



CMT400

Individual Project

2020/2021

**Ahmed Sultan Al-Qarni
ID: C1985143**

Supervisor: Neetesh Saxena

Moderated by: Amir Javid

Acknowledgements

Throughout the writing of this dissertation, I have received a great deal of support and assistance.

I would first like to thank my supervisor, Professor Neetesh Saxena, whose expertise was invaluable in formulating the research questions and methodology. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I would like to acknowledge my colleagues from my university at Cardiff University for their wonderful collaboration.


I would also like to thank my colleagues, Dr. Yazeed Alrowaili, for his valuable guidance throughout my studies. You provided me with the tools that I needed to choose the right direction and successfully complete my dissertation.

In addition, I would like to thank my parents for their wise counsel and sympathetic ear. You have been always there for me. Also, I could not have completed this dissertation without the support of my friends and my sister, Rawabi Sultan Al-Qarni who provided stimulating discussions as well as happy distractions to rest my mind outside of my research.

Finally, I would like to express my grateful feelings to the lady who supported me all over the way to get my Master degree and I owe her as much as I owe to my parents. Thanks to Ms.Bushra.F.AL-Meshaal for all her great contributions and support during my Master year.

Declaration of Originality

I certify that this thesis was written completely by me and that it has not previously been submitted, in whole or in part, in any prior application for a degree, except when stated otherwise by reference or acknowledgment.



Ahmed

Proforma

- Candidate Number: 1985143
- Title of the project: Risk Assessment and Advance Alert Notifications for Smart Grid
- Word Counts: 20327 Words
- Project Supervisor: Neetesh Saxena
- Project Moderator: Amir Javid
- The Aim: The initial objectives of the project were to create a cyber advance notification system for use in conjunction with a smart grid power system. This would then be utilized to enhance the system's situational awareness. This was accomplished by combining several risk assessments tools with cyber-attack monitoring systems in the smart grid. After analyzing and identifying the assets, a report of the incident is generated, including all pertinent information and recommendations on how to continue. The notification system must be completely customizable in order to assist users in detecting attacks in the real world.
- Abstract: Modern industry will be revolutionized by smart grid technology, which will provide innovative ways to improve the efficiency of current electric grids. It's a digital communications-based energy distribution network. A rise in demand for energy has resulted in an increase in electricity difficulties such as blackouts, overloads, and voltage drop, as well as significant carbon emissions from the present electrical network expanding and dealing with cyber-attacks first. Nevertheless, the Smart Grid technology is born with weaknesses and difficulties, particularly in terms of information security, which is the most critical issue. This study examined the threats and assesses the risk of smart grids based on the Internet of Things. We concentrate on the many kinds of cyber-attacks and offer detailed analysis. And provide cyber-security status of the smart grids.

Table of Contents

CHAPTER 1: INTRODUCTION	9
1.0 INTRODUCTION	9
1.1 INTRODUCTION TO THE TOPIC	9
1.2 MOTIVATION	11
1.3 SCOPE AND CONTEXT	11
1.3.1 THE SCOPE.....	11
1.3.2 CONTEXT OF THE PROBLEM	12
1.4 PROBLEM STATEMENT	13
1.5 AIMS AND OBJECTIVE.....	13
1.5.1 THE AIM	13
1.5.2 OBJECTIVES	14
1.6 REPORT ORGANIZATION.....	14
CHAPTER 2: BACKGROUND.....	15
2.0 OVERVIEW.....	15
2.1 TERMS.....	15
2.1.1 OPERATIONAL TECHNOLOGY (OT)	15
2.1.2 INDUSTRIAL CONTROL SYSTEMS (ICS)	16
2.1.3 SMART GRID	17
2.1.4 RISK ASSESSMENT.....	18
2.1.5 SITUATIONAL AWARENESS	19
2.1.6 ADVANCED ALERT NOTIFICATION	19
2.2 RELATED WORK.....	19
2.3 EXISTING TOOLS.....	22
2.3.1 NEXT GENERATION FIREWALL	22
2.3.2 THE SCADA FENCE PLATFORM	23
2.3.3 NOZOMI NETWORKS GUARDIANS.....	24
2.3.4 OTHER TOOLS	25
2.4 DATA CHARACTERISTICS	26
2.4.1 POWER SYSTEM FRAMEWORK CONFIGURATION	26
2.4.2 TECHNICAL DESCRIPTION.....	27
2.4.3 NON-ATTACK SCENARIO	28
2.5 ATTACK'S SCENARIO.....	29
2.5.1 INJECTION REMOTE CONTROL TRIPPING (ATTACK)	29
2.5.2 RELY SETTINGS CHANGE ATTACK.....	29
2.5.3 DATA INJECTION ATTACK	29
2.6 ATTACK SCENARIO TABLE	30
2.7 SUMMARY	33
CHAPTER 3: APPROACH	33

3.0	OVERVIEW.....	33
3.1	PROJECT PLANNING.....	33
3.2	METHODOLOGIES USED.....	33
3.3	REQUIREMENTS SPECIFICATIONS.....	35
3.3.1	FUNCTIONAL REQUIREMENTS	35
3.3.2	NON-FUNCTIONAL REQUIREMENTS	37
3.4	SUMMARY	38
CHAPTER 4: SYSTEM IMPLEMENTATION		38
4.0	OVERVIEW.....	38
4.1	PLATFORM USED.....	38
4.1.1	SETUP USED.....	38
4.1.2	EXPERIMENTAL SETUP	38
4.1.2.1	POWER WORLD	39
4.1.2.2	PYTHON	39
4.2	SYSTEM DESIGN.....	39
4.2.1	SYSTEM MODEL	39
4.3	PROPOSED RISK ASSESSMENT	41
4.3.1	SYSTEM ASSETS	41
4.3.1.1	Assets Identification (People).....	41
4.3.1.2	Asset Identification (OT and IT)	42
4.3.2	RISK CALCULATION	42
4.3.3	ESTIMATED RISK TO EACH SCENARIO.....	45
4.3.4	RISK MATRIX TABLE	46
4.3.5	POTENTIAL RISK	47
4.4	TOOL FUNCTIONALITY	48
4.5	THE OVERALL WORKFLOW OF THE IDEA	49
4.6	NOTIFICATION TECHNIQUE	49
4.7	SYSTEM VULNERABILITIES	52
4.7.1	GENERIC OS	52
4.7.2	MULTIPLE POINTS OF ENTRY AND FAILURE.....	52
4.7.3	COMMUNICATION PROTOCOLS	52
4.7.4	INTEGRAL PROTECTION	52
4.7.5	REAL-TIME AND COMPLEX INTERACTIONS.....	53
4.8	DATASET AND PRE-PROCESSING.....	53
4.8.1	DATASET PARAMETERS	53
4.8.2	PRE-PROCESSING	54
4.9	SUMMARY	54
CHAPTER 5: RESULTS AND EVALUATION.....		55
5.0	OVERVIEW.....	55
5.1	FINDINGS	55
5.2	TOOLS SNAPSHOTS	55

5.3	DISCUSSION.....	60
5.4	ATTACK SIMULATION.....	61
5.4.1	DATA INJECTION	61
5.4.2	REMOTE TRIPPING COMMAND.....	64
5.4.3	RELY SETTING CHANGE.....	65
5.4.4	RESULTS	66
5.5	EVALUATION.....	68
5.5.1	ASSESSMENT-EVALUATION.....	68
5.5.2	ATTACKS-EVALUATION.....	68
5.6	SUMMARY	69
	CHAPTER 6: CONCLUSION AND FUTURE WORK.....	69
6.0	BUILT-IN LIVE DATA CAPTURE.....	69
6.1	INTEGRATING MORE ADVANCE ALERT METHODOLOGIES	70
6.2	TOOL SUMMARY	70
6.3	THE IDEA AND TOOL.....	71
6.4	CONCLUSION.....	71
	CHAPTER 7: REFLECTION MADE ON LEARNING	72
7.0	REFLECTION ON LEARNING.....	72
	CHAPTER 8: APPENDICES	73
8.0	LIST OF TABLE.....	73
8.1	LIST OF FIGURES.....	73
	CHAPTER 9: BIBLIOGRAPHY	74
9.0	BIBLIOGRAPHY	74

Chapter 1: Introduction

1.0 Introduction

Smart grids, also known as networked power grid control equipment, rely on information and communication technology (ICT) to manage power flow and energy balance. A smart grid may include a variety of devices, including but not limited to measuring equipment (e.g., phasor measurement units (PMU) and smart metres), actuators (e.g., breaker-switches and disconnectors), and networking equipment (e.g., gateways and control nodes). These crucial gadgets, like traditional Internet technologies and consumer electronics, are vulnerable to Malicious Software (malware). Traditional power grid settings, on the other hand, concentrate on long-term stability and prepare for hardware life-spans of 10 years or more, as opposed to consumer devices. Unknown vulnerabilities in hardware, operating systems, software, and protocols arise as devices age. Such flaws represent a major risk to the infrastructure. While consumer gadgets do not have to meet the same life-cycle standards as industrial equipment, the underlying technology is the same.

1.1 Introduction to The Topic

As the world becoming more reliant on the digital technology, computer systems consider one of the most important systems ever. Since we are using these systems in our daily life for almost every process that we are in need to accomplish, nevertheless, that our lives today can be built up around computer systems. However, as we completely depending on the automated systems, the role is changed to make such systems very critical and if any disruption occurred, a severe damage and series issues will have critical impact to the other systems related to computerized systems. This has resulted in several of the issues, including inadequate requirements capture, software failures, misconfiguration, and a lack of competitive assessments. These implementation weaknesses and vulnerabilities may be exploited by cybercriminals in their desire for popularity, revenge, political gain, economic gain, cyber espionage, cyber terrorism, and cyberwar by bringing down systems and disrupting services. On the other side, cyber operations became very famous as the authority defending against political attacks such as cyberterrorism. Basically, cyberterrorism is meant by particular attacks for example, attack on websites using typical technics, attack on organization which known as APT (Advance Persistent Threat) attacks and the goal meant by this paper is political and the most sophisticated one which attacking the organizations core operational systems, e.g., Smart Grid or industrial systems. (Akhgar and Yates 2014) This paper will attempt to tackle the third and the most complicated category attacks, smart grid and industrial control systems.

Cyber-attacks have grown more common on the smart grid. Attacks on communication networks can dramatically raise operating expenses (Yeboah-Ofori 2019) or adversely affect proper system operation (McCary and Xiao 2015). In 2015, for example, cyber-attacks on Ukraine's power infrastructure resulted in a major power outage that lasted several hours. (Tang et al. 2016) To maintain the smart grid's secure and effective operation, power system operators must be able to detect, identify, and detect such threats quickly and take urgent action to safeguard the entire grid. Cyber resilience is the term for this procedure. The first stage in improving resilience in the offensive phase and/or post-attack phase, from the perspective of power system operators, is to successfully identify cyber-attacks. Because of the attack's unpredictability, this is true. As a result, several research projects using various techniques have been conducted over the last decade in order to successfully detect and identify cyber-attacks as part of improving the smart grid's resilience. (Mohammadpourfard et al. 2021)

Any city's energy infrastructure is regarded as the single most critical component. As a result, power grids are designated as vital national infrastructure (CNI). All other and important organizations/functions, such as security, police, and telecommunications, are affected if the internet is inaccessible for a long enough length of time. From the generating plant to the consumer premises through transmission and distribution, the smart grid incorporates intelligence in control and monitoring of the energy and water infrastructure at all levels. An automated, globally dispersed energy delivery network characterized by a two-way exchange of electricity and information, capable of monitoring and responding to changes in everything from power plants to consumer preferences to specific appliances, according to IEEE. Three types of functions are covered by a smart grid: (a) It uses digital power systems through self-healing designs, automation, remote monitoring and control, and the creation of microgrids; (b) it informs and educates consumers about their energy usage, costs, and alternative options, allowing them to make autonomous decisions about how and when to use electricity and fuels; and it informs and educates consumers about their energy usage, costs, and alternative options, allowing them to make autonomous decisions about how and when to use electricity and fuels. And (c) it efficiently integrates decentralized and renewable energy resources in a way that is safe, secure, and dependable, with customers actively engaging in the energy market. All of this contributes greatly to a more dependable, sustainable, and resilient energy system. As a result, a smart grid is at the heart of a smart city, which would not be complete without it. (Smart Grid: The Smart Grid | SmartGrid.gov. 2021) In this paper we will focus on level (b) by conducting risk assessment and apply one of proposed solutions with scenario attacks to identify assets criticality.

Smart grid is emerging as a confluence of information and communication technology with power system engineering to enable for ubiquitous control and monitoring. Smart grid consists of four levels started with: (A) Process

intelligent switchyard, sensors and I/Os (Input and output; (B) Bays and LEDs (Light Emitting Diodes); (C) Substations (SAS). And (D) Dispatch Center. In this paper we will focus on level (C) Substations by conducting risk assessment and apply one of proposed solutions with scenario attacks to identify assets criticality.

1.2 Motivation

This project might be useful in a variety of situations. Certain sorts of threats may need to be assessed against custom algorithm alert tools detection methods as part of a network security project. Both the tool and the article would assist a researcher in developing an advance alert technique to notify end-user if suspicious behavior is happening and testing cyberattacks using various methods. The application's versatility is critical for swiftly switching in and out algorithms to generate the most effective prediction approach. This research will also quickly identify the benefits and drawbacks of various methods in relation to the various forms of smart grid attacks. Finding these benefits and drawbacks will enable the researcher to combine algorithms that compliment one another. There are a variety of ways for combining these alerting, all of which will enhance the response technics in case of cyber-attack on smart grid based on an advance alert technic. When an event occurs, the enhanced degree of precision provided by this project will assist any users in determining their next steps.

1.3 Scope and context

We must first understand the background around smart grids, cyberattacks, and advance alert tools in order to appreciate why this study is essential. This will allow us to better understand any challenges or concerns that arise later in the project. However, because these topics are broad, any attempt to comprehend the entire issue would need significant research and would be far too time consuming to develop a respectable article and tool. We address this by setting a scope that establishes the project's maximum reach. If the scope was too broad, the job would be far too difficult to complete, but if it was too narrow, not enough work would be covered to make this paper relevant, therefore the right balance must be maintained.

1.3.1 The Scope

Because smart grids are generally extremely interconnected, an action taken on one end of the grid may have an impact on a component on the other. This reliance necessitates a thorough understanding of our smart grid's architecture and how each component interacts with one another. This is particularly essential for determining which portion of the smart grid an

attacker is seeking to penetrate or impact, as well as how data changes affect the real-world smart grid. While we don't need to know everything about the smart grid, we do need to know how the data we're working with is collected and transferred.

A smart grid can be targeted by a variety of attacks, but for this project, we'll focus on attacks that have been specifically targeted at smart grids. Remote trip attacks, command injection attacks, relay setting change attacks, and data injection attacks are all examples of these types of attacks. Other sorts of attacks will not be evaluated, despite the fact that each attack category has many subtypes.

Finally, there are alert tools technics to consider. Because the whole detection technique is built on the use of several situational awareness technics however, there is a limited understanding of the risk related to ICS or the smart grid hence, this project aims to assess risks related to the smart grid and based on the assessment notification tool should be designed. As a result, we require a full grasp of the benefits and drawbacks of each tool, as well as how each tool interacts when utilized in the field of notifying end-user what type of notification action should be taken to notify the right end-user. We need to understand how each component and kind of alert tools works in order to build an accurate notification technique to inform the end-user.

1.3.2 Context of The Problem

Attacks used to be limited to major infrastructure projects like nuclear power plants and legacy stations. Despite being among the first to be targeted, they also quickly adopted new cybersecurity measures, which made them the target of future attacks. While the benefits for successfully targeting these objectives will be substantial, the challenge is growing on a continuous basis. As a result, cybercriminals choose to attack projects that have poor security, or attack governments that cannot afford as much protection as other nations.

Physical attacks on the smart grid may have a catastrophic effect on the system's proper operation and have a major impact on any infrastructure or people who depend on the smart grid. It's difficult to identify when these attacks occur because hackers have grown more adept at concealing themselves on computer systems from standard antivirus or anti-ransomware software. Even if a person examines the voltage data provided by a smart grid, they will be unable to determine whether an attack has occurred without proper automated notification technics; the quantity of data they will get and the number of voltages they will have to monitor will be much too burdensome and overwhelming. Additionally, hackers may choose to conceal the rate at which they raise the voltage by spreading it over a lengthy period of time, such as weeks or even months, until the components are abused to the point of destruction. Disruption of critical services such as water, electricity, and natural gas may jeopardise the country's stability. A lack of these basic services

undermines popular confidence in the government's ability to provide for its people.

Attacks on the smart grid may not always have to result in physical damage to the system in order to have a major effect. For example, if the attacker was able to break into the AML (Advance Meter Infrastructure) he could manipulate the information values of more than thousands of customers causing harm to the company electricity systems and causing a blackout in different areas.

1.4 Problem Statement

Because these smart grids are constantly essential to those who rely on them, they are highly secured with cybersecurity. However, these cybersecurity technologies depend on detecting signs of compromise, which may include packet analysis, system log entries/files, and so on. If an attacker is able to evade the tool's detection techniques, no action will be done against the intruder owing to the automated nature of these tools and the absence of appropriate notification tools. Even if an attacker begins causing harm to portions of the smart grid, these cybersecurity technologies will remain inactive due to the lack of a warning mechanism on the smart grid. This is the knowledge gap that this research and tool will address in addition to risk assessment. Rather than depending on fragments of forensic data discovered on the smart grid system, it will utilize data straight from the smart grid.

As a result, our issue statement is to improve a smart grid's situational awareness by monitoring physical changes on the grid for indications of compromise or potentially hazardous circumstances and reporting on any occurrences. This report will provide advice on the best course of action to follow moving ahead. Previous research has tried to resolve this issue, but with insufficient precision to be applicable in a real-world setting.

1.5 Aims and objective

In order to have a clear understanding of what we want to do, we must first establish a goal and a set of goals that we must meet by the conclusion of this project's duration.

1.5.1 The aim

For the vast majority of smart grids, problems are dealt with by a team of experts; however, for medium or small grids, automated security solutions help deal with the occurrences. The lack of automation implies that they are susceptible to any attack that automation doesn't understand. As attackers usually leave behind forensic evidence that may be gathered and analyzed, automated cybersecurity solutions use such data to detect whether an attack occurred. If a malicious actor can defeat these automation technologies, it

would imply that the smart grid would be exposed. In order to avoid problems like these, the project will seek to identify the critical smart grid assets and assess the risks associated to each asset to develop a notification tool to inform end-users in the event of attacks.

1.5.2 Objectives

Design or use existing solutions to reduce or mitigate the risk of cyber-attacks
The work that this paper will attempt to cover accomplishes the following goals:

- 1- Identifying key assets and what are the potential risk associated to them in smart grid.
- 2- Developing attack scenarios through simulation tools e.g., Power World to check what is the attack consequences.
- 3- Developing an advance alert notification tool alerting users in SG systems in the event of attacks and give users a comprehensive view about what are the attacks are executed against their SG network.

1.6 Report Organization

Background information on the subjects covered in this part will be provided in the next chapter. This background information is required to comprehend both the solution and the results generated after that chapter. The next chapter has a comprehensive explanation of the approach and how this paper will solve the difficulties mentioned. Following the approach, a chapter will describe the solution concept and how it was executed. There is also a breakdown of all the tool's capabilities. The chapter on outcomes and assessment comes next. This section of the article will describe any findings from testing carried out in connection with the creation of the tool, as well as evidence that this study met the objectives stated. The last two research chapters are based on the study's findings and any future work that could make use of this project.

Chapter 2: Background

2.0 Overview

The concepts and background needed to comprehend the project will be extensively discussed in this chapter. This includes any limitations that were applied to the project scope to make it more reasonable.

2.1 Terms

Some standard terminology used in these areas will be defined below.

2.1.1 Operational Technology (OT)

While everyone understands what IT is, those without an OT background may be unsure of what OT or operational technology actually entails. The term "operational technology" refers to a group of computing and communication technologies used to manage, monitor, and control industrial operations, with an emphasis on the physical equipment and processes involved.

Industrial process assets and manufacturing/industrial equipment are monitored and managed by operational technology. OT has existed for far longer than IT or information technology, notably since we began to employ electricity-powered machinery and equipment in industries, buildings, transportation networks, the utility business, and other places. The phrase, on the other hand, is relatively modern. OT is the hardware and software that keeps things functioning, such as factories, power plants, and facility equipment.

According to Gartner, operational technology is "hardware and software that detects or creates a change in the business through direct monitoring and/or control of physical equipment, processes, and events."

Gartner's definition is geared toward IT professionals, which is presumably why it's so popular. Other definitions of OT exist, with some sticking to the bottom levels of the classic automation pyramid (field level, control level, production level, etc.) and some going higher.

Industrial Control Systems (ICS), which includes Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems, are examples of OT technology that interfaces with the physical environment (DCS). (Smart Grid: The Smart Grid | SmartGrid.gov. 2021), (Wang et al. 2018)

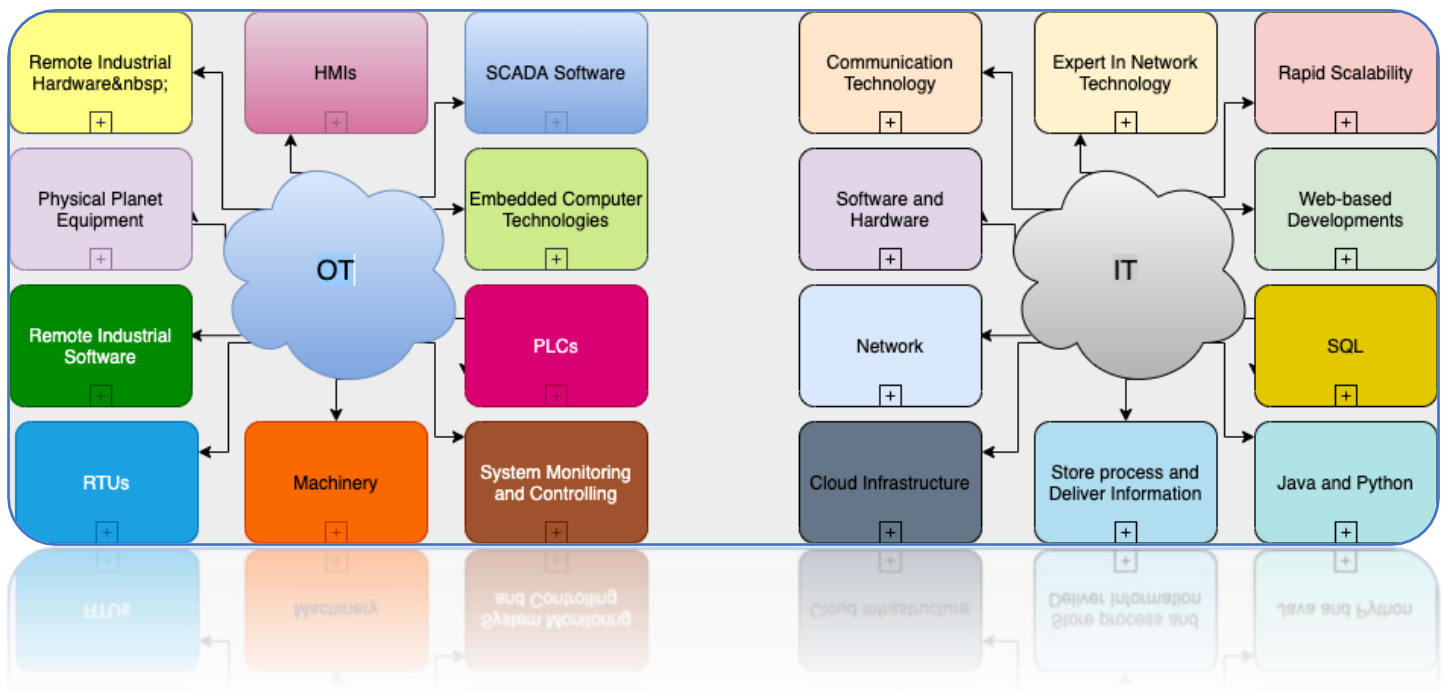


Figure 1: difference between OT systems and IT systems

2.1.2 Industrial Control Systems (ICS)

Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system topologies, such as Programmable Logic Controllers (PLC), are all examples of industrial control systems. An ICS is made up of a number of different control components (electrical, mechanical, hydraulic, and pneumatic) that work together to achieve a certain industrial goal (e.g., manufacturing, transportation of matter or energy). The process is the portion of the system that is primarily concerned with creating the output. The specification of the desired output or performance is part of the system's control. Control might be completely automated or contain a human component.

Open-loop, closed-loop, and manual modes of operation are available. The output is regulated by established parameters in open-loop control systems. The output of a closed-loop control system affects the input in such a way that the intended goal is maintained. The system is fully controlled by people in manual mode. The controller is the portion of the system that is primarily concerned with ensuring specification compliance (or control). Many control loops, Human Machine Interfaces (HMIs), and remote diagnostics and maintenance tools may be found in a typical ICS, which are created utilizing a variety of network protocols. Electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace,

and durable goods) industries all utilize ICS to manage industrial operations. (Stouffer et al. 2008)

2.1.3 Smart Grid

The term "grid" has traditionally been used to describe an electricity system that can handle all or part of the following four functions: energy generation, transmission, distribution, and control.

A smart grid (SG), also known as a smart electrical/power grid, intelligent grid, intelligrid, futuregrid, intergrid, or intragrid, is a modernization of the power grid from the 20th century. Traditional power networks transport energy from a few central sources to a large number of consumers or customers.

The SG, on the other hand, builds an automated and distributed advanced energy delivery network using two-way electrical and communication exchanges. The SG can supply electricity more efficiently and adapt to a wide range of situations and events by leveraging contemporary information technology. In general, the SG may react to events occurring anywhere in the grid, such as power generation, transmission, distribution, and consumption, and implement the appropriate strategies. For example, if a medium voltage transformer fails in the distribution grid, the SG may alter the power flow and restore power delivery service automatically. The SG can be defined as an electric system that integrates information, two-way, cyber-secure communication technologies, and computational intelligence across electricity generation, transmission, substations, distribution, and consumption to create a clean, safe, secure, reliable, resilient, efficient, and sustainable system. This description encompasses the complete energy system, from the point of generation to the point of consumption of power.

The basic concept of SG was to provide self-healing, dependable grid security against intentional sabotage and natural catastrophes using advanced metering infrastructure (AMI) with the goal of enhancing demand-side management and energy efficiency. New requirements and expectations, on the other hand, prompted the electrical industry, research groups, and governments to reconsider and broaden the scope of SG. The Energy Independence and Security Act of 2007 mandated that the National Institute of Standards and Technology (NIST) oversee research and development of a framework to ensure SG system and device interoperability. Although a clear and complete definition of SG has yet to be given, the following are the predicted benefits and needs of SG, according to the NIST study: (Jenkins et al. 2015)

- Enhancing voltage stability;
- Maximizing facility usage while avoiding the building of emergency (peak load) power plants;
- Increasing the capacity and efficiency of current electricity grids;

- Enhancing disruption resilience;
- Facilitating scheduling and self-healing responses to system disruptions;
- Facilitating the deployment of renewable energy sources on a larger scale;
- Allowing dispersed power sources to operate;
- Automating maintenance and operations;
- Reducing greenhouse gas emissions by allowing electric cars and new power sources to operate;
- Reducing oil use by eliminating the requirement for wasteful generating during peak periods;
- Demonstrating ways to increase grid security;
- Facilitating the transition to plug-in electric cars and innovative energy storage alternatives;
- Increasing the number of options available to consumers;
- Facilitating the development of new goods, services, and markets. [9]

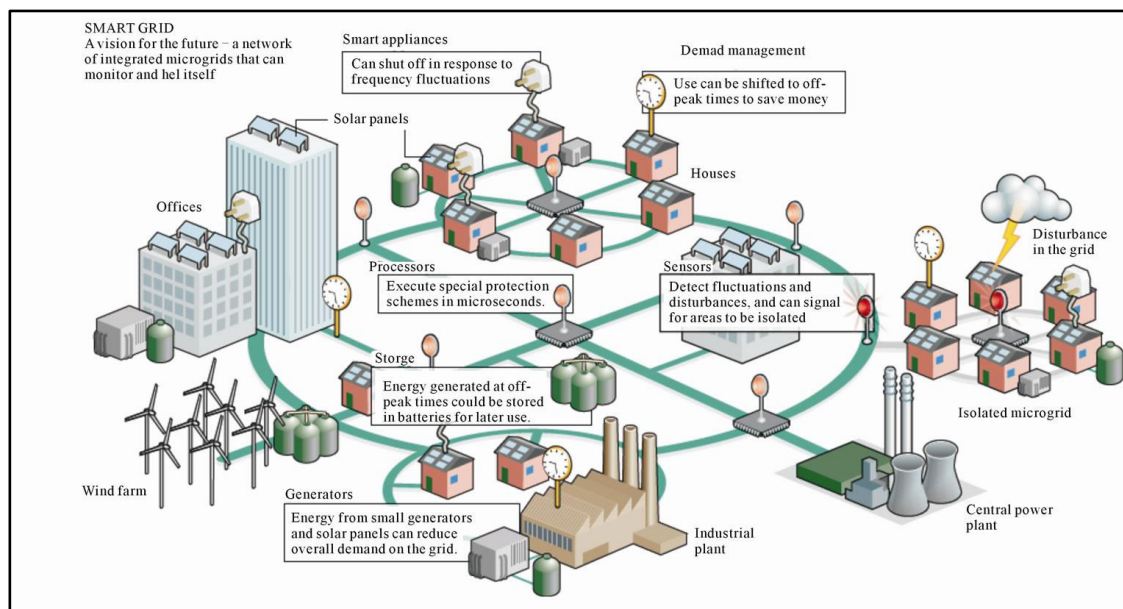


Figure 2: Smart Grid System (Vijayapriya and Kothari 2011)

2.1.4 Risk Assessment

The identification of dangers that might have a negative influence on an organization's capacity to do business is known as risk assessment. These evaluations aid in the identification of these inherent business risks, as well as the implementation of procedures, processes, and controls to mitigate their influence on corporate operations.

Various methodologies available can be used for both systems (IT & OT) since both systems serving the business continuity terms. Some of methodologies are

ISA/IES 62443, ISO 27001, NIST, CPNI and ENISA. Exploring and reviewing these methodologies will be explained in details in section (2.3 Related work).

2.1.5 Situational Awareness

In this context, situational awareness refers to how effectively the user knows what is going on in their smart grid right now.

2.1.6 Advanced Alert Notification

Important or time-sensitive machine-to-person communication. An alert might be a calendar reminder or an SMS notice.

The most frequent use of the service is machine-to-person communication, and alerts are generally given through a notification system. Notification services through email or SMS are provided by the most basic providers. Users of more complex systems can choose between e-mail, SMS, IM (Instant Messaging), voice portals, desktop notifications, and other methods of delivery.

2.2 Related work

This section will go through previous studies in current subject and show how it relates to this project.

There have been various researches discussed risk assessments methodologies in OT systems. However, the most closely related to this work is entitled Smart Grid Cybersecurity Risk Assessment. (Langer et al. 2015) The research discussed the available methodologies and issued a comparison among available frameworks and methodologies appropriate for both IT&OT systems and conclude what is the most related and appropriate method / framework should be applied to achieve the best and accurate predictions of the risk related to ICS systems or Smart Grid to take the optimum countermeasures. The research discussed the Cyber-attacks on Information Communication Technology (ICT) and Supervised Control and Data Acquisition (SCADA) with the available frameworks and tools to be applied on two aspects a) assess the impact of cyber-attack to information assets and the likelihood of attack occurring. Thus, based on the outcome of the conducted risk assessments, security requirements can be identified. The frameworks / methods discussed in this work were a) OCTAVE, b) HMG IS1 and c) Magerit -most of them are based on the principles identified on ISO 27005 (Langer et al. 2015). Carrying out the evaluation among frameworks / methods (Langer et al.2016) as part of European Committee for Electrotechnical Standardization (CEN-CENELEC-ETSI) response to Mandate 490 proposed SGIS Toolbox by support from the Smart Grid Information Security working group which is a set of high-level guidelines to assess the cybersecurity risks incidents related to smart grid. The SGIS toolbox offers a variety of smart grid-specific features, such as the

classification of several effect categories that represent the smart grid's characteristics. The SGIS toolbox has been reportedly not well accepted by the community, since it received a lot of criticism.

Table 1: Comparison shows the frameworks / methods available for OT, ICS and Smart Grids (ICS Cybersecurity Assessment Framework. 2021), (Langer et al.2016), (Langer et al.2015) and (Stouffer et al. 2021)

Framework / Methods	Short Description	Pros	Cons
ISO/IEC 31000	General risk management framework	A good starting point to set up a risk management process with all relevant subcategories	Only a few numbers of techniques are authorised. a limited scope The process of integration is not generally applicable. Key words have irrational interpretations and are defined in a limited manner.
ISA/IEC 62443	Industrial Automation and Control System (IACS) cyber-security elements and Cyber Security Management System (CSMS) for risks are part of a framework for the security of industrial automation and control systems.	Describes strategies to deal with IACS issues, such as smart grids.	Focusing on ICS with giving a little consideration to the smart grid
ENISA	General risk management framework	Same as NIST it covers wide range of assets of IT and OT systems.	Because ENISA does not provide a complete standard, it is not possible to create a complete cybersecurity system using only NIST's recommendations
NIST sp.800-82	Framework provides a guidance on how to	The main advantage of NIST lies in the wide	Because NIST does not provide a complete

	secure ICS, SCADA and DCS systems	coverage it provides, which is suitable for enhancing the network security of important parts of IT and OT.	standard, it is not possible to create a complete cybersecurity system using only NIST's recommendations.
CPNI	With various materials publicly available, the framework covers cybersecurity applied to IT and OT.	CPNI provides a wealth of free information on cybersecurity for both IT and OT. The Internet of Things is also covered by CPNI, which includes best practises and implementation suggestions. The standards span a wide range of technologies and are updated to reflect current cyber security developments.	Because CPNI does not provide a complete standard, it is not possible to create a complete cybersecurity system using only NIST's recommendations
OCTAVE	It focuses on activities, threats and vulnerabilities, and uses an expectation matrix to determine expectations of risk (including estimates of subjective effects and probabilities).	A risk assessment technique based on assets that stresses the need of self-evaluation. It has a broad definition of what defines an asset; thus, it may be a useful smart grid tool.	Not specifically generated to cover the smart grid cybersecurity incidents
SGIS Toolbox	Defines and analyses use cases to determine risk impact levels for each information asset, identifying supporting components and running an inherent risk analysis to appropriately select standards to protect every information asset based on security level	SGIS toolbox offers a variety of smart grid-specific features, such as the classification of several effect categories that represent the smart grid's characteristics	it does not consider deployed systems with certain security measures in place. Thus, it is not sufficient to perform a comprehensive risk assessment.

(Langer et al.2016) developed risk assessment framework for assessing risks in smart grid based on national reference which can be applied for both systems the deployed systems and near-term future developments and the method can support Distribution System Operators (DSOs). Framework following the Smart Grid Architecture Model (SGAM) to help to understand risk associated with different architectural choices. This method provides a unified approach that covers existing system components and recent developments. It is achieved through the use of two interrelated processes: concept assessment and implementation-based assessment, which use SGAM as a starting point. However, the methods are focus on near-to-mid-term developments of the smart grid and some of these systems typically not implemented yet. Another drawback is, implementation details of systems such as poor configuration and implementation vulnerabilities are not considered during the assessment. (Hasan et al., 2019) have assessed risk on power systems-based relaying on three aspects: locality, centrality and damage factor. The work consists of both IT-based systems and OT-based systems by assessing the degree of risk based on the mentioned aspects. However, the work assessed results extracted from network traffic which is not efficient to establish a comprehensive cybersecurity awareness specifically in the field of SG systems.

British Standards Institution (BSI) (ICS Cybersecurity Assessment Framework, 2021), proposed an approach after reviewing five frameworks (IEC 62443, ISO 27001, NIST, ENISA and CPNI) to develop best of breed from the mentioned frameworks. This research aimed to use a combination of best methods available to use. Thus, BSI besides SGIS toolbox and NIST sp.800-82 methodologies will be used to analyse a use-case scenario and the outcome of the assessment can lead to design or extend existing advance alert notification tool or methodology.

2.3 Existing Tools

Cybersecurity risk in the field of smart grid can be defined as new threats. However, a number of solutions and tools are already available to deal with such attacks. Here three proposed methods / tools to notify the end user will be described which will be utilized – extended if needed- to conduct our research.

2.3.1 Next Generation Firewall

A Next Generation Firewall is a hardware or software-based security device that constantly monitors and regulates network traffic transferred between target computers based on a predefined security policy and control rules. This security strategy, in particular, may be divided into two categories: a) negative policy and b) positive policy. On the one hand, the negative policy rejects all internal and external communications and, via the use of particular criteria, decides which connections are allowed. On the other hand, a positive policy

permits all communications and specifies which connections will be discarded via the use of control rules. Additionally, firewall systems may be classified according to their functionality or their deployment. Four types of firewalls may be specified in the first case: a) packet filtering firewalls, b) stateful inspection firewalls, c) application-level gateways, and d) circuit-level gateways. In the second instance, numerous architectural combinations are possible depending on the security management and risk assessment procedures. Finally, it's worth noting that a firewall is incapable of providing security against cyberattacks that circumvent it. For instance, a firewall may be incapable of dealing with malevolent insiders. As well as, the majority of the IDS systems dealing with attacks by monitoring the network traffic and neglecting the risk associated with electricity like voltage increasing. In other words, these systems dealing with cyberattacks from IT prospective not as an OT prospective. (Radoglou-Grammatikis et al. 2018)

2.3.2 The SCADAfence Platform

As a result of the SCADAfence Platform, IoT devices connected to the OT environment are discovered and the user is provided with granular visibility into their attributes such as the device's manufacturer as well as its model, operating system, and MAC address, as well as an analysis of the device's risk and contextual understanding. With the Check Point IoT Security Manager, the user can set up a security policy based on the characteristics of their devices and even take advantage of automatically produced policy suggestions. Having a security gateway policy for each device in an environment give the user the ability to take proactive steps to minimize the risk. One that is self-adaptive to changes in its characteristics, behavior, and degree of criticality. Using the combined solution, each device in the environment has a policy that is generated and enforced automatically. As soon as the SCADAfence Platform's detection engine spots an OT security threat, it notifies the Check Point IoT Security Manager and provides policy recommendations. With this automated procedure, policy settings can be completed in a relatively short time and the vast majority of IoT devices will be protected from the minute they join to the OT network. The auto-generated rules immediately reduce IoT attack surfaces by establishing network segmentation, which only enables authorized access to (and from) IoT devices and guarantees that devices utilize the communication protocols they were intended to use. In addition to detecting malware, illegal access, application-level abnormalities, and deep packet inspection of OT industrial protocols (for example, instructions that try to alter PLC settings or interrupt production operations), they may handle system or user specified scenarios. For example, the platform allows the AC systems to communicate with the building management systems and notify them in the critical situation (attack-events). On the other hand, the platform monitors the low-level communications e.g., communications protocols (M-to

-M). as well as, relying on the network traffic without considering the electricity or insider threats. (All of Your OT & IoT Security in One Place | SCADAfence. 2021)

Select objects from IoT Discovery Service - Asset Provider

Filters

- cloud-service
- device
- dhcp
- directory
- dns
- fw
- internal-service
- mail
- nac
- server
- Tags

Search device...

Name	Name in Discovery	Type	IP A...	Fun...	Manufac...	Loca...	Model	Risk...	OS...
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH...	device	192.168...	BACnet...	PCS System...	Floor B	PCS System...	MEDIUM	Linux
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH...	device	192.168...	BACnet...	PCS System...	Floor G3	PCS System...	MEDIUM	Linux
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH...	device	192.168...	BACnet...	PCS System...	Floor 1	PCS System...	MEDIUM	Linux
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH B...	device	192.168...	BACnet...	PCS System...	Floor 1	PCS System...	MEDIUM	Linux
PLC - 135	PLC - 135	device	192.168...	plc	Siemens AG	Floor G2	Siemens, SIMAT...	HIGH	Sieme...
Rivet Networks	Rivet Networks 192.168...	device	192.168...	host	Rivet Netwo...	Floor 4	Rivet Netwo...	MEDIUM	Windo...
Rivet Networks	Rivet Networks 192.168.1...	device	192.168...	host	Rivet Netwo...	Floor 3	Rivet Netwo...	MEDIUM	Linux
Rockwell Automation plc 192.16...	Rockwell Automation plc 1...	device	192.168...	plc	Rockwell Au...	Floor 2	Rockwell Au...	MEDIUM	Rockw...
Rockwell Automation Rockwell Auto	Rockwell Automation Rock...	device	192.168...	plc	Rockwell Au...	Floor E	Rockwell Auto...	MEDIUM	Rockw...
SCADA_Server	SCADA_Server	device	192.168...	hmi	Good WAY I...	Floor E	Good WAY I...	MEDIUM	Linux
Samsung Electronics	Samsung Electronics 192.1...	device	192.168...	workst...	Samsung Ele...	Floor 1	Samsung Ele...	MEDIUM	Windo...
Samsung Electronics Co. Ltd 192.1...	Samsung Electronics Co. Ltd...	device	192.168...	workst...	Samsung Ele...	Floor 5	Samsung Ele...	MEDIUM	Linux
Satec 192.168.0.138	Satec 192.168.0.138	device	192.168...	sensor	Satec	Floor 2	Satec	MEDIUM	Native
Siemens AG plc	Siemens AG plc 192.168.0.1...	device	192.168...	plc	Siemens AG	Floor 5	Siemens AG	MEDIUM	Sieme...
Siemens AG plc	Siemens AG plc 192.168.0.1...	device	192.168...	plc	Siemens AG	Floor 5	Siemens AG	MEDIUM	Sieme...
Siemens AG plc	Siemens AG plc 192.168.0.1...	device	192.168...	plc	Siemens AG	Floor G5	Siemens AG	HIGH	Sieme...
Siemens AG Siemens, SIMATIC S7, CP...	Siemens AG Siemens, SIMAT...	device	192.168...	plc	Siemens AG	Floor G5	Siemens, SIMAT...	MEDIUM	Siemat...
Siemens AG Siemens, SIMATIC S7, CP...	Siemens AG Siemens, SIMAT...	device	192.168...	plc	Siemens AG	Floor G2	Siemens, SIMAT...	MEDIUM	Siemat...
TP-Link Technologies Co. Ltd 192.1...	TP-Link Technologies Co. Lt...	device	192.168...	workst...	TP-Link Tech...	Floor 1	TP-Link Tech...	MEDIUM	Linux
TP-Link Technologies Co. Ltd 192.1...	TP-Link Technologies Co. Lt...	device	192.168...	workst...	TP-Link Tech...	Floor G5	TP-Link Tech...	MEDIUM	Linux
TP-Link Technologies Co. Ltd 192.1...	TP-Link Technologies Co. Lt...	device	192.168...	workst...	TP-Link Tech...	Floor 2	TP-Link Tech...	MEDIUM	Linux
Telemecanique Electrique Modicon...	Telemecanique Electrique M...	device	192.168...	plc	Telemecaniqu...	Floor 2	Modicon M580...	MEDIUM	Modic...
Telemecanique Electrique Modicon...	Telemecanique Electrique M...	device	192.168...	plc	Telemecaniqu...	Floor 2	Modicon M580...	MEDIUM	Modic...
WSTA_2	WSTA_2	device	192.168...	BACnet...	VMware, Inc.	Floor 3	VMware, Inc.	MEDIUM	Windo...

134 items

Figure 3: The SCADAfence Platform

2.3.3 Nozomi Networks Guardians

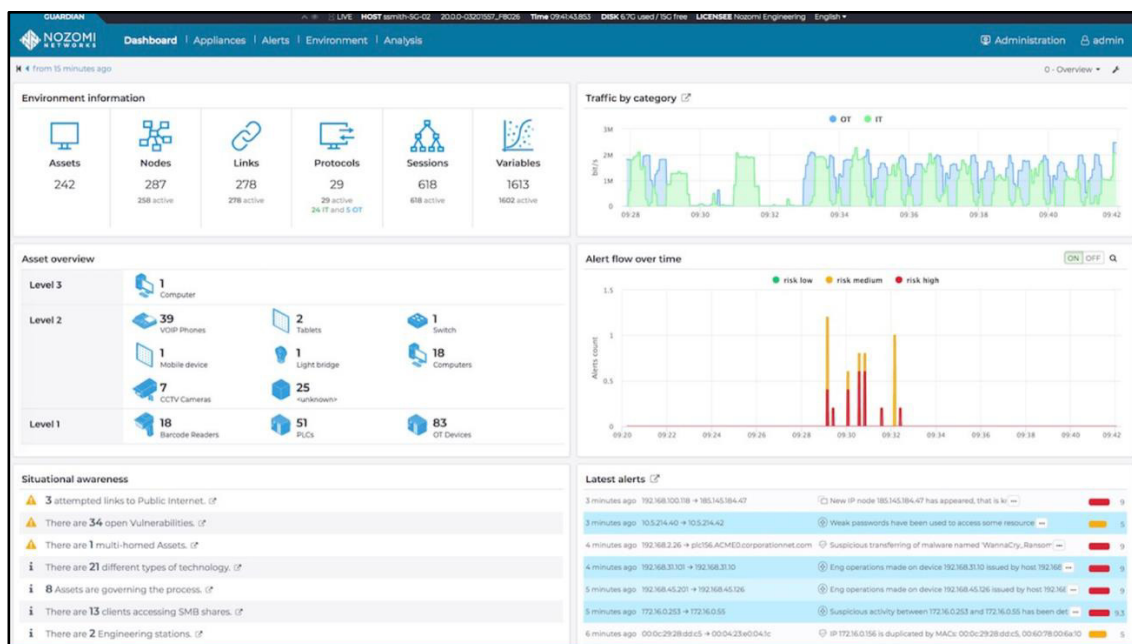


Figure 4: Nozomi Networks Guardians Platform

Its physical or virtual appliances monitor network communications and device behavior, providing real-time visibility into the OT/IoT network's activity patterns. The user can view the highest-priority vulnerabilities, threats, and abnormal behavior, which enables users to react more quickly while maintaining high dependability and security. Guardian mitigates operational risks for the world's biggest critical infrastructure, energy, industrial, mining, transportation, and building automation facilities. The platform is relying on 5 steps to assess and notify users the steps are Identify, Assess, Detect, Act and Scale. In the Identifying stage the platform is identifying the assets by asset discovery and set up network visualization. Next, assessing the vulnerabilities based on vulnerability dashboard and generated reports which result in detecting the associated threat related to the OT-systems based on the signature of the threat which gives the chance to act by using focused risk information and time saving response tools to notify the right users by creating accurate alert notifications. Finally, the platform is scaling the threat and keep updating the information related to it by unified security for thousands of distributed sites to provide visibility into all OT/IoT environments. The limitation of the Nozomi tools can be as follows, a) There is no integration capabilities with a Secure Remote Access solution. There is also no inline monitoring/IPS capability. B) The nature of the product requires the availability of a few external hardware and c) the filtering capabilities need more developments in order to sense the risk related to OT assets. (Nozomi Networks Guardian - Tempest Telecom Solutions. 2021)

2.3.4 Other Tools

There are numerous of notification tools in terms of SG, however, this research discussed the relevant to the purpose of the paper, the other tool will be mentioned in the below table to illustrate in case of future research.

Table 2: Tools Comparison

Tool	Developer	Pros	Cons
Darktrace Industrial Immune System	Darktrace	Simple user interface and can be understandable easily.	it produced a extensive amount of benign alerts (many "maybe you should look into this") but hardly any solid actionable information.
Kaspersky Industrial CyberSecurity (KICS)	Kaspersky	Secure network at all levels and immediately alert if any anomaly is found.	A bit expensive and the security automated settings

Lumeta	FireMon	the ease of viewing security information and the quick notification of detected problems,	The configuration is a bit hard to understand as well as the asset identification is tedious
The Clarity Platform	Clarity	Provides very useful information on very old systems	Alert technique needs to be improved
Xsense	CyberX	Alerts monitoring and assets discovery.	The implementation and configuration is slow and the bandwidth used for updates is very high

2.4 Data Characteristics

a power system attack data set published by the Mississippi State University and Oakland Ridge National Laboratory in 2014 was found. These data sets were produced in collaboration with Justin Beaver and Raymond Borge of Oakland Ridge National Laboratory. The raw data logs were provided to Justin by the MSU team, and the Oakland Ridge National Laboratory team formatted these logs into appropriate data sets.

The data they generated is divided into three sub-datasets: binary, three-class, and multi-class. When comparing these three, the only distinction is the level of detail used to describe the kind of scenario to which each instance of data belongs. The binary data collection is the least comprehensive, distinguishing simply between attack events and normal activities. By differentiating between attacks, naturally occurring events such as line maintenance or normal electrical failures, and no occurrences, the three-class data set enhances this. Finally, the multi-class data set is the most detailed. Its marker property differentiates across distinct situations, not only the kind of scenario to which the instance belongs. For example, the same attack may occur many times but on various intelligent electronic drivers.

2.4.1 Power System Framework Configuration

The figure below shows the power system framework configuration used in generating these scenarios. In the network diagram we have several components, firstly, G1 and G2 are power generators. R1 through R4 are

Intelligent Electronic Devices (IEDs) that can switch the breakers on or off. These breakers are labelled BR1 through BR4. We also have two lines. Line One spans from breaker one (BR1) to breaker two (BR2) and Line Two spans from breaker three (BR3) to breaker four (BR4). Each IED automatically controls one breaker. R1 controls BR1, R2 controls BR2 and so on accordingly. The IEDs use a distance protection scheme which trips the breaker on detected faults whether actually valid or faked since they have no internal validation to detect the difference. Operators can also manually issue commands to the IEDs R1 through R4 to manually trip the breakers BR1 through BR4. The manual override is used when performing maintenance on the lines or other system components.

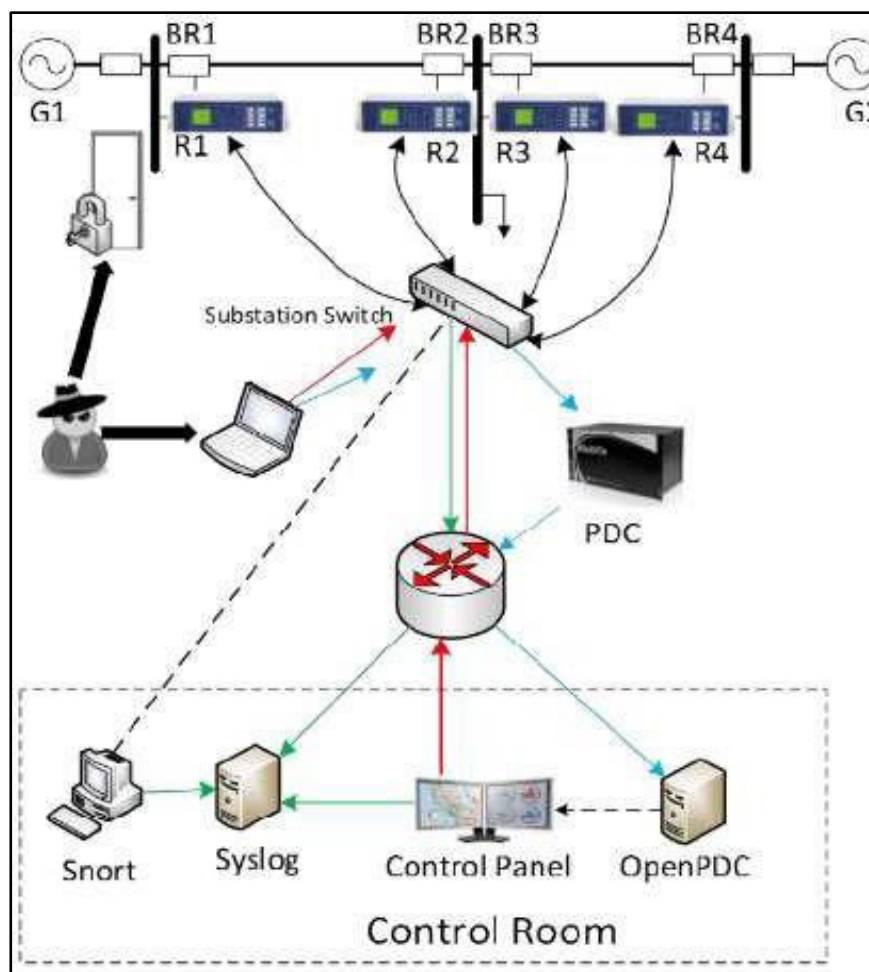


Figure 5: Smart Grid Model

2.4.2 Technical Description

The data collection consists of 37 different situations. Natural event scenarios are scenarios 1-6, 13 and 14. 7-12, 15-30 and 35-40 scenarios Attack scenarios

of events and form most of the data set scenarios. Scenario 41 is classified as a scenario for no event. In the data set, there are no scenarios 31 to 34.

Table 3: THREE-CLASS CLASSIFICATION GROUP

	Attack Events	Natural Events	No Events
Scenarios	7,8,9,10,11,12,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,35,36,37,38,39,40	1,2,3,4,5,6,13,14	41

2.4.3 Non-Attack Scenario

Within the data set, three distinct scenario types can be classed as non-attack scenarios.

2.5.3.1 Short circuit fault (Natural Event)

- 1- This is a short in the power line that can occur in various locations along the line; the percentage range indicates the location.
- 2- Six scenarios fall under this type.
- 3- Faults in these scenarios can either occur on line one or line two.
- 4- Three of the scenarios are dedicated to each line.
- 5- Faults range from 10% to 19%, 20% to 79% and 80% to 90% on both lines.

2.5.3.2 Line maintenance (Natural Event)

1. One or more relays are disabled on a specific line to do maintenance for that line.
2. This can occur on either line one or line two and only contains two separate scenarios.

2.5.3.3 Normal operation load changes (No Event)

1. This scenario describes the regular and expected load changes within the smart grid and can be considered the standard operating data.

2.5 Attack's Scenario

In this section attack's scenario will be explained further

2.5.1 Injection Remote Control Tripping (Attack)

This is an attack that sends a command to a relay, causing it to open a circuit breaker. It is possible only when an attacker has breached external defenses.

1. It is an attack that transmits a relay instruction to open a breaker. It can be done only after an attacker has breached outer defenses. (The National Laboratory of Oak Ridge and Mississippi State University, 2014).
2. Then this situation will be split into two attack kinds. This is an injection control with a single relay or Injection control with two relays.
3. For each single relay there is a command injection scenario that creates a total 4 relay attack subtypes for a command injection.
4. There is also a command scenario injecting rely one and relay two co-occurring and relay three and relay four command injection in a second scenario for a total of two scenarios for this subtype of assault. d.

2.5.2 Rely Settings Change Attack

Relays are setup with a distance protection system, and the attacker modifies the configuration to deactivate the relay function, preventing the relay from tripping in response to a legitimate fault or signal.

1. The attacker modifies the relay configuration to deactivate the relay function, preventing the relay from tripping for a legitimate fault or instruction. (Mississippi State University and Oak Ridge National Laboratory, 2014). There are three variants of this attack: disable relay function against a single relay disabled and fault, disable relay function against two relays disabled and fault, and lastly disable relay function with line maintenance.
2. This attack type is the largest of the three.
3. The first subtype of this attack causes a fault on one of the two lines inside the network, and disables one of the relays.
4. Repeat step 1 but disable 2 relays instead of 1.
5. Finally, the final subtype disables two relays and normal line maintenance.

2.5.3 Data Injection Attack

In this case, we simulate a legitimate defect by modifying the values of parameters such as current, voltage, sequence components, and so on. The goal of this attack is to blind the operator and produce a blackout.

1. In this step, we simulate a genuine fault by altering the values of parameters such as current, voltage, sequence components, and so on. The goal of this attack is to blind the operator and initiate a blackout. (Oak Ridge National Laboratory and Mississippi State University, 2014)
2. This attack scenario tries to disguise itself by replicating normal fault occurrences on lines one and two and adding a trip instruction to attack the system.

2.6 Attack Scenario Table

The information is divided into 37 distinct scenarios based on the three major categories. The table below explains this further.

Table 4. Data set Scenarios Breakdown Table

Scenario Number	Description	Type
1	Natural events (SLG faults): Fault from 10-19% on L1	Natural
2	Natural events (SLG faults): Fault from 20-79% on L1	Natural
3	Natural events (SLG faults): Fault from 80-90% on L1	Natural
4	Natural events (SLG faults): Fault from 10-19% on L2	Natural
5	Natural events (SLG faults): Fault from 20-79% on L2	Natural
6	Natural events (SLG faults): Fault from 80-90% on L2	Natural
7	Data Injection: Attack Sub-type (SLG fault replay) Fault from 10-19% on L1 with tripping command	Attack
8	Data Injection: Attack Sub-type (SLG fault replay) Fault from 20-79% on L1 with tripping command	Attack
9	Data Injection: Attack Sub-type (SLG fault replay) Fault from 80-90% on L1 with tripping command	Attack

10	Data Injection: Attack Sub-type (SLG fault replay) Fault from 10-19% on L2 with tripping command	Attack
11	Data Injection: Attack Sub-type (SLG fault replay) Fault from 20-79% on L2 with tripping command	Attack
12	Data Injection: Attack Sub-type (SLG fault replay) Fault from 80-90% on L2 with tripping command	Attack
13	Natural events (Line maintenance)	Natural
14	Natural events (Line maintenance)	Natural
15	Remote Tripping Command Injection Attack: Sub-type (Command injection against single relay): Command Injection to R1	Attack
16	Remote Tripping Command Injection Attack: Sub-type (Command injection against single relay): Command Injection to R2	Attack
17	Remote Tripping Command Injection Attack: Sub-type (Command injection against single relay): Command Injection to R3	Attack
18	Remote Tripping Command Injection Attack: Sub-type (Command injection against single relay): Command Injection to R4	Attack
19	Remote Tripping Command Injection: Attack Sub-type (Command injection against single relay): Command Injection to R1 and R2	Attack
20	Remote Tripping Command Injection: Attack Sub-type (Command injection against single relay): Command Injection to R3 and R4	Attack
21	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 10-19% on L1 with R1 disabled & fault	Attack
22	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 20-90% on L1 with R1 disabled & fault	Attack
23	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 10-49% on L1 with R2 disabled & fault	Attack

24	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 50-79% on L1 with R2 disabled & fault	Attack
25	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 80-90% on L1 with R2 disabled & fault	Attack
26	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 10-19% on L2 with R3 disabled & fault	Attack
27	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 20-49% on L2 with R3 disabled & fault	Attack
28	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 50-90% on L2 with R3 disabled & fault	Attack
29	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 10-79% on L2 with R4 disabled & fault	Attack
30	Relay Setting Change: Attack Sub-type (Disabling relay function - single relay disabled & fault): Fault from 80-90% on L2 with R4 disabled & fault	Attack
31	Scenario Not Used	N/A
32	Scenario Not Used	N/A
33	Scenario Not Used	N/A
34	Scenario Not Used	N/A
35	Attack Sub-type (Disabling relay function - two relays disabled & fault): Fault from 10-49% on L1 with R1 and R2 disabled & fault	Attack
36	Attack Sub-type (Disabling relay function - two relays disabled & fault): Fault from 50-90% on L1 with R1 and R2 disabled & fault	Attack
37	Attack Sub-type (Disabling relay function - two relays disabled & fault): Fault from 10-49% on L1 with R3 and R4 disabled & fault	Attack
38	Attack Sub-type (Disabling relay function - two relays disabled & fault): Fault from 50-90% on L1 with R3 and R4 disabled & fault	Attack
39	Attack Sub-type (Disabling relay function - two relay disabled & line maintenance): L1 maintenance with R1 and R2 disabled	Attack
40	Attack Sub-type (Disabling relay function - two relay disabled & line maintenance): L1 maintenance with R1 and R2 disabled	Attack
41	No Events (Normal operation): Normal Operation load changes	Natural

2.7 Summary

The many components of this project have been discussed in depth in this section. Although this subject is vast, a scope restriction was imposed to avoid being overburdened by the quantity of work that has to be done while yet being able to complete it in sufficient depth to make a meaningful contribution. This prior information helps us to get a deeper understanding of the subject and the pre-existing solutions. With this knowledge in place, this project may concentrate its efforts on areas that are important to both the research and application development components.

Chapter 3: Approach

3.0 Overview

This section covers the project methodology and methods used to create the tool. There will be list and explanations of the functional and non-functional needs that are identified for success or failure of the project. Furthermore, the desired purpose of the instrument using diagrams will also be explained.

3.1 Project Planning

During planning for this project's planning phase, an initial plan was issued to cover all the project requirements which include functional requirements and non-functional requirements. However, it is obvious that the project will go little bit further in order to meet all the requirements which include develop a tool to notify the user in case of attack event.

3.2 Methodologies Used

To organize how such a project should be done, a methodology must define the implementation cycles that will be utilized. This section will discuss the methods explored for applying the optimum risk assessment methodology, thus, develop the appropriate tool to notify the identified users.

When deciding on a technique, several elements of the project must be addressed. The overriding feature of the project in terms of development is the small number of developers required to create this solution. It's difficult to get frequent and informed feedback on the tool without describing every aspect of the project and the context in which it's being used, since no one other than the development team is as deeply engaged in the process. Working on this project also eliminates the possibility of frequent modifications or additions to

the requirements or solution by the client or target audience. This constraint does restrict the quantity of input that can be gathered from the intended audience. Clear and defined criteria will be set down, all of which must be fulfilled, but the manner by which this will be accomplished is not yet precisely specified. That is, as research progresses, the overall answer to the issue may alter. The last critical factor in determining the development process is the development team's expertise with different parts of the project.

After evaluating many risk assessment methods for smart grid risks, three were chosen for further consideration: the BSI ICS Cybersecurity Assessment Framework, the CEN-CENELEC-ETSI SGIS toolbox, and NIST sp.800-82. In this paper, a combination of best practices derived from the aforementioned approaches will be examined, with an emphasis on integrating the methods' advantages.

For the NIST sp.800-82 framework the cyber-defense initiative is aimed on strengthening the security of vital infrastructure. There are big, varied sets of guidelines and methods covering all kinds of IT and OT systems. NIST's strongest asset is that it has such broad applicability, as it can be used to enhance cybersecurity in major areas of IT and OT. A cyber security system cannot be developed using NIST guidelines since NIST doesn't provide a comprehensive standard. NIST, in fact, is a useful assistance for risk management and improved security posture. (Stouffer et al. 2021)

The second methodology considered is CEN-CENELEC-ETSI SGIS toolbox, the Smart Grid Information Security (SGIS) study establishes a methodology for determining the criticality of smart grid components by calculating the amount of energy lost due to possible ICT system breakdowns. It establishes five SGIS Security Levels to classify the inherent threats associated with smart grid information assets, which must be discovered through a use case study. The Security Level is determined by the impact and likelihood, with the impact expressed in five Risk Impact Levels (operational risks relating to availability; legal, human, repetitional, and financial risk), and the likelihood determined by the potential resources and intentions of various threat agents. Additionally, SGIS offers advice on the proper Security Levels for the cells of the smart grid plane, which are covered by SGAM domains and zones. Due to the fact that the SGIS risk assessment technique is designed to determine the organizational value of each smart grid information asset, it takes into account the inherent risk presented by an asset that lacks security measures.

As a result, this clean-slate method is not well-suited for evaluating cybersecurity risks associated with current infrastructure. Due to the gradual nature of smart grid deployment, in which the existing power grid is transformed into an intelligent grid, a realistic cybersecurity risk management strategy must be capable of dealing with a complicated mix of old systems and new technology. (Langer et al.2016), (Langer et al.2015)

As we continue exploring the methodologies the last method is BSI ICS Cybersecurity Framework Assessment which is the one to be used to conduct the risk assessment and it propose a new framework based on BSI with integrating some of the other methodologies. The proposed scheme is defined in 8 steps aimed to use the best practices of the mentioned methodologies. Moreover, and to address the continues on-going nature of the process all the steps are following the Plan-Do-Check-Act (PDCA) methodology. (ICS Cybersecurity Assessment Framework. 2021)

3.3 Requirements Specifications

The requirement specification is the tool's foundation. It aids in establishing a framework for the development process. It provides vital information required to complete our job. Functional requirements are criteria that must be met for the tool to operate properly. Non-functional criteria assist improve the tool's usability and increase its capability.

3.3.1 Functional Requirements

- Read a .CSV file extracted from system logs

The logs file is the only input of the date that the tool will receives. Therefore, the tool should also contain a small part of detection relying on ML (Machine Learning) and based on the tool detection a notification should be sent to the write end-user. Also, the file should be in CSV form to avoid any error that may occur in the execution stage.

- Check for error

the data extracted from the file is critical and must be double-checked to verify that it is not duplicated, redundant, or in the wrong format. This will include verifying that the file originated from the right place and is in the proper format to be analyzed.

- Remove unnecessary logs

Some logs included within the data do not contain any information that may be used by the program. As a result, they are completely ineffective for our objectives. By removing these, we can guarantee that we are not processing any additional information that is not required and has no effect on the estimate. We get exponentially more advantages from doing so as the amount of data we analyze increases in quantity. This will guarantee that a real-time prediction is made in a timely manner.

- Analyze and detection of short circuit fault

When a file is identified and error-checked, the tool that must look for indications of a short circuit fault and flag the necessary information. Because this is not an attack, no further action is required.

- Analyze and detection of Line maintenance

When a file is identified and error-checked, the tool that must look for indications of line maintenance and check the system if there is a maintenance scheduled, if not; the tool should consider this as an attack and should notify the right user of this behavior.

- Analyze and detection of rely setting attack

When a file is identified and error-checked, the tool that must look for indications of rely setting attack, if found it should be flagged and the tool should notify the end-user as soon as the attack flagged.

- Analyze and detection of data injection attack

When a file is identified and error-checked, the tool that must look for indications of data injection attack, if found it should be flagged and the tool should notify the end-user as soon as the attack flagged.

- Analyze and detection of remote trip command injection attack

When a file is identified and error-checked, the tool that must look for indications of remote trip command injection attack, if found it should be flagged and the tool should notify the end-user as soon as the attack flagged.

- Analyze and detection of suspicious behaviors

Basically, the tool should be able to identify any new installation on the system and based on connected database the tool should be able to identify any new or undetected attack and store its information with notifying the administrator.

- System monitoring

There must be continuous check by the tool for the system safety with the ability to analyze any file format in the future – if extended -.

- Give detailed information about the attack

One of the important features is the ability to show the report of the attack once the user asks for it. Thus, the tool should be able to retrieve any attack data to re-analyze it or suggest a new procedure in order to defend against such threats or attacks.

- Recommendation guide

The tool should show some recommendations about previous attacks detected and what are the best decision can be taken to mitigate the attack impact.

3.3.2 Non-Functional Requirements

- Easy data representation

Data should be implemented easily to be used widely by users. Another aspect is, ease of access to the tool, in other words the tool should be available as open source in case of future development or modification by others.

- GUI interface should be available

In order to implement the analysis, a GUI interface should be available shows information about the progress and what is to be analyzed by the tool. Basically, a GUI inter face should be able to show up the important information.

- The data is presented in a logical arrangement

The material given must be clear, precise, and well-organized in order for the reader to be able to readily comprehend it.

- The deployed data should be far from complication

As too much details could be destructive for normal users and serve only few kinds of users, the data deployed should be clear concise and well-organized which allow any reader to read the information.

- Color representation of the incidents

Using color representation to differentiate between the attack events and normal events is very powerful technics. Evidence of this, most of the ticketing system available in today's market using the color codes to differentiate between the critical events and normal and much more.

3.4 Summary

The project plan was presented as a Gantt chart to help visualize the various tasks and deadlines. This is in the appendix. The selected approach enables for ongoing project plan changes as new problems emerge. To address these issues, the strategy needs to be revised. This independence has been important since it implies this thought is unrestricted. These modifications may be made as long as the criteria are fulfilled in the final output.

Chapter 4: System Implementation

4.0 Overview

A summary of the platform and standards to be utilized for the tool's development can be found in this section. An explanation of how the tool works will be provided, including information about its various features and capabilities, while illustrating processes through flowcharts and screenshots of the tool. This section also will try to look deeply in the issues faced when such a tool is developed and come up with a solution to overcome the design limitations if possible.

4.1 Platform Used

This section, will focus on the specification of the computer used and the program language used to develop the tool and other relevant tools are to be discussed in order to provide a comprehensive view for the reader of this project.

4.1.1 Setup Used

This project was developed using my personal laptop, MACBOOK PRO 16 inches 2018 and the specifications can be found below:

- Processor: 2.6 GHz 6-Core Intel Core i7
- Memory: 16 GB 2400 MHz DDR4
- Architecture: 64 bits
- Operating System: macOS Big Sur (version 11.5.2)
- Operating System: Windows 10 (VM ware)
- Graphics: Intel UHD Graphics 630 1563 MB

4.1.2 Experimental Setup

In this section all tools related to this paper will be explained in the next sub-sections

4.1.2.1 Power World

Power World Simulator is an interactive power system simulation software that allows you to model the functioning of a high voltage power system over a time period ranging from few minutes to many days. The program includes a powerful power flow analysis tool capable of solving systems with up to 250,000 buses effectively. The system also allowing the users to simulate cyber-attacks on the whole grid or particular asset.

4.1.2.2 Python

Python, according to my research, would be a better fit for this application. The Python libraries comes in useful here. This module simplifies the execution of notification technique and other functions from inside Python 3. It can be built using python with many different ways to apply the techniques methods. This kind of application requires a certain amount of research, mostly in terms of choosing methods and choices for notification and alert methods, and Python is simpler to use and understand. however, power world will be used as a simulation platform while the notification tool will use Python for overall execution. Python will be utilized as the tool's programming language for these reasons.

4.2 System Design

In this section, system and assets related to system will be explained in details with tables and diagrams to illustrate how the tool will work and will provide a comprehensive view of the system model

4.2.1 System Model

This system contains two actors the first one is the operators working on the system room and monitoring the smart grid components and the second actor is the malicious attack. Based on predication, the tool should identify the malicious behavior against pre-identified assets; if an attack detected, the tool should capture the attack logs and notify the write operator to take a decision to mitigate attack impact on the smart grid system. This will allow us to taste a new kind of detection and notification in terms of smart grid security, as well as will improve our ability to design extended tools on the future to overcome the heterogeneity limitation in smart grid standardization system.

The power system framework setup utilized to generate these scenarios is shown in the image below. The network diagram has various components, the

first of which are power generators G1 and G2. R1–R4 are Intelligent Electronic Devices (IEDs) that can turn breakers on and off. These breakers are designated as BR1 through BR4. In addition, we have two lines. Line One connects breaker one (BR1) to breaker two (BR2), while Line Two connects breaker three (BR3) to breaker four (BR4) (BR4). Each IED is programmed to control one breaker. R1 controls BR1, R2 controls BR2, and son on as appropriate. Because they lack internal validation, IEDs utilize a distance protection method that trips the breaker on detected faults regardless of whether they are genuine or contrived. Operators may also give orders to the IEDs R1 through R4 to trip the breakers BR1 through BR4. When doing maintenance on the lines or other system components, the manual override is employed. These devices are connected to the substation switch which provide the communications phase between OT and IT systems. Finally, we have the IT systems which contains the IDS, System log, Control Panel and Open PDC in order to monitor the network traffic passing through the system.

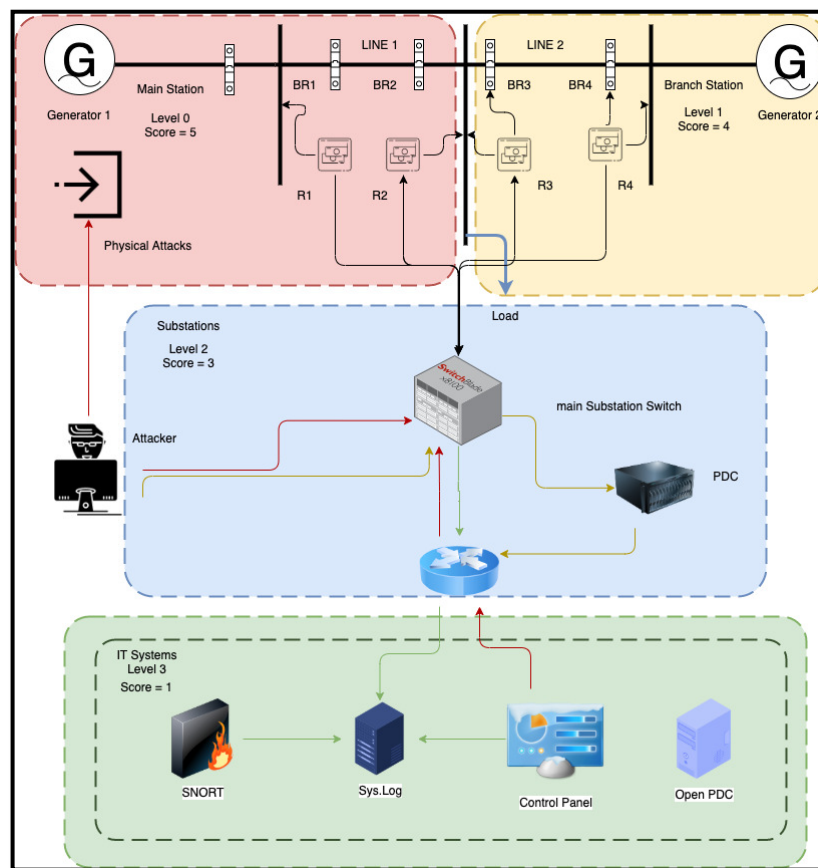


Figure 6: System Model Diagram

4.3 Proposed Risk Assessment

In the past, security was neglected in the first and second generations of SCADA systems due to vendor-proprietary settings. When such air-gapped SCADA systems were initially linked to the Internet, cyber attackers penetrated them by exploiting publicly known information security vulnerabilities. The majority of vulnerabilities in information technology systems have been fixed, including those in operating systems, commercial software, and communication protocols. Thus, the first step toward improving the security of SCADA systems is to minimize risks associated with known threats and vulnerabilities by regularly developing and implementing recommendations for security controls and alternative solutions.

Due to resource constraints, businesses must balance the expense of adopting security controls and solutions against the potential losses from cyber-attacks before implementing the suggested security measures.

4.3.1 System Assets

In this use-case scenario, the system contains two aspects the first aspect is the operators and it will be explained

4.3.1.1 Assets Identification (People)

This section will focus on identifying the people engaged in the given scenario and explain their responsibilities in the smart grid network. Table below shows the assets (people) identifications.

Table 5: Assets Identification (Saxena et al. 2016)

	Assets ID	Name	Description	Permission
People	1	Operator (1-2)	Controlling and monitoring the smart grid network remotely or in place	Full control of the network
	2	Security officer (4)	In place security for smart grid critical datacenter, Monitoring the system from the control room and notify the operators and maintenance in case of incidents	Read / Write / Modify
	3	Maintenance personnel (4)	Maintenance personnel is responsible for monitoring, fix and check the smart grid physically	Read Only
	4	Communication engineer (4)	Design and test the equipment's and check if they are working properly	Add / Modify

4.3.1.2 Asset Identification (OT and IT)

Table 6: Assets Identification

Asset ID	Name	Description	Priority
OT assets			
1	Generator 1	Generating the electricity and also transform them from form to another	
2	Generator 2	Generating the electricity and also transform them from form to another	
3	Breaker 1 (BR1)	a switch that protects an electrical circuit from overload or short circuit.	
4	Breaker 2 (BR2)	a switch that protects an electrical circuit from overload or short circuit.	
5	Breaker 3 (BR3)	a switch that protects an electrical circuit from overload or short circuit.	
6	Breaker 4 (BR4)	a switch that protects an electrical circuit from overload or short circuit.	
7	Rely1 (R1)	electrical switches that open and close circuits based on external electrical signals	
8	Rely2 (R2)	electrical switches that open and close circuits based on external electrical signals	
9	Rely3 (R3)	electrical switches that open and close circuits based on external electrical signals	
10	Rely4 (R4)	electrical switches that open and close circuits based on external electrical signals	
11	BUS1 (L1)	Line used to connect and transform voltage or current all over the smart grid network	
12	BUS2 (L2)	Line used to connect and transform voltage or current all over the smart grid network	
13	Substation	A switching station works on a single voltage level. Stations may serve as both collection and distribution locations as needed.	

As the tables shows the smart grid system in this case-study contains pre-defined assets consists both OT and IT assets. However, only OT assets will be undergoing through risk assessment, which means the IT assets will not be considered in the attack's scenarios.

4.3.2 Risk Calculation

As initial step some terms must identified and classified, this is because we are dealing with dataset never been used to conduct a risk assessment before. Thus, assumption should take a place to identify what are the boundaries of the selected system. For example, how critical is each asset and what are the expected loss on different scales. Basically, standard like DREAD and STRIDE should be used to identify our system boundaries. Hence, formula (1) is to be used to calculate to the overall risk on based on the attack traffic which using particular assets to exploit the other system assets. The assets used to exploit

attacks are: R1-R4 with L1-L2 applying three types of attacks affecting the other assets, hence the below formula is used to calculate the overall risk first on those attacked assets to give us the chance to measure the attacks on every single asset in the network.

$$\text{Overall Criticality} = \frac{(\sum Sc) * Bs}{Ac} + \text{Impact}$$

Where the Sc is the submission of the criticality of the scenario on selected relay (R) or bus (L) scaled using DREAD methodology where 7 – 10 represent **high** attack severity and from 4 – 6 is a **medium** attack while any attack scores 1 – 3 is a **low** attack criticality. Bs is the score of the bus-line on our network (0-5), and the impact is scaled by how critical is the location of the asset and how many attacks executed against that particular asset. For example, relay2 (R2) and bus1 (L1) are the most asset incurred attacks among the others, hence the impact will be high for both due to their location and the number of the attack was executed against those assets while the impact is declined gradually for relay 1 (R1) due to it has less attack than relay (R2) even though they are on the same bus (L1) (location) and so on. Ac_s represent the number of the attack was executed against particular asset among the six asset we have to calculate overall criticality.

e.g., if we want to calculate the criticality of R1 it should be as follows:

R1 (attack 2) = $(56 * 5 / 2) + 5 = 144$, this is the risk associated with attack 2 on relay one (R1).

R1 (attack 3) = $(56 * 5 / 6) = 50.6$, this is the risk associate with attack 3 on relay one (R1). Hence, the overall criticality should be the summation of attack 1, 2 and 3 divided by 3.

Which should be:

Overall criticality = risk 1 + risk 2 + risk 3 / 3

Overall criticality = $0 + 144 + 50.6 / 3 = 64.86 \sim 65 / 100 = 65\%$ and so on.

Regarding to the risk of attack 1 on the same asset (R1) it is zero because there is no appearance of risk 1 on the pointed asset.

Table 7: Overall criticality of the assets

Asset	$\sum Sc$	Bs (score)	impact (0-5)	accuracy -attack1	accuracy - attack2	accuracy - attack3	Risk-attack1	Risk-attack2	Risk-attack3	overall Risk
R1	56	5	4	0	2	6	0	144	50.66666667	65%

R2	62.6	5	5	0	2	7	0	161.5	49.71428571	70%
R3	49.4	4	3	0	2	5	0	101.8	42.52	48%
R4	42.8	4	2	0	2	4	0	87.6	44.8	44%
L1	89.7	5	5	3	0	11	154.5	0	45.77272727	67%
L2	50.1	4	3	3	0	5	69.8	0	43.08	38%
G1	24.6	5	4	0	3	0	0	45	0	15%
G2	24.6	4	2	0	3	0	0	34.8	0	12%

Based on the criticality table the most critical asset can be identified in the following table.

Table 8: Asset Criticality based on number of attacks and location Severity

Likelihood	Consequences				
	insignificant	Minor	Moderate	Major	Severe
Almost Certain			R4	R1	R2
Likely			L2		L1
Possible	G2		G1	R3	
Unlikely					
Rare					

As we have identified the assets and related attacks with their scenario, we should identify each attack impact based on DREAD scale.

Table below shows the three types of the attacks in this case-study and how are they measured on DREAD scale to identify which one is the most critical and so on.

Table 9: Impact of each attack on DREAD scale

DREAD scale Attack	Damage	Reprodu cibility	Exploitability	Affected users	Discoverability	total	Impact
Tripping command data injection	5	7.5	5	6	5	5.7	Medium

Remote code injection	10	8	8	7	8	8.2	Critical
Relay setting change	8	6	9	6	4	6.6	High

To control the risks associated with SCADA systems, an innovative and ongoing risk management cycle may be established. This cycle should include risk modeling, risk assessment, risk response, and risk monitoring (Plan-Do-Check-Act).

4.3.3 Estimated Risk to Each Scenario

In this section, as the assets and attacks were mentioned in beginning of this chapter and in chapter 2; estimated risk will be calculated based on the result of the overall risk to identify the risk matrix. As well as specify what are the critical assets to give the priority to be recovered as soon as possible.

To calculate the estimated risk related to each scenario separately a formula (2) is calculating the estimated risk based on the calculated overall risk and the attack severity targeting asset in assigned situation with addition of the volts of the scenario to differentiate among the scenarios.

$$E_R = \sum Overall Criticality * Attack Sevrity + V$$

Where E_R represent the estimated risk relying on values already calculated and the $\sum Overall Criticality$ represents the summation of the affected asset criticality which represented in table 6. V is the volt in the pointed scenario with taking in consideration the scenario with no volt (scenario 15 – 20) the volt will be assigned to 0 in order to calculate the risk in the different scenario. Furthermore, risk will be calculated using the maximum voltage e.g., scenario 7 the voltage is from 10% to 19% and in our calculation 19% (0.19) considering the maximum rate of the risk.

Where 11 – 15 = High Risk, 5 – 10 = Medium Risk, 1 – 5 = Low Risk and >15 is Critical

e.g., the risk associated with Scenario 7 (s7) can be calculated as follows:

S7 is affecting line 1 (L1) hence, the overall criticality should be 0.67 (67%) multiplied by attack severity (5.7) of the s7 based on DREAD scale, in addition to the volts in scenario 7 as mentioned the maximum volt will be considered. In this example, scenario 7 is calculated and the volt in scenario 7 is 0.19 (19%).

$$S7 = 0.67 * 5.7 + 0.19 = 4, \text{ (Low risk)}$$

4.3.4 Risk Matrix Table

Risk matrices, also known as risk severity matrices, may assist you in prioritizing risks. Once you've determined the severity and probability of your risks, priorities them. Color coding helps in visualizing risk rankings, and you can also label zones in your matrix as generally acceptable (GA), as low as reasonably possible (ALARP), or generally undesirable (GU) to provide an instant assessment of which risks to priorities.

Table 10: Risk Matrix Table

Scenario	Affected Assets	Risk score
7	Transmission lines and breakers	(4) Low
8	Transmission lines and breakers	(4.6) Low
9	Transmission lines and breakers	(4.7) Low
10	Transmission lines and breakers	(2.3) Low
11	Transmission lines and breakers	(3) Low
12	Transmission lines and breakers	(3) Low
15	Relays, Generators	(12) High
16	Relays, Generators	(12.4) High
17	Relays, Generators	(8) Medium
18	Relays, Generators	(7.7) Medium
19	Relays, Generators	(17.7) Critical
20	Relays, Generators	(11.2) High
21	Transmission lines, relays and breakers	(8.9) Medium
22	Transmission lines, relays and breakers	(9.6) Medium
23	Transmission lines, relays and breakers	(9.5) Medium
24	Transmission lines, relays and breakers	(9.8) Medium
25	Transmission lines, relays and breakers	(10) Medium
26	Transmission lines, relays and breakers	(5.8) Medium
27	Transmission lines, relays and breakers	(6) Medium
28	Transmission lines, relays and breakers	(6.5) Medium

29	Transmission lines, relays and breakers	(6.2) Medium
30	Transmission lines, relays and breakers	(6.3) Medium
35	Transmission lines, relays and breakers	(13.8) High
36	Transmission lines, relays and breakers	(14.2) High
37	Transmission lines, relays and breakers	(11) High
38	Transmission lines, relays and breakers	(11.3) High
39	Transmission lines, relays and breakers	(13.3) High
40	Transmission lines, relays and breakers	(13.3) High

4.3.5 Potential Risk

basically, we need to identify what is the potential risk which can be identified as a cyber or cybersecurity threat is an intentional act that aims to destroy data, steal data, or otherwise harm virtual world. Computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors are all examples of cyber dangers.

Cyber dangers can include the potential of a successful cyber-attack aimed at gaining unauthorized access to, damaging, disrupting, or stealing an information technology asset, network node, intellectual property, or any other kind of sensitive data. Cyber risks may originate from trusted people inside an organization or from distant places by unknown outsiders.

Unlike the IT system which can be measured on the scale of CIA triad (Confidentiality, Integrity and Availability) OT environment scale can be derived from IT scale with small change to look like this AIC triad (Availability, Integrity and Confidentiality) this is because the attack launched against availability can be the most dangers since it affecting wide range of customers and keep their neighbors in the dark for long periods. The table below shows all the attacks categories related to this use-case scenario and what are the affected assets with affected region in case of the active attack. This will be categorized on various areas based on the impact of the attack.

Table 11: Potential threat associated with each attack

Attack	Threat	Affected assets	Examples	Area
Data Injection	Possible blackout for long time and	BUS1(L1) and BUS2(L2), wide	Malware, DDOS attack and	Availability, Integrity

	can be spread to affect more than one spot of smart grid	range of customer network will be under effect of the blackout	injecting malicious code to manipulate current or voltage	
Remote tripping command (Aurora Vulnerability)	Possible damage to the generators and may cause complete failure to the system of smart grid besides, human losses and possible blackout due to the failure of the system	Generators (G1, G2), Operators (Vendor engineers, security officer and administrators), Relays (R1, R2, R3 and R4) and Breakers (BR1, BR2, BR3 and BR4)	As written in the name of this attack RCE is a possible example of Aurora Vulnerability, Insider attacker is a good example of this attack	Integrity
Relay setting change	Manipulation of the customer data so, it appears not accurate, also can manipulate the voltage and current to disable electric lines.	Relays (R1, R2, R3 and R4) and Breakers (BR1, BR2, BR3 and BR4 and BUS1 (L1) and BUS2(L2) and customers	Malware injected in the system either remotely or physically, customers may be able to manipulate some AMI functions to affect the smart grid relays and injecting false data	Integrity, confidentiality

4.4 Tool Functionality

The majority of the notification systems related to notification technology are not efficient in terms of smart grid. Smart grid system is a combination of OT systems interconnected with IT systems this is resulted in heterogeneity among these devices. Another issue is, standardization which allow the manufacturers to develop smart devices on their demand not caring about what others standards need or how to work all together without being in critical situations, this is resulted in wide market of smart grid component with different standards and less effective against cyber-attack due to the weak protection schema. Another aspect of the problem is, the detection systems or methodology which are agreed on the same technics by monitoring the network traffic while there is no single solution that may overcome the emerged attack in the smart grid systems. Thus, my proposed solution is by creating a tool to monitor traffic whether it is network or electricity inside the smart grid network and notify the end-user (operator) in case of suspicious behavior based on identified attacks database.

4.5 The Overall Workflow of The Idea

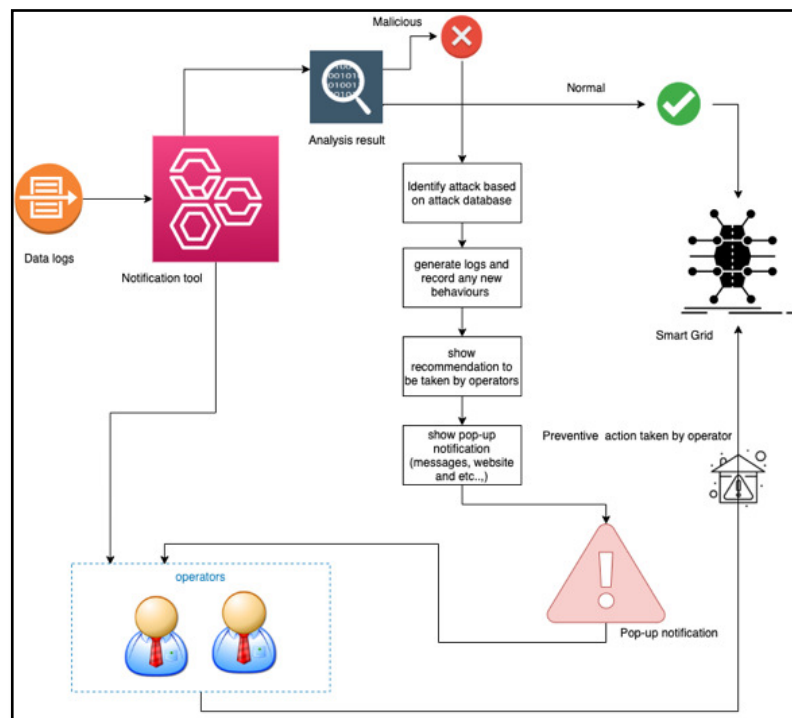


Figure 8: the overall Idea of the tool

As the figure shows, data imported from the dataset file and by using python code, tool should analyze the inserted data and based on the results user can choose from a list the scenario to be simulated. Once scenario is chosen by a user the tool should be able to show all information related to the attack based on predefined tables. Both normal and attack scenario can be simulate using the tool. In the notification action, the tool should be able to show what is the attack type, impacted assets and the severity of the attack which can be defined by the color code with ability to show the users to be notified based on table 4. After that, send instruction to a user by pop-up window showing the attack ID and some related information with the time remaining to take action, besides some recommendation can be taken. Finally, user notified and can take action based on what is the right defense action in that particular situation.

4.6 Notification Technique

Users can be notified using different techniques however, due to our use-case scenario which have only three types of cyber-attacks on smart grid our technique can be quite narrow which only limited to notify the users without taking actions. Thus, in this section the three types of scenarios will share the

same methods of notification and the difference only will be in the users notified for all possible scenarios.

Table 12: Notification Technique

Scenario	Description	Effect	Users
7	Data Injection Attack Sub-type (SLG fault replay) Fault from 10-19% on L1 with tripping command	Possible blackout for long time and can be spread to affect more than one spot of smart grid	Operator 1 (web), security officer 1 (web) and Maintenance personnel 1 (text)
8	Data Injection Attack Sub-type (SLG fault replay) Fault from 20-79% on L1 with tripping command		
9	Data Injection Attack Sub-type (SLG fault replay) Fault from 80-90% on L1 with tripping command		
10	Data Injection Attack Sub-type (SLG fault replay) Fault from 10-19% on L2 with tripping command		Operator 2 (web), security officer 2 (web) and Maintenance personnel 2 (text)
11	Data Injection Attack Sub-type (SLG fault replay) Fault from 20-79% on L2 with tripping command		
12	Data Injection Attack Sub-type (SLG fault replay) Fault from 80-90% on L2 with tripping command		
15	Remote Tripping Command Injection Attack Sub-type (Command injection against single relay) (R1)	Possible damage to the generators and may cause complete failure to the system of smart grid besides, human losses and possible blackout due to the failure of the system	Operator 1 Security officer 1 (web) / Communication engineer 1 (both)
16	Remote Tripping Command Injection Attack Sub-type (Command injection against single relay) (R2)		Operator 1 Security officer 2 (web) / Communication engineer 2 (both)
17	Remote Tripping Command Injection Attack Sub-type (Command injection against single relay) (R3)		Operator 2 Security officer 3 (web) / Communication engineer 3 (both)
18	Remote Tripping Command Injection Attack Sub-type (Command injection against single relay) (R4)		Operator 2 Security officer 4 (web) / Communication engineer 4 (both)
19	Remote Tripping Command Injection Attack Sub-type (Command injection against two relay) R1+R2		Operator 1, Security officer 1,2 (web) / Communication engineer 1,2 (both)
20	Remote Tripping Command Injection Attack Sub-type (Command injection against two relay) R3 + R4		Operator 2 Security officer 3,4 (web) / Communication engineer 3,4 (both)

21	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 10-19% on L1 with R1 disabled & fault	Manipulation of the customer data so, it appears not accurate, also can manipulate the voltage and current to disable electric lines.	Operator 1 (web), security officer 1 (web) and Maintenance personnel 1 (text) Communication engineer1 (both)
22	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 20-90% on L1 with R1 disabled & fault		Operator 1 (web), security officer 2 (web) and Maintenance personnel 2 (text) Communication engineer 2 (both)
23	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 10-49% on L1 with R2 disabled & fault		
24	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 50-79% on L1 with R2 disabled & fault		
25	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 80-90% on L1 with R2 disabled & fault		
26	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 10-19% on L2 with R3 disabled & fault		Operator 2 (web), security officer 3 (web) and Maintenance personnel 3 (text) Communication engineer 3 (both)
27	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 20-49% on L2 with R3 disabled & fault		
28	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 50-90% on L2 with R3 disabled & fault		
29	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 10-79% on L2 with R4 disabled & fault		Operator 2 (web), security officer 4 (web) and Maintenance personnel 4 (text) Communication engineer 4 (both)
30	Relay Setting Change Attack Sub-type (Disabling relay function - single relay disabled & fault) Fault from 80-90% on L2 with R4 disabled & fault		
35	Relay Setting Change Attack Sub-type (Disabling relay function - two relays disabled & fault) Fault from 10-49% on L1 with R1 and R2 disabled & fault		Operator 1 (web), security officer 1,2 (web) and Maintenance personnel 1,2(text) Communication engineer 1,2(both)
36	Relay Setting Change Attack Sub-type (Disabling relay function - two relays disabled & fault) Fault from 50-90% on L1 with R1 and R2 disabled & fault		
37	Relay Setting Change Attack Sub-type (Disabling relay function - two relays disabled & fault) Fault from 10-49% on L1 with R3 and R4 disabled & fault		Operator 1,2 (web), security officer 3,4(web) and Maintenance personnel 3,4(text) Communication engineer 3,4(both)
38	Relay Setting Change Attack Sub-type (Disabling relay function - two relays disabled & fault) Fault from 50-90% on L1 with R3 and R4 disabled & fault		
39	Relay Setting Change Attack Sub-type (Disabling relay function - two relay disabled & line maintenance) L1 maintenance with R1 and R2 disabled		Operator 1 (web), security officer 1,2 (web) and Maintenance personnel 1,2(text)
40	Relay Setting Change Attack Sub-type (Disabling relay function - two relay disabled & line maintenance) L1 maintenance with R1 and R2 disabled		Operator 1 (web), security officer 1,2 (web) and Maintenance personnel 1,2(text)

Table 11: Notification table

4.7 System Vulnerabilities

Considering the system to be a SCADA system it might consist of a series of vulnerabilities that might include:

4.7.1 Generic OS

SCADA systems often run over traditional working structures (OS), hence inheriting vulnerabilities that might compromise the SCADA system. The vulnerabilities of the running structures are periodically introduced through the vendors. The patches are typically issued after vulnerabilities are discovered, however there may be a full-size time lag to release patches or the patches might not be implemented in time.

4.7.2 Multiple Points of Entry and Failure

A SCADA system is geographically spread over a large vicinity beginning at the sensors, with inside the subject, to the person and control interface. Although SCADA servers might also additionally themselves be well included in opposition to cyber-attacks, but comparable ensures do now no longer exist for subject devices. The conversation network, comprising of Wi-Fi Internet, mobile and Bluetooth provide a couple of far-off access factors which may be exploited by attackers. Wireless networks are specifically prone using freely to be had gear like Air crack-NG that could sniff, check and even decrypt packets

4.7.3 Communication Protocols

The low-degree networking protocols used for industrial structures use easy plain-text messages primarily based totally on a master slave communications model. These lack safety and encryption, as those had been designed for remoted structures. Widely used protocols IEC60870-5-one zero one and IEC 60870-5-104 lack software and data hyperlink layer safety and feature vulnerabilities that may be exploited. With an expertise of the technique and the protocol, an attacker can maliciously adjust the technique manage through injecting legitimate manage instructions and responses with malicious intent. Attacks on protocol implementation can purpose screw ups ensuing in possible exploits

4.7.4 Integral Protection

With cyber safety recognition getting into prominence, SCADA producers additionally offer and emphasize safety in products. These functions offer encryption and safety functions which includes Kerberos and multiplexing proxy. Activating those in an assignment could make an intruder's project

difficult. SCADA structures additionally offer different integrated mechanisms such as User Groups, Historian, Encryption and Redundant Servers

4.7.5 Real-time and Complex Interactions

SCADA structures screen real-time procedures beneath Neath very tight timing and operational constraints. Time is essential for choice making, affecting a managing machine and crucial process deviations, which should be appropriately pondered and effectively managed. The stringent operational constraints (such as timing) of a SCADA machine imply that it is far extra susceptible to fail in reaction to small deviations due to an attacker. "Aurora Generator Test" in March 2007, simulated a remote cyber-attack ensuing in destruction of a \$1 million dollar diesel-electric powered generator. A patch application or loss of time synchronization can also additionally have accidental consequences adverse to the prescribed operation. Application of a software program replace led to computerized shutdown of a nuclear plant [10]. Analysing and exploiting vulnerabilities can also additionally be complex however unintelligent laptop viruses and mere malfunctions in small gadgets can bring about enormous accidental effects

4.8 Dataset and Pre-processing

It is critical to have a comprehensive knowledge of the data collection that will be used to test and assess all of the project's components. This knowledge will allow us to better evaluate and comprehend each attack' behavior, as well as any shortcomings that may emerge. The dataset components that are pertinent to the findings and assessment will be emphasized in this section.

4.8.1 Dataset Parameters

The data collection contains 37 distinct situations. These 37 distinct situations are then grouped into three distinct categories: natural disaster scenarios, no-event scenarios, and attack event scenarios. These distinct scenario types (with the exception of no-event scenarios) are then further classified into subclasses.

Natural occurrences may be classified into two distinct scenario categories. A single line to ground fault is the first kind of natural occurrence. This happens when one conductor falls to the ground or inadvertently contacts a neutral conductor on a transmission line. These faults may occur on electricity networks as a result of unrelated occurrences such as high-speed wind, a fallen tree breaking the line, or even lightning. The following natural occurrence is line maintenance. Line maintenance happens on a scheduled basis, and it is

necessary to do planned maintenance to maintain it in operating condition. This occurrence will cause certain errors, which the user should anticipate.

Three distinct kinds of attack event scenarios exist. The first is a relay setting modification; this happens when an attacker modifies the setting distance of a relay's protection scheme such that it no longer trips for a legitimate fault or instruction. The second of these attacks involves the insertion of a remote trip command. This happens when an attacker delivers instructions to a relay, causing it to open the Breakers. A data injection attack is the last kind of attack. Data injection happens when an attacker alters a value, such as current or voltage, to resemble a valid fault, with the intent of blinding the operator and causing a blackout. This is the kind of attack that we must be most vigilant about, since it directly affects the data on which we depend.

4.8.2 Pre-processing

The dataset used in this project was undergone a pre-processing procedure to assure the validity of being assessed by the available tool. Moreover, the dataset was examined to identify the fundamentals information to help to set the critical assets and the main lines to measure the risk against the available assets. As well as, this dataset contains an IT system asset which are not included in the risk assessment procedure. This is because, this paper meant to conduct a risk assessment in the OT systems only since the majority of IT systems can be measured by the available tools and framework of risk assessment and they are accurate to some extent.

4.9 Summary

In this section, risk assessment was conducted and each asset identified with risk associated to it and the requirement of this project are discussed. Also, the tool is identified and the mechanism of how the tool should work in terms of notification. From the information mentioned in this section, the evaluation of the results in the next section will take a place to achieve the project goals.

Chapter 5: Results and Evaluation

5.0 Overview

In this section, the overall work which examined in chapter 3 and 4 will be discussed and show how some of chosen attacks are affecting the power grid systems. As well as, the evaluation of the result will take place in this chapter.

5.1 Findings

This section will go through key points to consider while generating these assessments, as well as any key findings from the findings.

5.2 Tools snapshots

This section will be about the tool and how it works and it will be explained with testing the scenarios.

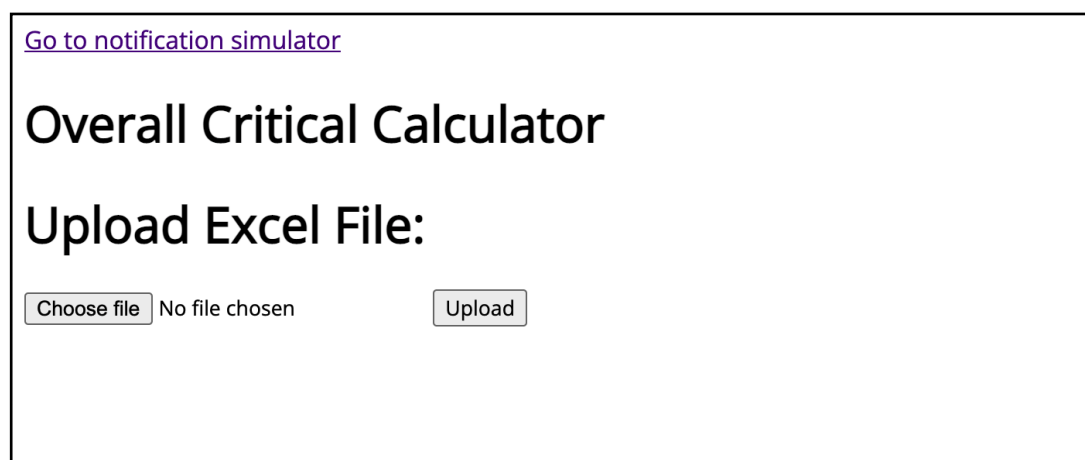


Figure 9: Tool 1.0 screenshots (the overall criticality calculator)

This is the first part of the tool where we can upload excel with the assets in our system and the tool will calculate the overall criticality of the assets inserted.

Risk-attac1	Risk-attack2	Risk-attack3	overall Criticality
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Figure 10: Tool 1.0 screenshots (table of the assets before using the tool)

As show in the above figure these values are all zero and once, we upload the file to our tool these values will be overall criticality will be calculated as the next figure shows.

[Go to notification simulator](#)

Overall Critical Calculator

Upload Excel File:

Choose file function_vars.xlsx

Upload

Figure 10: Tool 1.0 screenshots (file upload to the tool)

[Go to notification simulator](#)

Overall Critical Calculator

Upload Excel File:

No file chosen

Figure 11: Tool 1.0 screenshot

Now as shown in the above figure the file was uploaded and the values were created and saved to excel sheet as we will in the next figure. Once, we press the download button the tool will install our calculated version of the results.

s-36	s-37	s-38	s-39	s-40	ation of se	busline	mpact (0-5	rancy-att	rancy-att	rancy-att	risk1	risk2	risk3	overall-critical-risk
6.6	0	0	6.6	6.6	56	5	4	0	2	6	0	144	50.66666667	65%
6.6	0	0	6.6	6.6	62.6	5	5	0	2	7	0	161.5	49.71428571	70%
0	6.6	6.6	0	0	49.4	4	3	0	2	5	0	101.8	42.52	48%
0	6.6	6.6	0	0	42.8	4	2	0	2	4	0	87.6	44.8	44%
6.6	6.6	6.6	6.6	6.6	89.7	5	5	3	0	11	154.5	0	45.77272727	67%
0	0	0	0	0	50.1	4	3	3	0	5	69.8	0	43.08	38%
0	0	0	0	0	24.6	5	4	0	3	0	0	45	0	15%
0	0	0	0	0	24.6	4	2	0	3	0	0	34.8	0	12%

Figure 12: Tool 1.0 screenshots (criticality result)

The results were calculated and the formula was applied to get the results and the whole process can be done automatically.

Next part of the tool is the notification section where I can simulate one of the attacks and what the type of notification and to whom it should be sent and this is will be explained below.

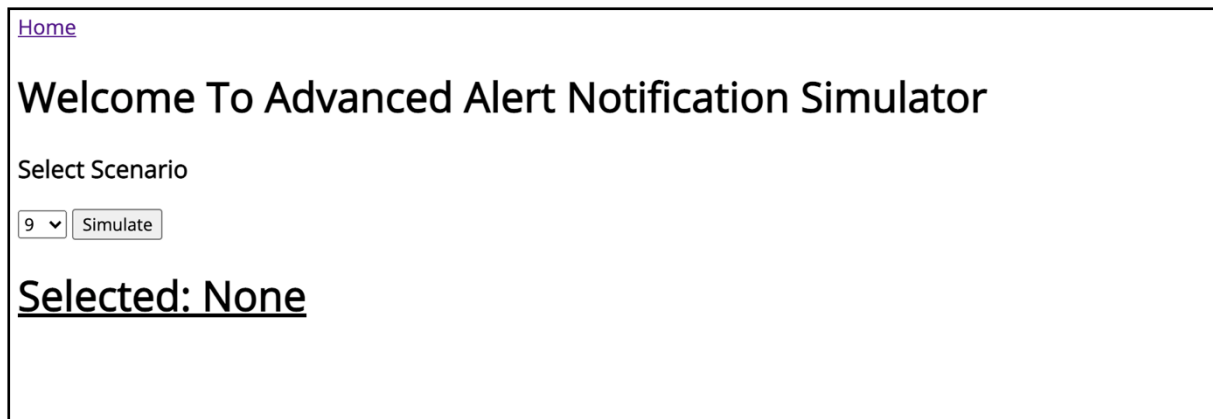


Figure 13: Tool 2.0 screenshots (first screen)

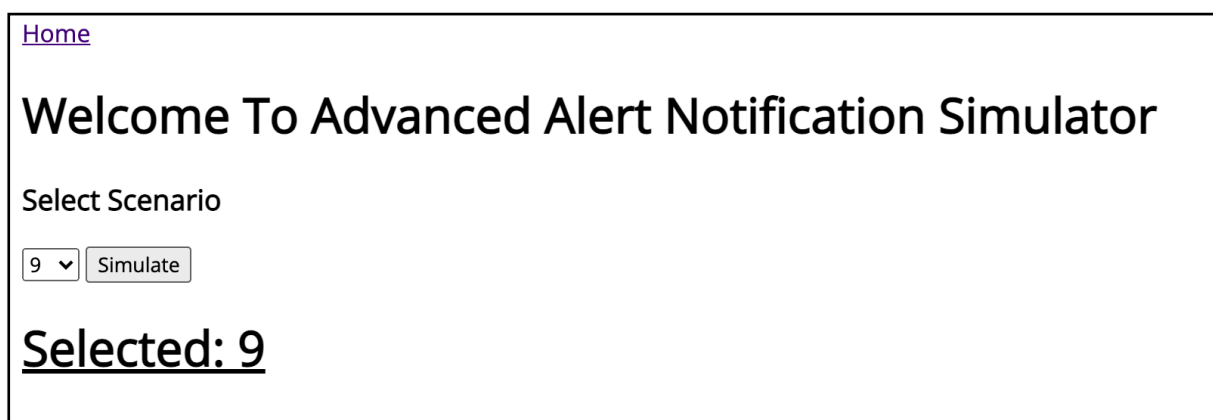


Figure 14: Tool 2.0 screenshots (attack specified)

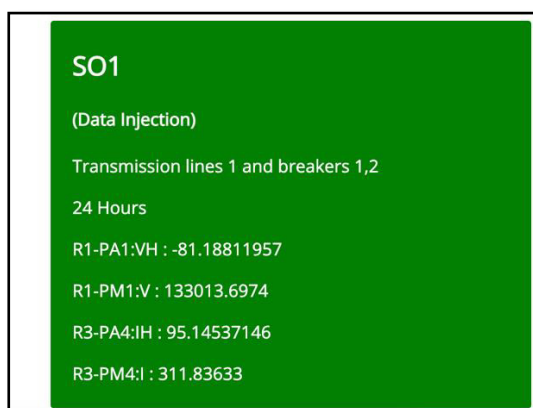


Figure 15: Tool 2.0 (Security Officer Notification)

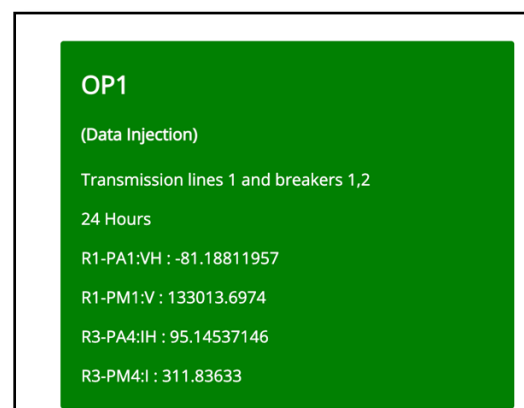


Figure 16: Tool 2.0 (Operator Notification)

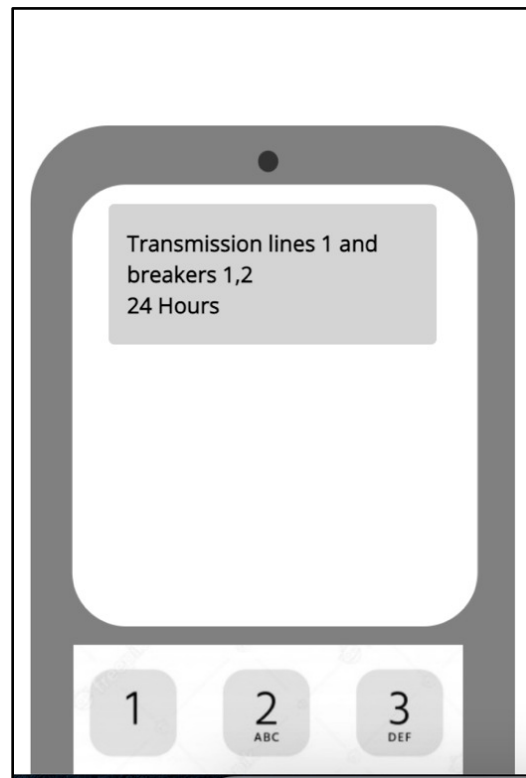


Figure 17: Tool 2.0 (Maintenance Personnel Notification "Text Message")

As the figure shows each window of notification is specified for special user based on the attack type. Moreover, the color code represents the severity of the attack where the tool contains 4 codes: **Green** which indicates low severity attack, **Yellow** indicates to medium attack severity, **Red** is high and **Dark Red** is Critical. Also, there is time to act specified based on the attack severity. For example, if the attack is critical and immediate action should be taken to prevent the consequences. Finally, the tool is measuring the readings coming from the PMUs (relays) to identify what is the behavior of the detected attack.

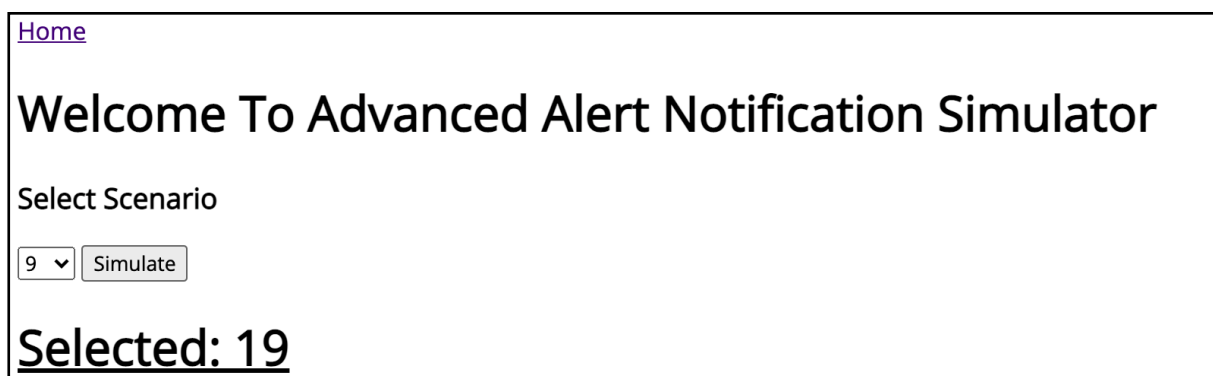


Figure 18: Tool 2.0 (Attack 19 is critical)

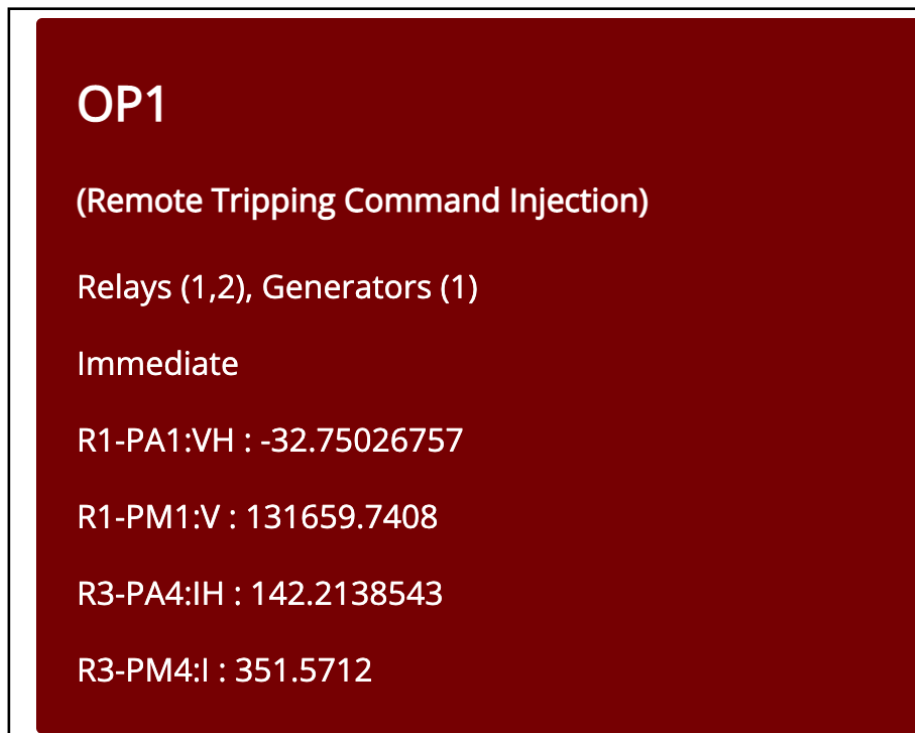


Figure 19: Tool 2.0 (color code for attack 19 and time specified to take action)

5.3 Discussion

Basically, the idea was to monitor the mentioned assets in the smart grid system and when the tool sensed any of the mentioned behaviors (scenarios) an alert should be sent to the right users. However, due to time limit we will use a python code to read form CSV file and based on the analysis of CSV file a user can choose what is the scenario to be simulated in the alert notification tool.

The work of the idea can be extended and applied to the real-world smart grid whether the tool should be installed in place between the OT and IT systems other than just monitoring the network traffic the variable values of the voltage and current should be monitored and this is can be done using this tool. The notification technique used in this work is based on real world scenario of cyber-attacks happened on smart grid and that's why we are not able to simulate the same case and rather trying to simulate the attacks we designed a tool to read form the attack table (CSV) and compare among them and should be able to justify why the attacks are different from scenario to another.

Another issue is, the tools of smart grid since the simulation application are very limited and cannot give an accurate result of the same case scenario we have in this work. Solving this issue by conduction of the risk assessment and identifying the system boundaries with each associated attacks and risk. This is can be found in the tool once the user chooses the scenario from the GUI, the tool shows the attack and what are the affected assets and what was the

voltage and current in that particular scenario. Thus, as mentioned above the work can be extended once we have the opportunity to apply the idea on a real smart grid network.

5.4 Attack Simulation

In this section, three of the attacks mentioned in this case will be simulated using (Power World) simulator app. The system will be represented exactly the same on the Power World simulator as the below figure shows.

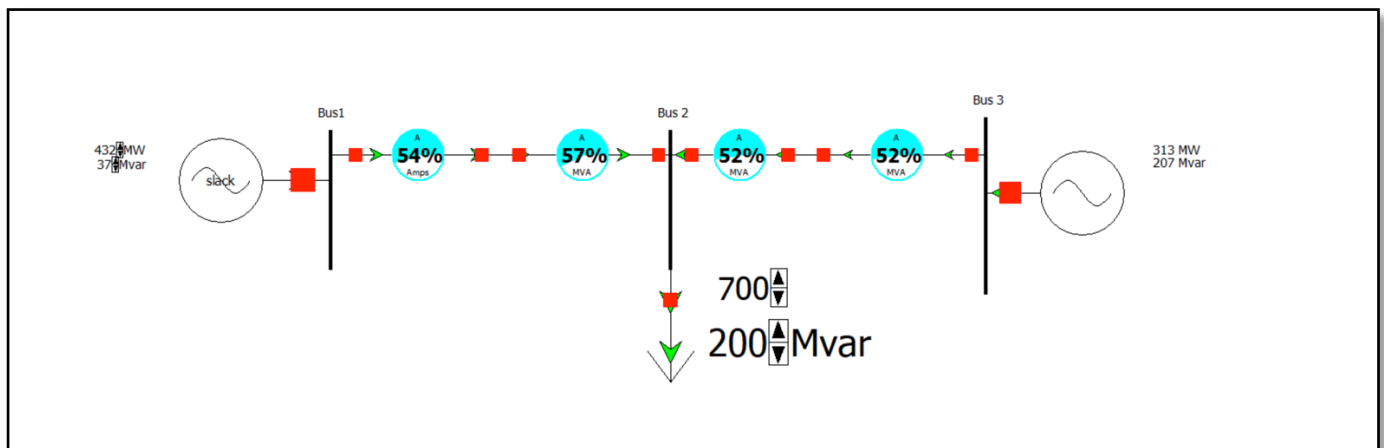


Figure 7: Three Bus System

The figure shows the normal traffic of the power in the system and as shown in the figure the line one is more critical than line two. As well as the assets on line one are considered as the main assets for the grid system. This means if an attack executed against line one; possible blackout will occur and in the opposed side line one may continue working with risk affecting line two resulting from attacks. However, due to limitation of the system parameters, three attacks will be implemented to show how these attacks affecting the entire power grid and further discussion will take place in this chapter.

5.4.1 Data Injection

Here, I will run the system and rise the volts passing through line 1 to see what are the behavior of the assets located in line 1.

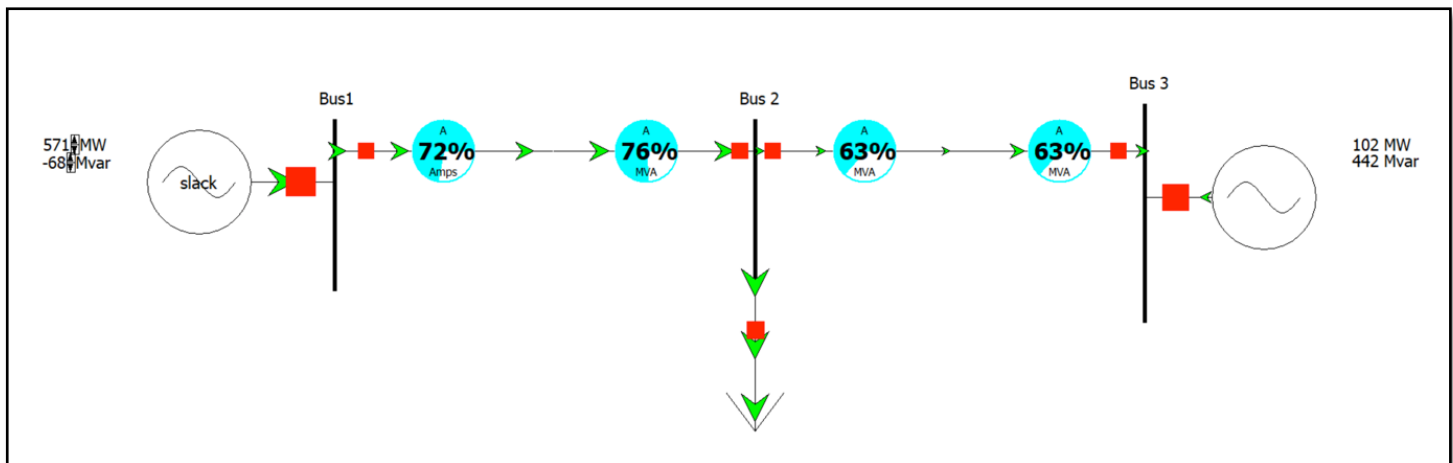


Figure 20: normal traffic of the system

As figure shows, this is how the normal traffic of the system should look like. However, by rising the volts passing through line one the traffic will be change to affect the breakers and generator and this is exactly what happening in data injection.

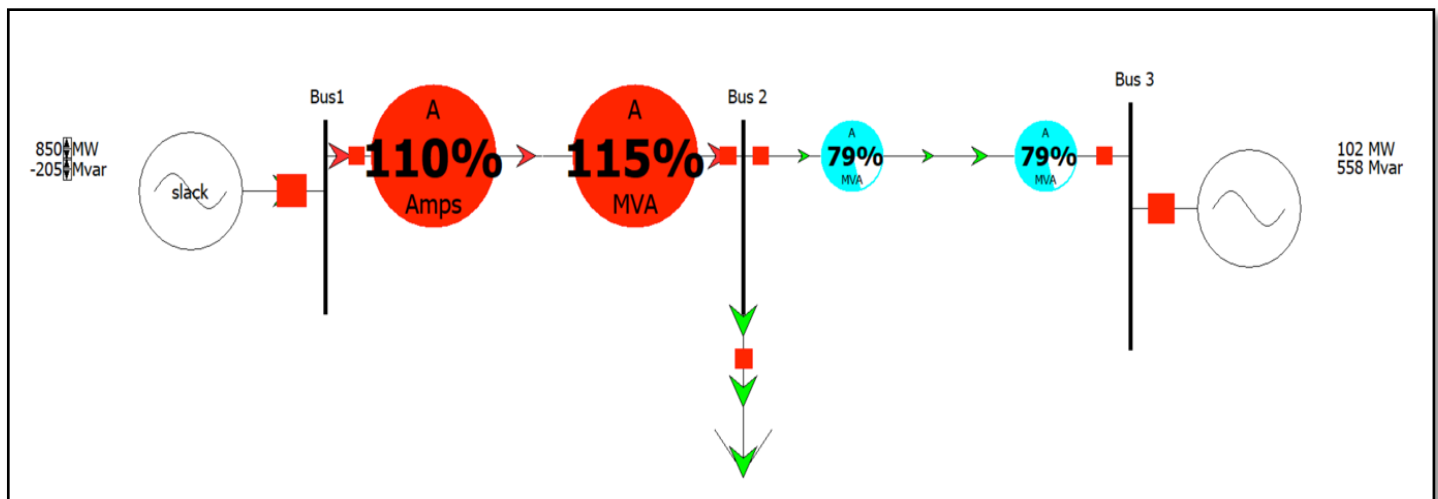


Figure 21: Data Injection Attack on Line1 (L1)

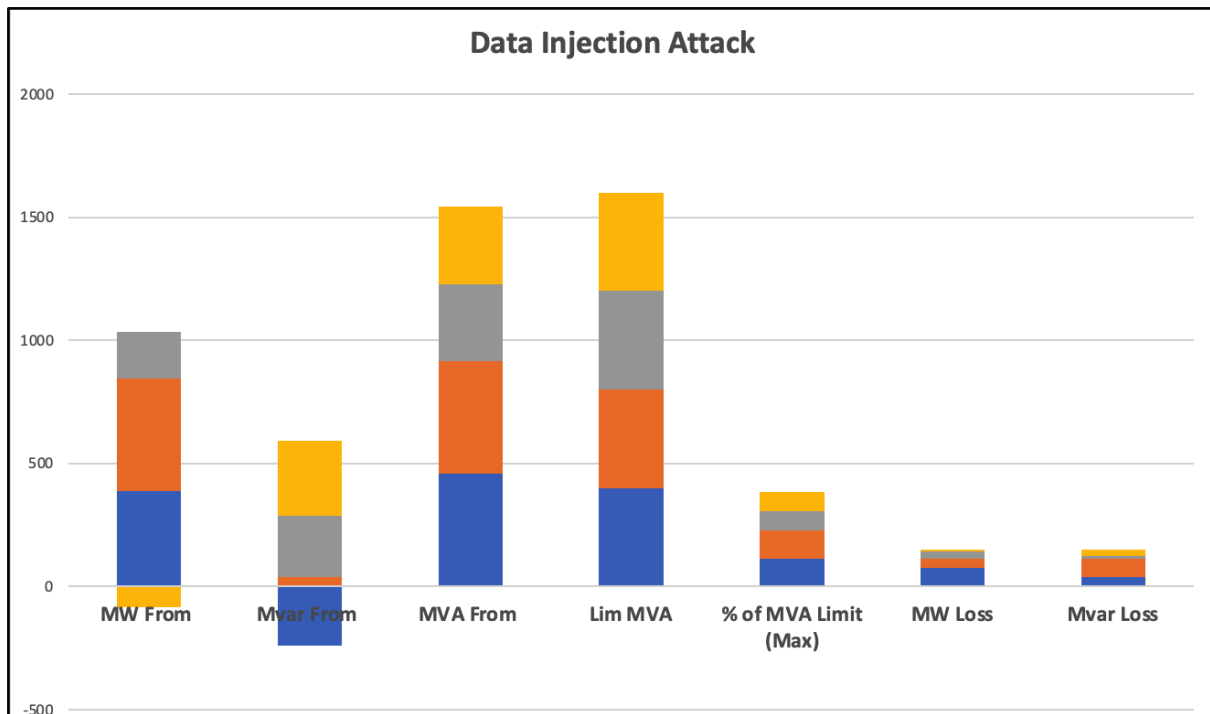


Figure 22: Data Injection Attack on Line1 (L1) chart

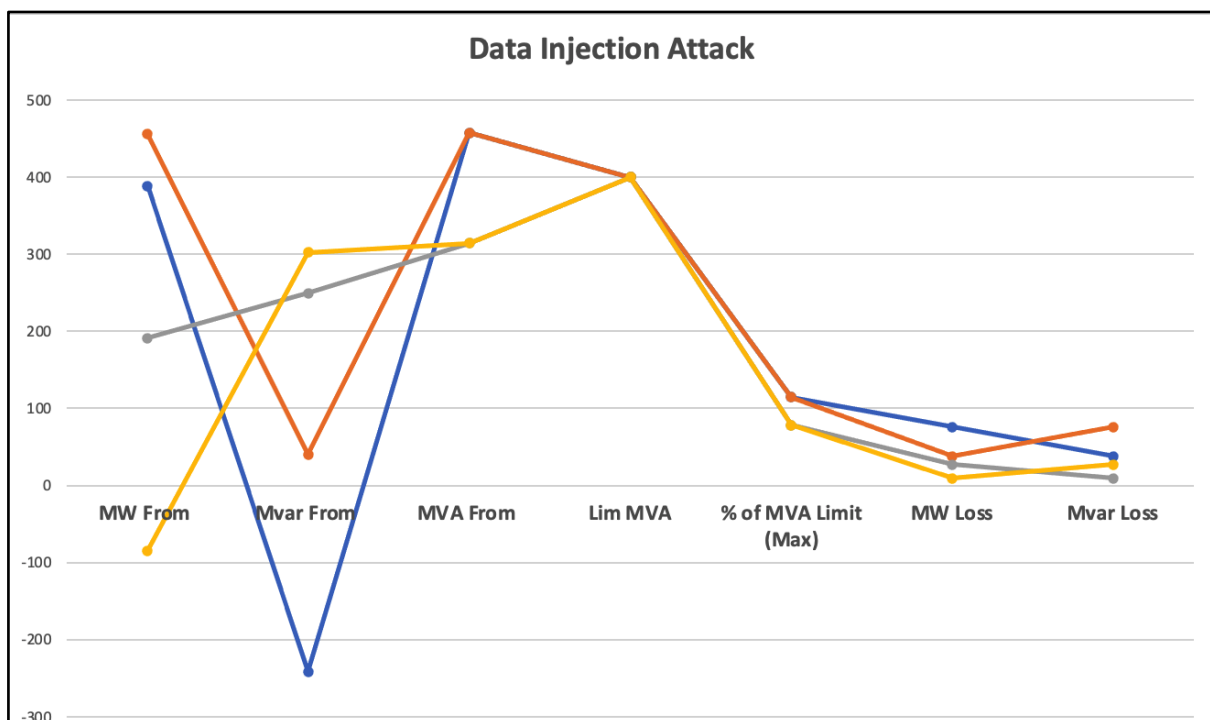


Figure 23: Data Injection Attack on Line1 (L1) Line Graph

As the figure shows, breakers 1,2 is under attack and by looking the generator it is noticeable that the measurement of Mega Watt (MW) are suspicious and clumsy.

5.4.2 Remote tripping command

This attack aims to disable relays and it is targeting the generator by modifying the legitimate values of relay which then affect the breakers to make them tripping illegitimately which causing damage to the generator which resulting to failure in the smart grid system. This attack is really dangerous because it can cause explosion to the generator and this may lead to human loss. This is why this attack is critical and it is consequences could be catastrophic.

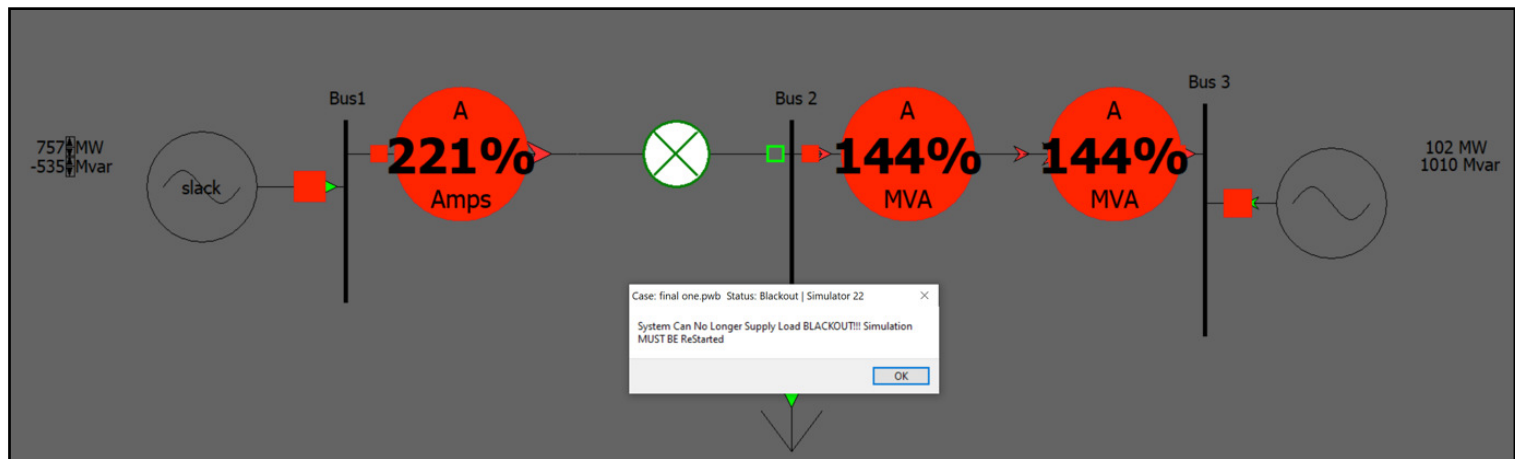


Figure 24: Remote Tripping Command (R2)

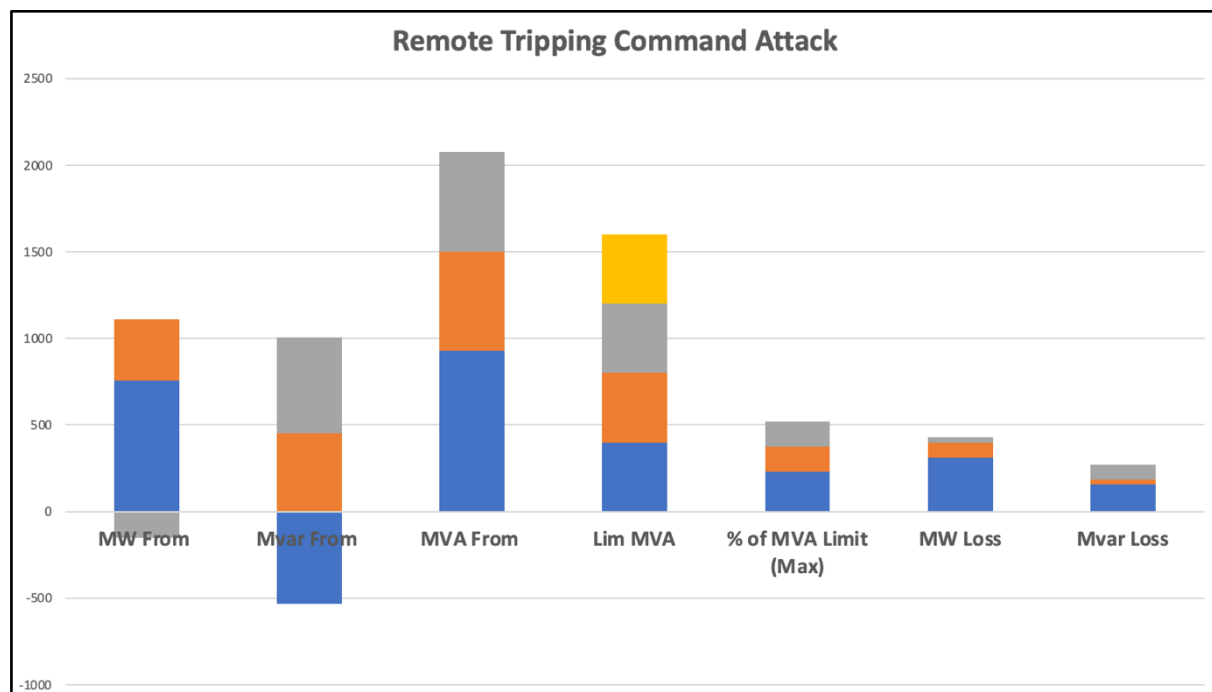


Figure 25: Remote Tripping Command (R2) chart.

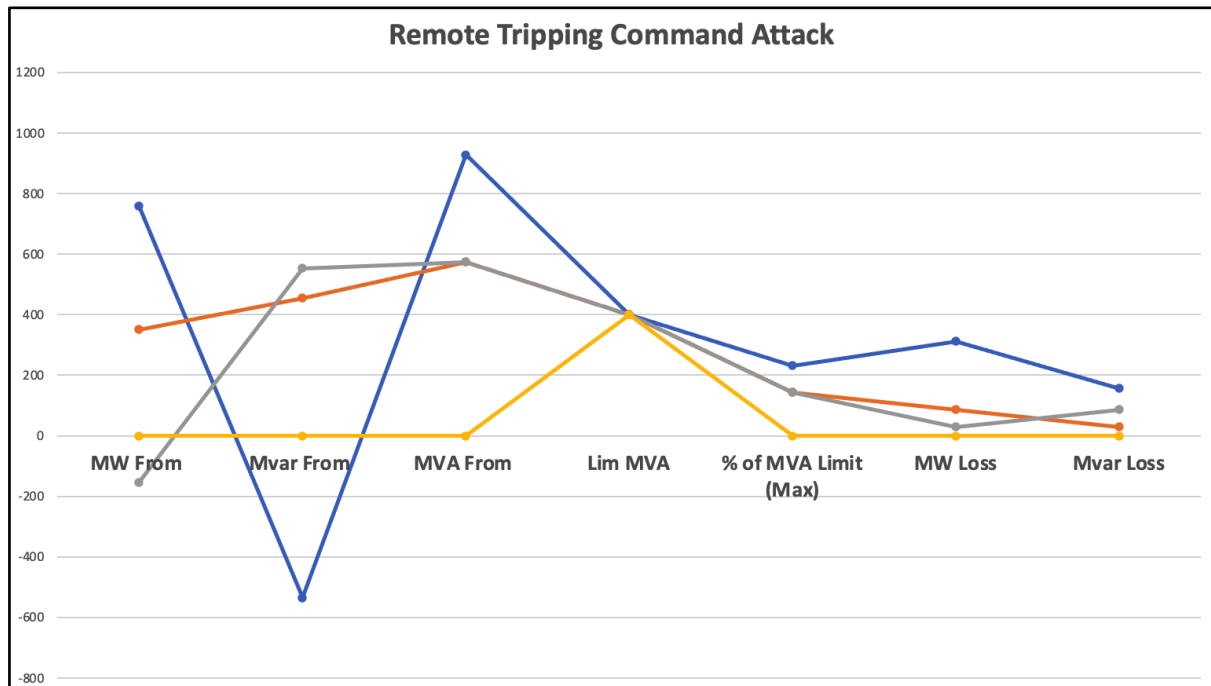


Figure 26: Remote Tripping Command line graph (R2)

5.4.3 Rely Setting Change

Smart grid systems with advanced cyber technologies are susceptible to attacks with incorrect data injection that prevent the monitoring of the online health estimate, steal energy through incorrect distribution in the electricity markets, and gain financial advantages. In the electricity markets, the case of a smart grid electricity system with connected micro grids is considered. The estimated transmitted power is changed, which leads to a change in electricity prices that benefits the attacker. It also affects the optimization of the production energy management for a micro grid. By exchanging electricity online with the main grid, micro grids can maintain the energy balance and reduce the generation costs of the entire electricity system of the smart grid system, as well as the various optimal generation capacities of micro grid and the total generation costs of the electricity system.

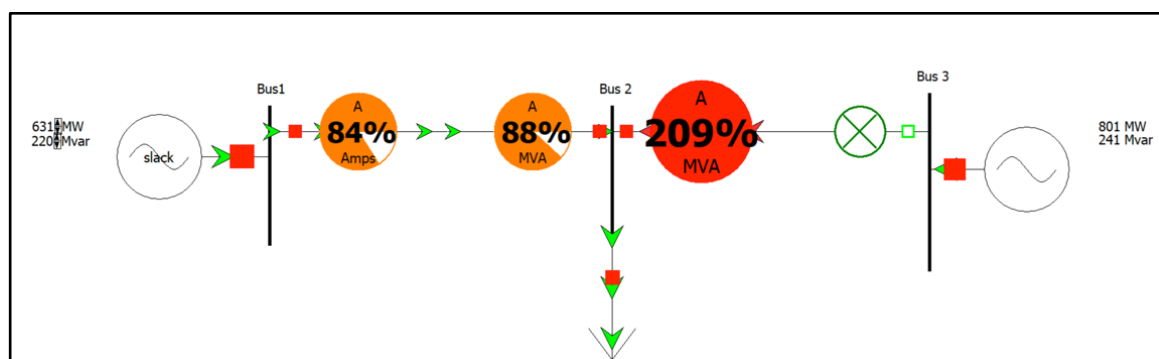


Figure 27: Relay Setting Change with (R4) disabled

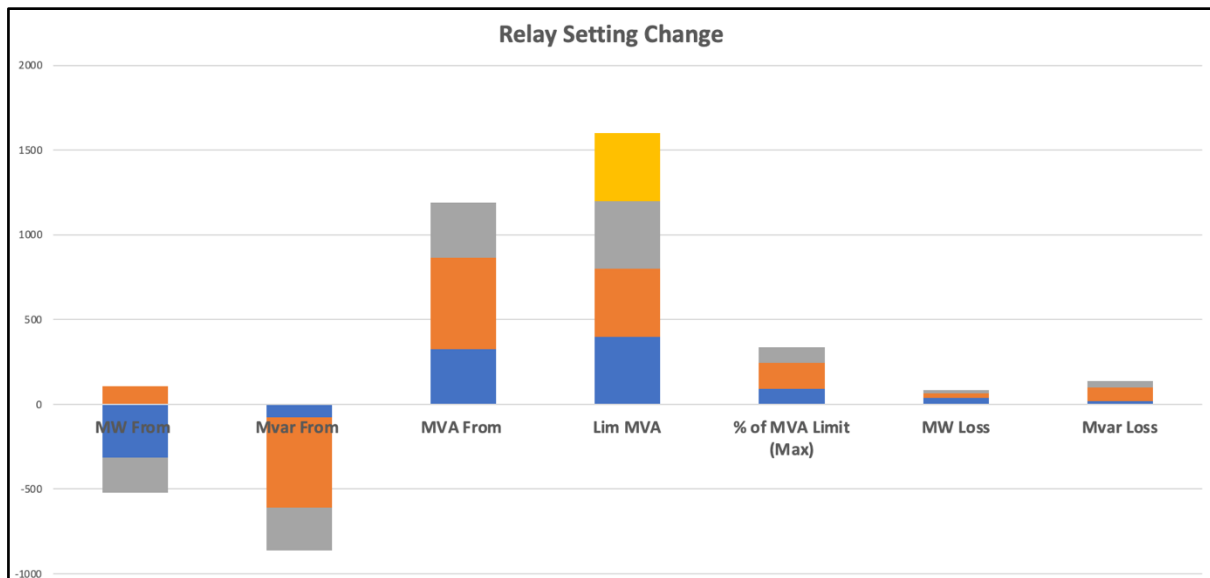


Figure 28: Relay Setting Change Attack chart (R4)

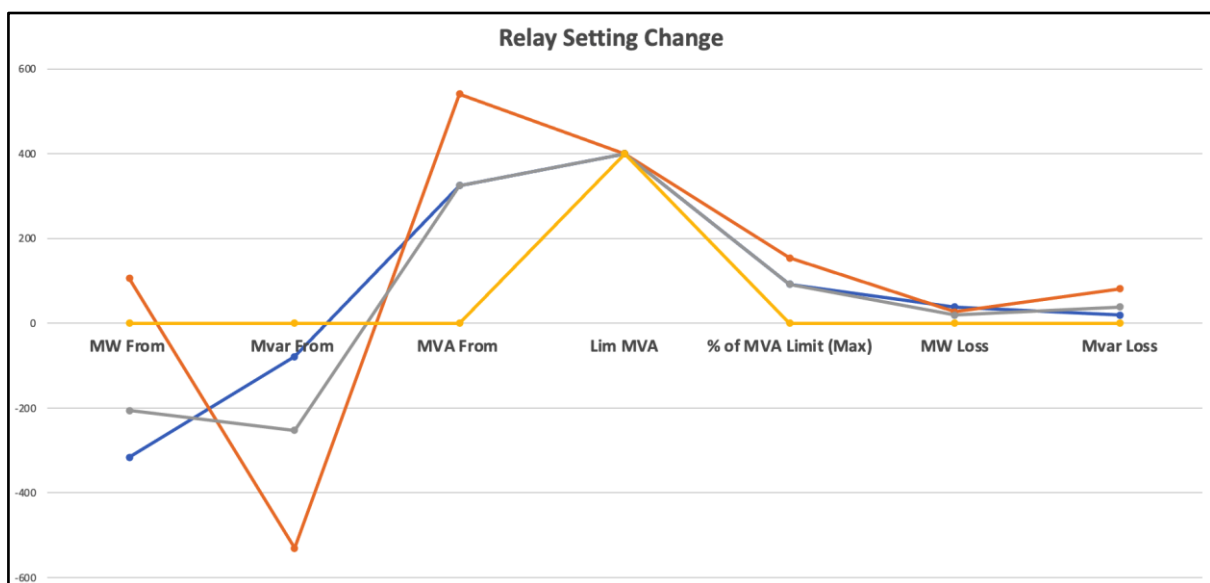


Figure 29: Relay Setting Change Attack line graph (R4)

5.4.4 Results

As I simulated different attacks, I found that risk assessment was accurate by setting Relay 2 (R2), as the most critical asset in the network. This is because any interruption may occur to this asset can be very risky and direct causing a blackout. Another aspect, the risk assessment conducted analyzed the assets accurately since this system consists 7 main assets without considering IT assets. The experiments show that L1 is incurred the highest number of attacks

by carrying 14 attacks while in the other side L2 incurred 8 attacks. To go deeper, risk assessment shows that R2 as well received 8 attacks in total but most of the attack were fluctuated between medium and critical, thus, R2 is the most valuable asset in the SG system. In the other side, R4 received only 5 attacks and the majority of these attacks were low severity. As well as, it was noticeable that if R4 is disabled the network can still working fine.

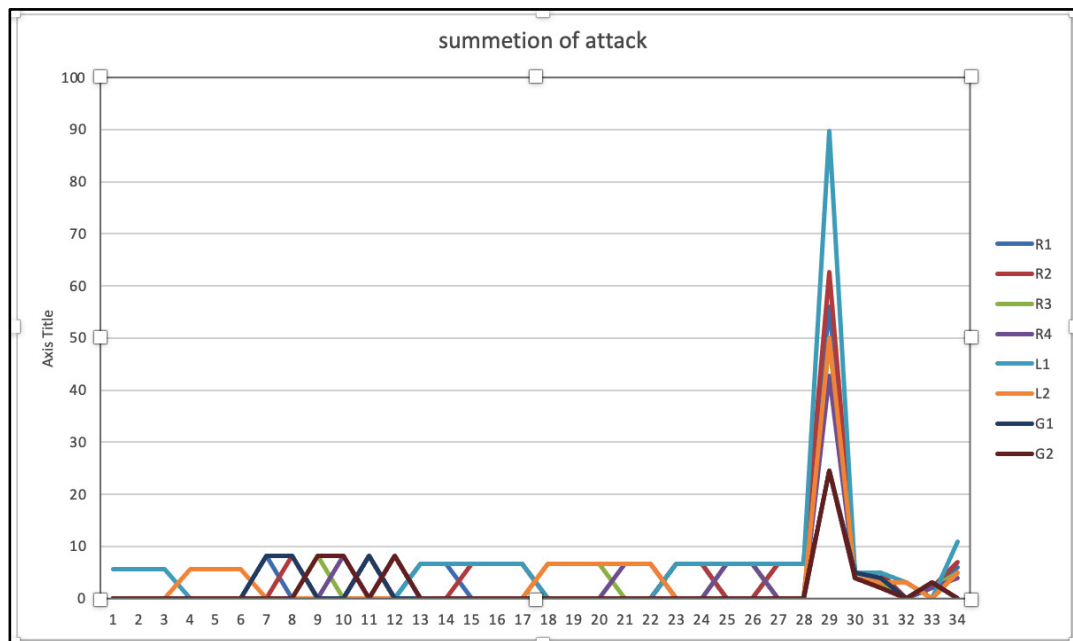


Figure 30: Summation of Attacks on each Asset

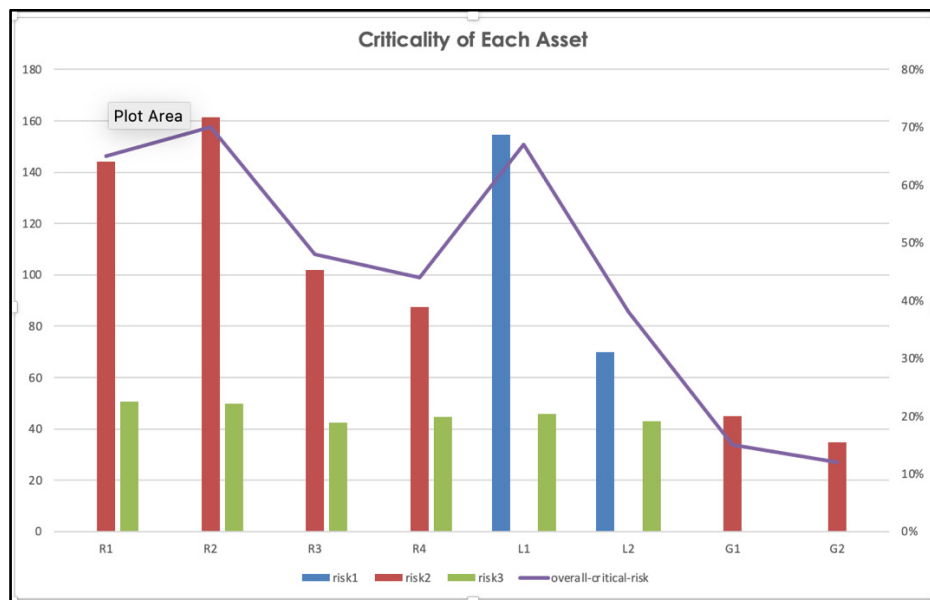


Figure 31: Criticality of Each Asset

5.5 Evaluation

It is necessary to conduct an evaluation in order to evaluate whether or not the project was effective. Throughout this part, I evaluate the work, describing what was achieved and any flaws that the project may have had. An expert opinion is also provided to provide further insight into how the project may be improved in the future.

5.5.1 Assessment-Evaluation

Overall, I think the project's primary goals were met. Network and electricity traffic are both monitored using an alerting tool and a software that determines the criticality. Using the detection algorithms, the tool was able to analyze the dataset's records and anticipate and comprehend the behavior of various smart grid attacks. In fact, the instructions for identifying and notifying the affected users of an attack were effectively implemented.

However, I am of the opinion that this initiative has flaws. Due to my lack of knowledge about electrical systems and equipment, the suggested solutions were limited and from a computer science aspect, which makes them difficult to put into practice. Another issue was that this tool only worked with data from the dataset stated at the beginning of this paper or comparable data that was customized by the user to make it suitable. Columns used just in this dataset are used to display the data. Using this tool may not give you the results you want since an excel file that was converted to csv doesn't use the same columns. The final limitation is that because of the manner the dataset was captured, the findings are unbalanced. In contrast to malicious communications, there are several recordings of the same event, thus collecting them all requires more system capability.

5.5.2 Attacks-Evaluation

I was able to simulate a few of the attack scenarios mentioned in this paper. This is because of the nature of the simulator (Power World). However, as risk assessment revealed the results of the simulated attacks comes to support the assessment. However, the majority of cyber-attack mentioned in this paper can cause a harm to the smart grid network in many different aspects which can be financial loss, human loss, operational loss and technical loss. To be more specific, I believe that the most critical attacks is remote code injection in the relays since it is controlling the main part of smart grid like IED devices (Breakers) and the PMU (Relays) as well as the generator of the station which may cause an explosion and human loss with service interruptions. The other two attacks aimed to misappropriate the legitimate values which can lead to financial loss or technical loss (blackout) and because of that both data

injection attack and relay setting change are not impactful as remote code injection. On the other side, data injection and relay setting change can affect wide range of customer by changing the legitimate values and rise the price which may lead at the end to service interruptions. Also, these two categories of attacks usually controlling the faults to cause more damage to SG networks.

5.6 Summary

For this project a three of the best frameworks (BSI, NIST 800-82 and SGIS toolbox) to assess risk related to OT systems were used as well as the data set named as power system attack dataset which provided by Mississippi State University and Oak Ridge National Laboratory. The dataset contains three main attacks (data injection, remote code injection and relay setting change). Comparing to previous work conducted in terms of risk assessment in smart grid I was able to calculate criticality for each asset based on invented formula. However, comparing to (Hasan et al., 2019) work in defence remediation, (Hasan et al., 2019) established their formula based on network monitoring traffic which resulted in capturing the traffic using Wireshark and Nessus's scan. My formula is assessing criticality based on severity of the attack and the location importance with monitoring volts passing through relay or any smart device, thus, integration -if extended- can contribute in creating a powerful tool to defence against cyber-attack in SG environment. Therefore, After evaluating the assets using integrated risk assessment methodology consists all of the three methods mentioned in this paper, I found that relay 2 is the most critical asset because it is located on the main line (L1) and after simulating the attacks on relay 2 I found if any disruption happened to relay 2 the service will be interrupted. Moreover, I believe that the main point of this research was successfully achieved but with some limitation regarding to the time. To sum up, there is still a good room to continue working and developing on this project on the future which will contribute to make the smart grid environment more secure.

Chapter 6: conclusion and future work

6.0 Built-in live data capture

The present tool that has been developed only accepts data that has been pre-recorded from this smart grid and has been imported by the user. This technique of data collection is not realistic since it requires continuous human input in order to maintain the tool updated with statistics from the smart grid. Improving upon this would effectively make the program working individually and allowed to operate in the background without interruption.

To achieve this enhancement, a separate script will be developed and that will have access to the data recording components of the smart grid and will be able to take that data and convert it into the CSV file type while also ensuring that it is in the proper format. The current tool may then utilize this information to generate auto-notification about the present condition of the smart grid based on the data collected.

6.1 Integrating more advance alert methodologies

The danger of poor measurements (or information corruption) in smart grids has only recently been recognized by academics, who have devised methods to overcome this problem. Since information corruption threats may originate from both the outside and the inside of a smart grid, they are very complicated. Some equipment, in particular, may be hacked and turned into insider attackers as a result of the increased openness brought about by integrating ICT into the power system. Due to the challenges posed by their secrecy and potentiality, insider attacks have received much less attention than external ones. While significant efforts have been made to defend against outsider attacks, far less has been done to defend against insider attacks. According to the 2013 U.S. State Cyber Crime Survey, insider threats account for 34% of all surveyed attacks (outsider threats account for 31%, and the remaining 35% have unknown/uncertain sources), which surprisingly demonstrates that insider threats have already established themselves as one of the most significant sources of potential vulnerabilities in cyber/cyber-physical system environments.

Despite the fact that insider threat detection for CPS has immediately captured considerable interest as a result of the potentially catastrophic consequences of CPS failure, effective and accurate detection techniques for CPS, particularly for smart grid, are still in their infancy, with only a few studies having been carried out. (Bao et al. 2016)

Insider threat can execute several kinds of the attacks on smart grid with being caught or captured and there is no specific technics alerting the operators that the power components are under attacks hence, a new methodology including insider threats should be developed by emerging monitoring network traffic and any suspicious traffic happening on the devices of the smart grid.

6.2 Tool Summary

Cyber-attacks on smart grids have the potential to cause substantial disruptions in the functioning of the smart grid, by this study. As a result of these attacks, connectivity between smart grid equipment may be disrupted, resulting in data corruption and loss. As a consequence of these attacks, regional outages in a targeted region are possible as well as human loss can be serious risk of this kind of attacks. The issue with this field's study is that the

tools' classifications and replies aren't accurate enough to let users make well-informed smart grid choices. Thus, the categories must reflect the fact that various kinds of assaults need distinct responses.

Therefore, the tool we developed illustrates the gathering and processing of smart grid data in order to generate warning notifications when a potential attack is identified, informing the targeted user of the smart grid's present status. The application's accurate and relevant alerts to the user will be insufficient in preventing and mitigating attacks. This is accomplished by extracting data from the smart grid system and continuously monitoring it. If an attack measurement is identified, the tool should be able to identify and record suspicious behavior on both communication protocols (network) and power measurements (volts and power) which then allow to act and alert the user in appropriate manner.

6.3 The idea and tool

This tool was created to help to overcome the issue of risk assessments since the majority of researches in this field are lacks to some aspects whether it is assets discovery or identifying the system boundaries and so on. the other issue is related to what the right spot of smart grid to be captured; is it the network communication or the power measurements? Hence, this project is monitoring both aspects, but more focused on the number measured by the PMUs (relays) and how the targeted asset behave under active attack. Therefore, take the right action to notification alert to the right selected user with describing the attack and its related information.

6.4 Conclusion

With all risk assessments done in the field of smart grid we still need more evolving methods since all the previous works including this work can be considered as the first step to secure the new emerging cyber-environments attacks. Focusing on the previous paper, it can be seen that the risk assessment lacks of some aspects and yet to be said it is ideal, thus, this work suggested a new methods in terms of assessing risk or alerting users to gain the situational awareness of both human and machine and contribute to mitigate the risk associated with OT critical infrastructure. The mitigation either can be automated or by human intervention. Speaking about the dataset, the dataset used in this project were tested in detection methodology of the attacks using ML (Machine Learning) and the results was approximately accurate where some of the classifiers achieved 90% detecting the attacks scenarios and filter them from the normal scenarios. To conclude, cyber-attack will continue emerging in terms of OT critical infrastructure and on the other side the cyber-security should continue developing their tool as well to remediate these attacks.

Chapter 7: Reflection made on learning

7.0 Reflection on Learning

During this project I learnt how the smart grids works and what are the structure of these systems. This project guided me through very excited pathways to build a good experience and know how to deal with attacks in terms of smart grids. Also, one of the most important aspects is the knowledge gained about what are the available development in this section. This is guided me to explore how promising are the smart OT systems and how they will be valuable in the near future and how important to secure such environments. Crossways among the IT systems and OT in line with the IoT development can lead to smart environments without human interventions and the promising part is that they are going to be to some extent safe and immune against attacks or system flaws. However, this is far to be achieved unless we work to close the gaps and keep developing towards securing the smart devices against hackers or intruders. Throughout the subject of this project's development, I broadened my technical knowledge and skill set in a variety of different areas of computer science. When I was contemplating a project, I knew I wanted it to be linked to one of three potential topics: forensics, cybersecurity, or penetration testing, since these are all areas in which I have had a strong interest for many years. When I initially heard about this project, I knew nothing about smart grids and had only a basic understanding of risk assessment concepts. Investigating this topic and its many aspects has widened my perspectives, and via meetings with my supervisor and reading other research papers, I've been able to extract this knowledge into a useful report that you've hopefully read through.

Chapter 8: Appendices

8.0 List of Table

- Table 1: Comparison shows the frameworks / methods available for OT, ICS and Smart Grids (ICS Cybersecurity Assessment Framework. 2021), (Langer et al.2016), (Langer et al.2015) and (Stouffer et al. 2021)
- Table 2: Tools Comparison
- Table 3: THREE-CLASS CLASSIFICATION GROUP (Mississippi State University and Oak Ridge National Laboratory, 2014)
- Table 4: Data set Scenarios Breakdown Table
- Table 5: Assets Identification (Saxena et al. 2016)
- Table 6: Assets Identification
- Table 7: Overall criticality of the assets
- Table 8: Asset Criticality based on number of attack and location Severity
- Table 9: Impact of each attack on DREAD scale
- Table 10: Risk Matrix Table
- Table 11: Potential threat associated with each attack
- Table 12: Notification Technique

8.1 List of Figures

- Figure 1: difference between OT systems and IT systems (Ghauri 2021)
- Figure 2: Smart Grid model (Vijayapriya and Kothari 2011)
- Figure 3: The SCADAfence Platform
- Figure 4: Nozomi Networks Guardians Platform
- Figure 5: smart grid model
- Figure 6: System Model Diagram
- Figure 7: Three Bus System
- Figure 8: the overall Idea of the tool
- Figure 9: Tool 1.0 screenshots (the overall criticality calculator)
- Figure 10: Tool 1.0 screenshots (file upload to the tool)
- Figure 11: Tool 1.0 screenshot
- Figure 12: Tool 1.0 screenshots (criticality result)
- Figure 13: Tool 2.0 screenshots (first screen)
- Figure 14: Tool 2.0 screenshots (attack specified)
- Figure 15: Tool 2.0 (Security Officer Notification)
- Figure 16: Tool 2.0 (Operator Notification)
- Figure 17: Tool 2.0 (Maintenance Personnel Notification “Text Message”)
- Figure 18: Tool 2.0 (Attack 19 is critical)
- Figure 19: Tool 2.0 (color code for attack 19 and time specified to take action)

Figure 20: normal traffic of the system
 Figure 21: Data Injection Attack on Line1 (L1)
 Figure 22: Data Injection Attack on Line1 (L1) chart
 Figure 23: Data Injection Attack on Line1 (L1) chart
 Figure 24: Remote Tripping Command (R2)
 Figure 25: Remote Tripping Command (R2) chart
 Figure 26: Remote Tripping Command line graph (R2)
 Figure 27: Relay Setting Change with (R4) disabled
 Figure 28: Relay Setting Change Attack chart (R4)
 Figure 29: Relay Setting Change Attack line graph (R4)
 Figure 30: Summation of Attacks on each Asset
 Figure 31: Criticality of Each Asset

Chapter 9: Bibliography

9.0 Bibliography

1. Akhgar, B. and Yates, S. 2014. *Strategic Intelligence Management*. Saint Louis: Elsevier Science.
2. All of Your OT & IoT Security in One Place | SCADAfence. 2021. Available at: https://www.scadafence.com/?utm_source=google&utm_medium=cpc&utm_campaign=brand&utm_term=scadafence&utm_campaign=WD+-+Brand&utm_source=adwords&utm_medium=ppc&hsa_acc=2666076862&hsa_cam=12502767024&hsa_grp=119215896219&hsa_ad=504483442944&hsa_src=g&hsa_tgt=kwd-314904786420&hsa_kw=scadafence&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwk6-LBhBZEiwAOUUDpyUy4IEcFV4uM0iWtE7h9iB1tXdYLA Czjy-1sKW h gKE6dxUpAdFaxoCR3EQAvD_BwE [Accessed: 18 October 2021].
3. Bao, H. et al. 2016. BLITHE: Behavior Rule-Based Insider Threat Detection for Smart Grid. *IEEE Internet of Things Journal* 3(2), pp. 190-205. doi: 10.1109/jiot.2015.2459049.
4. Ghauri, F. 2021. Operational Technology Threats in Developing Countries and Possible Solution. Available at: <http://dx.doi.org/10.5281/zenodo.4925666> [Accessed: 18 October 2021].
5. Hasan, K., Shetty, S., Ullah, S., Hassanzadeh, A. and Hadar, E., 2019. Towards Optimal Cyber Defense Remediation in Energy Delivery Systems. *2019 IEEE Global Communications Conference (GLOBECOM)*,.
- 6.
7. ICS Cybersecurity Assessment Framework. 2021. Available at: <https://www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/Resources/Whitepapers/ICS-Cybersecurity-Assessment-Framework/> [Accessed: 18 October 2021].
8. Jenkins, N. et al. 2015. An Overview of the Smart Grid in Great Britain. *Engineering* 1(4), pp. 413-421. doi: 10.15302/j-eng-2015112.
9. Langer, L. et al. 2015. Smart grid cybersecurity risk assessment. *2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST)* . doi: 10.1109/sedst.2015.7315255.

10. Langer, L. et al. 2016. From old to new: Assessing cybersecurity risks for an evolving smart grid. *Computers & Security* 62, pp. 165-176. doi: 10.1016/j.cose.2016.07.008.
11. McCary, E. and Xiao, Y. 2015. Smart Grid Attacks and Countermeasures. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* 2(2), p. e4. doi: 10.4108/inis.2.2.e4.
12. Stouffer, K. et al. 2008. *Guide to Industrial Control Systems (ICS) security*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.
13. Stouffer, K. et al. 2021. *Guide to Industrial Control Systems (ICS) Security*.
14. Tang, Y. et al. 2016. Challenge and evolution of cyber attacks in Cyber Physical Power System. *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)* . doi: 10.1109/appeec.2016.7779616.
15. Vijayapriya, T. and Kothari, D. 2011. Smart Grid: An Overview. *Smart Grid and Renewable Energy* 02(04), pp. 305-311. doi: 10.4236/sgre.2011.24035.
16. Mohammadpourfard, M. et al. 2021. Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. *Sustainable Cities and Society* , p. 103116. doi: 10.1016/j.scs.2021.103116.
17. Nozomi Networks Guardian - Tempest Telecom Solutions. 2021. Available at: <https://www.tempesttelecom.com/nozomi-networks-guardian/> [Accessed: 18 October 2021].
18. Radoglou-Grammatikis, P. et al. 2018. An Overview of the Firewall Systems in the Smart Grid Paradigm. *2018 Global Information Infrastructure and Networking Symposium (GIIS)* . doi: 10.1109/giis.2018.8635747.
19. Saxena, N. et al. 2016. Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security* 11(5), pp. 907-921. doi: 10.1109/tifs.2015.2512525.
20. Smart Grid: The Smart Grid | SmartGrid.gov. 2021. Available at: https://www.smartgrid.gov/the_smart_grid/smart_grid.html [Accessed: 18 October 2021].
21. Wang, D. et al. 2018. Review of key problems related to integrated energy distribution systems. *CSEE Journal of Power and Energy Systems* 4(2), pp. 130-145. doi: 10.17775/cseejpes.2018.00570.
22. Yeboah-Ofori, A. 2019. Cybercrime and Risks for Cyber Physical Systems. *International Journal of Cyber-Security and Digital Forensics* 8(1), pp. 43-57. doi: 10.17781/p002556.