they bring, have also generated problems in security. The most significant component in information security for ICS systems lies with availability, whilst Denial of Service (DoS) attacks remain the most dangerous threat to availability. ICS systems are often responsible for monitoring and controlling a variety of infrastructures that are critical. Due to this, vulnerabilities in security within systems that are responsible for control can enable ICSs to be targeted by attackers.

The primary aim of DoS attacks is to prevent a system from being able to access resources that are authorised or to stop the system from utilising the resources in the desired manner (Ciylan et al., 2018).

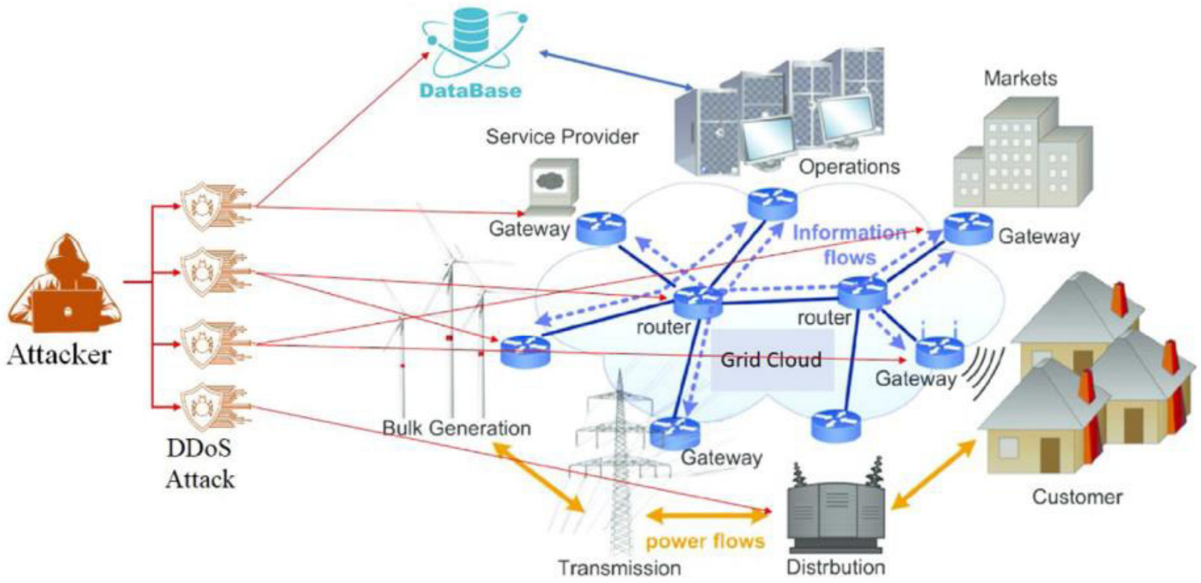


Figure 5 DoS attack on Smart Grid

According to (M. K. Hasan et al., 2023) Distributed Denial of Service cyber-attacks are particularly destructive when it comes to the infrastructure of smart grids. Attacks that are delivered by DDoS can result in multiple devices becoming compromised. During an attack, the flow of information or power in the layer that is physical is restricted. As the attack is taking place, data process skills of the smart grid are affected exponentially.

Furthermore, the attacker who has launched the attack will pinpoint several swarms of packets in the applications of the smart grid leading to significant damage and destruction. The attack's primary target is the smart meter due to the point of security protocol vulnerability that exists within networks used in the home (M. Hasan et al., n.d.).

2.1.4 Modbus DoS Attack in Industrial Control Systems

Whilst the Modbus protocol has a significant role when it comes to given communications in Industrial Control Systems as it can be used as a standard network protocol which contributes a significant role in the control and monitoring of field devices, its vulnerabilities to DoS attacks can pose a major challenge for it. Despite the value of Modbus, ICS can come under pressure from malicious traffic. This is partly because data generation increases as more devices that are physical are connected together as well as the fact that the Modbus protocol is considered insecure and the majority of SCADA systems are based on legacy systems.

As a result of the Modbus protocol's internal defects, the given systems can be targeted by an increasing amount of malicious traffic on the network, especially DoS attacks. An example of this is that in 2020, Venezuela’s power grid was paralyzed from infiltrators that were internal and resulted in major accident costs. The two primary reasons for the Modbus protocols insecurity are because the original design of the Modbus protocol lacked the function codes which ensure transmission that is secure as well as Modbus uses the base of the TCP/IP protocol, whereby the lower layers insecurity is inherited by the Modbus protocol.

DoS attacks pose a severe risk to the security of industrial equipment that is Modbus-based due to the low implementation cost. Although there have been improvements in DoS attack detection with regards to Modbus, there has been an emergence of threats to the security of the network. In addition, ICS face numerous threats due to the sophistication of the techniques utilised by attackers, with DDoS being one of the most prominent ones. Various researchers have attempted to create a system of traffic detection to deal with attacks of DDoS, some of these methods include applying Deep Learning as well as Machine Learning (Al-Abassi et al., n.d.).

In order to conduct the identification of traffic that is malicious, the network that is Modbus-based and at a level that is fine-grained, a model known as MODLSTM can be enforced which successfully identifies traffic that is malicious as well as locate targets that may come under attack. The MODLSTM has been able to give an accuracy score of 90.4% in DoS attacks as well as an accuracy score of 98.43% in the DoS dataset that is public (H. Zhang et al., 2023).

Recently, different approaches have been set out for the detection of attacks that are malicious on devices that are Modbus-based. For example, according to (Singh et al., 2014), the protocol Modbus/TCP can be targeted by flooding attacks. Thus, one key approach that can be taken is the development of a rule base which stops devices from getting hacked, however, it lacks the ability of being able to indicate sufficient detection.

2.1.5 Smart Grid Security

In a smart grid, nearly every component can be targeted by a cyber-attack. An example is, in 2016 a cyber-attack was launched at a northern Ukraine power grid by Russian hackers. The hackers were able to breach a data network that was IT-based (Information Technology) and resulted in a range of malfunctions in the OT devices (Operational Technology) of the substations and led to power outages for several hours. Because there has been a significant rise in cyber-attacks on smart grids, there is an urgency to conduct a review of the security of smart grids. Countermeasures that already exist are not efficient enough to provide effective security to smart girds against modern cyber-attacks (Kim et al., 2023).

The Stuxnet virus targeted infrastructures that are critical and utilised a variety of vulnerabilities that were zero-day. In comparison, there was an attack on power grids by a malware known as BlackEnergy which automated the activities of criminals.

An example of BlackEnergy in effect was, in 2015 an electric grid in Ukraine was targeted by BlackEnergy which disconnected a number of electric substations. This deprived 225,000 people of electricity. Furthermore, the Triton malware can be seen as a type of Remote Access Trojan which was designed to take control of the safety systems of ICS remotely. The given malware targeted the Triconex Safety Instrumented System (SIS) (Kumar et al., 2022).

2.1.6 Malware Attacks on Industrial Control Systems

A large amount of attacks that are launched against ICSs are utilised through Remote Access Trojans (RAT) including Stuxnet. These attacks can be completed through the exploitation of USB ports that are open and enable worms to conduct penetration of a network that is internal. These attacks can also exploit vulnerabilities of buffer overflows in the event that a program is attempting to place data in a location that is temporary where it exceeds the maximum space allocated. The buffer overflow often leads to Denial of Service but can also enable the execution of code that is arbitrary. An example of a DoS attack is a change in the chemical mix at a water treatment plant in the USA. This can be seen by the fact that, in 2015, a water treatment plant in the USA was hacked by what was suspected of being a group of Syrian hacktivists. The result of the attack was that hackers were able to change the amount of chemicals through utilising the web interface of the PLC, which disrupted the productivity of the plant. Moreover, in 2017, a number of cyber-attacks were launched against Ukraine, disrupting numerous websites including electricity firms. The attackers used a malware called NotPetya to launch the attack. The consequences of the attack were that manufacturers as well as hospitals became infected, resulting in over 10 billion dollars' worth of damages (Alladi et al., n.d.).

2.1.7 Multi-Stage Ransomware Attacks in Industrial Control Systems

Ransomware attacks are an increasingly prevalent and emerging threat to infrastructure that is critical. Infrastructure that is critical enforces various services that are essential for day-to-day life. Although the integration of the Internet with corporate and enterprise systems generates new techniques for the acquisition of data in real-time and thus has bolstered effectiveness, due to the diversity in the sectors of the infrastructures that are critical, there has been a lack of a framework that is secure. In addition as the protocol for IP is not secure, various cyber-attacks have been able to target infrastructure that is critical.

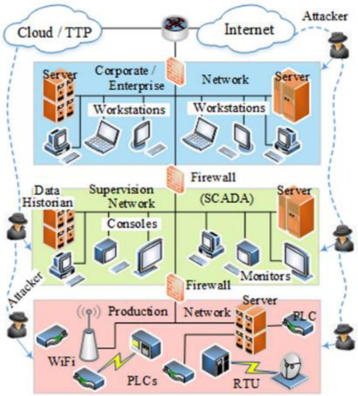


Figure 6 Overview of ICS

As a result, there have been a number of cyber threats whereby the differing design patterns within the networks of infrastructures that are critical have led to numerous cyber-attacks taking place targeting the points of entry of the infrastructures that are critical. The design of production networks consists of components such as Remote Terminal Units and Programmable Logic Controllers for access that is remote as well as Wi-Fi networks. In certain design patterns of networks, the components that are of a level that is low have a connection to the internet that is direct. This is a particular point of entry to which malware including ransomware can infiltrate.

Due to this, an attacker is able to undertake infiltration of the network supervision through the discovery of a vulnerability and attempt to direct the attack to the network production. Certain design patterns in networks connect the networks for enterprises as well as the networks for corporations through an approach that is cascaded including the Purdue Model. In this instance, the attacker will need to conduct infiltration of the network for corporations as a means of reaching the given ICS. (Zimba et al., 2018) produced a study in which they attempted to both, characterise and model techniques for cyber-attacking in order to break into an infrastructure that is critical from networks that are available publicly. They utilised attacks that included ransomware from conducting reverse engineering.

2.1.7.1 Model for Attacks

As soon as the Industrial Control System and Infrastructure that is critical are granted an internet connection, three entry points (being network that is corporate, a third party that is trusted and an internet connection that is direct) are identified where an attacker is able to conduct a delivery of the payload for the ransomware. The attack is modelled through the use of a graph designed to demonstrate an attack with the three points of entry. The given nodes provide three sources that can be used for infiltration, whereas the other section contained within the given graph demonstrates instances of nodes that are vulnerable contained within the three types of networks located within Industrial Control Systems and critical infrastructures. In the first graph, the edges that come in between the instances of the nodes provide potential vulnerability exploitation that can be used by ransomware throughout the given network.

A crypto ransomware attack's priority will be to infiltrate the availability through the use of setting encryption onto the files of the given victim in order to prevent the victim from being able to access the contents of the files. At the first node, the given malware will analyse if the host that has been targeted is already infected, if it is found to not be infected, it will then try to place a form of encryption on the files that it is targeting. The malware will then begin to analyse the production network and SCADA network for identifiable vulnerabilities within the network. As the malware utilises nodes that are vulnerable in various subnets the given attacks are classed as attacks that are multi-stage.

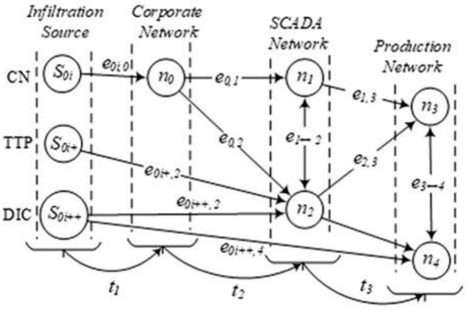


Figure 7 Infiltration, Corporate, Production and SCADA Network and Nodes

Ultimately, the study looked at different types of multi-stage crypto-ransomware attacks originating from numerous sources of infiltrations in infrastructures that are critical. The results of the malware analysis which are static indicate the various techniques that are employable through the ransomware as a means of propagating as well as launching attacks on the components of the infrastructure that is critical (Zimba et al., 2018).

2.1.8 The threat of ransomware on SCADA systems

Despite the fact that ICS components are connected heterogeneously, greater efforts are needed as a means of ensuring that the given components have secure communication between them. However, as a result of the design complexity, the systems that are critical are often vulnerable to ransomware.

Ransomware demands that the victim pay a steady ransom in exchange for the data being decrypted ("The Law and Politics of Ransomware," n.d.). If the victims refuse to pay the ransom, then the attacker who currently holds access to the files will either corrupt the files or erase them. Various experts signify that Ransomware takes two forms, with the most common being crypto-ransomware, whereby its purpose is to carry out data encryption on the device of a victim and maintain it until the ransom has been paid.

The other type of ransomware is locker ransomware that causes a system to become infected and prevents a user from accessing the data but does not impact the files that have been stored. With this, the demand is typically portrayed on the entire screen. Attackers will often demand a payment in the form of cryptocurrency after the attack has finished. According to (Symantec et al., 2017), the combined amount of devices that were protected and infected went from 340,000 in the year 2015 to as much as 463,000 in the year 2016.

2.1.8.1 Recent Attacks

This can be illustrated by the following example; In the year 2016, in May, a hospital in Kansas was targeted by multiple ransomware threats. The software was classified as the malware Samsam. Despite the fact that the hospital paid the ransom, the data was not provided with full access by the attackers (*Kansas Heart Hospital Hit with Ransomware; Attackers Demand Two Ransoms | CSO Online*, n.d.). Whereas in November 2016, a San Francisco transit system was hit by ransomware and had a demand of $70,000 (Javed Butt et al., 2019).

2.1.8.2 Factors leading to a rise in Ransomware in ICS

As ransomware encrypts files on a system and prevents access to those files, they are considered a significant threat to systems which make use of SCADA for operational process control. The SCADA architecture consists of two primary components; the network that is corporate and the SCADA network which shares a connection utilising networks that are public including the internet. The connection between the network that is corporate and the SCADA network enables communication to occur between different devices which in turn, allows for control of processes and transmission of data. Software that is malicious including ransomware is one of the most prominent threats that consistently target cyberspace in order to obtain information that is sensitive and cause a disruption in the operations of computer systems. Similarly to other systems, SCADA have a vulnerability to different forms of cyber-attacks including ransomware and thus require protection as a means of making sure that the systems environment has efficient resiliency.

Although devices that are SCADA are not designed to hold files and documents of users, cyber-attacks such as ransomware, can lead to severe disruptions including disabling surveillance access. Likewise, the data that is produced by numerous components of the SCADA system are susceptible to hijacking and can become encrypted, resulting in a disruption in the system's operations.

One of the primary factors that lead attackers to ransomware is the monetary benefit. Typically, an individual may pay from $300 to $700, alternatively, organisations usually pay roughly $10,000 and as much as $17000 (Everett, 2016). Furthermore, due to the fact that ransomware utilises cryptography in order for the user data to be hijacked, the best method will be to resort to a backup. In creating regular backups, various users are able to mitigate the damage dealt by the ransomware. Backups that are connected to the network can themselves become encrypted by the attacker. Organisations would need to employ offline backups at regular intervals in order to recover their systems.

In addition, it is largely seen as pivotal that the prevention of ransomware attacks needs efficient educational awareness from both, employees as well as management. Moreover, in SCADA systems, when ransomware attacks are targeted specifically at data, it would lead to the system becoming hindered when attempting to respond to the controller's signals and various attacks are able to conduct exploitation of numerous vulnerabilities in order to acquire data as well as perform an encryption of the data.

The SCADA's components can become possible ransomware targets as servers of data within SCADA have a connection to the network that is outside, they are able to be struck by attacks of crypto-ransomware which undertake data encryption as well as prevents access to crucial information on operations (Gazzan et al., n.d.).

2.1.9 Assessing vulnerabilities of ransomware attacks

Ransomware is one of the most significant types of techniques that attackers utilise in order to exploit the vulnerabilities within a computer system, with many encryption methods remaining unbroken as well as cryptocurrencies that can't be traced. Attacks that have occurred recently have been very successful in acquiring millions of dollars including an attack that took place in the year 2015 called CryptoWall which the FBI estimated to have cost 18 million dollars (Menlo Park, 2017).

Furthermore, Cybersecurity Ventures indicates in a 2019 statistical report on cybercrime that ransomware is growing faster than other types of cyber-attacks (Petrosyan, n.d.). In addition, more recent ransomware attacks on ICS systems signify that cyber-attacks do not solely target data but also target various resources including the source of electrical power.

Moreover according to (Stoyle, E., 2019) in 2019, three companies that manufacture chemicals which are located in the US and in Norway, came under ransomware attack. This is due to a program known as LockerGoga acquiring access to various files that are encrypted, accessing systems as well as performing operations that caused disruptions. As a result, on March 1, the company Norsk Hydro had to shut down numerous plants due to a breach in security that resulted in file access becoming blocked and the accounts of various users having their passwords being altered throughout a variety of production and corporate control systems. The ransomware then revealed that encryption had been placed on the files and required a payment in the form of Bitcoin for the access to be restored. At the same time, two chemical organisations that are American (Hexion and Momentive) made an announcement that they had been targeted by cyber-attacks and were forced to turn off their IT systems. As LockerGoga is fairly new and is a ransomware that is continuously adapting, it poses a severe threat and security experts indicated that chemical manufacturers have a vulnerability to cyber-attacks. It is thought that the cyber-attack resulted in Nork losing as much as £31 million.

2.1.9.1 Measures of vulnerability analysis

Ransomware vulnerability depends on the awareness of the user as attackers that utilise ransomware can use the lack of awareness of the user to their advantage before launching an attack. This could include an engineer working at a smart grid who may inadvertently enable an attacker to encrypt confidential information (Malkawe et al., 2019).

2.1.10 The effect of ransomware on ICS

Due to the fact that crypto-malware/ ransomware can be very profitable for attackers, Industrial Control Systems have become a prominent target for attackers. However, as there is often uncertainty as to whether the attackers are actually going to perform decryption on the data after receiving a ransom, based on statistics, fewer than 50% of the victims of ransomware will be willing to pay the ransom (Tripwire, 2016). At the same time, the quantity of ransom increased between the years 2016 and 2020 (Trend Micro, 2020). With ICS, ransomware often targets devices including remote terminal units and program logic controllers. Ransomware on ICS mainly prioritises operations and safety on ICS including locking ICS devices or writing a logic bomb in order to cause the operations to cease productivity or generate errors. The profit from ransomware is typically significantly greater when targeting ICS (Delaney, 2020). Additionally, ransomware that is successful in breaching the environment of the ICS should meet the following:

2.1.10.1 Low-Profile

The goal of the ransomware will be to initiate an attack as quickly as possible without being detected.

2.1.10.2 Attack on multiple terminals

When attacking ICS systems, ransomware may not just attack industrial devices such as remote terminal units and programmable logic controllers but may also target PCs including a computer that is supervisory.

2.1.10.3 Cheap Cost

With an attacker who is sophisticated, initiating an attack which has a relatively low cost usually implies a greater profit from the attack.

Ultimately, ransomware that targets ICSs are extremely deadly and can inflict catastrophic damages. In addition, ransomware that targets ICS is able to encrypt highly crucial information that can have a major impact on whether or not the ICS is able to function properly and can thus affect the lives of millions of people (Y. Zhang et al., 2020).

2.2 Implementing Cyber Resiliency Metrics in ICS

This section will discuss implementing cyber resiliency metrics into ICS in order to initiate recovery/ mitigation measures when a system is under attack.

2.2.1 Introduction to Cyber Resiliency Framework for ICS

In the modern era, with the development of Information and Communication Technologies, ICS systems are increasingly targeted by cyber-attacks. An instance of this is Advanced Persistent Threats (APTs), whereby an attacker is able to obtain information related to user authentication and then travel throughout the network, moving from each host in a manner in which they remain undetected until they finally find a target that is valuable. For example, in 2015, a number of attackers utilised spear-fishing as a means of acquiring the credentials of three Ukrainian energy companies.

2.2.2 Cyber Resiliency of ICS and R4 Framework

When it comes to making an ICS system resilient, there are various characteristics that can be considered resilient. This includes the ability to lower the consequences that are undesirable of a given incident. The ability to reduce the majority of the incidents that are undesirable and the ability to ensure that ordinary operations are restored within a short period of time. These characteristics reside in the R4 resilience framework. In addition, when analysing the R4 framework, 4 cyber resiliency metrics can be formed, including Robustness, Redundancy, Resourcefulness and Rapidity. Due to the fact that resiliency is dependent on the successful operational capacity of every aspect related to the ICS, the structure of metrics needs to take into account practices that are organisational, security that is physical as well as technology which has been enforced within the system that is cyber-physical.

2.2.3 Formulation of Metrics

A major challenge to producing cyber resiliency metrics with regard to ICS systems is that there is often a lack of data related to the ICS's cyber security due to the fact that it is not readily available. When considering the lack of available system data, metrics for resiliency are able to be evaluated through an approach that is qualitative by using a set of questionnaires. The questionnaires go through a design process whereby they are able to successfully address every separate sub-metric and thus obtain information that is qualitative regarding the resilience posture of the system (Haque, Teyou, et al., n.d.).

2.2.4 Improving Cyber Resiliency

Various attempts to conduct measurements of cyber resiliency have leaned towards the system's ability of being able to defend against threats that are predictable, by means of avoiding the state of being compromised. The primary notion regarding cyber resilience is the ability to accept the fact that a cyber compromise is a likely occurrence, whereby the focus is on the targeted system's ability to be able to recover from the incident as well as being able to adapt and not simply resist. The premise of cyber resiliency is characterising the events that take place in the aftermath of an event that is adverse and demands preparation for both, threats that are known and unknown. One efficient method of improving cyber resilience is through directly measuring the resilience both, with a control set and without one (Kott & Linkov, 2021).

Industrial Control Systems that are resilient have been designed in a manner in which the impact of events that are undesirable is reduced significantly. Five criteria that can be used as a means of measuring a control system's resilience include; Protection time, which is a given time whereby a computer system is able to withstand the effects of an incident or an attack without suffering from a degradation of performance. Moreover, degradation time can be considered a given time which a system needs in order to approach its greatest disruption of performance as a result of an incident. In addition, Identification time is the time taken by a given computer system in order to conduct identification of a particular incident. Finally, performance degradation is the highest degradation of a system's performance as a result of an incident.

2.2.5 Improving Resiliency with Redundancy

As various cyber incidents are difficult to completely eliminate, one way of reducing the impact they have on Industrial Control Systems is through the use of integrating components that are redundant. Furthermore, with control redundancy, making use of programmable logic controllers that have been duplicated where one of them is readily available to handle control activities in the event one fails is also highly useful.

At the same time, there are a number of characteristics of redundancy in independence; this redundancy can only be achieved if a component that is redundant is able to take over the operations of a primary component that has failed. Similarly with the propagation characteristic, propagation failure, which can generate effects that are cascading, comes to play in the event that a failure of a component leads to the failure of an additional component or system (Chaves et al., n.d.).

2.2.6 Industrial Control Environment Redundancy

With Industrial Control Systems, there is a reliance on designs that are robust in order to help protect the systems from various cyber-attacks. In order to produce an ICS which is resilient, the system will need to have a design that is cyber-tolerant and fault-tolerant (Chaves et al., n.d.).

2.2.7 The Importance of Cyber Resiliency

A system's ability to be able to restore its functionality in the event of a compromise or an attack is important for a variety of computer systems, especially ICS systems. In the event of a significant cyber-attack, the given system will absorb the threat and the functionality of the system will start to degrade. Whilst cyber security prioritises system hardening as a means of preventing system degradation, cyber resilience prioritises system recovery. Cyber resiliency is naturally dependent on a number of system aspects including controls, design, anticipation and preparation which take place prior to the cyber-attack or event which is adverse (Kott & Linkov, 2021).

2.2.8 Observations of Resiliency Metrics

While cyber resiliency becomes more and more important and the need for resiliency becomes ever more present, defining it, as well as making use of cyber resilience metrics has become essential.

Cyber resiliency can be utilised in the following areas: systems that encompass systems-of-systems, various missions that acknowledge systems of systems, organisations whereby the CERT Resilience Management Model is applicable and enterprises that are transnational which boast support from systems-of-systems that are virtual.

Cyber resiliency metrics predominantly relate to the objective of being able to recover from conditions that are adverse as well as cyber-attacks. Metrics which revolve around anticipation have attributes related to cyber-defence or contingency planning whilst metrics which revolve around adaptation usually have attributes regarding acquisition agility. At the same time, metrics that are utilised with recovery are able to render in terms of capabilities that require reconstituting. Whereas, metrics revolving around availability, which have to deal with disruption lack the efficiency for cyber resiliency measurements.

2.2.9 Cyber Resiliency Metrics Evaluation

Cyber resiliency metric evaluation includes an assumption or representation in relation to an environment's characteristics whereby resilience is analysed. With the resilience of a system, it can be a challenge to actually define the system, and in a cyber environment that is contested as systems need to be seen as a system that is socio-technical that encompasses cyber defenders, adversaries and mission users.

However, no single set of metrics for cyber resiliency will be applicable to every environment. It can be difficult to define a set of metrics for cyber resiliency that are related to a particular system as they need to take into account the various stakeholders whose choices with be decided through the metrics (D. Bodeau & Graubart, 2016).

2.2.10 Cyber Resilience Control Systems Analysis and Measurement

The emergence of cyber resiliency has taken the form of a type of strategy which complements efforts of security as well as risk management contribution. Efforts of cyber resiliency understand the impossibility of being able to ensure that the degradation of systems is prevented from all forms of cyber-attacks. Cyber resiliency efforts are intended to make sure that operations that are essential, are able to continue operating functionally in the event of a cyber-attack.

Cyber resiliency metrics which focus on reliability include System Average Interruption Frequency Index (SAIFI) as well as System Average Interruption Duration Index (SAIDI) which conduct measurements on the ability of an infrastructure to be able to enable service delivery continuously have previously been the main measure when it comes to evaluating the operations of infrastructure. A number of metrics for cyber resiliency are designed with the intention of conducting an evaluation of the readiness of an organisation. An example is the CERT Resilience Management Model that contains various metrics of resilience measures that take place at organisational levels (Jacobs et al., n.d.).

2.2.11 ICS-CRAT

The ICS-CRAT is a Cyber Resilience Assessment Tool for Industrial Control Systems that is designed to produce metrics for cyber resilience based on the R4 cyber resilience framework. Through the use of the seismic resilience metrics detailed in R4, a productive framework for cyber resilience can be developed as well as metrics that are designed specifically for ICS systems. The given tool for simulation that is qualitative takes into account the framework for cyber resilience as the analysis's foundation. The metrics of R4 resilience can be split into three primary domains, being physical, technical and organisational. Every area of the domains is further split into numerous sub-metrics in order to provide an assessment for resilience to the ICS which is comprehensive. An example is that the metric of Robustness can be split into Technical Robustness, Physical Robustness and Organisational Robustness.

Robustness that is Physical has two main sub-metrics including Physical Diversity and Physical Access Control. Whilst Robustness that is Technical contains ICS Segmentation and Segregation, Product Diversity and ICS Security. Likewise, robustness that is organisational includes Insider Threat Management and Access Control that is Role-based. The R4 metrics are known as metrics that are strategic, whilst the metrics that are in a domain are known as metrics that are dimensional whereas the sub-metrics are known as metrics that are operational. In total, there consist of four metrics that are strategical, twelve metrics that are dimensional as well as thirty-eight sub-metrics that are operational which are utilised as a means of assessing an ICS's cyber resilience (Haque, …, et al., n.d.).

2.2.12 Aspects of Recovery of Cyber Resilience

With cyber resilience, there are four main aspects, being; prepare, withstand, recover as well as adapt. The first aspect, prepare, revolves around planning, prediction as well as anticipation of the potential of a given cyber-attack and also contains the steps that need to be taken and what order as well as by whom. Preparations for cyber recovery would be lacking if they did not consist of processes, principles as well as procedures. The next aspect is withstand which details how to withstand or absorb a cyber incident whereby standard operations of business remain operational and the recover aspect which includes how a system can recover from a cyber incident such as being able to restore key operations to how they were before the attack or incident. Moreover, adapt refers to a system being able to adapt to a given incident e.g. by improving its features and operations. Although Cyber resilience within cyberspace consists of recovery, absorption and adaption, the majority of the focus lies within how the impact of an incident is absorbed. Cyber recovery ultimately prioritises various measures that are needed in order for recovery to take place in the aftermath of a cyber incident.

2.2.13 Framework for Cyber Recovery

Despite the fact that cyber recovery activities can be very beneficial, there remains a chance that a cyber incident will occur in a way that the recovery activities have not prepared for. For this, a framework for cyber recovery can be established, which consists of a total of 8 primary parts being; Identify, Control, Map, Plan, Playbook, Measure, Test and Improve.

2.2.14 Cyber Resilience of Cyber-Physical Systems

When it comes to cyber-physical systems, cyber resilience prioritises the steady operation of a system to enable it to keep functioning after being attacked and provide the system with services that are essential even whilst it is being attacked. At the same time, stability relates to a system's ability to be able to reach the point of equilibrium after disturbances have occurred in the system. Likewise, performance focuses on operating at a dynamic response that is desired and in a mode of control which is optimised.

2.2.15 Resilience Metrics of Cyber-Physical Systems

Stability and performance analysis looks at whether or not a system can retain its stability as well as achieve a minimum threshold for performance whilst it is under attack. It enables quantifying the total amount of time in which a system is able to withstand the phase of the attack that is absorption. In addition, it also revolves around being able to determine the different states in which the system could reach throughout the time it is being attacked and provide an estimation of the maximum amount of damage which the attacker could inflict on performance. Ordinarily, performance is utilised as a means of conducting measurements of the given deviation between the models that are used to control it as well as process dynamics. Furthermore, it can be utilised as a means of conducting an evaluation of the system's resilience through the use of undertaking an analysis of the capacity to recover from a given attack (Segovia et al., n.d.).

2.2.16 Cyber Resilient PLC Architecture for Industrial Control Systems

As a result of the importance of infrastructure that is critical such as environments that are industrial, it is paramount that programmable logic controllers are safeguarded from various forms of cyber-attacks such as DoS and ransomware. When an Industrial Control Systems programmable logic controller is targeted by a cyber-attack, significant damage can be caused. In ICS that are conventional, programmable logic controllers are designed to be robust, isolated and redundant as well as being detached from a network that is enterprise. However, in reality, these conventions are often not the case and generate vulnerabilities within cyber security and as soon as malware, such as ransomware is able to breach the network perimeter of an ICS, a lack of security that is internal can result in the ransomware spreading throughout the network unchecked. As a consequence, if an attacker is able to place ransomware into a component that has a less critical level then they can utilise this as a base for carrying out various cyber-attacks that target programmable logic controllers that are critical through the network of the ICS (Luo et al., 2021).

2.3 Related Work

2.3.1 Potential Attacks on ICS

In this part of the dissertation, potential attacks on ICS, including Denial of Service/ Distributed Denial of Service and ransomware are presented from various literature available (Gunduz & Das, 2019) (Raja et al., 2022) (Ibrahim & Al-Hindawi, 2019) (the & 2016, 2016) (Asri & Pranggono, 2015).

Possible cyber-attacks

Table 1 Cyber Attacks on ICS

Category of assets	Type of attack	Attack Description	Target of Attack	Level of Severity	Impact of Attack
Smart Grid	DoS/ Distributed Denial of Service (DoS)/ (DDoS)	Flooding will distribute the given traffic in a manner that is unrestricted as a means of causing the network to overload.	Smart Meter	High	Compromises availability of data in the smart meter.
		Jamming is a typical technique used by DDoS to restrict given information or cause it to slow down in the layer that is physical. This will result in information in the Advanced Metering Infrastructure being restricted.	Advanced Metering Infrastructure (AMI)	High	This will lead to a disruption in data availability within the smart grid.
Chemical Plant	Ransomware	Crypto-ransomware will encrypt confidential files and data that are crucial for the chemical plant to be able to operate effectively. In doing so, certain features of the chemical plant won’t be able to operate.	Programmable Logic Controller (PLC)	High	The particular component in the chemical plant may not be able to operate efficiently as certain information that is required will be locked behind an encryption barrier and will be inaccessible.
Nuclear Power Plants	Man-In-The-Middle	This given attack is able to be undertaken and completed as soon as the attacker acquires a connection such as an access point in WiFi between two given sources which will grant the given attacker access to the transmitter for communication via eavesdropping.	Enterprise System Management Computer	High	This type of attack can have a major impact on nuclear power plants as an attacker will be able to use eavesdropping to “listen in” to the communication channel and obtain sensitive information from this.
Nuclear Power Plants	Spoofing	Nuclear power plants often do not have sufficient controls for security in place. An example is that SCADA utilises protocols such as TCP/IP which are vulnerable to IP spoofing.	SCADA systems	Medium	This will enable an attacker to impersonate a computer system in the nuclear power plant and disrupt standard operations.

2.3.2 Available Solutions to Given Attacks

For Table 2, a range of available solutions to the attacks listed in Table 1 based on the research and analysis conducted (Huseinović et al., 2020) (Rudd et al., 2017).

Table 2 Solutions

Name of Solution	Category of Solution	Solution Description	How the solution is implemented	Advantages of Solution	Disadvantages of Solution
NIST Framework for Improving Critical Infrastructure Cybersecurity	Non-Technical Security Controls for Denial of Service	Controls that are physical and used to prevent or deter access that is unauthorised to areas that are sensitive and are relatively efficient at guarding against particular forms of DoS attacks.	Following and adhering to NIST guidelines regarding the given framework.	It can be beneficial when implemented efficiently and can be useful in being able to prevent or deter various DoS attacks.	It is not practical or technical and does not provide any form of actual mechanism to guard against DoS attacks.
Filtering	Practical method of defending against DoS attacks	Packet filtering can be initiated onto devices in a perimeter including firewalls. When being applied to security, filtering can assist in preventing attacks that are DoS.	An example would be that a firewall which has been configured with a set of hosts that are trusted can be utilised as a relatively simple but effective form of security against Denial of Service attacks.	It is practical and can be a useful solution to tackling Denial of Service attacks in certain situations.	In the event that attackers breach within the network of the industrial control systems such as the smart grid through utilising devices that are malicious, and within the perimeter that is trusted by the personnel of the given organisation. With this, filtering would not necessarily be a feasible choice.
Intrusion Detection/ Prevention System	Practical method to detect Denial of Service attacks or to prevent them from taking place	Intrusion Detection Systems are able to analyse the packets within the Industrial Control System, including both, the header as well as the payload before then initiating an alert when a network event that is suspicious is detected.	The IDS obtain information regarding the Industrial Control Systems from sensors. Intrusion Detection Systems take on three separate categories being signature-based detection, anomaly-based detection and specification-based detection. As an attack of DoS is considered an anomaly, anomaly-based detection would be the most efficient form of IDS.	Intrusion Detection Systems, especially ones that are anomaly-based will be able to detect and intercept DoS packets and minimise damage done to the Industrial Control System.	If there is encryption on the packets, then the IDS may have trouble identifying whether or not they are malicious.
Cryptographic Authentication	Practical measure of countering Denial of Service (DoS)	Cryptography can be considered a powerful tool which is used as a means of detecting as well as rejecting messages that are unauthorised which are transferred by outsider sources.	When all sources that are communicating as well as their given packets are all authenticated cryptographically, various Denial of Service attacks are able to be avoided.	Authentication that is Cryptographic can enable confidential information to remain hidden in the event that a DoS attack affects it.	Cryptography can become vulnerable to an attack of Denial of Service. This can be seen by the fact that, if verifying a packets authentication leads to an enormous quantity

					of resources being consumed, then an attacker would be able to successfully carry out an attack via fraudulent packets.
Machine Learning and Artificial Intelligence	Practical Protection against Ransomware	AI and Machine Learning can be seen as critical concepts of protection against ransomware as they allow for detecting various patterns of behaviour that are malicious.	Machine Learning is a useful mechanism for defending against ransomware attacks as it results in an improvement in the ability of being able to conduct detection of information that is unrecorded.	Through the use of solutions such as machine learning and artificial intelligence industrial control systems such as smart grids are able to utilise the ability of technology to adapt and improve.	Machine learning and artificial intelligence can be difficult to implement, especially in industrial control systems.

2.3.3 Commercial Tools

In order to overcome and recover from the given cyber-attacks or mitigate their impact, it is crucial to understand the nature of the attacks. Table 3 provides a list of tools available that can be used to launch cyber-attacks including Denial of Service and ransomware (Catillo et al., 2020) (Cabrera et al., 2002) (Lypa et al., n.d.) (Alves & Morris, 2018) (Xavier et al., 2023) (*8 Best DDoS Protection Tools & Anti-DDoS Software 2023 (Paid & Free)*, n.d.).

Table 3 Tools

Name of Tool	Tool Source	Primary features	Advantages	Disadvantages
HULK (Http Unbearable Load King)	AllAboutTesting (Installation on GitHub)	• Denial of Service tool that is utilised as a means of attacking servers on the web through producing volumes of traffic that are both obfuscated as well as unique.	• It is efficient at initiating DoS attacks due to the fact that it is able to launch communication that is disguised.	• It can launch attacks which can be incredibly challenging when it comes to identification.
Low Orbit Ion Canon (LOIC)	Praetox Technologies (original developer, but now available on the public domain)	• Low Orbit Ion Canon is a tool that is open-source that is used to carry out Denial of Service attacks. It can also be used as a stress tester for networks.	• The mode “HIVEMIND” enables the user to control LOIC systems that are distant. • It is useful in attacks that are DDOS whereby a large quantity of volumes in involved.	• LOIC is unable to conceal the attacker's IP address.
High Orbit Ion Canon (HOIC)	Praetox Technologies	• High Orbit Ion Canon is a Denial of Service attack tool that is open-source.	• It has support for concurrently launching attacks on a multitude of domains. • Utilises various capabilities of scripting in order for the	• It needs a group of coordinated users in order for the attack to be successful and efficient.

			customisation of parameters of attacks.	
OpenPLC	OpenPLC	• OpenPLC is an integrated development environment that contains a programmable logic controller that contains substantial functionality. Various projects can be produced from the OpenPLC editor whilst they can be executed by the Runtime for OpenPLC. • It consists of two primary elements being Editor and Runtime where the runtime can be seen as a software that is portable and intended to run on both servers that are powerful as well as microcontrollers. • Whereas the editor is the given software which operates on the computer and is utilised to produce PLC programs.	• It is open-source, standardised and is fully functional. • The Editor can be run in Linux, Windows and MacOS and maintains support for all of the IEC 61131-3 languages including Function Block Diagram, Ladder Logic, Structured Text etc.	• Can be difficult to use if the user is unfamiliar with the languages.
Tor’s Hammer		• Tor’s Hammer is a tools for testing DoS attacks and was created using the Python programming language. • Initiates an attack that is DoS/ DDoS through utilising requests from HTTP POST at a pace that is slow at the same time as the given session of HTTP us taking place.	• It can be utilised as a means of displaying the capacity of a server through directing attacks on web applications. • Can hold a connection post that is HTTP for a maximum of 30,000 seconds.	• Its primary network only moves at a standard pace and so its overall effectiveness is curbed by its speed.
Pyloris		• Pyloris is a relatively slow tool for carrying out DoS attacks and allows the attacker to produce their own HTTP header requests.	• It is able to directly carry out a DoS attack on a network. • It has a user-friendly GUI.	• It is Python dependent.

2.4 Summary

This chapter has covered the most important aspects of cyber resiliency metrics in industrial control systems including the biggest state-of-the-art attacks on industrial control systems such as Denial of Service and crypto malware/ ransomware as well as discussing implementing cyber resiliency metrics into industrial control systems. It first goes into extensive detail by explaining the most pivotal state-of-the-art attacks and how they can affect industrial control systems before then indicating how to apply cyber resilience metrics to the industrial control systems and how important they are to implement. It then goes into the related works section whereby the attacks on industrial control systems are listed, as well as the solutions to the attacks before finally discussing the commercial tools that can initiate the given attacks.

Chapter 3 Methodology

3.1 Overview

This chapter describes the research methodology and approach that is utilised in the project as well as the various methods of research that were undertaken. It indicates the given criteria which were undertaken as a means of producing the use cases, test cases and the necessary requirements regarding the rules formation of the cyber resiliency metrics.

3.2 Approach of Research

For this project, the first part primarily leans towards the elements that are theoretical as well as the present knowledge state of the obtained research and the various standards and methodologies on cyber resiliency metrics in relation to industrial control systems. The given thesis utilises an approach that is qualitative. Cyber resiliency metrics and rules formation encompasses a large area including cyber security, computer science, IoT as well as networking and demanded a significant amount of literature work to acquire all of the necessary materials and information to be able to develop use cases and test cases to ultimately produce the rules formation for cyber resiliency metrics. A variety of different sources were used to obtain the key information including ScienceDirect, IEEE Xplore, ACM Digital Library etc, as these provided highly useful as well as reliable information for the given project at hand.

The research papers were chosen going by a set of criteria:

- Papers that revolved around industrial control systems.
- Papers that were relevant to cyber resiliency.
- No specified date of publishing due to being able to obtain papers from a wide range.
- Cyber resiliency metrics that can be applied to ICS, especially smart grids, chemical plants and power plants.
- Papers that emphasise the impact of cyber-attacks on ICS, particularly ones that focus on Denial of Service and crypto malware/ ransomware.

- Papers that discussed resiliency in relation to smart grids and chemical plants.

Thus, this thesis combines work from a variety of research articles including state-of-the-art attacks on ICS and methods of implementing cyber resiliency metrics into ICS in order to improve the overall resilience of these systems from cyber-attacks. This is due to the fact that the vast majority of articles reviewed discussed the cyber-attacks on ICS such as Denial of Service and ransomware whilst others detailed ways of implementing cyber resiliency including steps for recovery/ mitigation and adaptation.

3.3 Producing the given rules formation

The first part of producing the given methodology revolved around obtaining sufficient research and information available from the most relevant literature and utilising the methodologies that had been acquired as well as their methods of classification. The majority of the methodologies focused on the security and the resiliency of the systems in being able to effectively initiate methods of recovery/ mitigation from numerous cyber-attacks, thus these were deemed to be the most applicable and the most suitable.

The development of the given methodology was based on a number of criteria in order to shape it efficiently:

- Efficiency of the results for analysis.
- Relatively straightforward to utilise and understand.
- The ability of the results for analysis to be reproduced.
- Wide range of stakeholders.
- Establish efficient formation of rules to be used in the cyber resiliency metrics of the ICS systems.
- The ability of being able to link both security as well as analysis of cyber-attacks during the formation of the rules for cyber resiliency.

3.3.1 The rules formation

The given project will be developed off the cyber resiliency metrics that have been analysed from applying them onto ICS. As a result, in the given thesis, a study that was well-researched was undertaken as a means of understanding as well as analysing the given problem and ultimately answering the relevant questions for research that were identified in the earlier sections of this thesis. A research methodology that consisted of **identifying, analysing** and **evaluating the results and reviewing them** was produced.

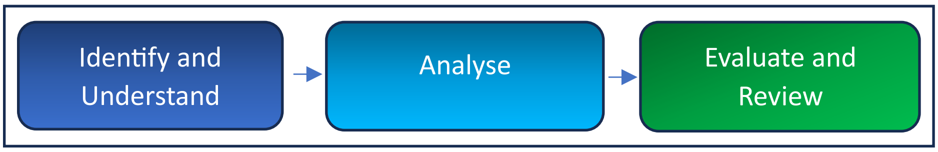


Figure 8 Methodology Steps

3.3.1.1 Identify and Understand: From the start of the methodology, it will be important to be able to identify as well as understand the shape of the whole project at hand, and this was accomplished through the use of being able to understand the various terminology used throughout the course of the project such as “industrial control system”, “smart grid”, “chemical plant”, “nuclear power plant”, the overall layout and structure of smart grids and chemical plants and industrial control systems as well as their given vulnerabilities. From this method, various information and data was obtained and different areas of the project were acknowledged through utilising numerous sources including ScienceDirect, IEEE Xplore and ACM Digital Library. These sources were reliable and provided highly useful and sufficient information for the given thesis and enabled substantial information related to both cyber resiliency metrics in industrial control systems as well as the various attacks on industrial control systems to be gathered.

3.3.1.2 Analyse: With the second stage of the methodology, being “analyse”, the information acquired from extensive research went through an analysis whereby two use cases were produced from creating a scenario based on the attacks such as Denial of Service and ransomware. This revolved around simulating an attack on industrial control systems, particularly chemical plants and the steps that chemical plants take in order to recover from the given attack/ mitigate the damage caused by the attack as well as how they will adapt from the attack. Furthermore, it also revolved around developing 6 test cases (three for each use case) that were based on the scenarios given in the use cases before finally implementing them into an actual setup. It also included designing and producing various flowcharts, activity diagrams and sequence diagrams to have different overviews as well as both, simplified and more in-depth explanations as to what was going on in each attack scenario. From this, it would be possible to finally produce the rules formation that would be applied to cyber resiliency metrics. Moreover, an open-source tool was then chosen and connected to a simulator of a chemical plant to enable the test cases to be validated.

3.3.1.3 Evaluate and Review: With the final stage of the methodology, the progress and achievements of the given projects went through an evaluation and a review in order to see the level of efficiency that has been accomplished as well as what could be changed and improved. This would be important as it was crucial to address how useful and beneficial the given work has been and what ways it could be improved to make it even better.

3.3.2 Utilising the Tool for Rules Formation

After the standard methodology for the rules formation, the tool will be based off the MoSCoW methodology. The MoSCoW methodology was chosen as it is a useful technique when it comes to managing as well as handling various requirements. The term “MoSCoW” embodies a total of four categories including “must-have”, “should-have”, “could-have” and “won’t-have”. It is very productive and efficient as it allows for the prioritization of various requirements in order to gain a good understanding of the sheer amount of resources as well as effort which the project needs. This can result in an improvement in the management of time, making the probability that the project will be completed by the deadline higher as well as ensuring that the project is easier to manage (Kravchenko et al., 2022). The tool itself will be an open-source tool that can initiate DoS and ransomware attacks and will be used to connect to a simulator in order to simulate the cyber-attacks on a chemical plant.

3.3.3 Conducting simulations of Cyber-attacks with the tool

After producing the rules formation and making use of the tool to demonstrate it, the tool will be put to proper use through a simulation of a cyber-attack as a means of indicating the efficiency of the rules formation and the tool. It will also be utilised to indicate the effectiveness of the tool being able to launch DoS and ransomware attacks on ICS, particularly on a chemical plant and the recovery/ mitigation methods that can be initiated in order to reduce the damage caused by the attacks.

3.4 Summary

This chapter covered important aspects related to the approach for research, the given methodology and the chosen criteria for obtaining relevant papers. It provided a detailed overview of the particular way the methodology would shape the thesis and how it would structure each step of the project. It also discussed the implementation of the MoSCoW methodology in order to ensure that each phase of the project would be completed smoothly and sufficiently.

Chapter 4 Design and Implementation

4.1 Overview

This chapter will cover key details regarding the design and implementation phase. This will include a detailed system model of the given industrial control system (in this instance being a chemical plant) as well as threat models. It will also provide two primary **use cases** that indicate specific scenarios in which the ICS system will be under attack, with the first use case being an attack from Denial of Service whilst the second use case will be an attack from ransomware. Furthermore, it will then display a number of **test cases** that signify how the ICS will be able to recover from the attacks as well as adapt. It will then detail the tool that will be used to simulate the given attacks, as well as discuss how the setup was formed.

4.2 System Model

An ICS model was created in order to understand the particular areas of the ICS that could be attacked with the focus being DoS and ransomware attacks.

4.2.1 Conceptual Chemical Plant Structure

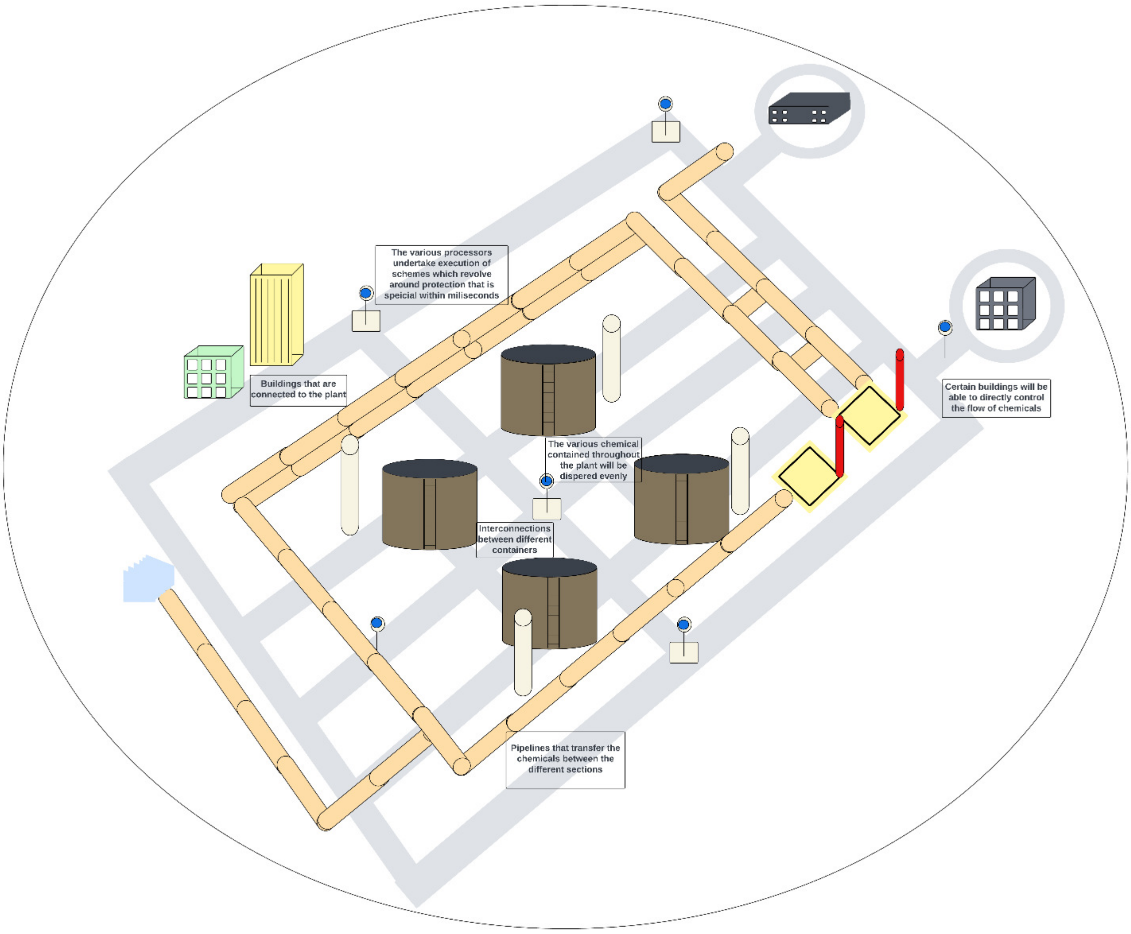

The various processors undertake execution of schemes which revolve around protection that is speicial within miliseconds
Buildings that are connected to the plant
Certain buildings will be able to directly control the flow of chemicals
The various chemical contained throughout the plant will be dispered evenly
Interconnections between different containers
Pipelines that transfer the chemicals between the different sections

Figure 9 Chemical Plant Structure

The given model represents a conceptual chemical plant structure and how it is all connected as well as its features. A successful attack on a chemical plant could lead to catastrophic damages which could include chemical overload or spill and potentially a total meltdown.

4.2.2 Chemical Plant Process Flow

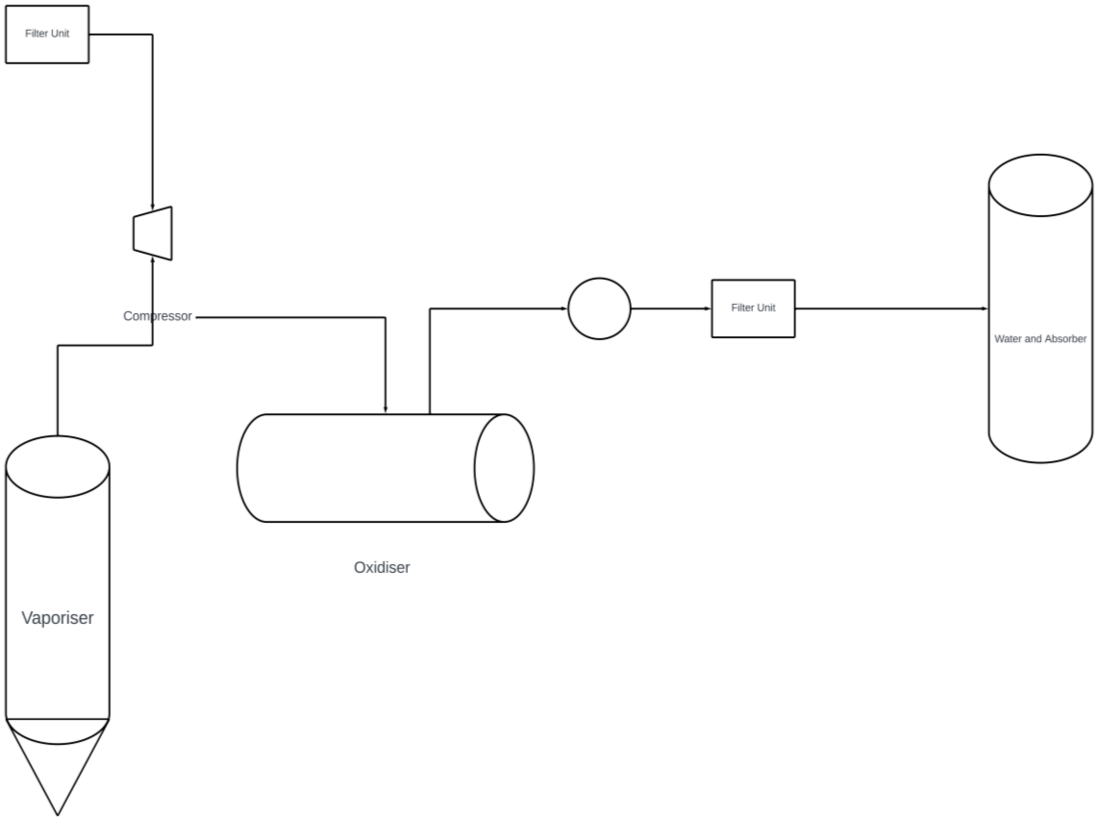


Figure 10 Flow of Chemicals

4.2.3 Key Vulnerabilities within the chemical plant infrastructure

In order to simulate how a chemical plant would come under attack by cyber-attacks such as Denial of Service and ransomware, it is important to understand which components or sectors of chemical plants are most vulnerable and are most likely to be targeted by a cyber-attack (or used by an attacker to launch a cyber-attack). Due to this, additional research was undertaken to identify the most critical components/ sectors of a chemical plant that could come under attack.

4.2.3.1 Vulnerabilities of the Programmable Logic Controller

One of the most crucial components of a chemical plant is the programmable logic controller which contains numerous vulnerabilities and can be frequently targeted by cyber-attacks (or utilised as a means of carrying out cyber-attacks). Some of the vulnerabilities of the programmable logic controller reside within application software that is industrial as well as devices that are connected and protocols for industrial communication.

The industrial application software predominantly contains programming software for Programmable Logic Controller (PLC) as well as software for SCADA. With this, after the software has become compromised, the ability of the PLC to be manipulated directly is terminated. This results in malicious code being uploaded as well as the parameters of the PLCs being modified and data that is industrial being revealed.

Furthermore, when it comes to the vulnerabilities of the protocols for industrial communication, despite the fact that standard protocols for networking operate productively when it comes to communication with PLCs, unfortunately, the protocols security does not come under consideration with their design. As a result, there are significant drawbacks in the encryption, authorisation, authentication and integrity of the protocols. Due to this, malicious users who are malicious are able to obtain privileges, as well as produce protocol packets that are forged without the need for any form of method for identification. (Wang et al., 2023).

4.2.4 PLC Model

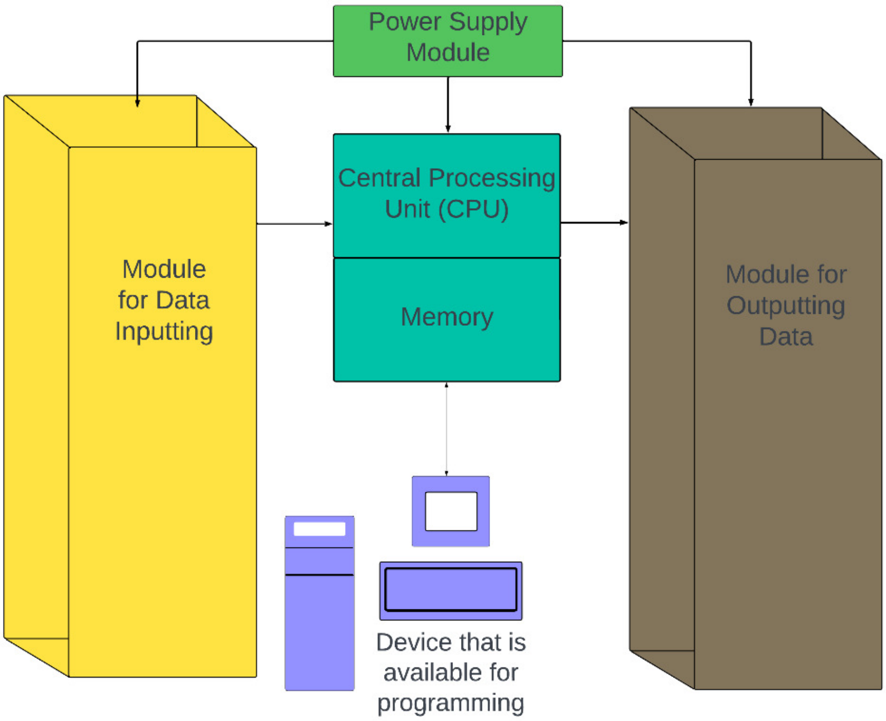

Power Supply Module
Module for Data Inputting
Central Processing Unit (CPU)
Memory
Module for Outputting Data
Device that is available for programming

Figure 11 PLC Structure

The given PLC model demonstrates the overall design of the programmable logic controller including its various features as well as how the various components connect together and how the PLC operates as a whole. The PLC will be very important as it can be utilised to launch attacks on other devices and systems, such as chemical plants whilst it can also be a target for cyber-attacks.

4.2.4.1 PLC Cyber-Attack

With the PLC of the chemical plant, one of the most prolific attacks is Denial of Service attacks. This is due to the fact that PLCs often respond to all requests that come from a MAC address or IP and do not have any filters. As a result, DoS is a very serious threat to chemical plants, particularly the PLC (Wang et al., 2023).

4.3 Threat Model

4.3.1 Denial of Service Attack on Chemical Plant

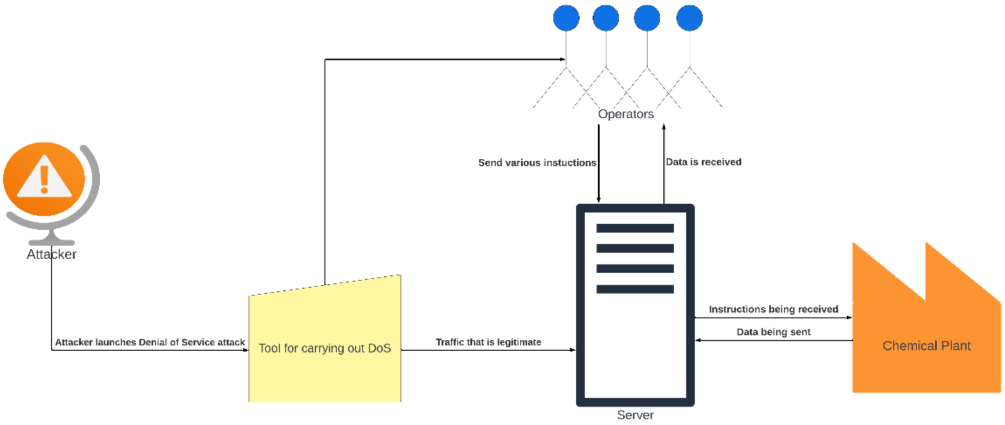

Operators
Send various instuctions
Data is received
Attacker
Attacker launches Denial of Service attack
Tool for carrying out DoS
Traffic that is legitimate
Instructions being received
Data being sent
Chemical Plant
Server

Figure 12 DoS attack on Chemical Plant

This represents a Denial of Service attack on the chemical plant and indicates the routes in which the DoS will go to reach the chemical plant and the aspects of the chemical plant that will be targeted and come under attack. As can be seen, the attacker will utilise a tool for carrying out a DoS attack and send data traffic which appears to be legitimate to the server.

4.3.2 Ransomware Attack on Chemical Plant

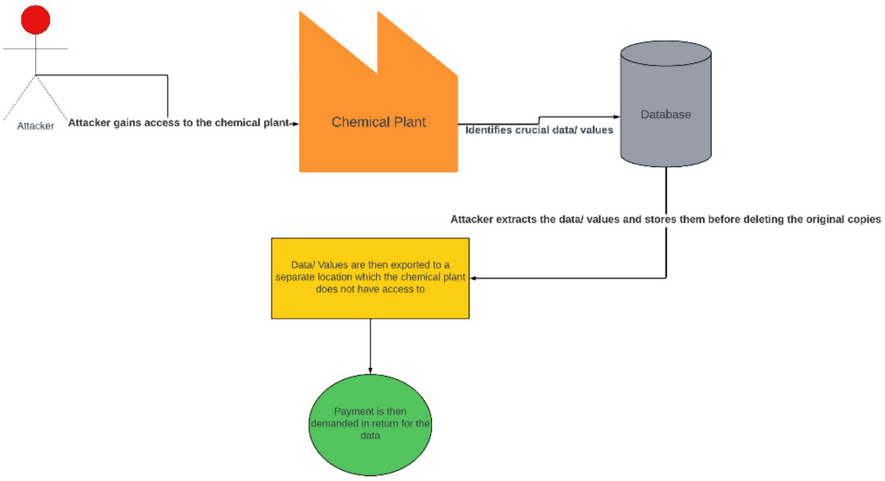

Attacker
Attacker gains access to the chemical plant
Chemical Plant
Identifies crucial data/ values
Database
Attacker extracts the data/ values and stores them before deleting the original copies
Data/ Values are then exported to a separate location which the chemical plant does not have access to
Payment is then demanded in return for the data

Figure 13 Ransomware attack on Chemical Plant

This diagram demonstrates a ransomware attack on a chemical plant and details the various phases/ steps of the attack. As displayed by the diagram, the attacker will attempt to gain access to the chemical plant before stealing crucial data/ values from it, whilst erasing the original data and demanding a payment in order to return the data.

4.3.3 Use Case 1

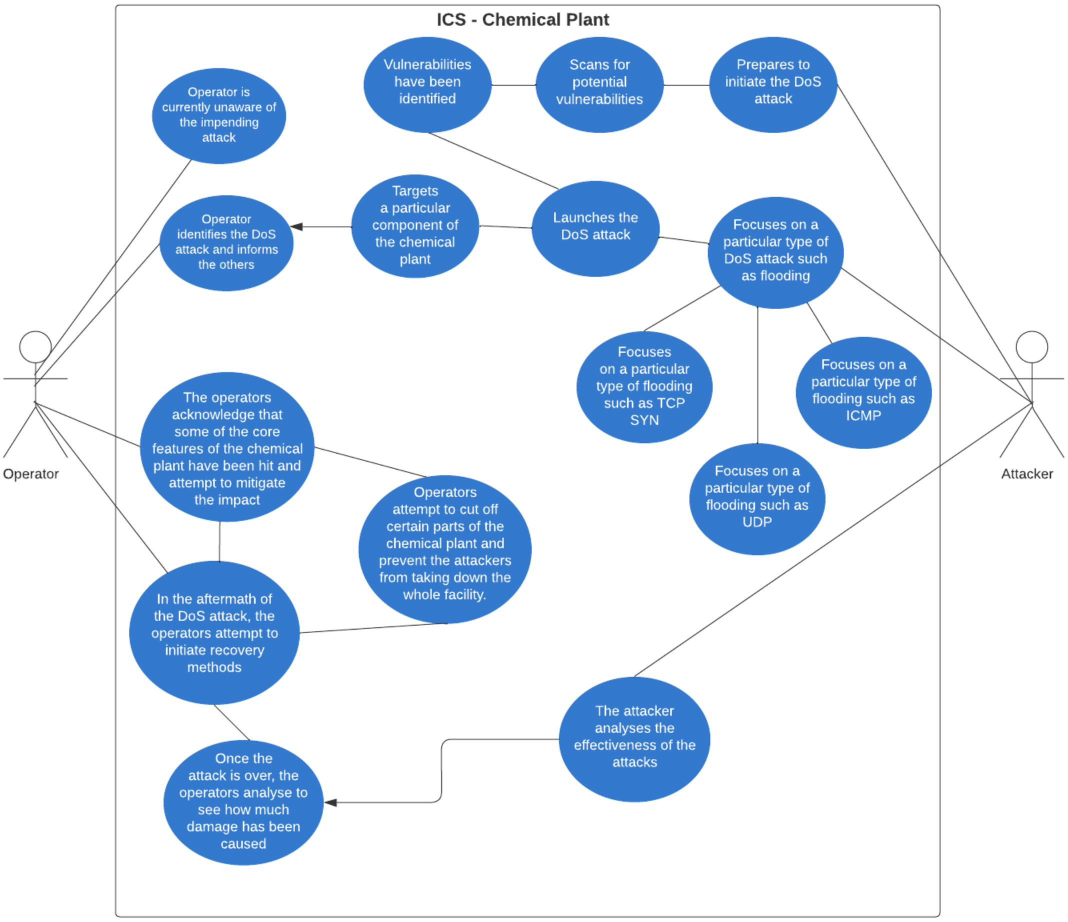

ICS - Chemical Plant
Operator is currently unaware of the impending attack
Vulnerabilities have been identified
Scans for potential vulnerabilities
Prepares to initiate the DoS attack
Operator identifies the DoS attack and informs the others
Targets a particular component of the chemical plant
Launches the DoS attack
Focuses on a particular type of DoS attack such as flooding
Focuses on a particular type of flooding such as TCP SYN
Focuses on a particular type of flooding such as ICMP
Focuses on a particular type of flooding such as UDP
Operator
Attacker
The operators acknowledge that some of the core features of the chemical plant have been hit and attempt to mitigate the impact
Operators attempt to cut off certain parts of the chemical plant and prevent the attackers from taking down the whole facility.
In the aftermath of the DoS attack, the operators attempt to initiate recovery methods
The attacker analyses the effectiveness of the attacks
Once the attack is over, the operators analyse to see how much damage has been caused

Figure 14 Use Case 1

The first use case diagram demonstrates the scenario of an attacker launching a Denial of Service attack on a chemical plant and the steps to which the attack is launched. It also provides an overview of the reaction of the chemical plant (operators) to the given attack. The first attack carried out by the attacker would be a flooding attack whereby the attacker attempts to ensure the network is overwhelmed (Swami et al., 2021), which leads to a delay or an interruption in the device's communication. This can lead to serious disruption in the network.

The attacker or attackers will then initiate a jamming attack in which the physical layer signals will be jammed in order to delay or prevent the devices within a chemical plant from communicating effectively (Cheng et al., 2020). The given attacker(s) would be able to use numerous techniques including attacks that are advanced which seek to undertake vulnerability exploitation on protocols within the application layer.

Followed by a de-synchronisation attack. This could be carried out through spoofing. The de-synchronisation attack would occur once the attacker starts changing the time for sampling through the use of producing a GPS signal that is forged. This will lead to the device that is utilised for measuring to carry out signal sampling at the wrong time.

4.3.4 Use Case 2

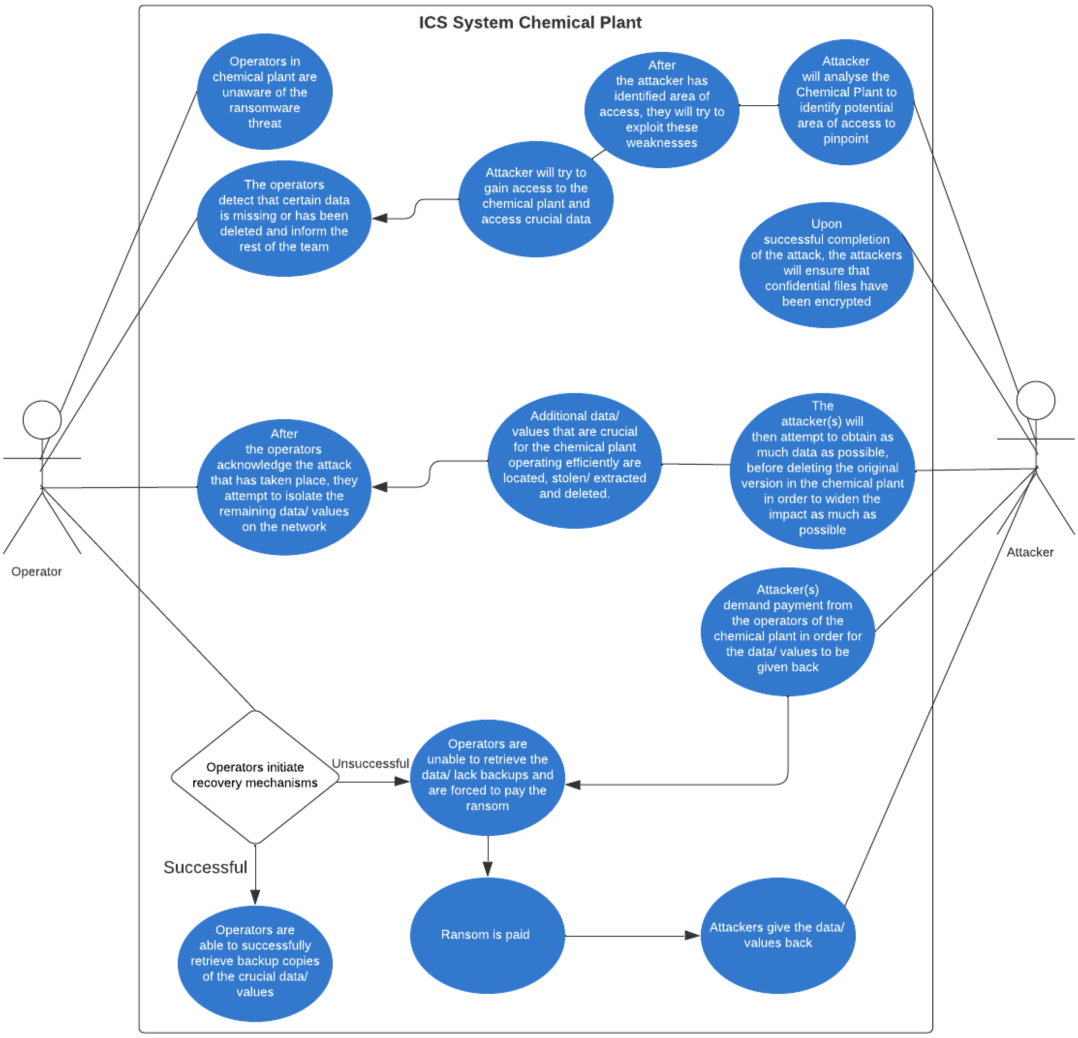

ICS System Chemical Plant
Operators in chemical plant are unaware of the ransomware threat
The operators detect that certain data is missing or has been deleted and inform the rest of the team
Attacker will try to gain access to the chemical plant and access crucial data
After the attacker has identified area of access, they will try to exploit these weaknesses
Attacker will analyse the Chemical Plant to identify potential area of access to pinpoint
Upon successful completion of the attack, the attackers will ensure that confidential files have been encrypted
After the operators acknowledge the attack that has taken place, they attempt to isolate the remaining data/ values on the network
Additional data/ values that are crucial for the chemical plant operating efficiently are located, stolen/ extracted and deleted.
The attacker(s) will then attempt to obtain as much data as possible, before deleting the original version in the chemical plant in order to widen the impact as much as possible
Operator
Attacker
Attacker(s) demand payment from the operators of the chemical plant in order for the data/ values to be given back
Operators initiate recovery mechanisms
Unsuccessful
Operators are unable to retrieve the data/ lack backups and are forced to pay the ransom
Successful
Operators are able to successfully retrieve backup copies of the crucial data/ values
Ransom is paid
Attackers give the data/ values back

Figure 15 Use Case 2

The second use case diagram indicates how an attacker launches a ransomware attack on a chemical plant and how the attack impacts the chemical plant. It demonstrates the process in which an attacker is able to initiate the attack on the given chemical plant. It also signifies how the chemical plant (the operators of the chemical plant) would react to the given attack and how the attack could affect the chemical plant as well as what damages it may inflict.

It starts by indicating that the attacker will attempt to obtain crucial data once they have located a weakness in the chemical plant, and will try to exploit that weakness. As soon as the operators detect the attack, they will inform others within the chemical plant and try to isolate the remaining files within the network. At the same time, the attacker will try to encrypt as many files as possible and attempt to cause the maximum amount of damage before demanding a payment in return for the files to be given back and decrypted. If the operators pay the ransom, they may get their files back, otherwise, the files will be lost. Alternatively, if the operators have created backups of the files, they may be able to restore them without paying the ransom.

4.3.5 Pseudocode

The pseudocode will provide an overview of the steps of the given scenarios (the given cyber-attacks of DoS and ransomware) including launching the attacks on the chemical plant and the methods that the chemical plant and its operators will take to mitigate the attacks as well as try to recover from them.

```
Scenario 1 = DoS attack

INPUT = Attackers scan and analyse the chemical plant to look for weaknesses and vulnerabilities.

OUPUT = Operators currently unaware of the situation that is unfolding

Vulnerability is located = attackers launch first DoS attack (flooding) and target critical components in chemical plant

Attack Detected! Operators inform rest of their team about the situation

Operators attempt to initiate recovery methods to reduce/ mitigate the effects of attack

If damage inflicted = high

then

Operators isolated certain sections of the chemical plant or restricted certain IP addresses

Attacker then analyses chemical plant to see extent of damage caused by the attack.

If damage = low

Attacker re-launches attack to inflict greater damage

In the event of a DoS attack = the attacker after launching a flooding attack, launches a jamming attack, followed by a de-synchronisation attack to cause as much disruption to the chemical plant as possible.

Scenario 2 = Ransomware attack

Attacker scans chemical plant and undertakes reconnaissance to detect weaknesses and vulnerabilities

If Attacker locates weakness = true then

Ransomware attack is launched and attacker gains access to the data in the chemical plant

Else if Attacker locates weakness = false then

Attacker continue scanning for weaknesses

Operators detect the ransomware attack that has been deployed and initiate an alert throughout the whole chemical plant
```

The attack encrypts a large amount of important files and results in significant disruption of chemical plant operations

Attackers demand a payment in return for decrypting the files

If ransom is paid then

Attacker decrypts the files and returns them

Else

The files remain encrypted and are lost

Else if

The operators refuse to pay the ransom but are able to recover offline backup files

4.3.5 DoS Flowchart

Figure 16 – DoS Attack

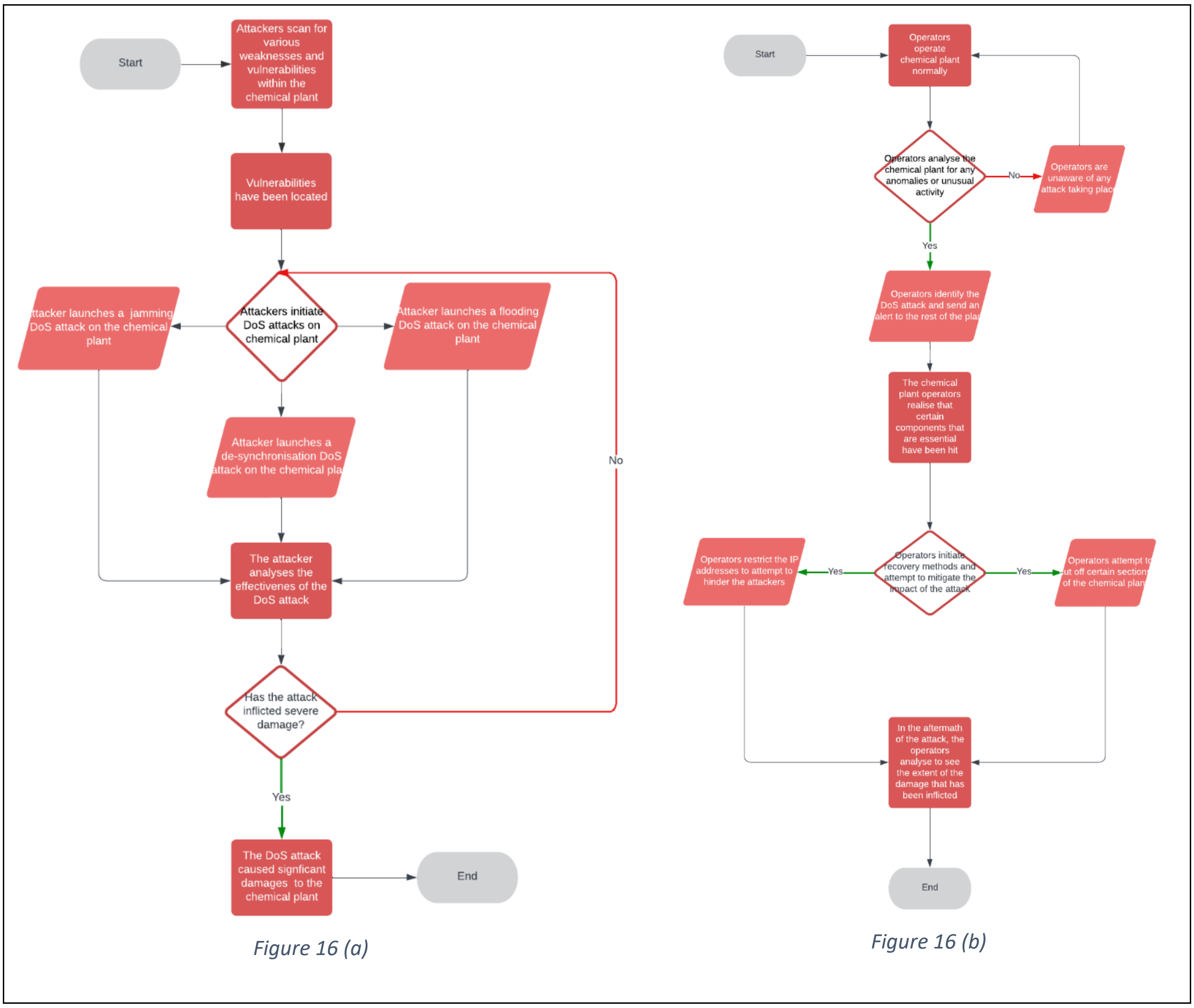

Start
Attackers scan for various weaknesses and vulnerabilities within the chemical plant
Vulnerabilities have been located
Attackers initiate DoS attacks on chemical plant
ttacker launches a jamming DoS attack on the chemical plant
Attacker launches a flooding DoS attack on the chemical plant
Attacker launches a de-synchronisation DoS attack on the chemical pla
The attacker analyses the effectivenes of the DoS attack
Has the attack inflicted severe damage?
No
Yes
The DoS attack caused signficant damages to the chemical plant
End
Start
Operators operate chemical plant normally
Operators analyse the chemical plant for any anomalies or unusual activity
No
Operators are unaware of any attack taking plac
Yes
Operators identify the DoS attack and send an alert to the rest of the pla
The chemical plant operators realise that certain components that are essential have been hit
Operators initiate recovery methods and attempt to mitigate the impact of the attack
Yes
Operators restrict the IP addresses to attempt to hinder the attackers
Yes
Operators attempt to ut off certain section of the chemical plan
In the aftermath of the attack, the operators analyse to see the extent of the damage that has been inflicted
End

Figure 16 (a)

Figure 16 (b)

The first DoS flowchart represents the process in which the attacker initiates a DoS attack and the second one signifies the approach that the operators will take to mitigate the attack and recover from it. Unlike the use cases which indicate what is going on from both sides at the same time, the flowcharts go into more specific detail regarding the steps that each side goes through, with the attacker attempting to cause damage through launching a DoS attack whereas the operator will be attempting to minimise the damage caused by the attack.

With the first Flowchart, the attacker begins their routine by carrying out scanning on the chemical plant to detect and identify various vulnerabilities and areas that contain weak points within the chemical plant. Once the vulnerabilities have been identified, the attacker will then initiate a DoS attack (with them being able to launch a flooding, jamming or de-synchronisation attack) on the chemical plant with the intention of causing disruptions to the chemical plant services. The attacker will then conduct an analysis to see how severe the damage was and if it is severe, then the attack will terminate. Otherwise, they may make another attempt.

Likewise, with the second DoS Flowchart, the operator(s) will undertake ordinary operations within the chemical plant as usual before analysing the chemical plant to check for any abnormalities in the network. If the operator(s) do not detect anything unusual, they will continue to work as normal, however, once they detect/ acknowledge that a DoS attack has taken place, they will alert the rest of the plant before either attempting to restrict the number of IP addresses or sectioning off certain areas of the network. After the attack has taken place, the operator(s) will analyse the chemical plant to see how much damage has been caused.

4.3.6 Ransomware Flowchart

Figure 17 Ransomware Attack

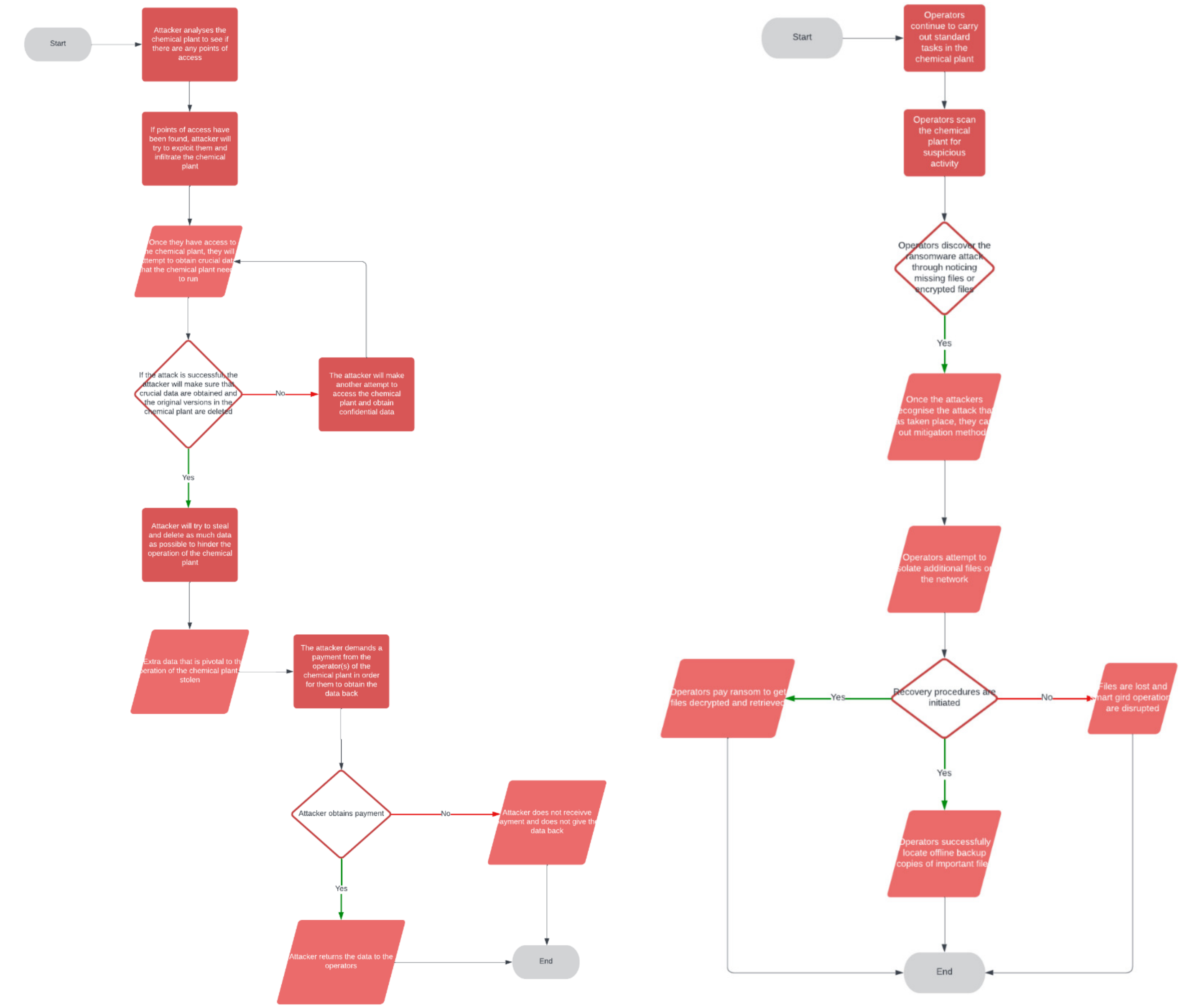

Start
Attacker analyses the chemical plant to see if there are any points of access
If points of access have been found, attacker will try to exploit them and infiltrate the chemical plant
Once they have access to he chemical plant, they will ttempt to obtain crucial dat hat the chemical plant need to run
If the attack is successful, the attacker will make sure that crucial data are obtained and the original versions in the chemical plant are deleted
No
The attacker will make another attempt to access the chemical plant and obtain confidential data
Yes
Attacker will try to steal and delete as much data as possible to hinder the operation of the chemical plant
Extra data that is pivotal to th eration of the chemical plant stolen
The attacker demands a payment from the operator(s) of the chemical plant in order for them to obtain the data back
Attacker obtains payment
No
Attacker does not receivve ayment and does not give th data back
Yes
Attacker returns the data to the operators
End
Start
Operators continue to carry out standard tasks in the chemical plant
Operators scan the chemical plant for suspicious activity
Operators discover the ransomware attack through noticing missing files or encrypted files
Yes
Once the attackers ecognise the attack tha as taken place, they ca out mitigation method
Operators attempt to solate additional files o the network
Recovery procedures are initiated
Yes
Operators pay ransom to get files decrypted and retrieved
No
Files are lost and mart gird operation are disrupted
Yes
Operators successfully locate offline backup copies of important file
End

Figure 17 (a)

Figure 17 (b)

Similarly to the DoS flowcharts, two flowcharts were constructed to indicate the scenario of a ransomware attack on the chemical plant, and like the previous DoS flowcharts, the first implies the procedure that the attacker will undertake in order to carry out a ransomware attack and the second one indicates the steps the operator(s) will take to recover from the attack and mitigate its impact.

With the first Flowchart, the attacker will attempt to initiate scans on the chemical plant to look for weaknesses and vulnerabilities. Upon detection of a weakness, the attacker will carry out a ransomware attack onto the chemical plant. If the attack has been successful, then the attacker will try to obtain as many files as possible and provide them with a layer of encryption. However, if the attack was not successful, then the attacker will attempt to re-encrypt the files etc.

At the same time, with the second ransomware Flowchart, the operator(s) will initiate various scans within the chemical plant, and upon detecting the ransomware attack, they will carry out methods of mitigation and recovery such as by isolating the remaining files on the network.

4.3.7 DoS UML Activity Diagram

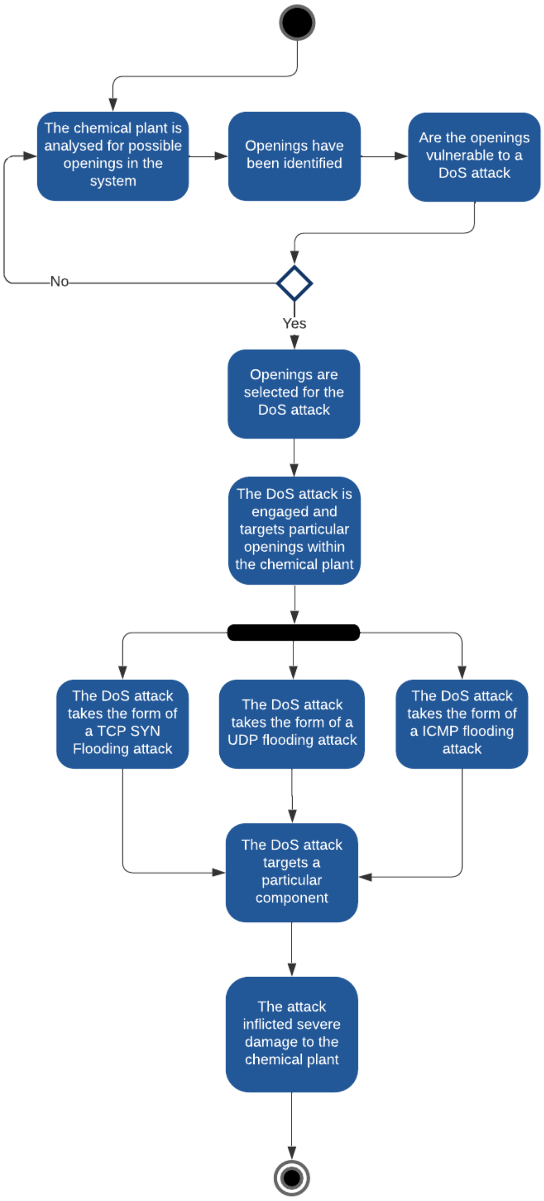

The chemical plant is analysed for possible openings in the system
Openings have been identified
Are the openings vulnerable to a DoS attack
No
Yes
Openings are selected for the DoS attack
The DoS attack is engaged and targets particular openings within the chemical plant
The DoS attack takes the form of a TCP SYN Flooding attack
The DoS attack takes the form of a UDP flooding attack
The DoS attack takes the form of a ICMP flooding attack
The DoS attack targets a particular component
The attack inflicted severe damage to the chemical plant

Figure 18 UML DoS flooding attack

With the first UML Activity Diagram, the chemical plant undergoes analysis for potential vulnerabilities/ openings. If the openings/ vulnerabilities that have been identified are vulnerable to an attack then the openings will be breached before a DoS attack is initiated and targets a particular part of the chemical plant. The DoS attack either takes the form of a TCP SYN attack, UDP or ICMP attack. The DoS attack will target a specific component in the chemical plant. As a result of the attack, significant damage has been inflicted on the chemical plant.

4.3.8 Ransomware UML Activity Diagram

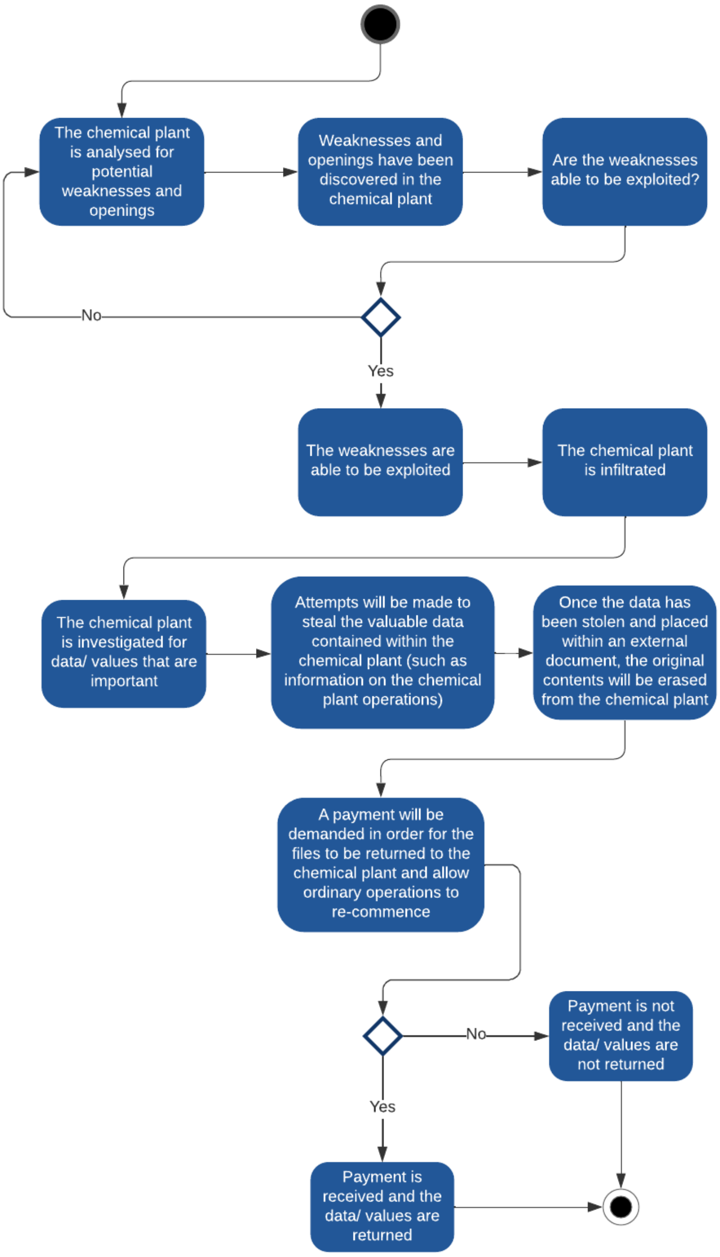

The chemical plant is analysed for potential weaknesses and openings
Weaknesses and openings have been discovered in the chemical plant
Are the weaknesses able to be exploited?
No
Yes
The weaknesses are able to be exploited
The chemical plant is infiltrated
The chemical plant is investigated for data/ values that are important
Attempts will be made to steal the valuable data contained within the chemical plant (such as information on the chemical plant operations)
Once the data has been stolen and placed within an external document, the original contents will be erased from the chemical plant
A payment will be demanded in order for the files to be returned to the chemical plant and allow ordinary operations to re-commence
No
Payment is not received and the data/ values are not returned
Yes
Payment is received and the data/ values are returned

Figure 19 UML Ransomware attack

This UML Activity diagram represents a ransomware attack, at the start the chemical plant will be analysed extensively in order to identify various weaknesses and openings. If the weaknesses or openings are vulnerable to exploitation then the chemical plant will be infiltrated. Once infiltrated, the chemical plant will then be investigated for various data or values that are considered important and attempts will be made to acquire the data that is stored within the chemical plant before extracting the given data and finally deleting the original values from the chemical plant. Finally, payment will be demanded in order for the data or values to be returned and enable standard operations to be undertaken. If payment is delivered, then the attacker will return the values, otherwise, the values will be permanently lost.

4.3.9 DoS Sequence Diagram

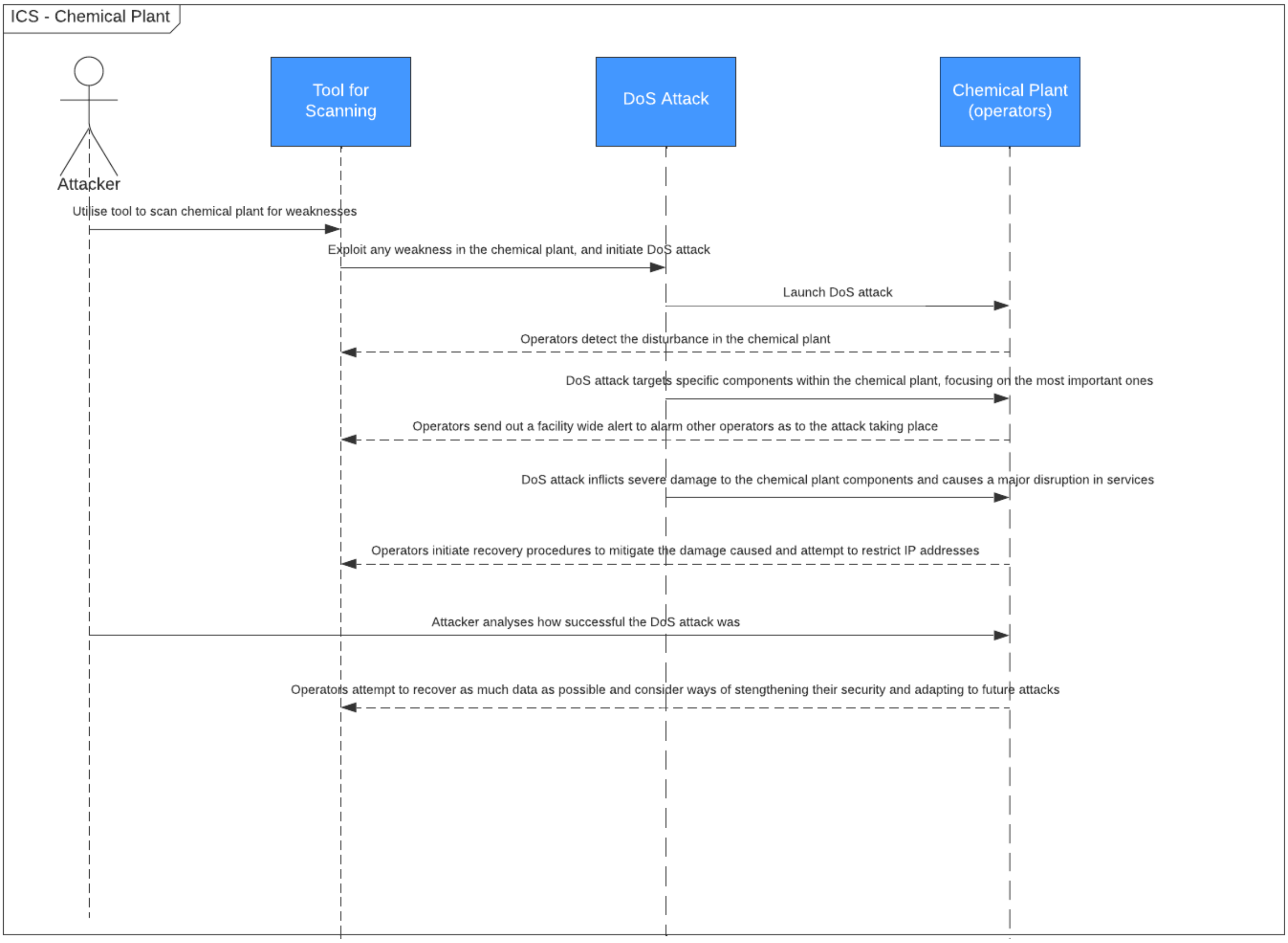

ICS - Chemical Plant
Attacker
Tool for Scanning
DoS Attack
Chemical Plant (operators)
Utilise tool to scan chemical plant for weaknesses
Exploit any weakness in the chemical plant, and initiate DoS attack
Launch DoS attack
Operators detect the disturbance in the chemical plant
DoS attack targets specific components within the chemical plant, focusing on the most important ones
Operators send out a facility wide alert to alarm other operators as to the attack taking place
DoS attack inflicts severe damage to the chemical plant components and causes a major disruption in services
Operators initiate recovery procedures to mitigate the damage caused and attempt to restrict IP addresses
Attacker analyses how successful the DoS attack was
Operators attempt to recover as much data as possible and consider ways of stengthening their security and adapting to future attacks

Figure 20 Sequence DoS attack

After completing the use cases, flowcharts and activity diagrams, the final representations of the attack scenarios were displayed through sequence diagrams, whereby the exact sequence and order of events that take place between the attack and chemical plant (operator(s)) is signified. Unlike the flowcharts and activity diagrams, the sequence diagrams showcase the situation from both sides within the same diagram, being the attacker launches an attack and the operator(s) respond to it.

4.3.10 Ransomware Sequence Diagram

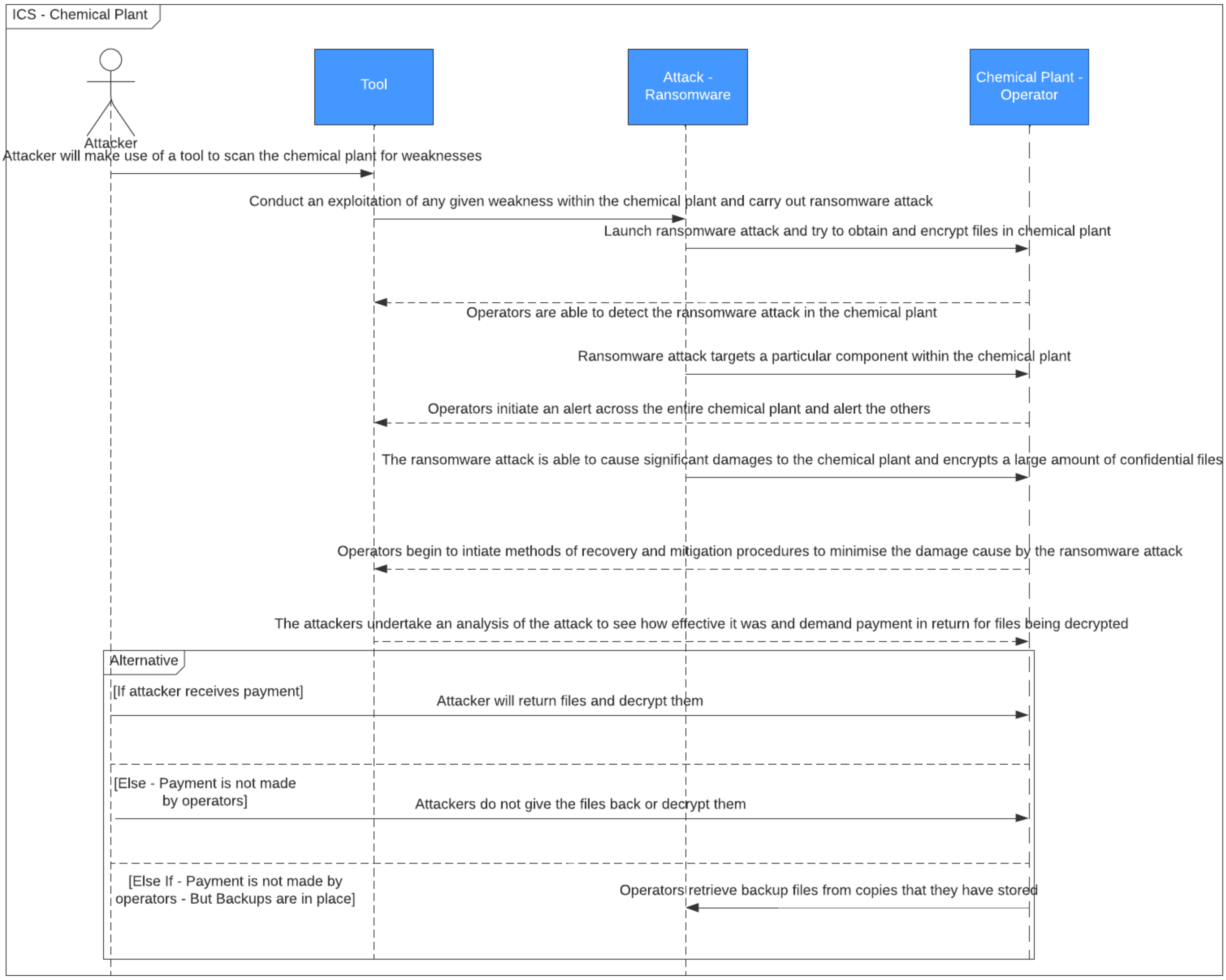

ICS - Chemical Plant
Attacker
Tool
Attack - Ransomware
Chemical Plant - Operator
Attacker will make use of a tool to scan the chemical plant for weaknesses
Conduct an exploitation of any given weakness within the chemical plant and carry out ransomware attack
Launch ransomware attack and try to obtain and encrypt files in chemical plant
Operators are able to detect the ransomware attack in the chemical plant
Ransomware attack targets a particular component within the chemical plant
Operators initiate an alert across the entire chemical plant and alert the others
The ransomware attack is able to cause significant damages to the chemical plant and encrypts a large amount of confidential files
Operators begin to intiate methods of recovery and mitigation procedures to minimise the damage cause by the ransomware attack
The attackers undertake an analysis of the attack to see how effective it was and demand payment in return for files being decrypted
Alternative
[If attacker receives payment]
Attacker will return files and decrypt them
[Else - Payment is not made by operators]
Attackers do not give the files back or decrypt them
[Else If - Payment is not made by operators - But Backups are in place]
Operators retrieve backup files from copies that they have stored

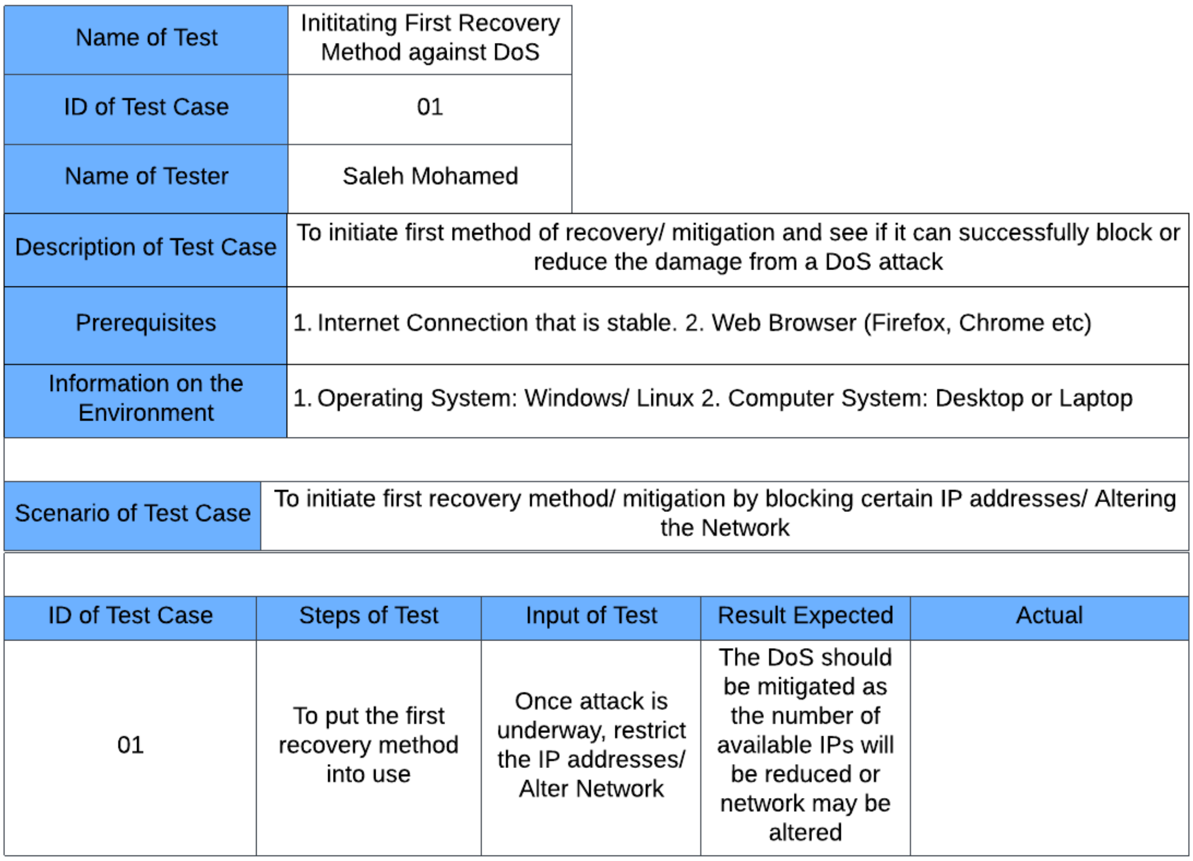
Figure 21 Sequence Ransomware attack

Likewise, with this sequence diagram, an additional box being “Alternative” was produced and placed within the diagram to indicate the various options that the attacker and operator(s) have. This came about in the form of an If statement whereby if the ransom is paid, then the files will be decrypted and returned. Else the files will be lost. Else if the operators have backups in place, they can restore the files without having to pay the ransom.

4.4 Establishing the Rules Formation (Mitigation Methods)

The rules formation will come in the form of a step-by-step procedure in which the chemical plant initiates recovery/ mitigation methods and attempts to adapt to the given attacks. This can be related to the test cases and can detail ways in which the damage caused by cyber-attacks is kept to a minimum.

4.4.1 Test Case 1



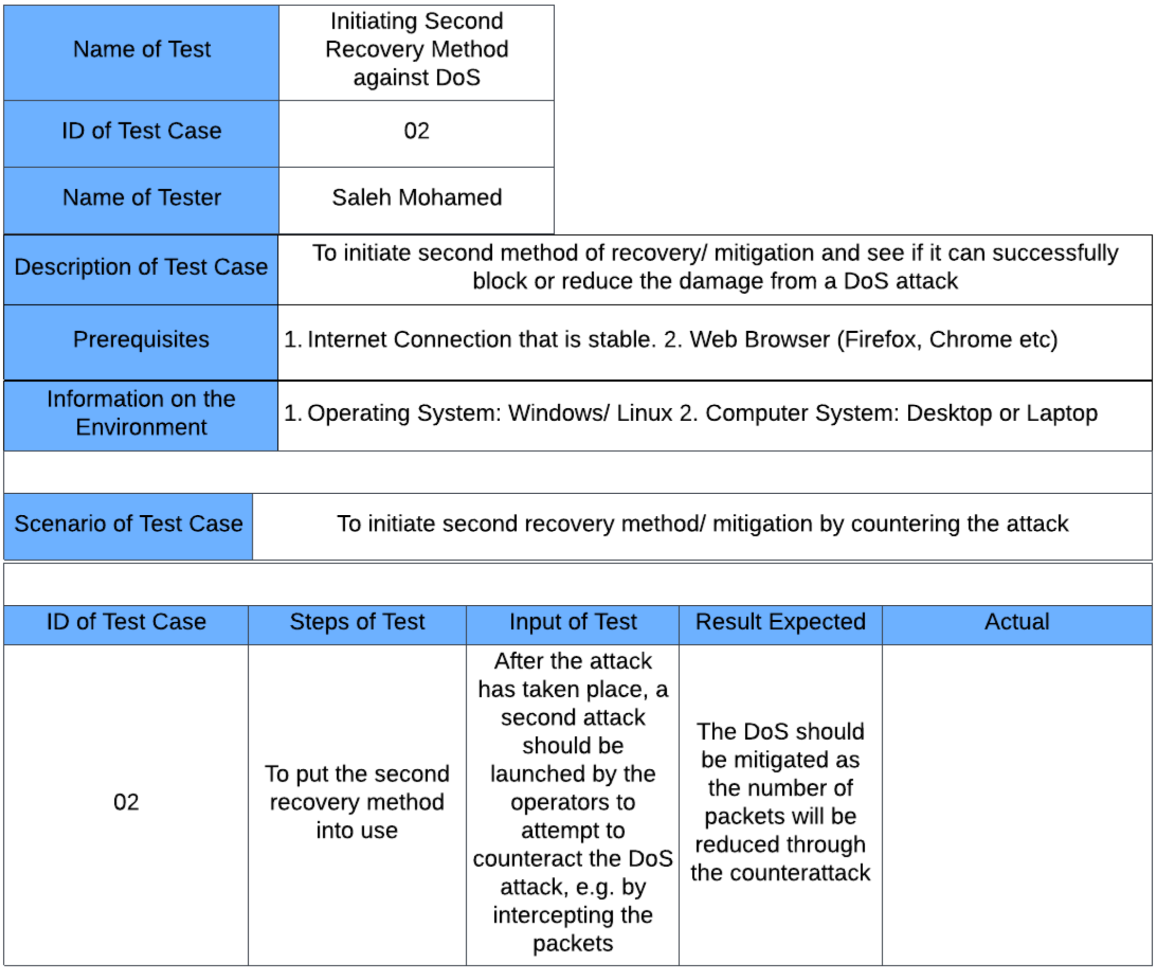
Name of Test	Inititating First Recovery Method against DoS
ID of Test Case	01
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate first method of recovery/ mitigation and see if it can successfully block or reduce the damage from a DoS attack
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate first recovery method/ mitigation by blocking certain IP addresses/ Altering the Network

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
01	To put the first recovery method into use	Once attack is underway, restrict the IP addresses/ Alter Network	The DoS should be mitigated as the number of available IPs will be reduced or network may be altered	

Figure 22 First Mitigation

Upon completing the use cases which showcase a Denial of Service and ransomware attack on a chemical plant, it was important to then begin working on a number of test cases to demonstrate how the chemical plant could implement methods of recovering from the attack. The first test case revolves around initiating IP address blocking whereby the number of IP addresses on the network is restricted to limit the amount of targets that the DoS can reach. Through this, the chemical plant could limit the amount of IP addresses to only ones that are legitimate. For instance, 192.154.0.0/16 would only enable IP addresses from the range 192.154.0.0 and 192.154.255.255. This rule will deny all IP addresses that exist outside the specific range.

4.4.2 Test Case 2



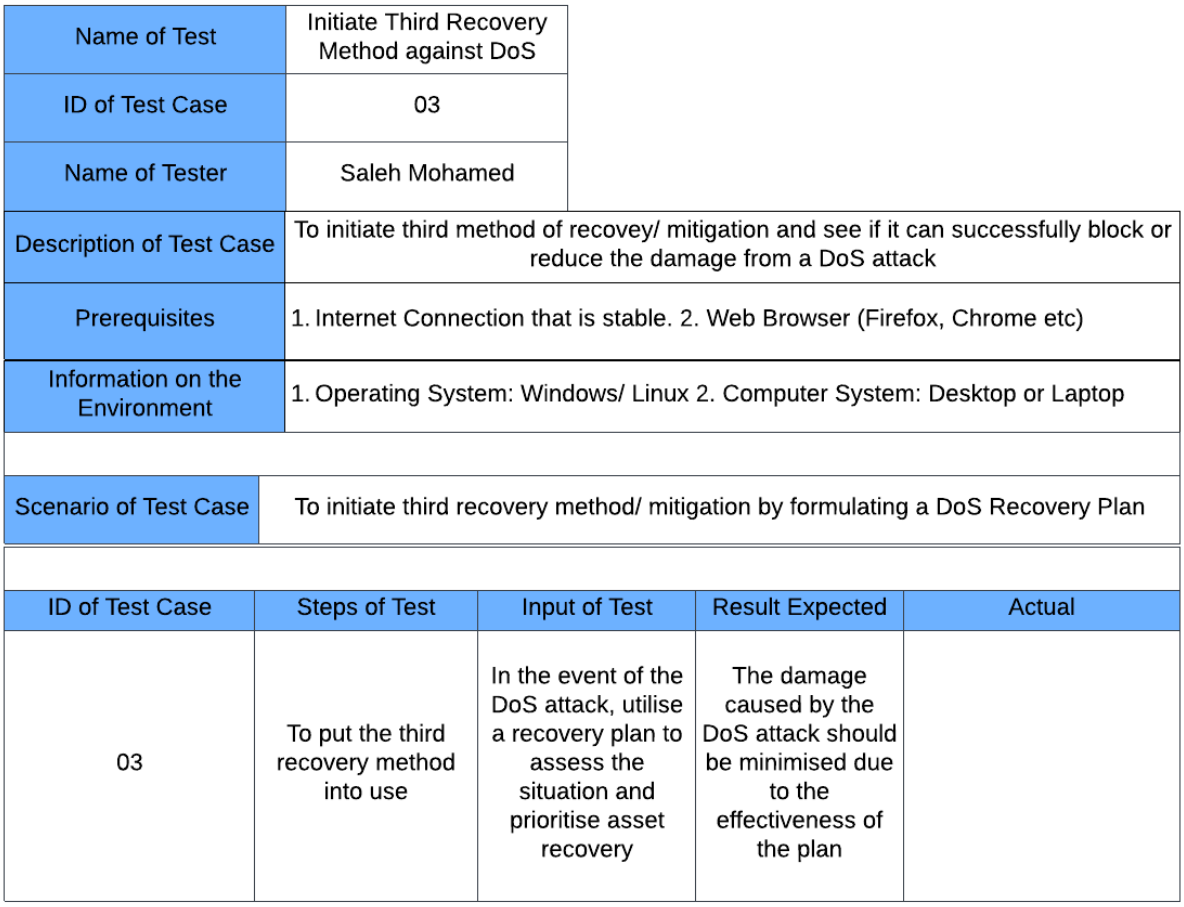
Name of Test	Initiating Second Recovery Method against DoS
ID of Test Case	02
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate second method of recovery/ mitigation and see if it can successfully block or reduce the damage from a DoS attack
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate second recovery method/ mitigation by countering the attack

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
02	To put the second recovery method into use	After the attack has taken place, a second attack should be launched by the operators to attempt to counteract the DoS attack, e.g. by intercepting the packets	The DoS should be mitigated as the number of packets will be reduced through the counterattack	

Figure 23 Second Mitigation

The second test case indicates an alternative procedure in which the chemical plant can attempt to counter the given cyber-attack. This revolves around waiting for a potential attack to occur (in this case being a DoS attack) and then attempting to initiate a counter-attack to reduce the impact of the first attack. This could include launching an attack that intercepts the packets sent from the DoS attack.

4.4.3 Test Case 3



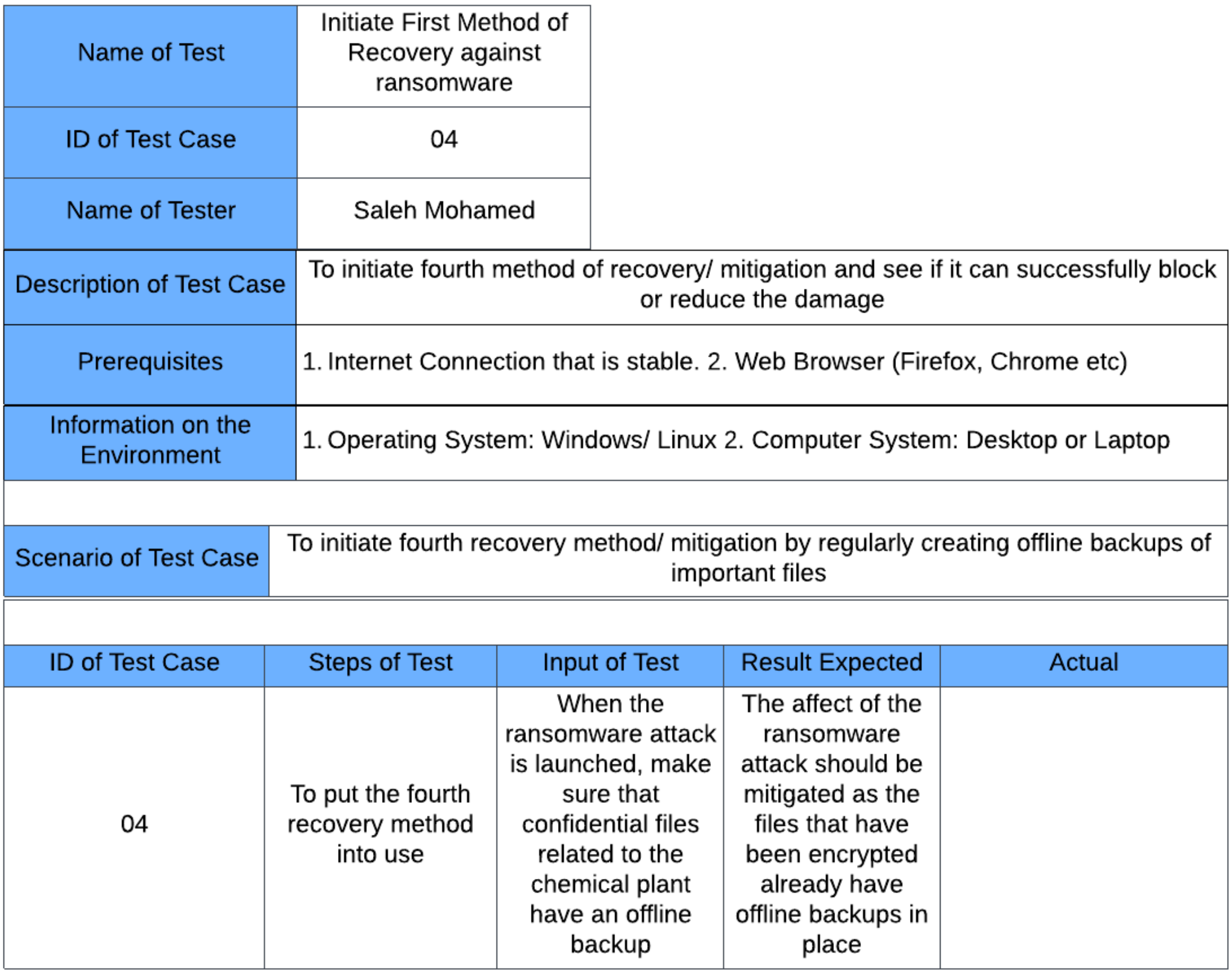
Name of Test	Initiate Third Recovery Method against DoS
ID of Test Case	03
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate third method of recovey/ mitigation and see if it can successfully block or reduce the damage from a DoS attack
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate third recovery method/ mitigation by formulating a DoS Recovery Plan

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
03	To put the third recovery method into use	In the event of the DoS attack, utilise a recovery plan to assess the situation and prioritise asset recovery	The damage caused by the DoS attack should be minimised due to the effectiveness of the plan	

Figure 24 Third Mitigation

The third test case represents the last resort for the chemical plant in implementing methods of recovery/mitigation in relation to the given DoS attack. With the third test case (which is the last one for the DoS attack scenario), the recovery method revolves around formulating a DoS attack recovery plan that takes into account the effect of the given attack, how much damage it has caused and what assets need to be prioritised. This will be important as it would enable a company to put in place an effective plan that could place the most pivotal assets and resources first and reduce the damage caused by the DoS attack.

4.4.4 Test Case 4



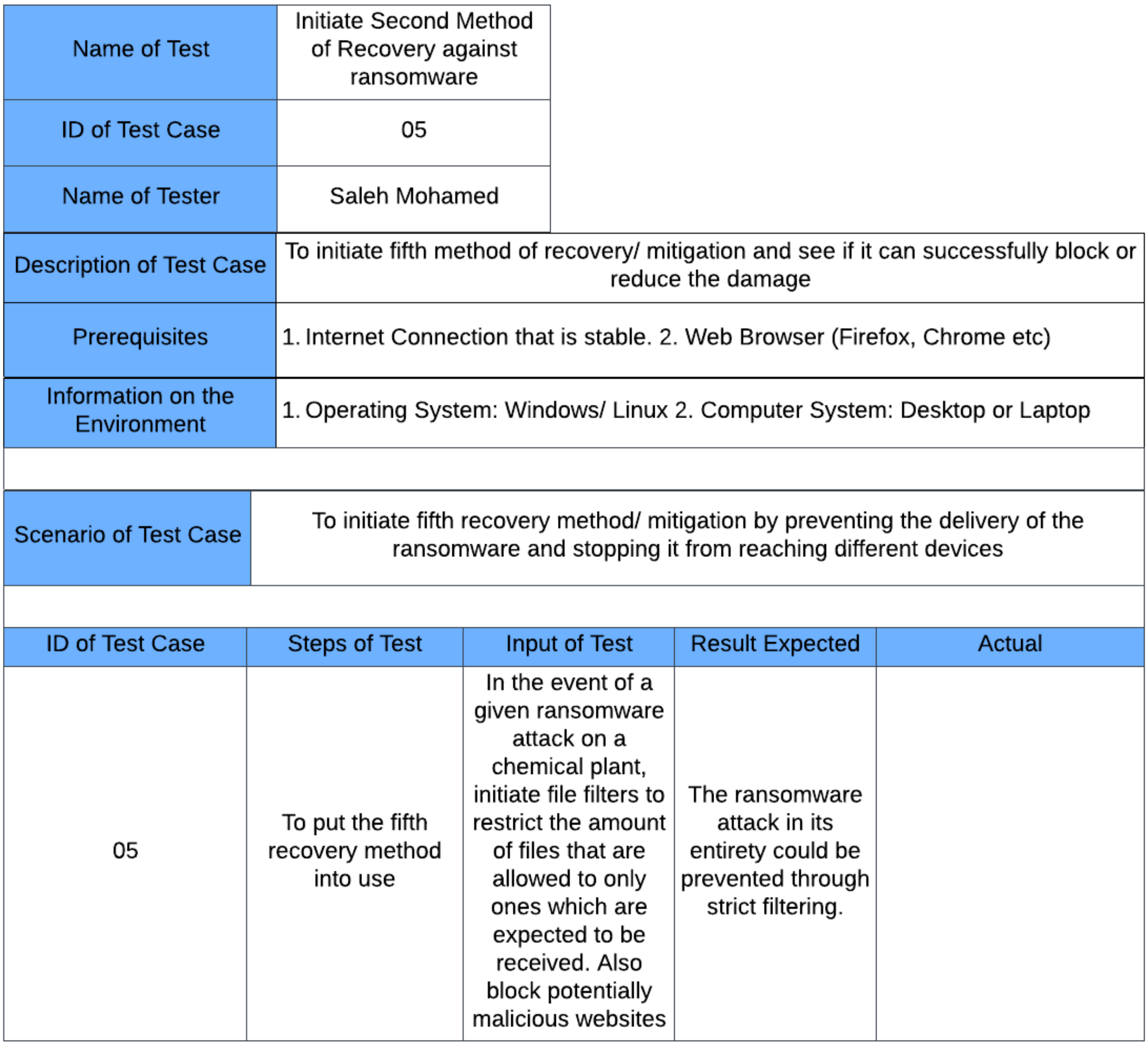
Name of Test	Initiate First Method of Recovery against ransomware
ID of Test Case	04
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate fourth method of recovery/ mitigation and see if it can successfully block or reduce the damage
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate fourth recovery method/ mitigation by regularly creating offline backups of important files

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
04	To put the fourth recovery method into use	When the ransomware attack is launched, make sure that confidential files related to the chemical plant have an offline backup	The affect of the ransomware attack should be mitigated as the files that have been encrypted already have offline backups in place	

Figure 25 Fourth Mitigation

After completing the test cases for the DoS attacks, it was important to begin designing test cases for the ransomware attack. With ransomware attacks on chemical plants, there are a number of methods to recover/ mitigate from them or attempt to mitigate their impact. One of the given methods comes in the form of producing offline backups, whereby in the event that a ransomware attack occurs, the most important files on the network already have backups so if the primary files become encrypted, the operators can revert back to the copies. These backups should be initiated regularly and frequently in order to ensure that they are up-to-date.

4.4.5 Test Case 5



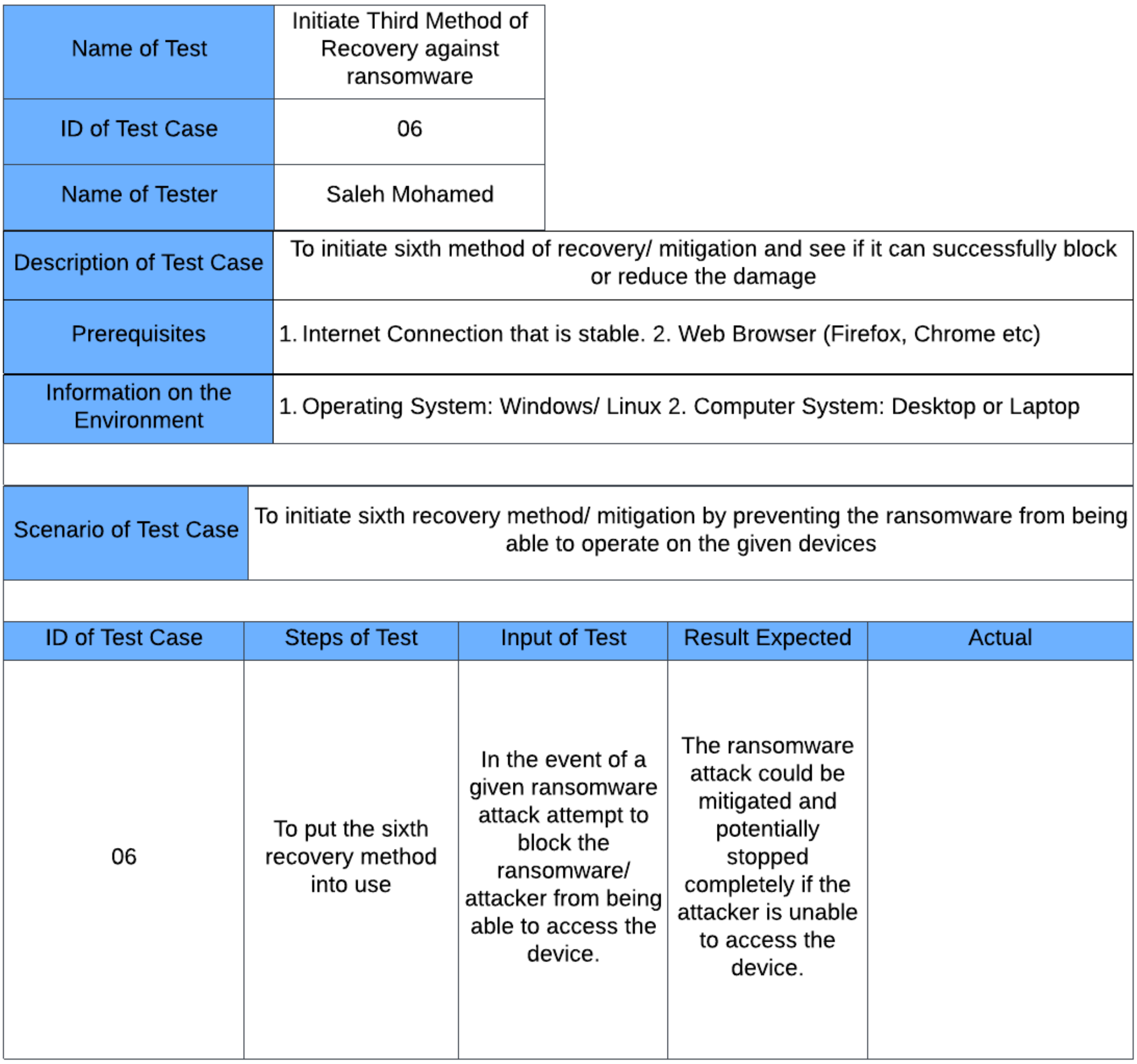
Name of Test	Initiate Second Method of Recovery against ransomware
ID of Test Case	05
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate fifth method of recovery/ mitigation and see if it can successfully block or reduce the damage
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate fifth recovery method/ mitigation by preventing the delivery of the ransomware and stopping it from reaching different devices

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
05	To put the fifth recovery method into use	In the event of a given ransomware attack on a chemical plant, initiate file filters to restrict the amount of files that are allowed to only ones which are expected to be received. Also block potentially malicious websites	The ransomware attack in its entirety could be prevented through strict filtering.	

Figure 26 Fifth Mitigation

With the fifth test case, the recovery method/ methods of mitigating the ransomware attack revolved around preventing the ransomware from being delivered to the device in the chemical plant and ultimately stopping its delivery. This can be completed by restricting the types of files allowed to only allowing ones that are expected to be received. Moreover, it can also include blocking code that is known to be malicious through utilising certain signatures as well as blocking suspicious websites.

4.4.6 Test Case 6



Name of Test	Initiate Third Method of Recovery against ransomware
ID of Test Case	06
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate sixth method of recovery/ mitigation and see if it can successfully block or reduce the damage
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate sixth recovery method/ mitigation by preventing the ransomware from being able to operate on the given devices

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
06	To put the sixth recovery method into use	In the event of a given ransomware attack attempt to block the ransomware/ attacker from being able to access the device.	The ransomware attack could be mitigated and potentially stopped completely if the attacker is unable to access the device.	

Figure 27 Sixth Mitigation

The sixth and final test case indicates the final resort which the chemical plant will take in relation to putting forth recovery/ mitigation mechanisms for the given ransomware attack. It revolves around stopping the given ransomware from being able to successfully run on the particular device and hindering its ability to carry out its malicious intentions. This can also include only allowing applications which have been permitted and are considered trusted to operate on the given devices whilst also taking into account whether or not anti-virus software that is enterprise is necessary to have and ensuring that it is kept up to date. Furthermore, it can also include making sure that updates for security become installed as soon as possible as well as setting OS updates to occur automatically and utilising the most up-to-date version of the given OS.

4.5 Practical Implementation of the Open-source tool

After completing the use cases, which demonstrated the scenarios in which an attacker could launch a cyber-attack (including DoS and ransomware) onto a chemical plant and test cases to indicate how a smart grid would be able to initiate recovery methods following the cyber-attacks, the next step in the project was to utilise an open-source tool, called “OpenPLC “, which can be used to launch Denial of Service attacks and connect that to a simulator known as ChemicalPlant. The simulator replicates a chemical plant and allows for practice attacks to be conducted and indicates the impact of the attack.

4.5.1 Why choose OpenPLC and ChemicalPlant

The tool OpenPLC was chosen as it is founded on software that is relatively straightforward to use and is a software programmable logic controller that can be used to launch Denial of Service attacks as well as ransomware attacks and was thus useful and applicable to the given thesis at hand. Additionally, it supports a variety of programming languages such as Function Block and Ladder Logic, as well as many others and was thus an effective option for the dissertation. It can also be used to connect to the simulator ChemicalPlant, which in this instance was incredibly ideal due to the fact that it allowed for the simulation of attacks to take place and can run on a wide variety of different platforms. Moreover, OpenPLC represents the software version of an actual PLC (programmable logic controller) which can be used in chemical plants and other industrial control systems and thus, this seemed like a logical and practical tool for the given simulator.

4.5.2 The benefits of OpenPLC and ChemicalPlant

The open-source tool OpenPLC has many advantages as it has support for multiple platforms including Windows and Linux and provides several programming languages to make use of.

4.5.3 Applying the MoSCoW method to the OpenPLC tool

The functionalities of the given tool and utilising its features to be able to successfully connect to the simulator can be categorised under the MoSCoW methodology. This is due to the fact that some requirements that are functional will be required in order to connect the OpenPLC tool to the ChemicalPlant Simulator. When making use of the given methodology, the tool will need:

<u>It must be able to:</u>

- Initiate DoS attacks on the simulator

The given open-source tool will need to be able to initiate attacks on the simulator through various functions and core features through the use of successfully identifying the simulator and connecting to it, locating areas that are open for attacks and initiating the attacks.

- Be reliable, accurate and consistent

The output and utilisation of the tool have to be reliable, accurate and consistent and be able to operate efficiently at all times and have the ability to carry out intended tasks whenever needed.

<u>It should be:</u>

- Run smoothly and sufficiently

The tool itself should be able to run sufficiently when being utilised and maintain its effectiveness in being able to launch DoS and ransomware attacks on the ChemicalPlant simulator.

It can:

- Conduct an analysis of the simulator including pinpointing the exact places to launch an attack.

The tool can analyse the simulator (e.g. when connecting to it, it will be able to decide where it can launch the given attack) and initiate an attack at certain points in the simulator.

- Be relatively straightforward and easy to utilise

The tool should be able to be put to use relatively easily and be straightforward when being used.

It will not:

- Be able to launch a wide range of attacks on the simulator

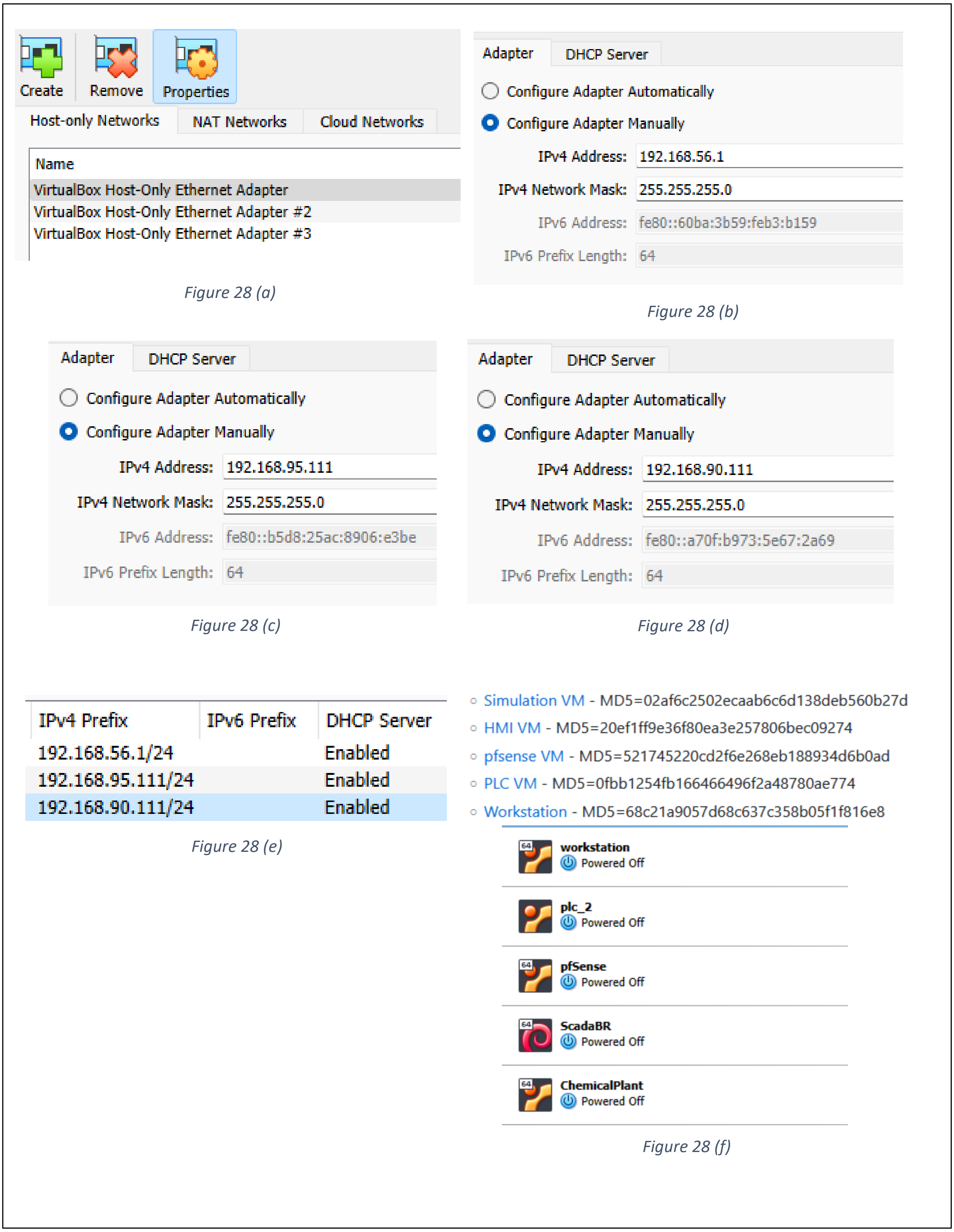
The tool will not be able to carry out unlimited forms of attacks but will instead be focused primarily on launching DoS and ransomware attacks.

4.6 Initiating the setup

The setup took place using Oracle Virtual Box, with each of the applications coming in the form of Virtual Machines (VMs). In order to set up the interface between OpenPLC and ChemicalPlant, it was necessary to connect a pfsense firewall, a workstation and an HMI (Human Machine Interface). This was due to the fact that the HMI makes use of an HMI operator that has been produced utilising software that is ScadaBR and works by monitoring the measurements of the processes which are obtained through the OpenPLC.

Before uploading the VMs onto the VirtualBox, two network adapters were created and provided with IP addresses, with adapter 1 having the IP address 192.168.56.1, adapter 2 having the address 192.168.95.111 and adapter 3 having the address 192.168.90.111. In addition, the DHCP servers were then enabled for the adapters. This can be seen in Table 5.

Figure 28 Setting up the VMs



Name
VirtualBox Host-Only Ethernet Adapter
VirtualBox Host-Only Ethernet Adapter #2
VirtualBox Host-Only Ethernet Adapter #3

Figure 28 (a)

○ Configure Adapter Automatically
● Configure Adapter Manually
IPv4 Address: 192.168.56.1
IPv4 Network Mask: 255.255.255.0
IPv6 Address: fe80::60ba:3b59:feb3:b159
IPv6 Prefix Length: 64

Figure 28 (b)

○ Configure Adapter Automatically
● Configure Adapter Manually
IPv4 Address: 192.168.95.111
IPv4 Network Mask: 255.255.255.0
IPv6 Address: fe80::b5d8:25ac:8906:e3be
IPv6 Prefix Length: 64

Figure 28 (c)

○ Configure Adapter Automatically
● Configure Adapter Manually
IPv4 Address: 192.168.90.111
IPv4 Network Mask: 255.255.255.0
IPv6 Address: fe80::a70f:b973:5e67:2a69
IPv6 Prefix Length: 64

Figure 28 (d)

IPv4 Prefix	IPv6 Prefix	DHCP Server
192.168.56.1/24		Enabled
192.168.95.111/24		Enabled
192.168.90.111/24		Enabled

Figure 28 (e)

- Simulation VM - MD5=02af6c2502ecaab6c6d138deb560b27d
- HMI VM - MD5=20ef1ff9e36f80ea3e257806bec09274
- pfsense VM - MD5=521745220cd2f6e268eb188934d6b0ad
- PLC VM - MD5=0fbb1254fb166466496f2a48780ae774
- Workstation - MD5=68c21a9057d68c637c358b05f1f816e8

workstation
Powered Off

plc_2
Powered Off

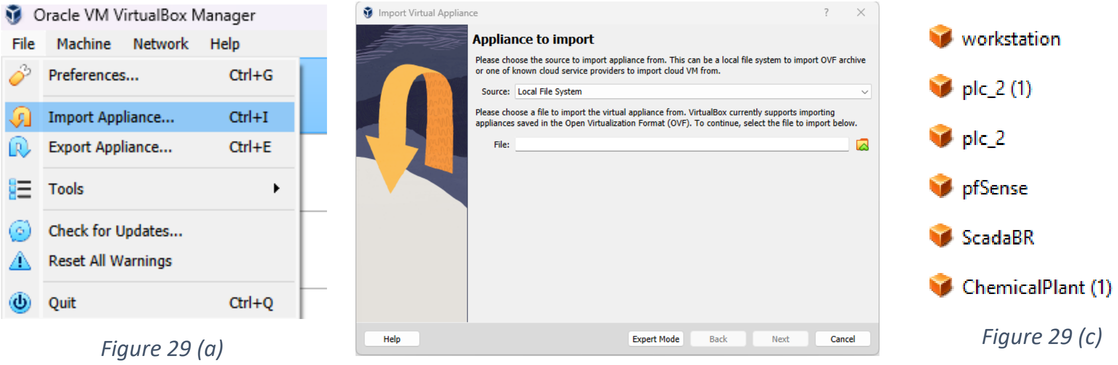
pfSense
Powered Off

ScadaBR
Powered Off

ChemicalPlant
Powered Off

Figure 28 (f)

Figure 29 Setting up the VMs 2



Appliance to import

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File:

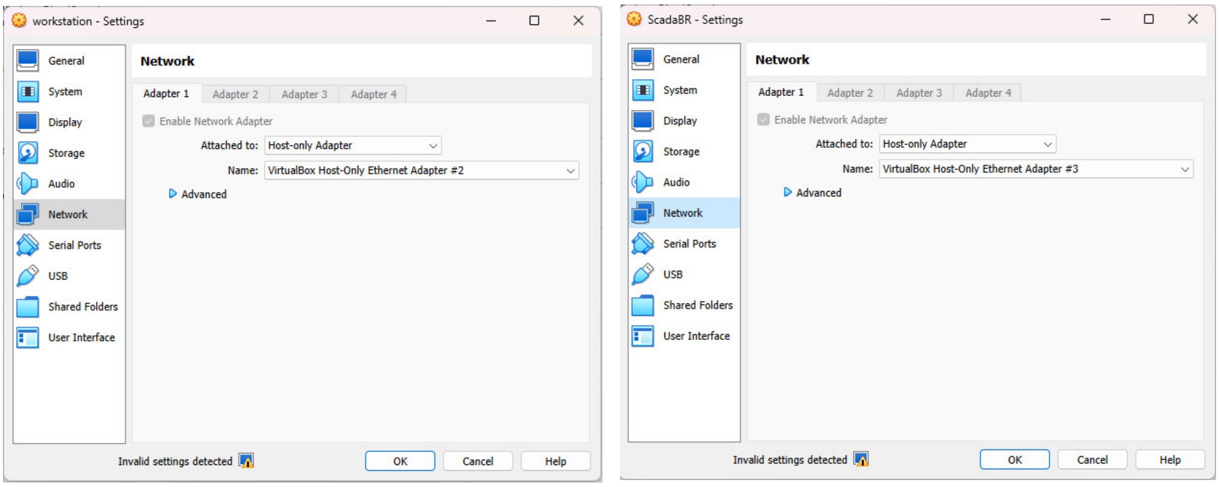
Figure 29 (a)

Figure 29 (b)

Figure 29 (c)

Once the adapters had been provided with the correct IP addresses, the VMs were then uploaded onto the VirtualBox.

Figure 30 Setting up the VMs 3



workstation - Settings — Network, Adapter 1

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #2

ScadaBR - Settings — Network, Adapter 1

☑ Enable Network Adapter

Attached to: Host-only Adapter

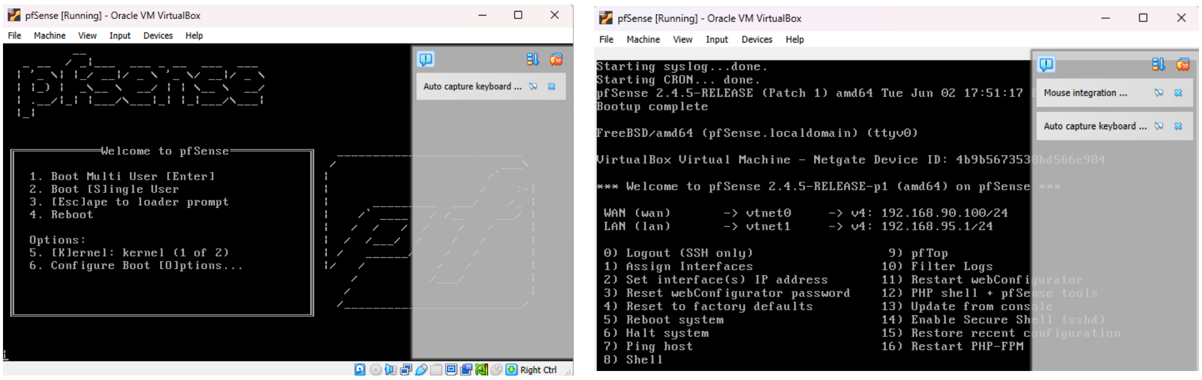
Name: VirtualBox Host-Only Ethernet Adapter #3

Figure 30 (a)

Figure 30 (b)

Upon uploading the VMs to the VirtualBox, each VM was then assigned to one of the network adapters. For instance, the VM workstation was provided with ethernet adapter 2. Whereas the ScadaBR VM was provided with ethernet adapter 3.

Figure 31 Launching pfSense


pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Auto capture keyboard ...
Right Ctrl

```
pfSense

        Welcome to pfSense

  1. Boot Multi User [Enter]
  2. Boot [S]ingle User
  3. [Esc]ape to loader prompt
  4. Reboot

  Options:
  5. [K]ernel: kernel (1 of 2)
  6. Configure Boot [O]ptions...
```

Figure 31 (a)

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 4b9b5673530bd566e984

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4: 192.168.90.100/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.95.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell
```

Figure 31 (b)

After allocating each VM with the appropriate ethernet adapter, the VM pfSense was then booted up and provided with the correct network settings such as "vtnet0".

From this, the main simulator was then loaded up on the web address 192.168.95.10

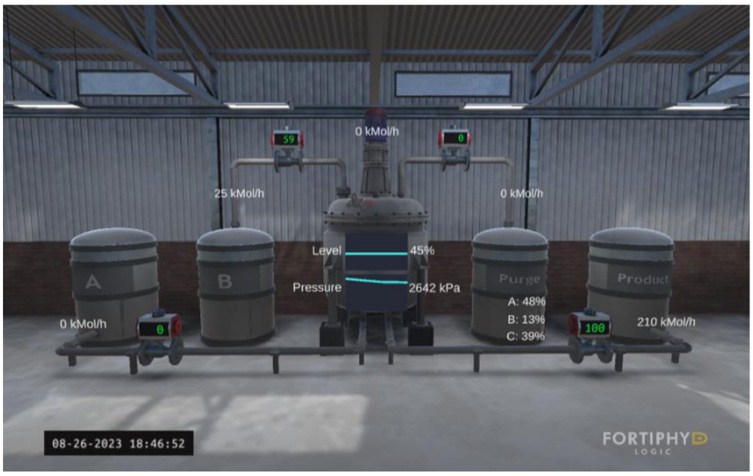
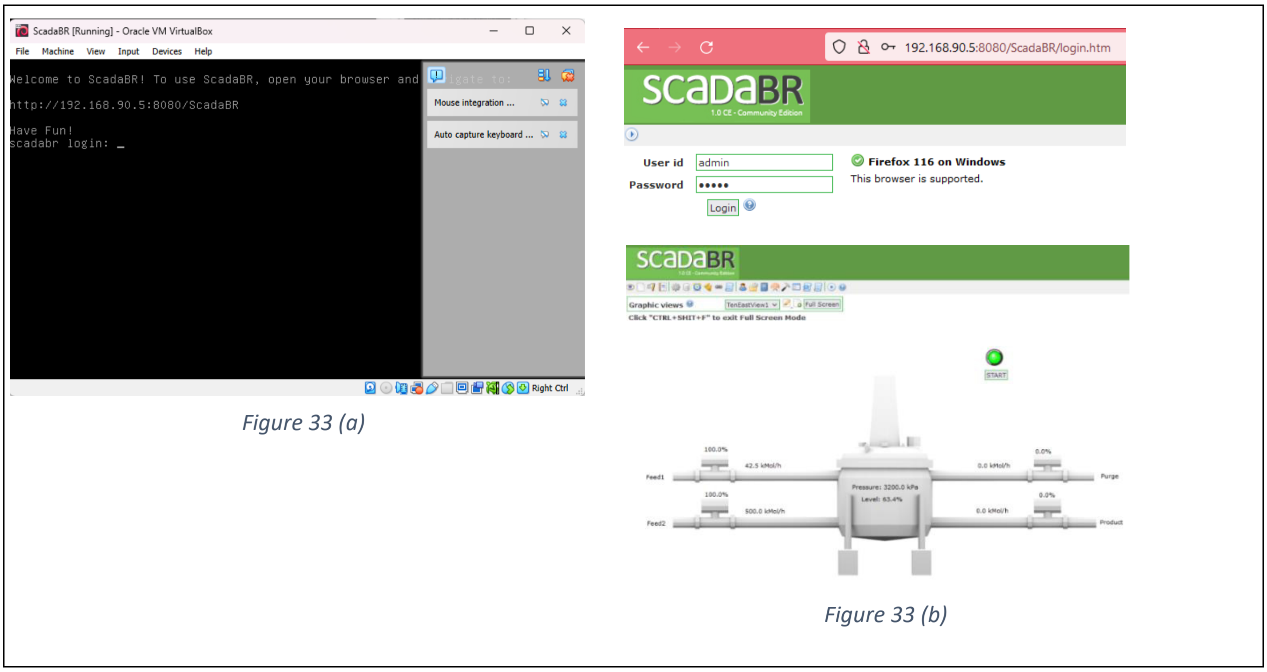


Figure 32 Chemical Plant Simulator

As can be seen, this is the primary simulator for the Chemical Plant, which represented a fully working plantation with various values and readings such as level and pressure.

Figure 33 Launching ScadaBR



ScadaBR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
Right Ctrl

```
Welcome to ScadaBR! To use ScadaBR, open your browser and
http://192.168.90.5:8080/ScadaBR

Have Fun!
scadabr login: _
```

Figure 33 (a)

192.168.90.5:8080/ScadaBR/login.htm
ScadaBR
1.0 CE - Community Edition
Login
Graphic views
Full Screen
START
Feed1
Feed2
Purge
Product

User id: admin
Password: •••••

Firefox 116 on Windows
This browser is supported.

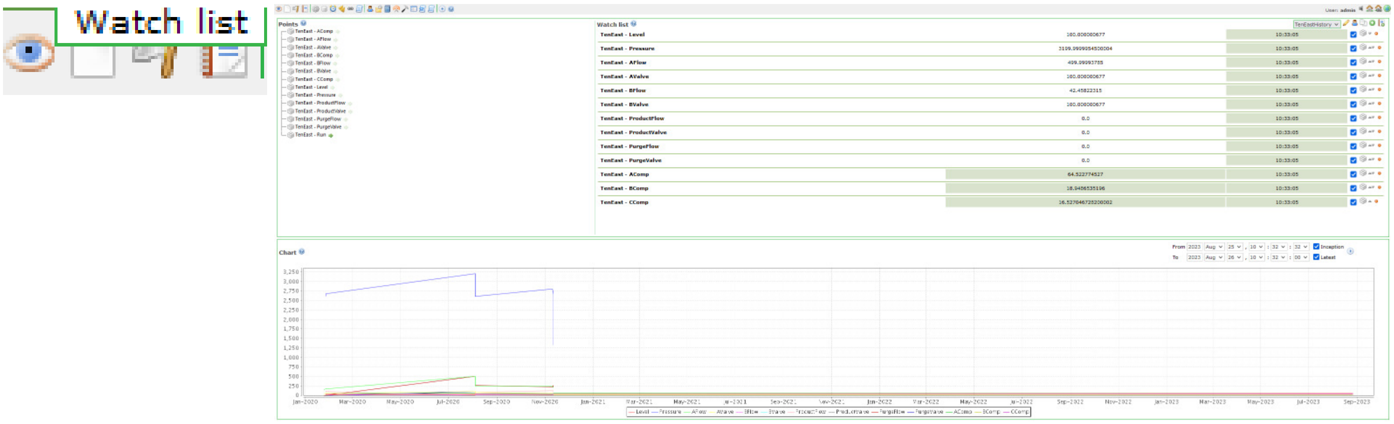
TenEastView1

Click "CTRL+SHIFT+F" to exit Full Screen Mode

100.0% 42.5 kMol/h
100.0% 500.0 kMol/h
0.0% 0.0 kMol/h
0.0% 0.0 kMol/h
Pressure: 3200.0 kPa
Level: 63.4%

Figure 33 (b)

Following this, the VM ScadaBR was then initiated which provided a Human Machine Interface. The terminal for the ScadaBR provided the main IP web address to go to. Upon going to the address in the Scada VM (192.168.90.5:8080/ScadaBR) it displayed a login page for accessing the website. After accessing the site, it displayed a graphical user interface for a chemical plant. These screenshots demonstrate the Human Machine Interface of the chemical plant as well as the values that the plant contains.



Watch list

TenEast - Level	100.000000677	10:33:05
TenEast - Pressure	3199.9999954500004	10:33:05
TenEast - AFlow	499.99993785	10:33:05
TenEast - AValve	100.000000677	10:33:05
TenEast - BFlow	42.45822315	10:33:05
TenEast - BValve	100.000000677	10:33:05
TenEast - ProductFlow	0.0	10:33:05
TenEast - ProductValve	0.0	10:33:05
TenEast - PurgeFlow	0.0	10:33:05
TenEast - PurgeValve	0.0	10:33:05
TenEast - AComp	64.522774527	10:33:05
TenEast - BComp	18.9486535196	10:33:05
TenEast - CComp	16.527046725200002	10:33:05

From 2023 Aug 25 , 10 : 32 : 32 ☑ Inception
To 2023 Aug 26 , 10 : 32 : 00 ☑ Latest

Figure 34 Additional Information on HMI

Moreover, at the top left-hand side corner of the ScadaBR interface, there was an icon called "watch list" which provided further information. Thus, the watch list provided additional information regarding the HMI and listed various values.

However, whilst the HMI gives various users and operators an efficient way of interfacing with an ICS process, it is unable to manipulate the process. This can be done through utilising the PLC (in this case OpenPLC). As such, the web browser for the HMI is communicating with the ScadaBR VM, whilst the ScadaBR VM communicates with the PLC VM, which in turn is able to communicate with the ChemicalPlant simulator.

Figure 35 Connecting the VMs together

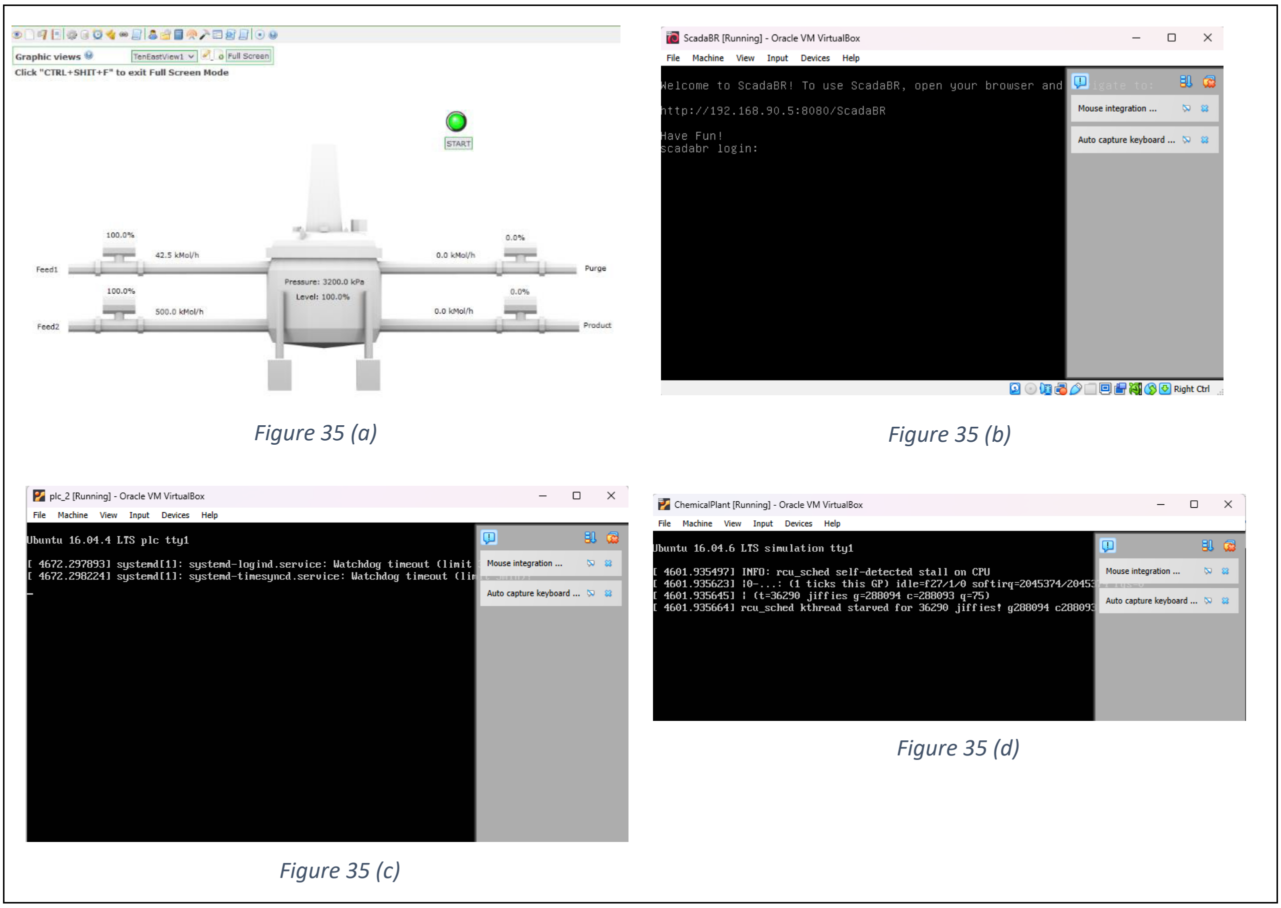

Graphic views
TenEastView1
Full Screen
Click "CTRL+SHIT+F" to exit Full Screen Mode
START
100.0%
42.5 kMol/h
Feed1
100.0%
500.0 kMol/h
Feed2
Pressure: 3200.0 kPa
Level: 100.0%
0.0%
0.0 kMol/h
Purge
0.0%
0.0 kMol/h
Product
ScadaBR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
plc_2 [Running] - Oracle VM VirtualBox
ChemicalPlant [Running] - Oracle VM VirtualBox

Figure 35 (a)

```
Welcome to ScadaBR! To use ScadaBR, open your browser and

http://192.168.90.5:8080/ScadaBR

Have Fun!
scadabr login:
```

Figure 35 (b)

```
Ubuntu 16.04.4 LTS plc tty1

[ 4672.297893] systemd[1]: systemd-logind.service: Watchdog timeout (limit
[ 4672.298224] systemd[1]: systemd-timesyncd.service: Watchdog timeout (li
_
```

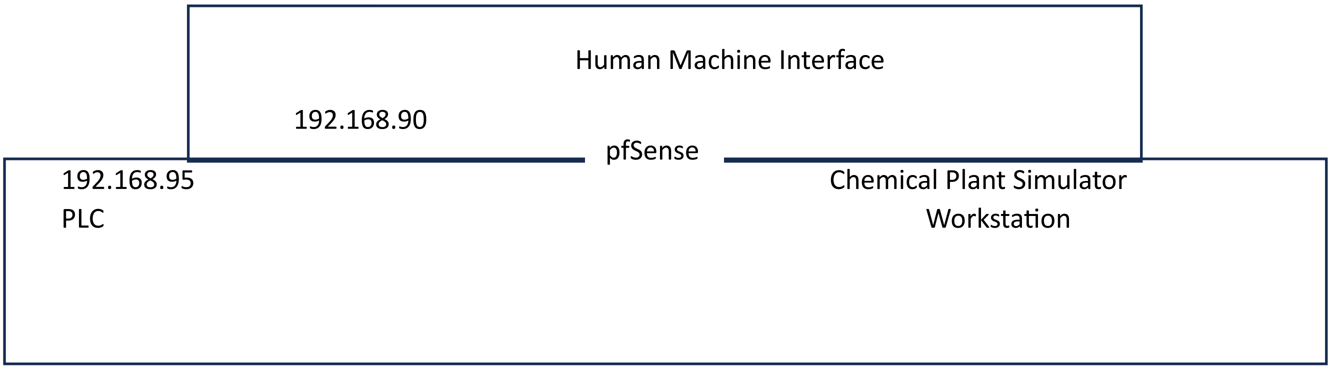
Figure 35 (c)

```
Ubuntu 16.04.6 LTS simulation tty1

[ 4601.935497] INFO: rcu_sched self-detected stall on CPU
[ 4601.935623] |0-...: (1 ticks this GP) idle=f27/1/0 softirq=2045374/20453
[ 4601.935645] | (t=36290 jiffies g=288094 c=288093 q=75)
[ 4601.935664] rcu_sched kthread starved for 36290 jiffies! g288094 c288093
```

Figure 35 (d)

In effect, the VMs can be placed into two sections.


Human Machine Interface

192.168.90

pfSense

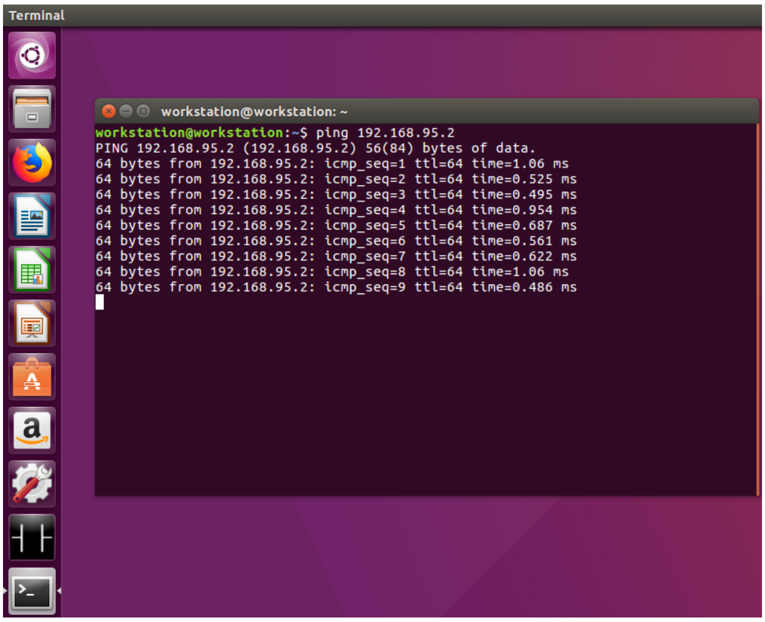
192.168.95

PLC

Chemical Plant Simulator

Workstation

Furthermore, within the workstation VM, a terminal was then opened to check to see if it is connected to the Scada VM.



```
workstation@workstation:~$ ping 192.168.95.2
PING 192.168.95.2 (192.168.95.2) 56(84) bytes of data.
64 bytes from 192.168.95.2: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.95.2: icmp_seq=2 ttl=64 time=0.525 ms
64 bytes from 192.168.95.2: icmp_seq=3 ttl=64 time=0.495 ms
64 bytes from 192.168.95.2: icmp_seq=4 ttl=64 time=0.954 ms
64 bytes from 192.168.95.2: icmp_seq=5 ttl=64 time=0.687 ms
64 bytes from 192.168.95.2: icmp_seq=6 ttl=64 time=0.561 ms
64 bytes from 192.168.95.2: icmp_seq=7 ttl=64 time=0.622 ms
64 bytes from 192.168.95.2: icmp_seq=8 ttl=64 time=1.06 ms
64 bytes from 192.168.95.2: icmp_seq=9 ttl=64 time=0.486 ms
```

Figure 36 Pinging Scada VM

Likewise, with everything set up and connected, it was now possible to utilise the OpenPLC Editor within the workstation VM to carry out attacks on the simulator.

4.7 Utilising OpenPLC and Modifying Control Logic

With OpenPLC, this application was utilised as a means of writing ladder logic programming and manipulating that in order to launch attacks at the ChemicalPlant simulator. All the necessary features and components were added to them to ensure that the ladder logic would function correctly and undertake operations efficiently. This was especially important for DoS attacks, as they would be launched from the OpenPLC program onto the simulator.

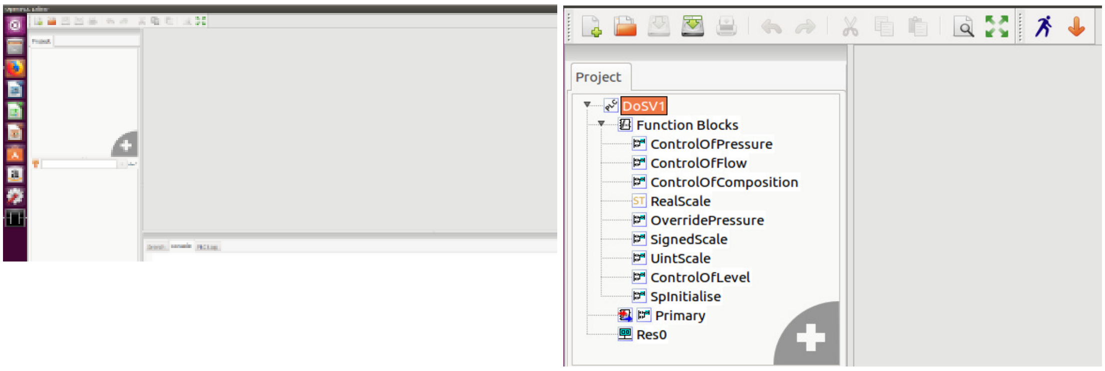
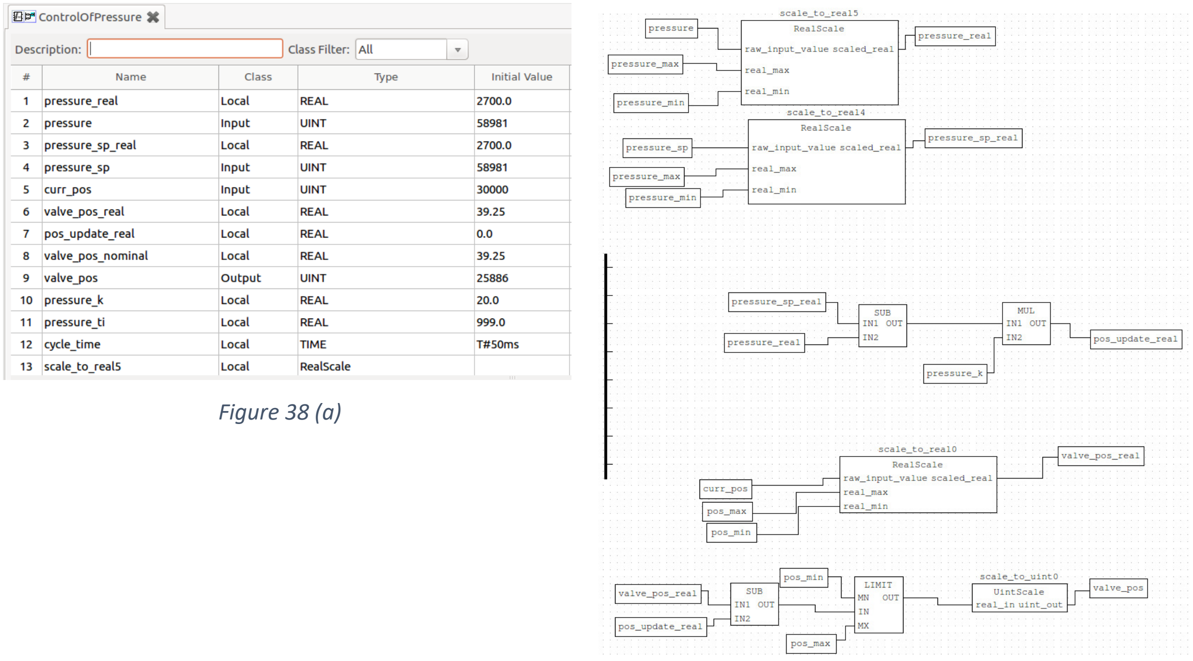


Figure 37 Utilising OpenPLC Projects

In total, three main OpenPLC projects were established, with the first one being related to DoS, the second being on ransomware and the third one being on counteracting the ransomware attack. The projects were given the names “DoS” and “Ransomware” to indicate what their purpose was. Furthermore, each of them contained an area called “Function Blocks” which contained several functions such as “ControlOfPressure” and “ControlOfLevel” whereby each function was intended to manipulate the ChemicalPlant when being uploaded.

Figure 38 Control of Pressure Function



ControlOfPressure

Description:

Class Filter: All

#	Name	Class	Type	Initial Value
1	pressure_real	Local	REAL	2700.0
2	pressure	Input	UINT	58981
3	pressure_sp_real	Local	REAL	2700.0
4	pressure_sp	Input	UINT	58981
5	curr_pos	Input	UINT	30000
6	valve_pos_real	Local	REAL	39.25
7	pos_update_real	Local	REAL	0.0
8	valve_pos_nominal	Local	REAL	39.25
9	valve_pos	Output	UINT	25886
10	pressure_k	Local	REAL	20.0
11	pressure_ti	Local	REAL	999.0
12	cycle_time	Local	TIME	T#50ms
13	scale_to_real5	Local	RealScale	

Figure 38 (a)

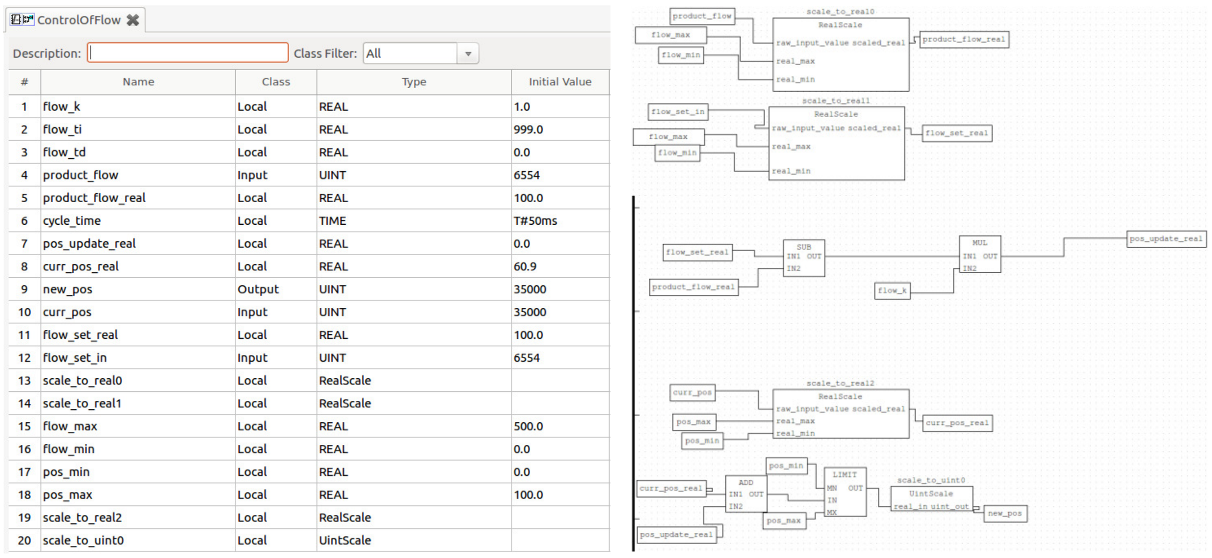
Figure 38 (b)

The first function, called “ControlOfPressure” contained a list of variables including “pressure_real”, “valve_pos_real”, “cycle_time”, “pos_min”, “pos_max” etc. All of these were used as a means of controlling the pressure of the simulator and contained various values such as 2700, 58981, 32000 etc. This indicated that it set the real pressure to that of 2700 as well as the maximum pressure to 32000. Whereas the position of the valve implied where the valve was and gave it a real value of 39.25 whilst the cycle_time depicted the time for each cycle. The variables dictated the balancing of the pressure within the ChemicalPlant and were necessary to ensure that everything remained stable.

Furthermore, when applying these variables to the actual ladder logic code, a number of blocks were utilized whereby each block was set to “scale_to_real”. This signified that each of the variable’s functionalities were being applied to the real values of the chemical plant and setting the features for the standard pressure, minimum pressure and maximum pressure, etc.

As a result, the given blocks, were used as a means of providing necessary stability to the chemical plant and governed the overall pressure control.

Figure 39 Control of Flow Function



#	Name	Class	Type	Initial Value
1	flow_k	Local	REAL	1.0
2	flow_ti	Local	REAL	999.0
3	flow_td	Local	REAL	0.0
4	product_flow	Input	UINT	6554
5	product_flow_real	Local	REAL	100.0
6	cycle_time	Local	TIME	T#50ms
7	pos_update_real	Local	REAL	0.0
8	curr_pos_real	Local	REAL	60.9
9	new_pos	Output	UINT	35000
10	curr_pos	Input	UINT	35000
11	flow_set_real	Local	REAL	100.0
12	flow_set_in	Input	UINT	6554
13	scale_to_real0	Local	RealScale	
14	scale_to_real1	Local	RealScale	
15	flow_max	Local	REAL	500.0
16	flow_min	Local	REAL	0.0
17	pos_min	Local	REAL	0.0
18	pos_max	Local	REAL	100.0
19	scale_to_real2	Local	RealScale	
20	scale_to_uint0	Local	UintScale	

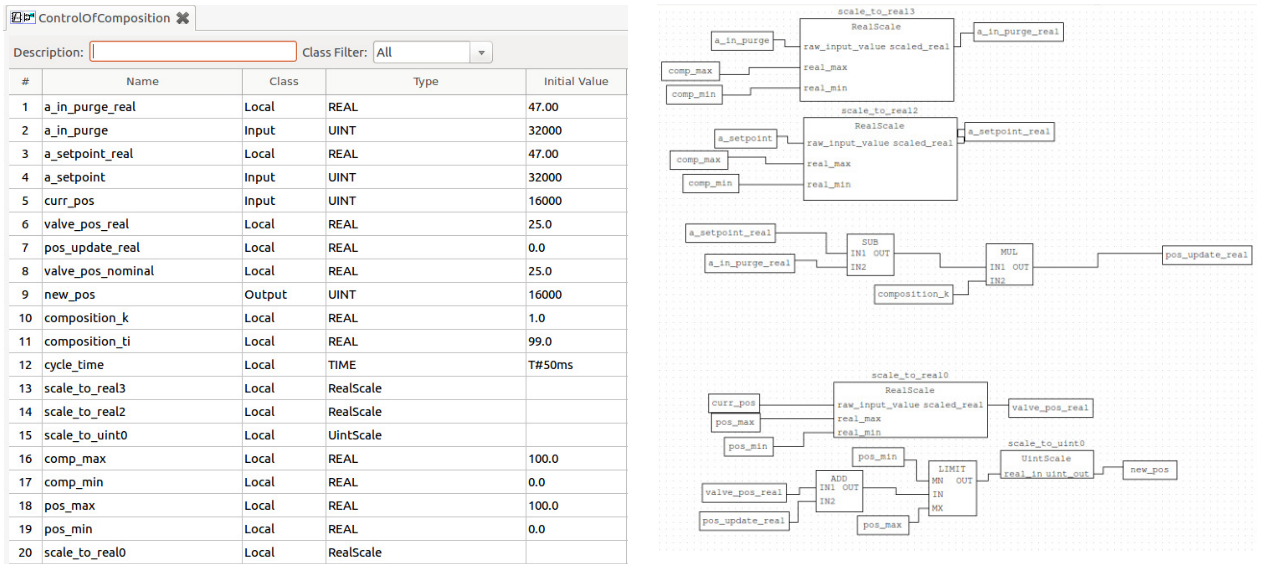
Figure 39 (a)

Figure 39 (b)

The second function, "ControlOfFlow" revolved around how the OpenPLC project would be able to establish overall flow control. This function consisted of variables including "flow_k", "product_flow", "product_flow_real", "flow_max" and "flow_min" etc. Whilst the previous function related to the governing of pressure control, this function revolved around controlling the flow. This was also important as it was needed in order to ensure that the flow was relatively stable within the chemical plant. Additionally, the variables were allocated certain values which indicated how the flow would be controlled or altered for example, "flow_max" was the variable that set the maximum flow value to the chemical plant whilst "flow_min" placed the lowest value that it could have.

Likewise, the ladder logic code transferred the variables into various blocks that represented the flow of the chemical plant including the product flow, maximum and minimum flow. It also included a block for "LIMIT" which represented the minimum and maximum values as well as adding input and output.

Figure 40 Control of Composition Function



ControlOfComposition

Description: | Class Filter: All

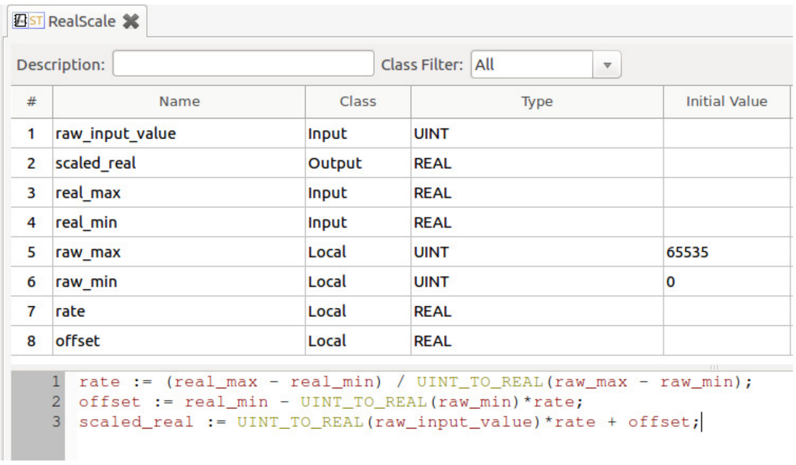
#	Name	Class	Type	Initial Value
1	a_in_purge_real	Local	REAL	47.00
2	a_in_purge	Input	UINT	32000
3	a_setpoint_real	Local	REAL	47.00
4	a_setpoint	Input	UINT	32000
5	curr_pos	Input	UINT	16000
6	valve_pos_real	Local	REAL	25.0
7	pos_update_real	Local	REAL	0.0
8	valve_pos_nominal	Local	REAL	25.0
9	new_pos	Output	UINT	16000
10	composition_k	Local	REAL	1.0
11	composition_ti	Local	REAL	99.0
12	cycle_time	Local	TIME	T#50ms
13	scale_to_real3	Local	RealScale	
14	scale_to_real2	Local	RealScale	
15	scale_to_uint0	Local	UintScale	
16	comp_max	Local	REAL	100.0
17	comp_min	Local	REAL	0.0
18	pos_max	Local	REAL	100.0
19	pos_min	Local	REAL	0.0
20	scale_to_real0	Local	RealScale	

Figure 40 (a)

Figure 40 (b)

Similarly, the third function was called "ControlOfComposition". The variables here are relatively similar to the ones in some of the previous functions (as they consist of features such as the minimum and maximum values of the composition) and revolve around the functionality and control of the composition. E.g., the variable "comp_max" is set to the value of 100 whilst the "comp_min" is set to 0.

Moreover, the function “RealScale” contained various variables such as“raw_input_value”, “real_max”, “real_min”, “raw_max” and “raw_min”. These variables were utilised as a means of converting the real values to scale. The primary variable here is the “raw_max” variable with the value 65535. This is important as it indicates that the highest value which the chemical plant can be pushed to is over 65000 and could be considered a tipping point. Furthermore, the code below signifies that the rate is produced by the “real_max” variable subtracted from the “real_min” variable and divided by the “UINT_TO_REAL” and finally subtracted by the “raw_max taken away from “raw_min”.



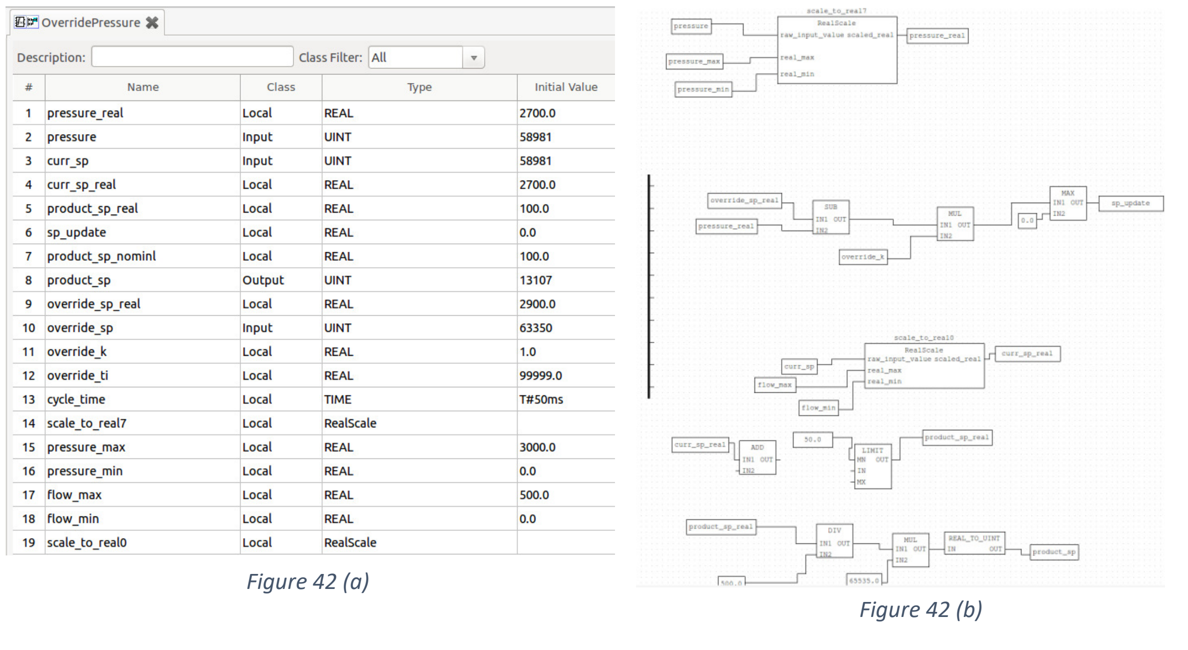
#	Name	Class	Type	Initial Value
1	raw_input_value	Input	UINT	
2	scaled_real	Output	REAL	
3	real_max	Input	REAL	
4	real_min	Input	REAL	
5	raw_max	Local	UINT	65535
6	raw_min	Local	UINT	0
7	rate	Local	REAL	
8	offset	Local	REAL	

```
rate := (real_max - real_min) / UINT_TO_REAL(raw_max - raw_min);
offset := real_min - UINT_TO_REAL(raw_min)*rate;
scaled_real := UINT_TO_REAL(raw_input_value)*rate + offset;
```

Figure 41 RealScale Function

The following function consisted of the “OverridePressure” which depicted how pressure could be overridden within the chemical plant. This function was also unique as it signified the way in which pressure could be overridden with different variables and features. At the same time, it also had similarities to the first function, with it containing variables such as “pressure_real”. “pressure_max” and “pressure_min”. It also contains the same values for pressure_real and pressure, (being 2700.0 and 58981) as this function somewhat overlaps with the first one and can simply be used to override the pressure within the simulator. The variables are put to use in the ladder logic code.

Figure 42 Override Pressure Function



OverridePressure

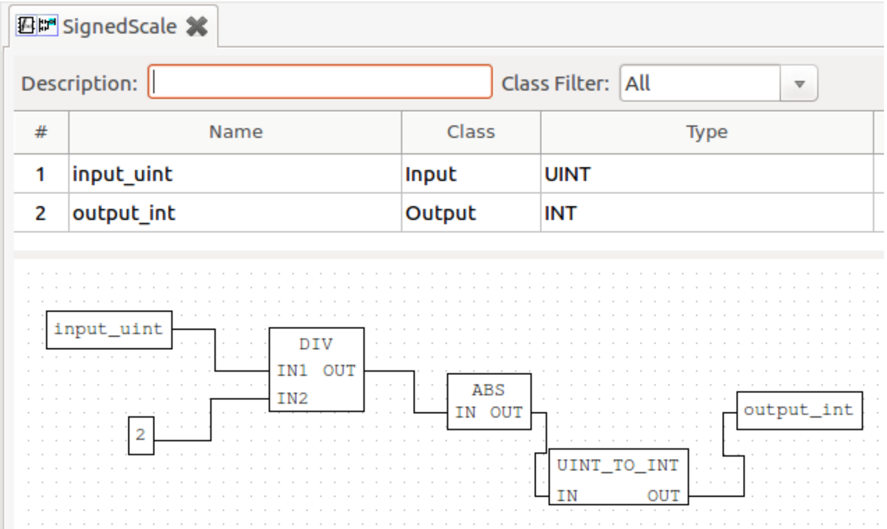
Description: Class Filter: All

#	Name	Class	Type	Initial Value
1	pressure_real	Local	REAL	2700.0
2	pressure	Input	UINT	58981
3	curr_sp	Input	UINT	58981
4	curr_sp_real	Local	REAL	2700.0
5	product_sp_real	Local	REAL	100.0
6	sp_update	Local	REAL	0.0
7	product_sp_nominl	Local	REAL	100.0
8	product_sp	Output	UINT	13107
9	override_sp_real	Local	REAL	2900.0
10	override_sp	Input	UINT	63350
11	override_k	Local	REAL	1.0
12	override_ti	Local	REAL	99999.0
13	cycle_time	Local	TIME	T#50ms
14	scale_to_real7	Local	RealScale	
15	pressure_max	Local	REAL	3000.0
16	pressure_min	Local	REAL	0.0
17	flow_max	Local	REAL	500.0
18	flow_min	Local	REAL	0.0
19	scale_to_real0	Local	RealScale	

Figure 42 (a)

Figure 42 (b)

Furthermore, the “SignedScale” function is more simplistic and simply contains two variables for the input and output that have been defined as “UINT” and “INT”.

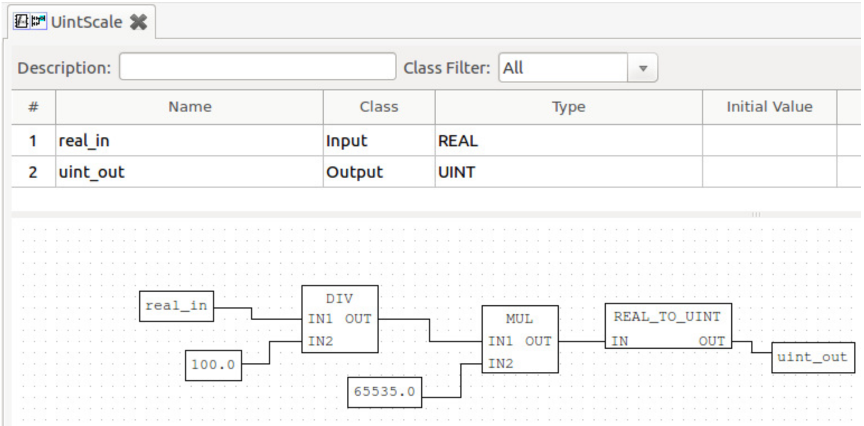


SignedScale

Description: Class Filter: All

#	Name	Class	Type
1	input_uint	Input	UINT
2	output_int	Output	INT

Figure 43 SignedScale Function



UintScale

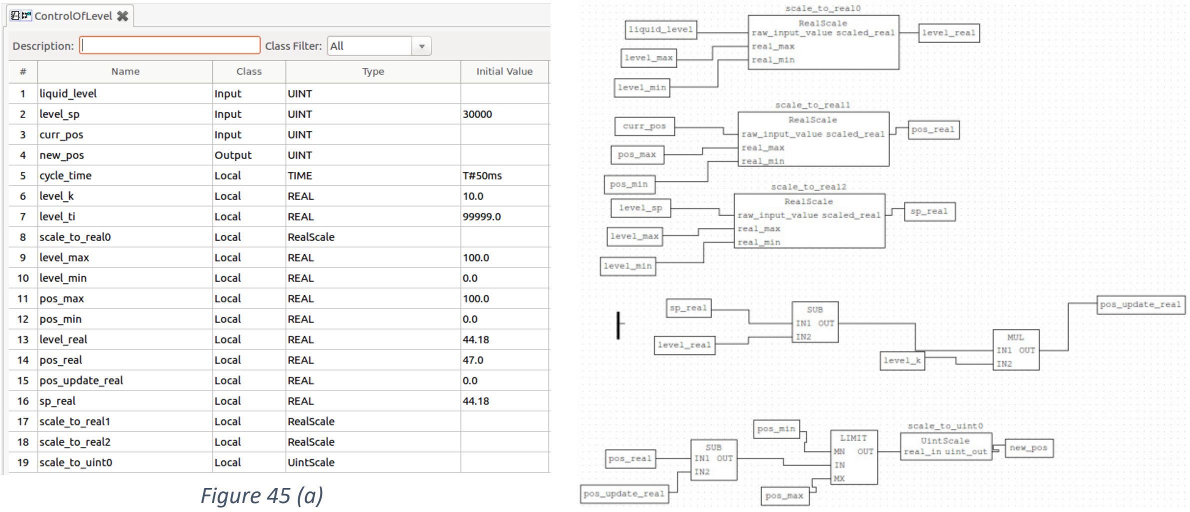
Description: Class Filter: All

#	Name	Class	Type	Initial Value
1	real_in	Input	REAL	
2	uint_out	Output	UINT	

Figure 44 UintScale Function

Moreover, the "UintScale" function, like the previous one is straightforward and just contains the variables for the real input and uint output.

Figure 45 Control of Level Function



ControlOfLevel

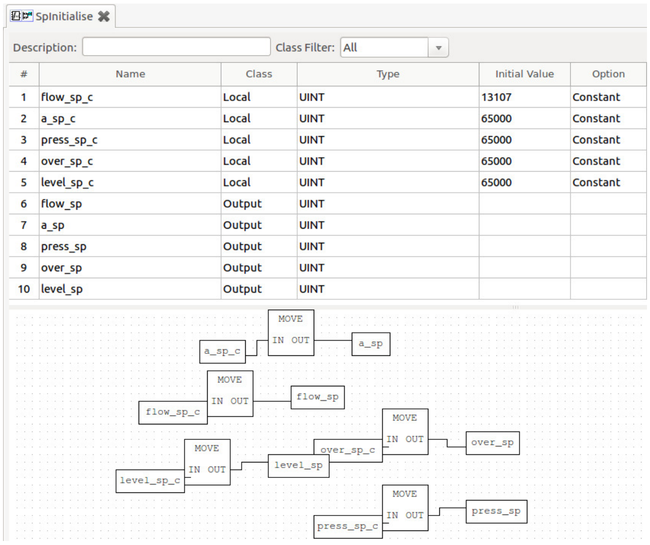
Description: Class Filter: All

#	Name	Class	Type	Initial Value
1	liquid_level	Input	UINT	
2	level_sp	Input	UINT	30000
3	curr_pos	Input	UINT	
4	new_pos	Output	UINT	
5	cycle_time	Local	TIME	T#50ms
6	level_k	Local	REAL	10.0
7	level_ti	Local	REAL	99999.0
8	scale_to_real0	Local	RealScale	
9	level_max	Local	REAL	100.0
10	level_min	Local	REAL	0.0
11	pos_max	Local	REAL	100.0
12	pos_min	Local	REAL	0.0
13	level_real	Local	REAL	44.18
14	pos_real	Local	REAL	47.0
15	pos_update_real	Local	REAL	0.0
16	sp_real	Local	REAL	44.18
17	scale_to_real1	Local	RealScale	
18	scale_to_real2	Local	RealScale	
19	scale_to_uint0	Local	UintScale	

Figure 45 (a)

Figure 45 (b)

The "ControlOfLevel" function related to how the level was controlled within the chemical plant.



SpInitialise

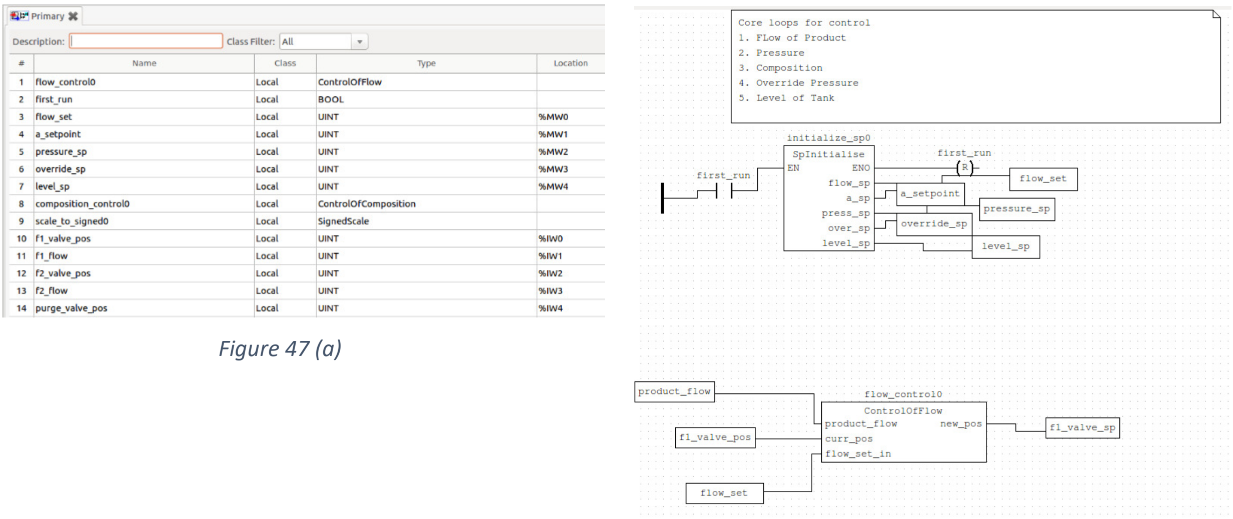
Description: | Class Filter: All

#	Name	Class	Type	Initial Value	Option
1	flow_sp_c	Local	UINT	13107	Constant
2	a_sp_c	Local	UINT	65000	Constant
3	press_sp_c	Local	UINT	65000	Constant
4	over_sp_c	Local	UINT	65000	Constant
5	level_sp_c	Local	UINT	65000	Constant
6	flow_sp	Output	UINT		
7	a_sp	Output	UINT		
8	press_sp	Output	UINT		
9	over_sp	Output	UINT		
10	level_sp	Output	UINT		

Figure 46 SpInitialise Function

Finally, the last function, "SpIntialise" revolved around how the chemical plant could be manipulated and modified to alter aspects such as pressure and flow. This function was very important as it directly allowed the values (especially the pressure) of the chemical plant to be changed.

Figure 47 Primary Function



Primary

Description: | Class Filter: All

#	Name	Class	Type	Location
1	flow_control0	Local	ControlOfFlow	
2	first_run	Local	BOOL	
3	flow_set	Local	UINT	%MW0
4	a_setpoint	Local	UINT	%MW1
5	pressure_sp	Local	UINT	%MW2
6	override_sp	Local	UINT	%MW3
7	level_sp	Local	UINT	%MW4
8	composition_control0	Local	ControlOfComposition	
9	scale_to_signed0	Local	SignedScale	
10	f1_valve_pos	Local	UINT	%IW0
11	f1_flow	Local	UINT	%IW1
12	f2_valve_pos	Local	UINT	%IW2
13	f2_flow	Local	UINT	%IW3
14	purge_valve_pos	Local	UINT	%IW4

Figure 47 (a)

Core loops for control
1. FLow of Product
2. Pressure
3. Composition
4. Override Pressure
5. Level of Tank

Figure 47 (b)

In addition to the functions, the other major function within the OpenPLC projects was called "primary". This could be considered the "main" function of the project and combined various aspects of the functions together. In addition, it was also provided with a comment at the top of the ladder logic indicating what it contained. The ladder logic was programmed in a way in which it increased the values of the chemical plant to the point in which it overloaded before eventually malfunctioning and exploding. After the ladder logic program had been completed, it was exported as an .st file which would be used to connect to the simulator.

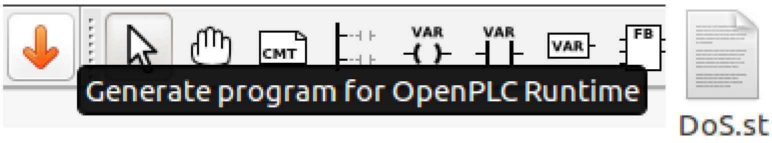


Figure 48 Generating ST file

The second and third projects (ransomware and countering the ransomware attack) are discussed in Chapter 5 where the attacks are initiated. The second project is very similar to the first except its values are set to 0 whereas the third project has lower values than the first for balance against the attack.

4.8 Pseudocode for Attacks

Prior to initiating the attacks, it was first useful and logical to write some pseudocode for the given attacks as this would improve their delivery and make the process of conducting the attacks smoother.

```
Start of DoS attacks
IF pressure chamber is switched to > 55000
Then
Pressure in chamber = critical
Result = overload
Disruption to the chemical plant
Else
SET pressure < 55000
Then
Pressure remains stable
End
Start of Ransomware attack
IF OpenPLC Editor project is accessible
Then
Attacker infiltrates OpenPLC – Extracts data from project before erasing data currently contained within project
SET Excel document/ Word document to contain data/ values
```

```
Output = Payment demanded in return for data/ values
IF Payment is made
Then
Output = Data/ values are returned to the project
Else
Output = Data/ values are lost
Simulator is unable to operate efficiently
End
```

4.9 Summary

This chapter covered producing various designs for the given scenarios and system/ threat model. This included designing the basic structure of a chemical plant and components as well as designing the situations in which an attacker would launch a DoS/ ransomware attack on the chemical plant and how the chemical plant/ operators would react to it. In addition, it detailed several test cases which could be considered the foundations of the rules formation as they provided several procedures in terms of how the chemical plant could mitigate the damage caused by the attack as well as attempt to recover from the attack(s). Furthermore, it then went onto the implementation stage whereby the appropriate tool was selected, as well as the simulator, ChemicalPlant was utilised. The implementation then proceeded on towards establishing an interface between them before finally carrying out DoS/ ransomware attacks from the OpenPLC tool to the ChemicalPlant simulator.

Chapter 5 Results and Evaluation

This chapter will discuss the findings that were obtained through launching the attacks before analysing and evaluating the results. It will also explain the effects of the attacks as well as the methods of mitigation/ recovery that could be applied.

5.1 Findings

The findings indicate what was revealed during the attack scenarios and what impact the attacks (DoS and ransomware) had on the simulator.

5.1.1 Initiating Attacks on the Simulator

Having successfully established the setup between OpenPLC, HMI, Pfsense, workstation and ChemicalPlant simulator and utilising the Ladder Logic programming within the OpenPLC projects, it became possible to begin launching cyber-attacks in order to analyse and understand the effect that they have on the simulator. For launching attacks, as mentioned previously, the programming language Ladder Logic was used and enabled DoS attacks to be simulated by the open-source tool

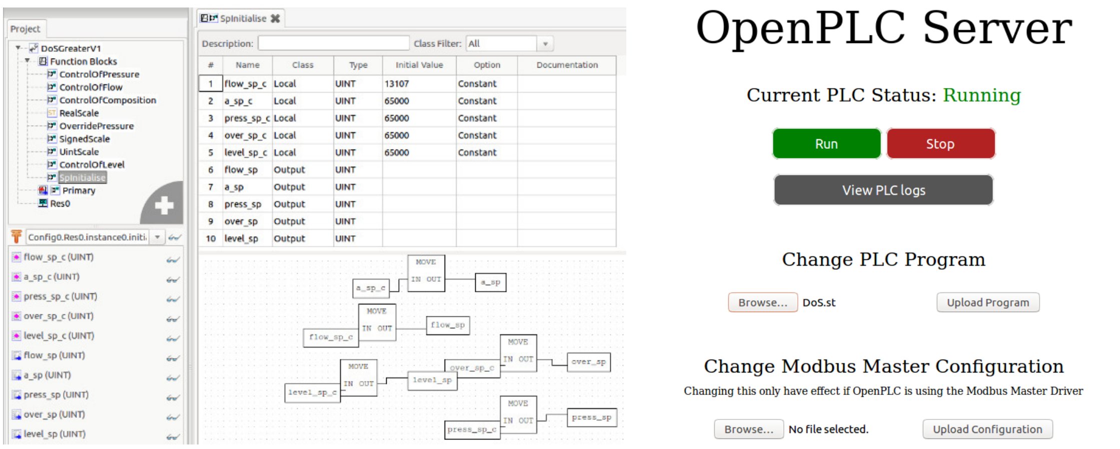
OpenPLC onto ChemicalPlant. As such, the previous OpenPLC projects were finally being applied to the ChemicalPlant simulator. The Ladder Logic had been programmed maliciously in order to conduct a manipulation of the control loop and launch attacks against the simulator. The ChemicalPlant simulator itself allowed for DoS attacks to be simulated in order to see what effect this had on the simulator and how much damage it could cause.

5.1.2 DoS

When launching DoS attacks from OpenPLC to the ChemicalPlant simulator, the primary objective was to cause the overall facility to overload, ultimately causing service disruption and to hinder the chemical plant's ability to run as expected.

5.1.2.1 Primary Test

Figure 49 Initiating the DoS attack



Description: Class Filter: All

#	Name	Class	Type	Initial Value	Option	Documentation
1	flow_sp_c	Local	UINT	13107	Constant	
2	a_sp_c	Local	UINT	65000	Constant	
3	press_sp_c	Local	UINT	65000	Constant	
4	over_sp_c	Local	UINT	65000	Constant	
5	level_sp_c	Local	UINT	65000	Constant	
6	flow_sp	Output	UINT			
7	a_sp	Output	UINT			
8	press_sp	Output	UINT			
9	over_sp	Output	UINT			
10	level_sp	Output	UINT			

OpenPLC Server

Current PLC Status: Running

Change PLC Program

Browse... DoS.st Upload Program

Change Modbus Master Configuration

Changing this only have effect if OpenPLC is using the Modbus Master Driver

Browse... No file selected. Upload Configuration

Figure 49 (a)

Figure 49 (b)

With this attack, the OpenPLC DoS project was utilised and tested on the simulator. Upon testing it, it proved to be detrimental to the chemical plant as it pushed the pressure values up to the point that the plant eventually exploded (once it reached 3100 points). This proved the attack was successful as it ultimately denied service to the chemical plant and left it inoperable.

Figure 50 Results of the DoS attack

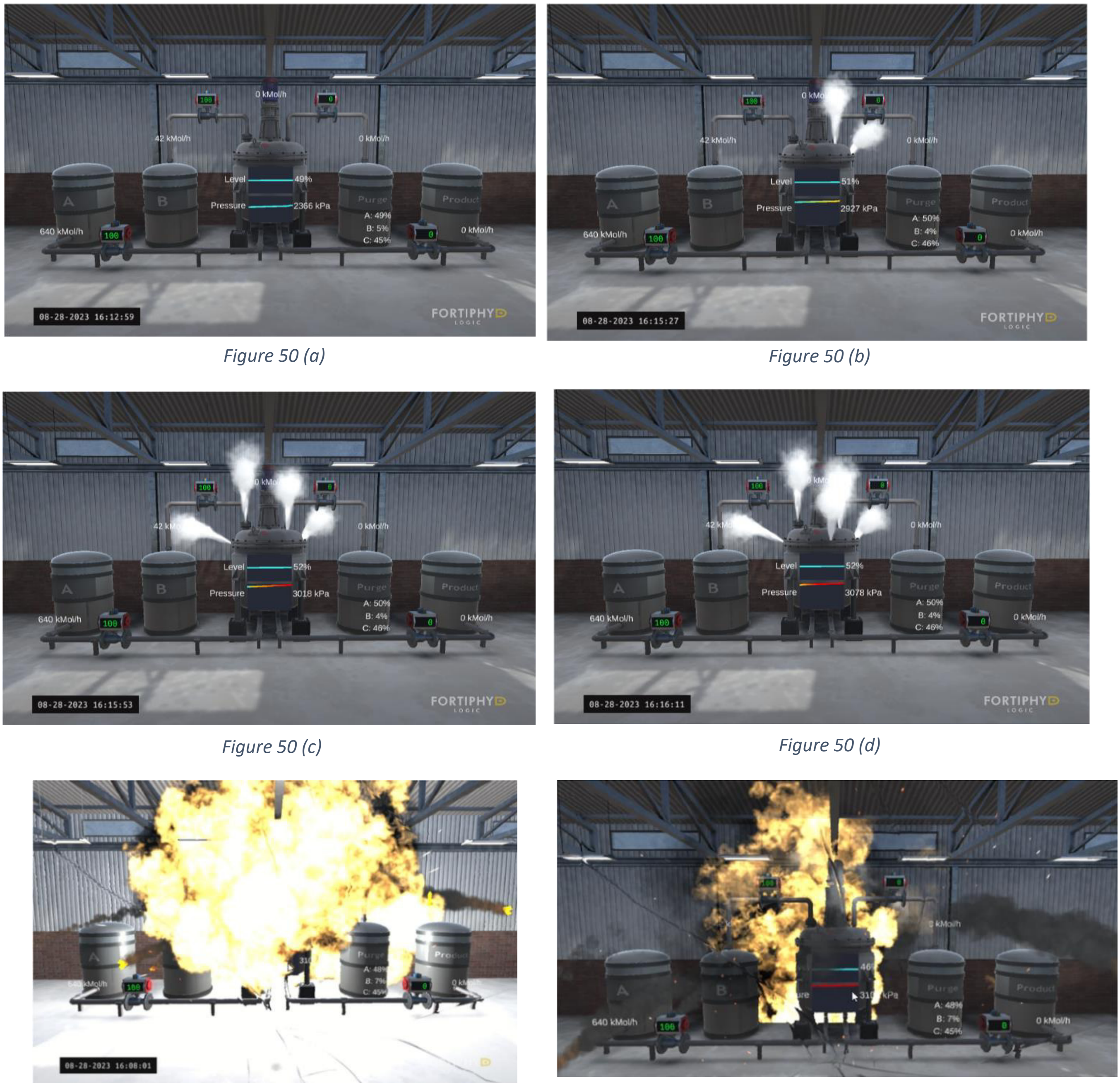


Figure 50 (a)

Figure 50 (b)

Figure 50 (c)

Figure 50 (d)

Figure 50 (e)

Figure 50 (f)

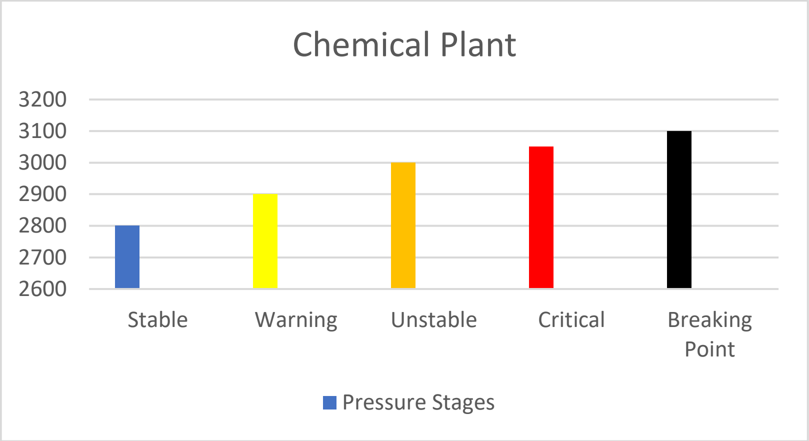


Figure 51 Graph of Pressure Stages

When uploading the DoS OpenPLC project, it steadily increases the pressure of the chemical plant, with it initially having a blue line indicator between roughly 2000 – 2900 before then entering a yellow state with multiple openings in the chamber signifying that the pressure is getting higher, before then going into the red state once it reaches 3000 and finally exploding once it reaches 3100.

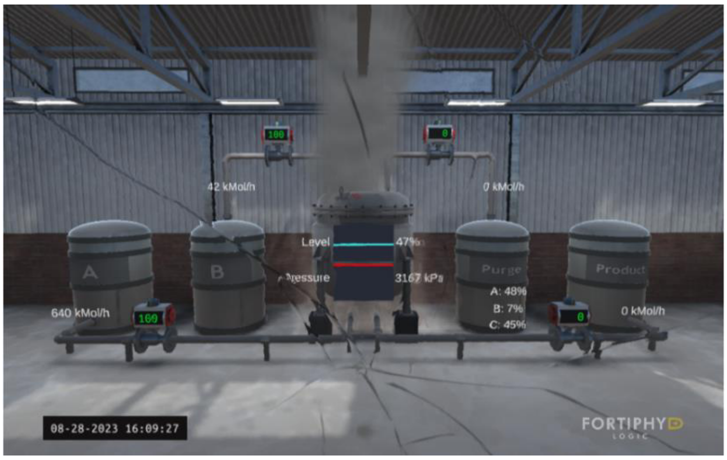


Figure 52 Aftermath of DoS attack

The reason that this inflicted such severe damage on the chemical plant was because the values within the "SpInitialise" were set to "65000" which was too much for the chemical plant to handle and thus placed it into a meltdown. In doing this, the attacker would be able to compromise the facility and potentially hinder its operational capacity as the necessary data that the facility needs to operate sufficiently would be erased.

5.1.3 Initiating the ransomware attack

The next scenario was to carry out a ransomware attack on the simulator. Due to the nature of the given attack, it did not seem possible to simulate a "true" ransomware attack, whereby an attacker steals confidential files and encrypts them before demanding payment in return for the files to be returned and decrypted.

As a result, another approach was taken to launch the ransomware attacks, whereby an attacker would extract the information/ data that is contained within the OpenPLC project and place it into an Excel file or Word document before deleting all values that were present within the project. This way, the overall principle and objective of the attack mirrored that of ransomware as it enabled an attacker to steal information that is crucial to the system (as the project could manipulate the simulator) and extract it before clearing all values. In doing so, the attacker could then demand a payment in order for the values to be returned.

Whilst this differed from traditional ransomware attacks, the strategy resulted in a very similar circumstance that accurately portrayed the typical procedure of a ransomware attack and would lead to significant difficulties in the chemical plant being able to undertake basic operations as the necessary data and information needed to do so would be missing. This would also make it incredibly challenging for the operators of the chemical plant to successfully analyse the data held within it and could potentially have further repercussions for the rest of the plant.

Figure 53 Initiating the Ransomware Attack

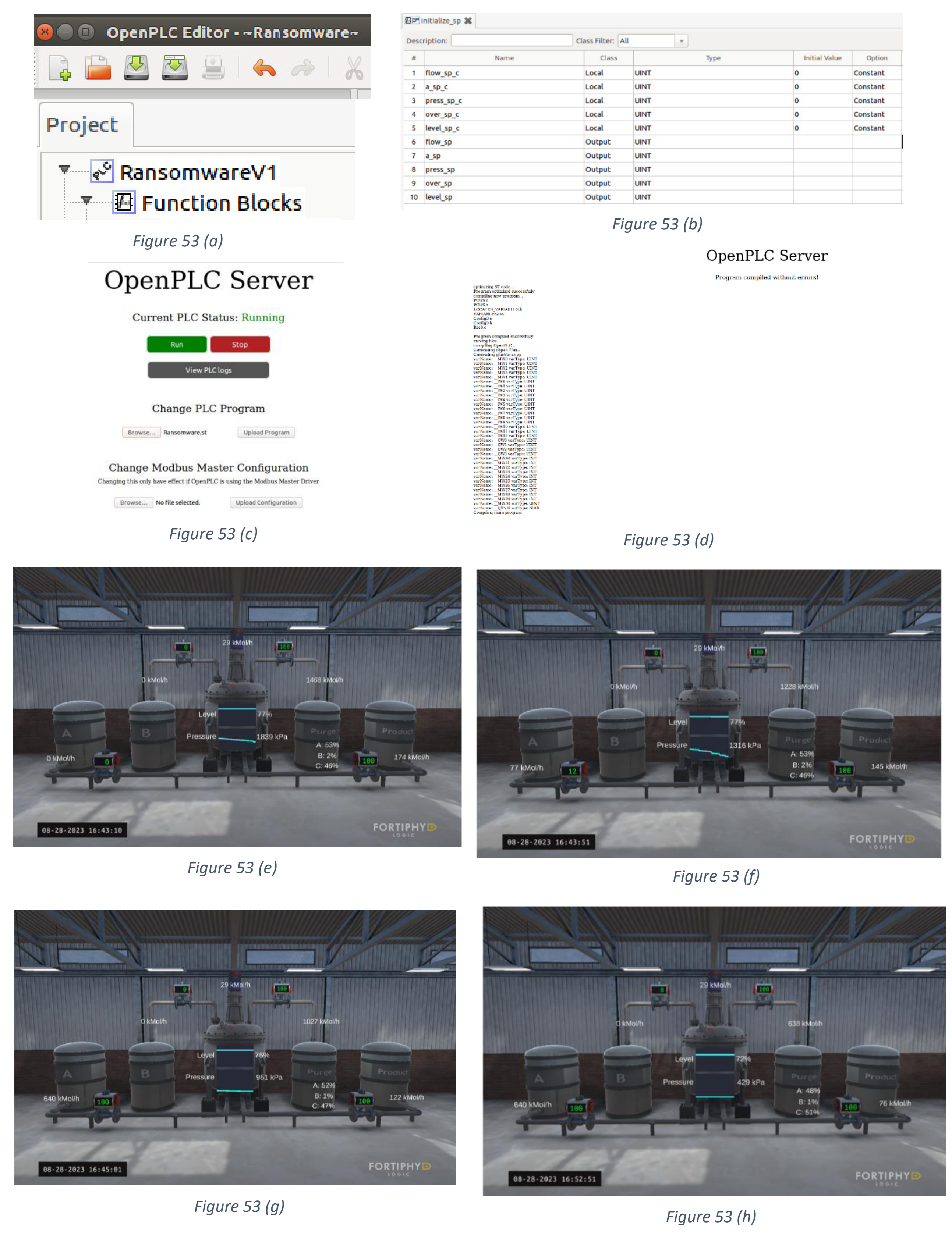


Figure 53 (a)

initialize_sp

Description: Class Filter: All

#	Name	Class	Type	Initial Value	Option
1	flow_sp_c	Local	UINT	0	Constant
2	a_sp_c	Local	UINT	0	Constant
3	press_sp_c	Local	UINT	0	Constant
4	over_sp_c	Local	UINT	0	Constant
5	level_sp_c	Local	UINT	0	Constant
6	flow_sp	Output	UINT		
7	a_sp	Output	UINT		
8	press_sp	Output	UINT		
9	over_sp	Output	UINT		
10	level_sp	Output	UINT		

Figure 53 (b)

OpenPLC Server

Current PLC Status: Running

Change PLC Program

Ransomware.st

Change Modbus Master Configuration

Changing this only have effect if OpenPLC is using the Modbus Master Driver

No file selected.

Figure 53 (c)

OpenPLC Server

Program compiled without errors!

```
optimizing ST code...
Program optimized successfully
compiling new program...
POUS.c
POUS.h
LOCATED_VARIABLES.h
VARIABLES.csv
Config0.c
Config0.h
Res0.c

Program compiled successfully
moving files...
compiling OpenPLC...
Generating object files...
Generating glueVars.cpp
varName: __MW0 varType: UINT
varName: __MW1 varType: UINT
varName: __MW2 varType: UINT
varName: __MW3 varType: UINT
varName: __MW4 varType: UINT
varName: __IW0 varType: UINT
varName: __IW1 varType: UINT
varName: __IW2 varType: UINT
varName: __IW3 varType: UINT
varName: __IW4 varType: UINT
varName: __IW5 varType: UINT
varName: __IW6 varType: UINT
varName: __IW7 varType: UINT
varName: __IW8 varType: UINT
varName: __IW9 varType: UINT
varName: __IW10 varType: UINT
varName: __IW11 varType: UINT
varName: __IW12 varType: UINT
varName: __QW0 varType: UINT
varName: __QW1 varType: UINT
varName: __QW2 varType: UINT
varName: __QW3 varType: UINT
varName: __MW20 varType: INT
varName: __MW21 varType: INT
varName: __MW22 varType: INT
varName: __MW23 varType: INT
varName: __MW24 varType: INT
varName: __MW25 varType: INT
varName: __MW26 varType: INT
varName: __MW27 varType: INT
varName: __MW28 varType: INT
varName: __MW29 varType: INT
varName: __MW30 varType: UINT
varName: __QX5_0 varType: BOOL
Compiling main program
```

Figure 53 (d)

Figure 53 (e)

Figure 53 (f)

Figure 53 (g)

Figure 53 (h)

As a result, when undertaking a ransomware attack on the chemical plant, another OpenPLC project was created (and named "Ransomware") and utilised the same features as the previous ones. However, the values were set to 0 for the final function and this caused the pressure in the chemical plant to drop dramatically. Whilst it did not turn the pressure off completely, it did significantly affect the chemical plant as it meant that it could no longer increase its pressure and put its pressure at a very low state.

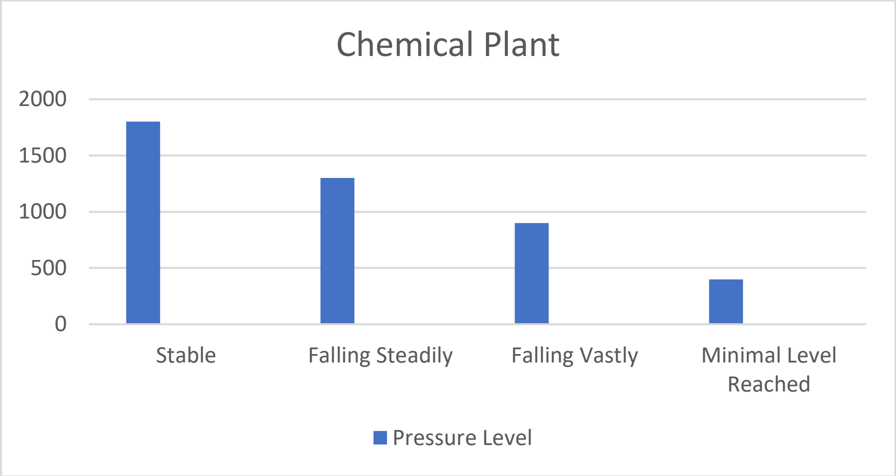


Figure 54 Graph of Pressure Falling

Due to this, once the ransomware attack had taken place, various data/ values that were important to the simulator were taken away whilst the original copies were erased. This had disastrous effects on the simulator as, without the given data/ values, the simulator was unable to run sufficiently.

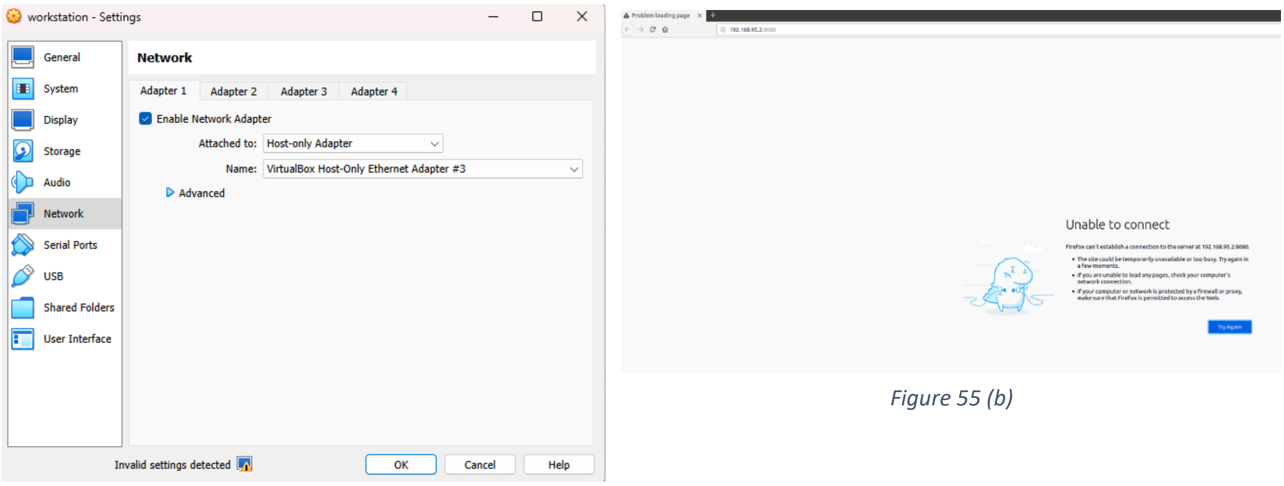
5.2 Applying Rules Formation (Mitigation Methods) to the Cyber-Attacks

After the attacks had been carried out, it was then necessary to initiate methods of recovery/ mitigation to analyse ways of reducing the impact of the attacks and understanding how the damage caused by the attacks could be subsidised in order to minimalize the effect they have on the simulator. These mitigation methods were directed from the test cases produced previously. As such, the mitigation methods were applied to the given simulator. These were the overall embodiment of the **rules formation** and came in the form of step-by-step procedures as to what methods could be applied to the scenarios.

5.2.1 IP Blocking/ Network Alteration

When it came to the DoS attacks, the first method of mitigation was IP blocking/ network alteration in which the IP of the attacker was blocked to prevent them from being able to send malicious traffic over. With the given scenario, the workstation VM had its "Host-Only Network Adapter" changed from 2 to 3. This was because this VM contained the OpenPLC project that was used to initiate the attacks on the simulator.

Figure 55 Altering Network Settings



workstation - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #3

Invalid settings detected

Figure 55 (a)

Unable to connect

Firefox can't establish a connection to the server at 192.168.95.2:8080.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figure 55 (b)

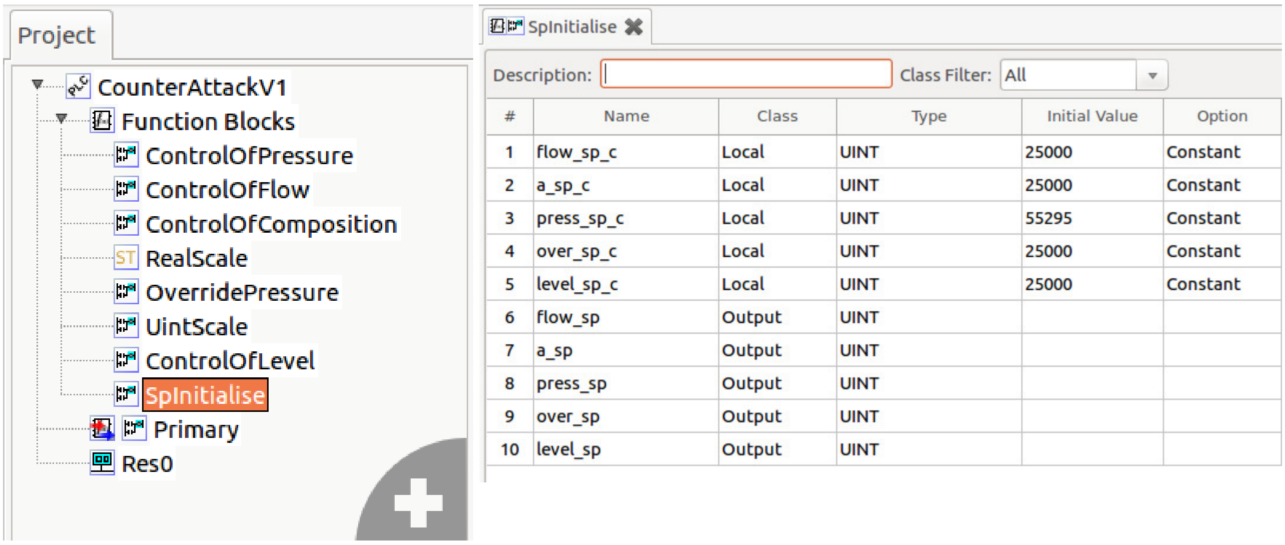
Although this is different from traditional IP address restriction, this was useful at blocking the workstation VM from being able to successfully connect to the OpenPLC server on the web and thus prevent it from being able to launch attacks against the simulator VM.

Name of Test	Inititating First Recovery Method against DoS			
ID of Test Case	01			
Name of Tester	Saleh Mohamed			
Description of Test Case	To initiate first method of recovery/ mitigation and see if it can successfully block or reduce the damage from a DoS attack			
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)			
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop			
Scenario of Test Case	To initiate first recovery method/ mitigation by blocking certain IP addresses/ Altering the Network			
ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
01	To put the first recovery method into use	Once attack is underway, restrict the IP addresses/ Alter Network	The DoS should be mitigated as the number of available IPs will be reduced or network may be altered	Result = Success

Figure 56 – First Mitigation Success

5.2.2 Counteracting the Attack

Furthermore, the second mitigation method revolved around counteracting the attack. In the event of a DoS attack, another attack could be used to counter it by sending new values to the chemical plant which could counteract the previous values sent from the first attack. As a result, another OpenPLC project was produced that had lower values than the other DoS projects and was intended to balance the pressure from the previous DoS attack. This was called “CounterAttack”.



Project

- CounterAttackV1
  - Function Blocks
    - ControlOfPressure
    - ControlOfFlow
    - ControlOfComposition
    - RealScale
    - OverridePressure
    - UintScale
    - ControlOfLevel
    - SpInitialise
  - Primary
  - Res0

SpInitialise

Description: Class Filter: All

#	Name	Class	Type	Initial Value	Option
1	flow_sp_c	Local	UINT	25000	Constant
2	a_sp_c	Local	UINT	25000	Constant
3	press_sp_c	Local	UINT	55295	Constant
4	over_sp_c	Local	UINT	25000	Constant
5	level_sp_c	Local	UINT	25000	Constant
6	flow_sp	Output	UINT		
7	a_sp	Output	UINT		
8	press_sp	Output	UINT		
9	over_sp	Output	UINT		
10	level_sp	Output	UINT		

Figure 57 – CounterAttack OpenPLC Project

Figure 58 Second DoS attack

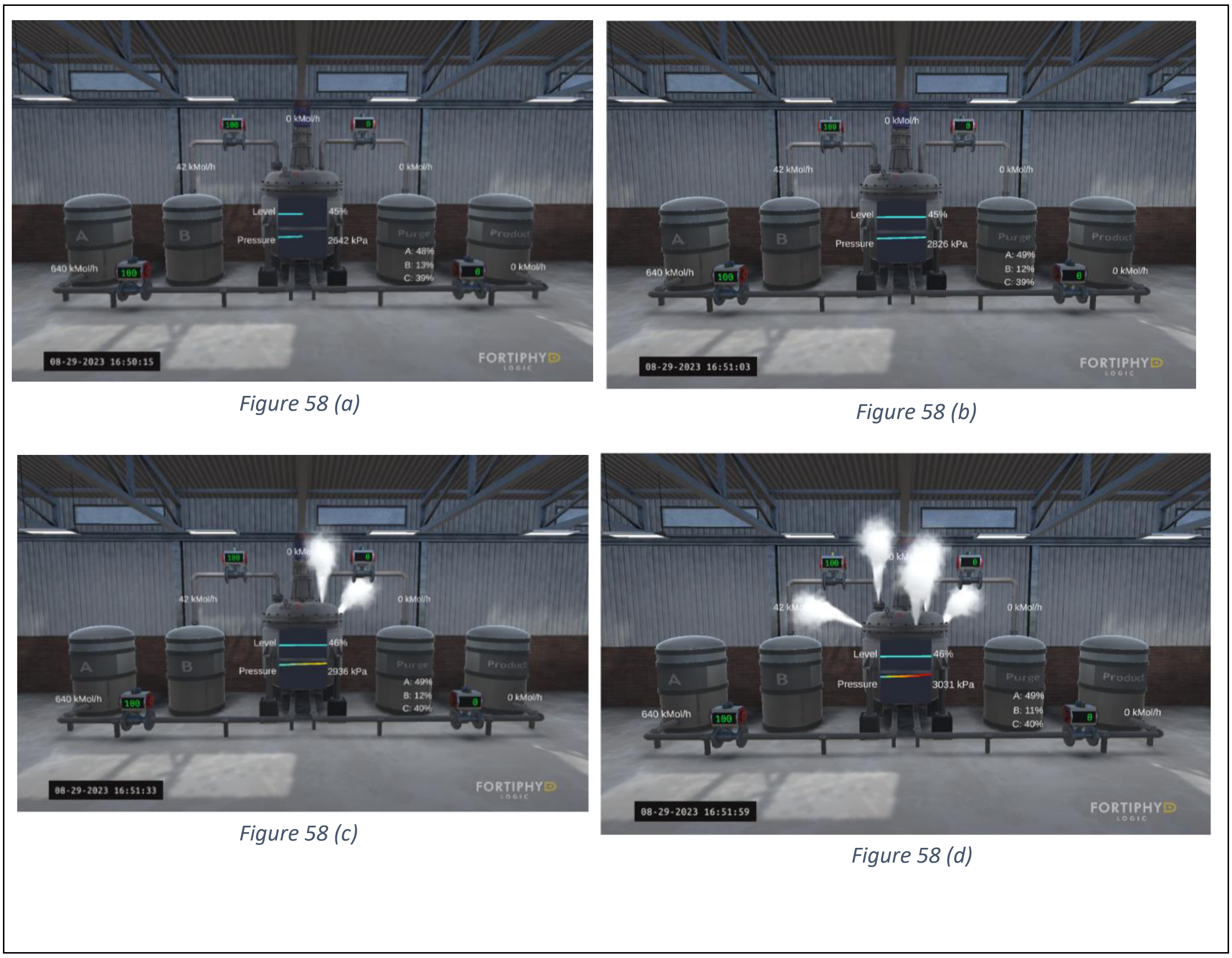


Figure 58 (a)

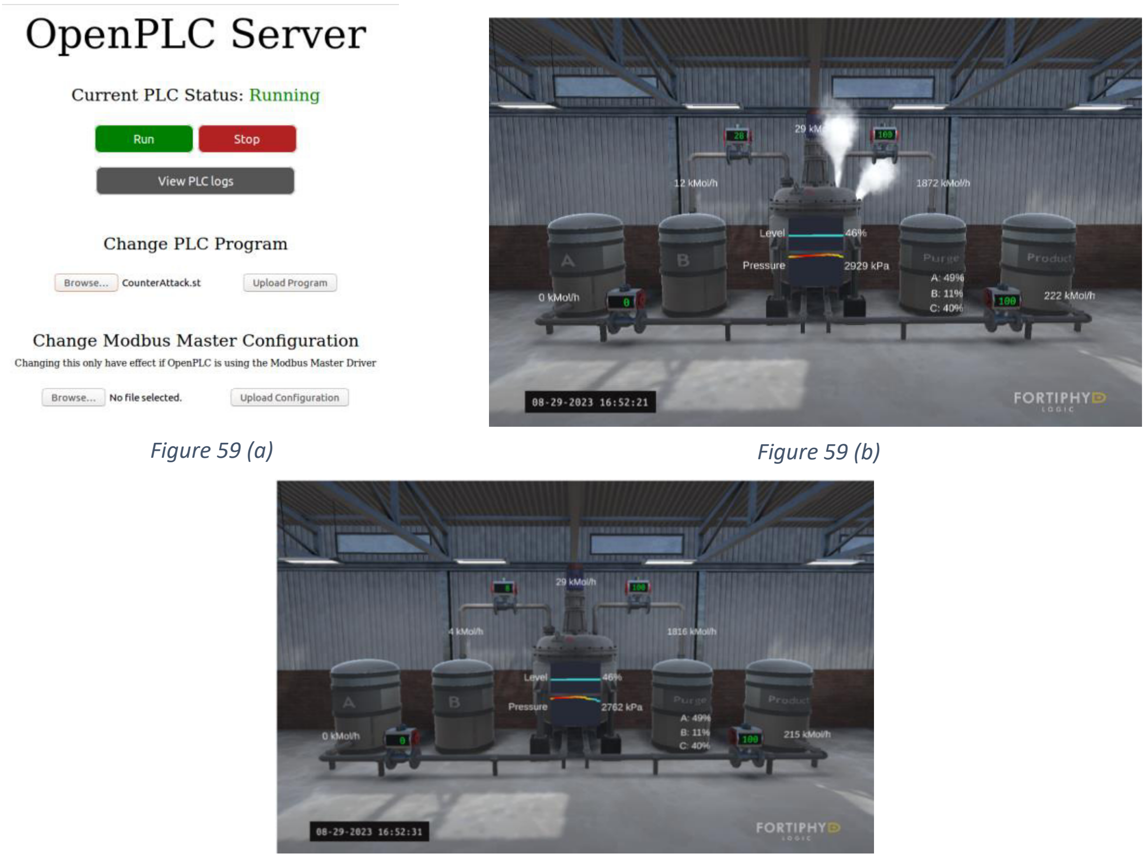
Figure 58 (b)

Figure 58 (c)

Figure 58 (d)

The DoS attack was then uploaded to the chemical plant.

Figure 59 Launching Counterattack



OpenPLC Server

Current PLC Status: Running

Run Stop

View PLC logs

Change PLC Program

Browse... CounterAttack.st Upload Program

Change Modbus Master Configuration

Changing this only have effect if OpenPLC is using the Modbus Master Driver

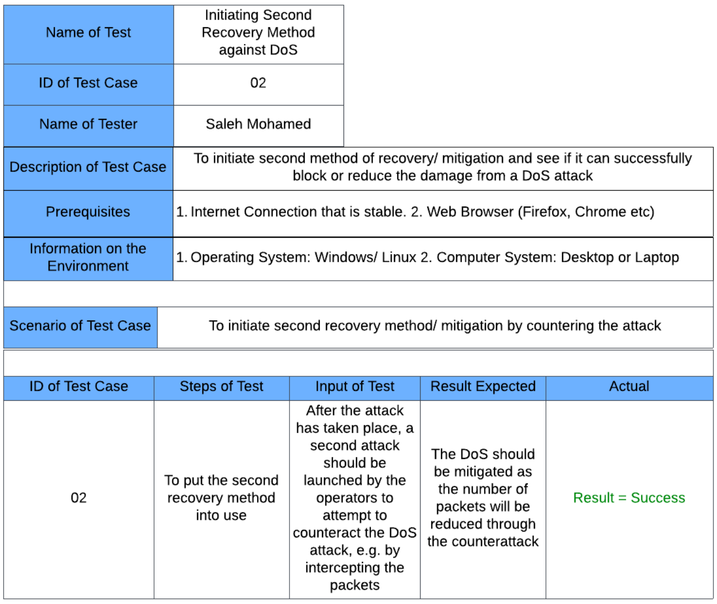
Browse... No file selected. Upload Configuration

Figure 59 (a)

Figure 59 (b)

Figure 59 (c)

When uploading the DoS attack onto the chemical plant, it pushes it to its tipping point, however, when uploading the CounterAttack file, the pressure decreases rapidly. Thus, stabilising the chemical plant. This indicates that the pressure can be re-stabilised during an attack and prevent the chemical plant from exploding.



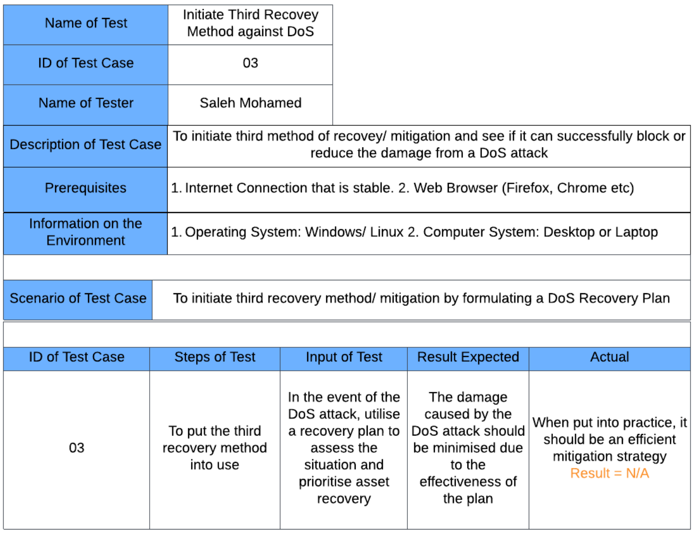
Name of Test	Initiating Second Recovery Method against DoS
ID of Test Case	02
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate second method of recovery/ mitigation and see if it can successfully block or reduce the damage from a DoS attack
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate second recovery method/ mitigation by countering the attack

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
02	To put the second recovery method into use	After the attack has taken place, a second attack should be launched by the operators to attempt to counteract the DoS attack, e.g. by intercepting the packets	The DoS should be mitigated as the number of packets will be reduced through the counterattack	Result = Success

Figure 60 – Second Mitigation Success

5.2.3 Formulating a DoS Attack Recovery Plan

Likewise, the third and final mitigation method for DoS attacks was establishing a response plan. This can include organising a special team that can formulate a plan in response to the DoS attack taking place and decide upon the best course of action to take such as by prioritising essential assets and resources to ensure that they do not get negatively impacted by the attack. These assets could include the OpenPLC files which have all the necessary data related to the simulator and placing them into certain directories that only certain users can access or have knowledge of. This will require efficient communication between different members of the team as well as being able to act accordingly in response to the attack. **Unfortunately, this strategy could not be validated on the given setup.**



Name of Test	Initiate Third Recovey Method against DoS
ID of Test Case	03
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate third method of recovey/ mitigation and see if it can successfully block or reduce the damage from a DoS attack
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate third recovery method/ mitigation by formulating a DoS Recovery Plan

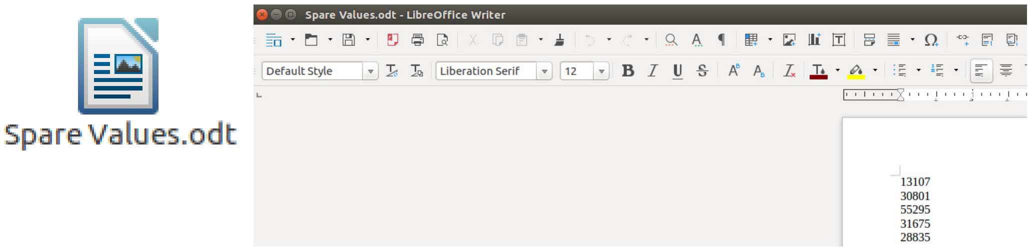
ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
03	To put the third recovery method into use	In the event of the DoS attack, utilise a recovery plan to assess the situation and prioritise asset recovery	The damage caused by the DoS attack should be minimised due to the effectiveness of the plan	When put into practice, it should be an efficient mitigation strategy Result = N/A

Figure 61 Third Mitigation Unable to Validate

5.2.4 Creating Backups

For the ransomware mitigation methods, the first procedure revolved around checking to see if backups of the data stored within the chemical plant had been put in place so that if the original data was erased/ deleted, the simulator would have backups to turn to. In the event that this was the case, this led to huge benefits in the simulator as it would not be required to give in to the payment demand whilst ensuring that the primary data was safe and secure.

With this, a new document was created and with it, the core values of the OpenPLC project were copied into it in order to provide a safe and secure backup in case the values in the main project were to get removed or deleted. This was highly useful, as the data within the document could simply be inserted back into the project in the event that it was removed from the main project.



13107
30801
55295
31675
28835

Figure 62 Creating backups

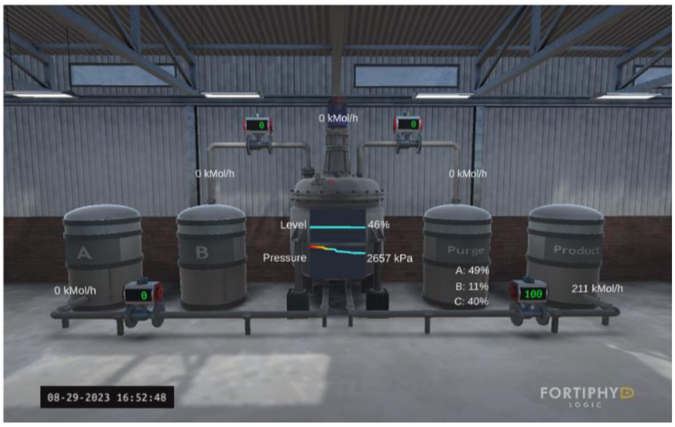
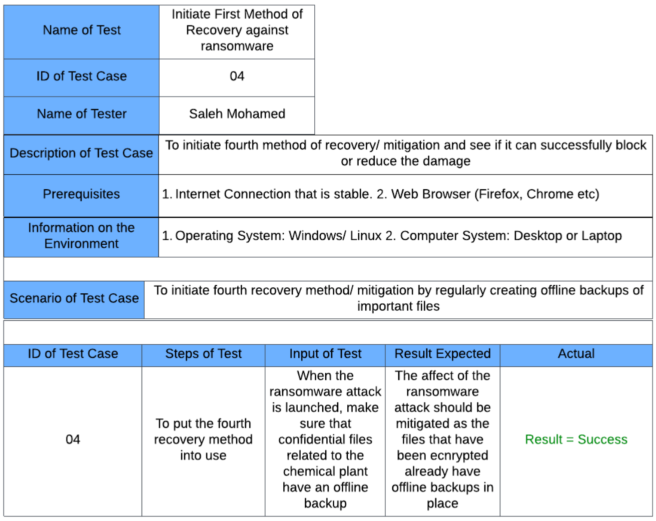


Figure 63 Values re-stabilising



Name of Test	Initiate First Method of Recovery against ransomware
ID of Test Case	04
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate fourth method of recovery/ mitigation and see if it can successfully block or reduce the damage
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate fourth recovery method/ mitigation by regularly creating offline backups of important files

ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
04	To put the fourth recovery method into use	When the ransomware attack is launched, make sure that confidential files related to the chemical plant have an offline backup	The affect of the ransomware attack should be mitigated as the files that have been ecnrypted already have offline backups in place	Result = Success

Figure 64 Fourth Mitigation Success

5.2.5 Preventing Access to the System/ Simulator

The second procedure related to preventing the ransomware or attacker from being able to access the simulator. In this instance, the attack could be prevented altogether by blocking the ransomware/ attacker from gaining access to the simulator. This could work in a similar way to the first mitigation for the DoS attack. As the simulator itself did not contain a built-in security feature, the best method of denying access to it would be to block users from accessing the IP address “192.168.95.10”.

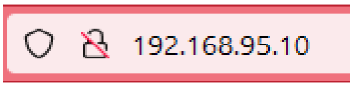
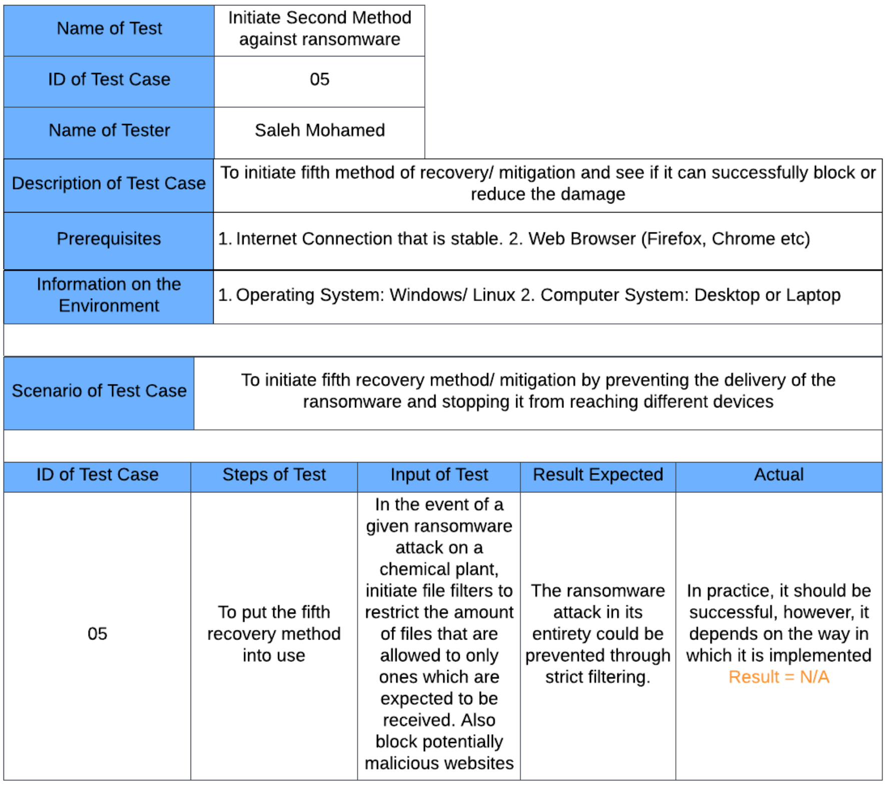


Figure 65 IP address of simulator

Similarly, to the last DoS mitigation, it was not possible to formally validate this strategy.



Name of Test	Initiate Second Method against ransomware
ID of Test Case	05
Name of Tester	Saleh Mohamed
Description of Test Case	To initiate fifth method of recovery/ mitigation and see if it can successfully block or reduce the damage
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop
Scenario of Test Case	To initiate fifth recovery method/ mitigation by preventing the delivery of the ransomware and stopping it from reaching different devices

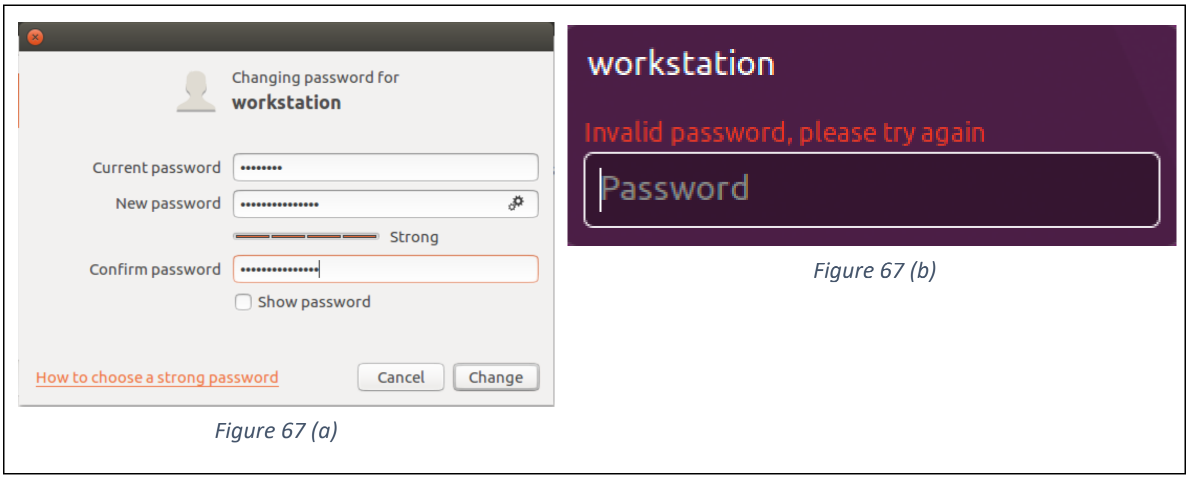
ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
05	To put the fifth recovery method into use	In the event of a given ransomware attack on a chemical plant, initiate file filters to restrict the amount of files that are allowed to only ones which are expected to be received. Also block potentially malicious websites	The ransomware attack in its entirety could be prevented through strict filtering.	In practice, it should be successful, however, it depends on the way in which it is implemented Result = N/A

Figure 66 Fifth Mitigation Unable to Validate

5.2.6 Restricting the attacker from being able to access the device

The third procedure revolves around preventing the launching of the ransomware attack in the first place and stopping it from being able to reach the targeted devices. It also includes stopping an attacker from reaching the devices and hindering their ability to successfully operate on the device. One method for this would be to change the default password of the workstation VM and provide it with a strong and relatively complex one in order to prevent the attacker from being able to access the VM. The method could revolve around giving the password various letters, numbers and symbols to make it sophisticated.

Figure 67 Restricting Access to Device



Changing password for
workstation

Current password: ••••••••

New password: •••••••••••••••

Strong

Confirm password: •••••••••••••••

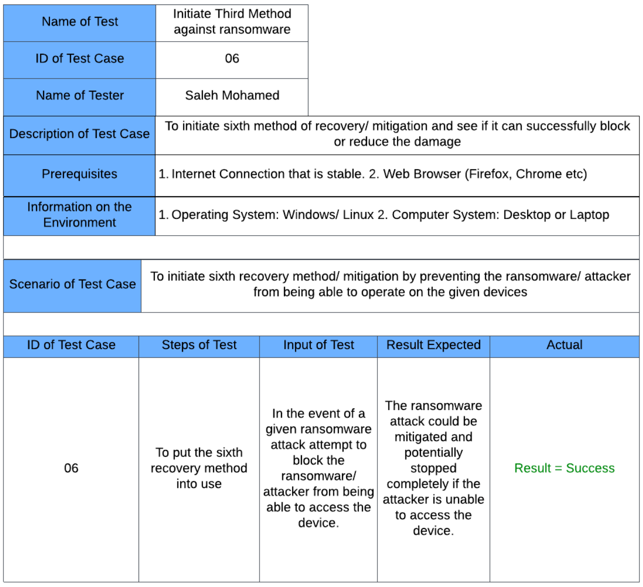
□ Show password

Figure 67 (a)

workstation

Invalid password, please try again

Figure 67 (b)



Name of Test	Initiate Third Method against ransomware			
ID of Test Case	06			
Name of Tester	Saleh Mohamed			
Description of Test Case	To initiate sixth method of recovery/ mitigation and see if it can successfully block or reduce the damage			
Prerequisites	1. Internet Connection that is stable. 2. Web Browser (Firefox, Chrome etc)			
Information on the Environment	1. Operating System: Windows/ Linux 2. Computer System: Desktop or Laptop			
Scenario of Test Case	To initiate sixth recovery method/ mitigation by preventing the ransomware/ attacker from being able to operate on the given devices			
ID of Test Case	Steps of Test	Input of Test	Result Expected	Actual
06	To put the sixth recovery method into use	In the event of a given ransomware attack attempt to block the ransomware/ attacker from being able to access the device.	The ransomware attack could be mitigated and potentially stopped completely if the attacker is unable to access the device.	Result = Success

Figure 68 Sixth Mitigation Success

5.2.7 Alternative Mitigation Methods

As well as the mitigation methods discussed above, it would also be useful if other solutions such as **rate limiting**, **upstream filtering** and utilising anti-virus/ anti-ransomware tools were put to use.

However, unfortunately, due to the given setup, there was uncertainty as to how they would be put into practice and thus were not tested or used.

5.3 Analysing the Results

After obtaining the findings from launching the various cyber-attacks, it became necessary to then conduct an analysis of the attacks to have a clear understanding as to whether or not they were effective at carrying out their intended purpose (that being causing disruptions to the simulator and hinder its ability to operate as normal) and how successful they were.

From carrying out the attacks on the chemical plant, it was clear that the first attack was very successful and effective as it resulted in the chemical plant going into a meltdown and eventually exploding, causing widespread damage and disruption and ultimately denying service.

Moreover, when it came to the ransomware attack, by altering the values to 0 in the OpenPLC project and uploading it to attack the chemical plant simulator, it resulted in the pressure decreasing rapidly and ultimately destabilising the chemical plant. Whilst this did not cause the chemical plant to shut down or have the pressure reach 0, it did have negative effects on the plant as it still led to the pressure reaching a very low level and potentially hindering standard operations.

This also included checking whether or not the simulator was able to recover from these attacks. E.g., if the simulator was disrupted by the DoS attack or if the simulator could recover from its values being deleted and continue undertaking standard operations.

5.4 Effectiveness of Mitigation Strategies

As well as analysing the results of the attacks carried out on the chemical plant and understanding how effective they were, it was also important and necessary to conduct an analysis of the various mitigation strategies employed in order to minimise the damage caused by the cyber-attacks and reduce their impact on the chemical plant. This was because the mitigation strategies were crucial in enabling the chemical plant to be able to recover from a given cyber-attack and devise measures to reduce the impact of the attack.

Due to this, each mitigation strategy formulated in the test cases was put to use and analysed appropriately in order to see which one was the most effective and suitable. This also put the rules formation into practice. The first mitigation strategy that was analysed was IP Blocking/ Network Alteration. This proved to be effective overall as when applied, it prevents an attacker from utilising the workstation VM to upload the malicious OpenPLC file onto the OpenPLC server.

The second mitigation method which was analysed revolved around counteracting the attack that was initiated. This also proved successful and efficient as it was able to stop the chemical plant from reaching boiling point and exploding.

Moreover, the last mitigation method for DoS attacks was initiating a plan that revolved around how a team could prioritise asset recovery in the event of a DoS attack. Unfortunately, due to the nature of the scenario, it was not possible to produce the actual plan and thus this was not as effective as the other mitigation methods.

Similarly, when it came to mitigating the damage caused by the ransomware attack, the first method of mitigation revolved around ensuring there were backups in place in order to restore previous iterations of data that had been lost or deleted. This method proved highly useful when being applied to the attack scenario as it enabled swift recovery of data after having placed the data in a Word document.

Likewise, the second method of mitigation for the ransomware attack related to denying access to all users who are not permitted to access the simulator. Whilst this mitigation method could be effective in theory, it was not possible to put it into practice in the given scenario.

Furthermore, the last ransomware mitigation method included preventing the ransomware/ attacker from being able to run on the device. As the given attack, was slightly different from traditional ransomware, instead of preventing it from running on the device (and specifically the simulator), the mitigation method revolved around preventing unauthorised users from being able to operate on the main Workstation VM. This included making the password complex. This ultimately proved effective.

Overall, the mitigation strategies were a success as the vast majority of them had successful results and provided efficient means of mitigating the attacks from a DoS and ransomware attack.

5.5 Summary

This chapter included crucial elements of the thesis as it described the attacks that were initiated on the simulator as well as the findings discovered from undertaking the attack scenarios and analysing the results obtained before indicating the effects they had on the simulator as well as how the simulator could recover from them.

Chapter 6 Conclusion

6.1 Conclusion

This thesis produced a rules formation that was adapted and developed from past and current formations in order to ensure that it can be applied to cyber resiliency metrics in industrial control systems efficiently including providing useful ways of enabling recovery methods as well as ways of being able to adapt from various forms of cyber-attacks including Denial of Service and ransomware. Existing literature primarily focused on a wide range of cyber-attacks on industrial control systems and how they can affect them, which generalised the existing information with the side effect being the diversity of the various cyber-attacks can make it more difficult to enforce cyber resiliency metrics to each one of them. Whereas this thesis takes into account more specific cyber-attacks and the best ways of recovering from them as well as building off of previous literature.

The process began by first identifying the most critical cyber-attacks to industrial control systems in this case it was determined that Denial of Service and ransomware before then determining which critical infrastructure (i.e. smart grids, chemical plants and nuclear power plants) was most at risk of these attacks. An analysis was undertaken to deduce the capability of an attacker and as a result, the probability of an attack as well as the effect of the given attack. It then revolved around developing various use cases and test cases for the given scenario before ultimately utilising an open-source tool to connect to a simulator known as ChemicalPlant and finally launching cyber-attacks (DoS and ransomware) onto the simulator and analysing what effects these had on the simulator. Moreover, the process then included producing the results from the attacks and undertaking an evaluation of the given results. Past studies looked into a fairly wide range of areas in the industry, but this thesis prioritised looking into chemical plants, smart grids as well as nuclear power plants. Not every type of industry may be targeted by the particular state-of-the-art attacks and so the focus was derived to industrial control systems in particular due to the fact that they are the primary target of these given cyber-attacks. Furthermore, although industrial control systems could be targeted by a number of cyber-attacks, for the purpose of this thesis, two types of attacks in particular were investigated, being Denial of Service and ransomware.

One of the initial challenges early on was finding appropriate information including examples to assist with the required research. In addition, it was also relatively difficult to choose the most appropriate open-source tool for the given project. Finally, understanding the best methods of mitigating the damage caused by the attacks also proved to be a challenge as there was uncertainty as to which method was the most efficient and applicable at mitigating the attack.

6.2 Future Work

For future work, the project could take into account a wider range of attack types on industrial control systems rather than focusing solely on Denial of Service and ransomware. Furthermore, it would also be more useful to widen the scope of the types of industrial control systems being analysed, and instead of simply prioritising chemical plants, smart grids and nuclear power plants, it would be beneficial to look at other types of systems as well. Thus, another study that could take place in the future, could include and encompass a wider area to analyse.

6.3 Learning Reflection

Throughout the course of the project, my knowledge and understanding of cyber resiliency metrics greatly improved and expanded. One of the biggest challenges that I encountered at first was understanding the way in which cyber resiliency metrics can be applied to industrial control systems as well as being able to apply a rules formation. Furthermore, it was also relatively challenging to utilise an open-source tool to carry out DoS and ransomware attacks and make use of a simulator to initiate the attacks on a chemical plant. Methods of undertaking critical analysis were produced and improved through the use of reviewing a range of scholarly and academic papers. During the development and production of the given project, one of the most significant skills I acquired was effective time management and organisational skills when undertaking each of the tasks through each stage of the given project. Time management was a crucial skill that I was able to improve as I was able to appropriately manage my time for a given task to ensure that each task was provisioned enough time to be completed to a high standard. Moreover, in relation to practical hands-on skills, I was able to demonstrate my ability through utilising the open source tool OpenPLC and connecting it to a simulator called ChemicalPlant to simulate Denial of Service and ransomware attacks and provide validation to my test cases. Ultimately, this dissertation provides an in-depth analysis of implementing a rules formation with regards to cyber resiliency metrics when being applied to industrial control systems as well as explaining two severe attacks to industrial control systems, Denial of Service and ransomware.

Due to the work completed in this dissertation, I was able to acquire a vast amount of knowledge in relation to cyber resiliency metrics as well as industrial control systems and the attacks on them. In addition, I also gained experience in applying a rules formation to the cyber resiliency metrics including the steps that can be taken to recover from a cyber-attack and methods of being able to adapt to them. Furthermore, I was able to put my hands-on practical skills to the test through the implementation of the open-source tool and being able to connect it to the ChemicalPlant simulator as well as being able to simulate cyber-attacks. This in itself provided me with hands-on experience with numerous software applications and allowed me to both, refine my skills in practical implementation and acquire new skills with the given applications.

References

Bodeau, D.J., Graubart, R.D., McQuaid, R.M. and Woodill, J., 2018. *Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods*. Mitre Corp Bedford Ma Bedford United States.

https://www.nopsec.com/resources/whitepapers-ebooks/the-cyber-resilience-framework-and-index-a-blueprint-to-improve-the-organizations-cyber-attack-defendability/

Linkov, I. and Kott, A., 2019. Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, pp.1-25.

Alshammari, T.S. and Singh, H.P., 2018. Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research*, *6*(12).

https://cybermagazine.com/articles/ddos-protection-market-to-grow-amid-increase-in-attacks

Galiardi, M., Gonzales, A., Thorpe, J., Vugrin, E., Fasano, R. and Lamb, C., 2020, August. Cyber resilience analysis of scada systems in nuclear power plants. In *International Conference on Nuclear Engineering* (Vol. 83778, p. V002T08A003). American Society of Mechanical Engineers.

Ghiasi, M., Dehghani, M., Niknam, T. and Kavousi-Fard, A., 2020. Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power system. *Network*, *1*(1).

Ylmaz, E.N., Ciylan, B., Gönen, S., Sindiren, E. and Karacayılmaz, G., 2018, April. Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect. In *2018 6th international istanbul smart grids and cities congress and fair (icsg)* (pp. 81-85). IEEE.

Bhatia, S., Kush, N.S., Djamaludin, C., Akande, A.J. and Foo, E., 2014. Practical modbus flooding attack and detection. In *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]* (pp. 57-65). Australian Computer Society.

Zhang, H., Min, Y., Liu, S., Tong, H., Li, Y. and Lv, Z., 2023. Improve the Security of Industrial Control System: A Fine-Grained Classification Method for DoS Attacks on Modbus/TCP. *Mobile Networks and Applications*, pp.1-14.

Hasan, M.K., Habib, A.A., Islam, S., Safie, N., Abdullah, S.N.H.S. and Pandey, B., 2023. DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports*, *9*, pp.1318-1326.

Alladi, T., Chamola, V. and Zeadally, S., 2020. Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, pp.1-8.

Drias, Z., Serhrouchni, A. and Vogel, O., 2015, August. Analysis of cyber security for industrial control systems. In *2015 international conference on cyber security of smart cities, industrial control system and communications (ssic)* (pp. 1-8). IEEE.

Khoei, T.T., Slimane, H.O. and Kaabouch, N., 2022. A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. *arXiv preprint arXiv:2207.07738*.

Kim, Y., Hakak, S. and Ghorbani, A., 2023. Smart grid security: Attacks and defence techniques. *IET Smart Grid*, *6*(2), pp.103-123.

Stoyle, E., 2019. Hexion, Momentive and Norsk Hydro all hit by ransomware cyber-attacks. Chemistry World, 3010328

Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, p.107094.

Kumar, R., Kela, R., Singh, S. and Trujillo-Rasua, R., 2022. APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, *37*, p.100521.

Al-Abassi, A., Karimipour, H., Dehghantanha, A. and Parizi, R.M., 2020. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, *8*, pp.83965-83973.

Zimba, A., Wang, Z. and Chen, H., 2018. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *Ict Express*, *4*(1), pp.14-18.

M. Robinson, "The SCADA Threat Landscape," in Celtics Spings, Newport, Celtics Spings, 2013.

Lubin, A., 2022. The law and politics of ransomware. *Vand. J. Transnat'l L.*, *55*, p.1177.

Symantec Corporation, "Internet Security Threat Report," Symantec Security Threat Report, vol. 22, no. April 2017, 2017

Butt, U.J., Abbod, M., Lors, A., Jahankhani, H., Jamal, A. and Kumar, A., 2019, January. Ransomware Threat and its Impact on SCADA. In *2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3)* (pp. 205-212). IEEE.

Everett, C., 2016. Ransomware: to pay or not to pay?. *Computer Fraud & Security*, *2016*(4), pp.8-12.

Gazzan, M., Alqahtani, A. and Sheldon, F.T., 2021, January. Key Factors Influencing the Rise of Current Ransomware Attacks on Industrial Control Systems. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1417-1422). IEEE.

M. P. Calif, "Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019," CyberSecurity Ventures, 14 November 2017. [Online]. Available: https://cybersecurityventures.com/ransomware-damagereport-2017-part-2/.

Statista, "The Statistics Portal," Statista, 1 January 2019. [Online]. Available: https://www.statista.com/topics/4136/ransomware/.

Malkawe, R., Qasaimeh, M., Ghanim, F. and Ababneh, M., 2019, December. Toward an early assessment for Ransomware attack vulnerabilities. In *Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems* (pp. 1-7).

D.Bisson, "Half of american ransomware victims have paid the ransom, reveals study." https://www.tripwire.com/state-of-security/half-of-american-ransomware-victims-have-paid-the-ransom-reveals-study

Trend Micro, "Boosting Impact for Profit: Evolving Ransomware Techniques for Targeted Attacks." https://www.trendmicro.com/en_us/research/20/i/boosting-impact-for-profit-evolving-ransomware-techniques-for-targeted-attacks.html

Anna Delaney, "Analysis: Why Ransomware Gangs Getting Bigger Payoffs." https://www.bankinfosecurity.com/interviews/analysis-ransomware-gangs-getting-bigger-payoffs-i-4752

Zhang, Y., Sun, Z., Yang, L., Li, Z., Zeng, Q., He, Y. and Zhang, X., 2020, December. All your PLCs belong to me: ICS ransomware is realistic. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 502-509). IEEE.

Haque, M.A., De Teyou, G.K., Shetty, S. and Krishnappa, B., 2018, November. Cyber resilience framework for industrial control systems: concepts, metrics, and insights. In *2018 IEEE international conference on intelligence and security informatics (ISI)* (pp. 25-30). IEEE.

Kott, A. and Linkov, I., 2021. To improve cyber resilience, measure it. *arXiv preprint arXiv:2102.09455*.

Chaves, A., Rice, M., Dunlap, S. and Pecarina, J., 2017. Improving the cyber resilience of industrial control systems. *International journal of critical infrastructure protection*, *17*, pp.30-48.

Bodeau, D. and Graubart, R., 2016. *Cyber resilience metrics: Key observations*. MITRE CORP MCLEAN VA.

Jacobs, N., Hossain-McKenzie, S. and Vugrin, E., 2018, August. Measurement and analysis of cyber resilience for control systems: An illustrative example. In *2018 Resilience Week (RWS)* (pp. 38-46). IEEE.

Haque, M.A., Shetty, S. and Krishnappa, B., 2019, May. ICS-CRAT: a cyber resilience assessment tool for industrial control systems. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)* (pp. 273-281). IEEE.

Segovia, M., Rubio-Hernan, J., Cavalli, A.R. and Garcia-Alfaro, J., 2020, November. Cyber-resilience evaluation of cyber-physical systems. In *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)* (pp. 1-8). IEEE.

Luo, J., Kang, M., Bisse, E., Veldink, M., Okunev, D., Kolb, S., Tylka, J.G. and Canedo, A., 2020. A quad-redundant plc architecture for cyber-resilient industrial control systems. *IEEE Embedded Systems Letters*, *13*(4), pp.218-221.

Gunduz, M.Z. and Das, R., 2018, September. Analysis of cyber-attacks on smart grid applications. In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)* (pp. 1-5). IEEE.

Raja, D.J.S., Sriranjani, R., Parvathy, A. and Hemavathi, N., 2022, June. A review on distributed denial of service attack in smart grid. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 812-819). IEEE.

Ibrahim, M. and Al-Hindawi, Q., 2018, June. Attack graph modeling for nuclear power plant. In *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1-6). IEEE.

Masood, R., 2016. Assessment of cyber security challenges in nuclear power plants security incidents, threats, and initiatives. *Cybersecurity and Privacy Research Institute the Ge orge Washington University*.

Asri, S. and Pranggono, B., 2015. Impact of distributed denial-of-service attack on advanced metering infrastructure. *Wireless Personal Communications*, *83*, pp.2211-2223.

Huseinović, A., Mrdović, S., Bicakci, K. and Uludag, S., 2020. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access*, *8*, pp.177447-177470.

Rudd, E.M., Rozsa, A., Günther, M. and Boult, T.E., 2016. A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions. *IEEE Communications Surveys & Tutorials*, *19*(2), pp.1145-1172.

Catillo, M., Pecchia, A. and Villano, U., 2020. Measurement-based analysis of a DoS defense module for an open source web server. In *Testing Software and Systems: 32nd IFIP WG 6.1 International Conference, ICTSS 2020, Naples, Italy, December 9–11, 2020, Proceedings 32* (pp. 121-134). Springer International Publishing.

Nagpal, B., Sharma, P., Chauhan, N. and Panesar, A., 2015, March. DDoS tools: Classification, analysis and comparison. In *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 342-346). IEEE.

Lypa, B., Iver, O. and Kifer, V., 2019. Application of machine learning methods for network intrusion detection system. *Proceeding of Processing, Transmission and Security of Information*, pp.233-240.

Alves, T. and Morris, T., 2018. OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research. *Computers & Security*, *78*, pp.364-379.

Xavier, B.M., Dzaferagic, M., Collins, D., Comarela, G., Martinello, M. and Ruffini, M., 2023. Machine learning-based early attack detection using open ran intelligent controller. *arXiv preprint arXiv:2302.01864*.

Kravchenko, T., Bogdanova, T. and Shevgunov, T., 2022, April. Ranking requirements using MoSCoW methodology in practice. In *Computer Science On-line Conference* (pp. 188-199). Cham: Springer International Publishing.

Swami, R., Dave, M. and Ranga, V., 2021. Detection and analysis of TCP-SYN DDoS attack in software-defined networking. *Wireless Personal Communications*, *118*, pp.2295-2317.

Cheng, Z., Yue, D., Hu, S., Ge, H. and Chen, L., 2020. Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks. *Neurocomputing*, *400*, pp.458-466.

Alhijawi, B., Almajali, S., Elgala, H., Salameh, H.B. and Ayyash, M., 2022. A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers and Electrical Engineering*, *99*, p.107706.

Abughazaleh, N., Bin, R. and Btish, M., 2020. DoS attacks in IoT systems and proposed solutions. *Int. J. Comput. Appl.*, *176*(33), pp.16-19.