A FRAMEWORK FOR CYBER SECURITY RISK MODELING AND MITIGATION IN SMART GRID COMMUNICATION AND CONTROL SYSTEMS

by

Lukumba Phiri.

A Thesis submitted in full fulfillment of the requirements of the degree of Doctor of Philosophy in Information Communication Technology Security.

The University of Zambia

2023

A FRAMEWORK FOR CYBER SECURITY RISK MODELING AND MITIGATION IN SMART GRID COMMUNICATION AND CONTROL SYSTEMS

by

Lukumba Phiri

A Thesis submitted in full fulfillment of the requirements of the degree of Doctor of Philosophy in Information Communication Technology Security.

The University of Zambia

March 2023

DECLARATION

I **Lukumba Phiri** do declare that this thesis is my work and that it has not previously been submitted for a degree or other qualification at this or another University.

Signature:.......................... ....

Date:..............March 20, 2023...

APPROVAL

This Thesis of **Lukumba Phiri** has been approved as a full fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Information Communication Technology Security by the University of Zambia.

NAME **SIGNATURE** **DATE**

____________ ____________ ____________

Supervisor

____________ ____________ ____________

External Examiner

____________ ____________ ____________

Internal Examiner

____________ ____________ ____________

Internal Examiner

____________ ____________ ____________

Thesis Chairperson

ABSTRACT

The objective of this research was to present a risk analysis methodology for enhancing cyber security and defending the crucial parts of Zambia's electric power grid. By building on the basic concerns of risk assessment and management and using a Design Science Research Methodology (DSRM) as a research methodology, this framework tried to advance the current risk analysis debates on the electric power system. By conducting a review of the literature and providing a stochastic risk-based framework, this thesis stresses the need for a coordinated cybersecurity effort toward developing strategies and actions conducive to defending the nation against attacks on the electric power infrastructure.

We used PIPE (Platform-Independent Petri Net Editor) and Great Stochastic Petri Nets (GSPN) to model and analyze the GSPN attack model of the SCADA network. Additionally, it enables the user to animate the model through direct user manipulations or the arbitrary firing of transitions. These instruments' analysis environments include a variety of modules, including steady-state, steady-space, and GSPN analyses. Fifty simulations of the designed GSPN model of the DoS attack were performed using various starting random firings of 100, 300, 500, 700, 1000, and 1200. The transition triggering rates of the Defense Scenario’s firewall, password, and combined SPN models, respectively. The results show that the net probability of being attacked with only a password as an intrusion protection mechanism was 95.59 percent, compared to 95.11 percent for the firewall model, and 78.902 percent for the combined model. This indication demonstrates that given a firewall and a password as a combined intrusion protection mechanism, the probability of being hit by a cyber-attack is relatively high.

To enable proactive cybersecurity and threat intelligence sharing for the digitalized power infrastructure, it can be said that there is a need for a general cybersecurity framework. In contrast to previous efforts on AGC cyber-physical security, we model AGC false data injection attacks (FDIA) and explore the potential vulnerabilities that could result from ignoring them. First, we showed that the AGC's behavior and, consequently, the control decision, differ if the FDIA is taken into consideration. We demonstrated that the linear AGC models that do not account for FDIA do not offer adequate protection against cyber-physical attacks that work in the nonlinear region of the system. Second, we suggested and put into practice a two-stage strategy based on LSTM to identify and reduce the compromised signals to handle these threats. Its better performance in attack detection with good statistical metrics is confirmed by the examination of the detection model. The mitigation model can also improve the system's behavior and dramatically lower the RMSE of the attacked signals. The results obtained were later compared with findings from other studies such as PRIME (PNNL cybeR physIcal systeMs tEstbed), and edge-based multi-level anomaly detection framework for SCADA networks named EDMAND.

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude and thanks to all members of staff of the Department of Electrical and Electronic Engineering in particular and the School of Engineering in general for their support, patience, and encouragement offered during my research period. In particular, I express my gratitude and thanks to **my supervisor Dr. Simon Tembo** for his untiring professional guidance throughout the research and production of this thesis.

I would like to thank my exam committee: Dr. Smart Charles Lubobya, Dr. Jackson Phiri, and Prof. Mbuyu Sumbwanyambe.

I also thank the lecturers of the Department of Electrical and Electronic Engineering for their tireless effort to make sure I had all the requirements to carry out my research work thereby making my academic life easier. Not to forget, thanks also go to the department and school colleagues for the encouraging discussions we randomly had on my research directions.

This research work wouldn't have been complete without contributions from collaborators. First and foremost I would also like to acknowledge the Adjunct Professor Manohar Chamana who provided access to the Wind Energy Lab at Texas Technical University. Professor Niamat from Arkansas State University, and Prof. G Kabanda from the University of Zimbabwe for their insights during the various stages of the study. The following collaborators in some of my journal articles and conference papers; Dr. Umair Shahzad for his contributions to the fourth journal article, and Eng. Kumbuso Joshua Nyoni for his input on a number of my publications, Rabindra Bhatta, Rajendra Shrestha, Dr. Manohar Chamana, and Konrad Schmitt. I also thank several engineering professionals from UNZA; (Eng. Shadrach Mpanga, and Eng. Lusungu Ndovi for their morale support), ZESCO, CEC, and Mopani, among others not mentioned for their insights and cooperation during my data collection period.

I would like to thank my wife Edina for her support and sacrifices over the years toward my successes and achievements. In addition, to my sons Lukumba Temwani, Kumbukani, and Salifyanji, I set this example for you,

work hard and fight for your dreams and goals. In addition, I send my love and appreciation to my brothers Chipayeni, Munenula, Weluzani, and Zewelanji sisters Rose, and Mpunga. Thank you for your unwavering, unconditional love. I dedicate this work to Dad Zackey N, and my mother, the late Annie Nanyangwe. My mother taught me that accomplishments should always not be just about you, but changing something you see that is wrong to right, helping someone in need, lifting others, and remembering your existence is about serving others above yourself. My mom is the most giving, loving, person I ever met. Finally, I recognize God as the head of my life and Jesus as the reason I can say that. I give glory, and honor to God, and thank him for allowing me to take this long, hard journey. Thank You for the will and strength through troubled times, health issues, and doubt to keep on moving. Through Jesus, all things are possible!

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC – Alternating Current

ACSI – Abstract Communication Service Interface

ADU – Application Data Unit

AGC – Automatic Generation Control

AI – Artificial Intelligence

AMI – Advanced Metering Infrastructure

APCI–Application Protocol Control Information

APDU - Application Protocol Data Unit

APT – Advanced Persistent Threat

ASDU – Asynchronous Data Unit

AU – African Union

AUCSEG – African Union Council

B2B – Business to Business

BAN – Body Area Network

BES – Bulk Energy Supply

BIS – Business Information Systems

C2 – Central Control

CC – Control Centre

CCDF – Cyber

CDC – Common Data Classes

CDF – Cumulative Distribution Function

CEC – Copperbelt Energy Corporation

CI – Critical Infrastructure

CIA – Confidentiality Integrity Availability

CIP – Critical Infrastructure Protection

CKC – Cyber Kill Chain

CO2 – Carbon Dioxide

COT – Cost of Transmission

CPN – Colored Petri Nets

CPS – Cyber-Physical Systems

CRC – Cyclic Redundancy Control

CTMC – Continous Time Markov Chains

CVE – Critical Vulnerability

CWE – Common Weakness Enumeration

DC – Direct Current

DCS – Distributed Control Systems

DDoS – Distributed Denial of Service

DES – Distributed Energy Sources

DG – Distributed Generation

D-LAA – Dynamic Load Altering Attack

DMS – Distributed Energy Systems

DMZ – Demilitarized Zone

DNP3 – Distributed Network Protocol 3

DOE – Department of Energy

DSO – Distribution Systems Operator

DSRM – Design Science Research Method

DTMC – Discrete Time Markov Chain

ECT – Electronic Communication Transaction

EIZ – Engineering Instittute of Zambia

EMS – Energy Management Systems

EPS – Energy Physical Systems

ERB – Energy Regulation Board

ERP – Enterprise Resources Planning

ESS – Energy Storage Systems

EU – European Union

FDI – False Data Injection

FW – Firewall

G2V – Grid to Vehicle

GSPN – Generalized Stochastic Petri Nets

GW – Giga Watts

HAN – Home Area Network

HARM – Hierarchical Attack Representation Model

HFO – Heavy Fuel Oil

HIL – Hardware in the Loop

HMI – Human Machine Interface

HPP – Hydro Power Plant

IaaS – Information as a Service

IAN – Industrial Area Network

ICCP – Inter Control Centre Protocol

ICS – Industrial Control Systems

ICT - InformationCommunications Technology

ICTAZ – Information Communications Technology Association of Zambia

IED – Intelligent Electronic Device

IoT – Internet of Things

LAN – Local Area Network

LMP – Locational Marginal Prices

LN – Logical Node

LFC – Load Frequency Control

LSTM – Long Short Term Memory

LTE – Long-Term Evolution

MES – Manufacturing Execution System

MG – Micro Grid

MitM – Man in the Middle

MMS – Manufacturing Messaging Systems

MOMS – Manufacturing Operations Management Systems

MTTF – Mean Time To Failure

MTTR – Mean Time to Repair

NAN – Neighborhood Area Network

NCSACC – National Cyber Security Audit Coordination Council

NIDS – Intrusion Detection Systems

NIST – National Institute of Standards and Technology

NSS – Noise to State Stability

NSS-LF - Noise to State Stability Lyapunov

OOS – Out of Step

OPC – OLE for Process Control

OPF – Optimal Power Flow

OSI – Open Systems Interconect

OT – Operational Technology

PC – Personal Computer

PDC – Phasor Data Concentrator

PDU – Phasor Data Unit

PIPE – Platform Independent Petri Nets

PMU – Phasor Measurement Unit

PN – Petri Nets

POC – Point of Connection

PSSE – Power Systems State Estimation

QoS – Quality of Service

RaaS – Ransom as a Service

RAM – Reliability Availability Maintainability

RAS – Remedial Action Scheme

RAT – Routine Activity Theory

RMP – Risk Management Process

RTS – Real-Time Systems

RTU – Remote Terminal Unit

SADC – Southern African Development Community

SCADA – Supervisory Control and Data Acquisition

SCL – System Configuration Language

SCOPF – Security Constrained Optimal Power Flow

SDE – Stochastic Differential Equation

SG – Smart Grid

SHS – Stochastic Hybrid Systems

SMP – Semi-Markov Process

SUC – Stochastic Unit Commitment

TCP/IP – Transmission Control Protocol/Internet Protocol

TSO – Transmission System Operator

TTU – Texas Technical University

UAS – Utility Automation Systems

UDP – User Datagram Protocol

UFLS – Under Frequency Load Shedding Relay

UVLS – Under Voltage Load Shedding

V2G – Vehicle to Grid

VPN – Virtual Private Network

WAMPAC – Wide Area Monitoring, Protection, and Control

WAN – Wide Area Network

WSN – Wireless Sensor Network

XML – Crossed Markup Language

ZESCO – Zambia Electricity Supply Corporation

ZHPC – Zengamina Hydro Power Corporation

ZICSCF - Zambia Industrial Control Systems Cybersecurity Framework

CHAPTER 1: INTRODUCTION

One of the most complex engineering machinery ever created by humans is the electric power grid. It's a highly interconnected cyber-physical system in which one system's dynamics are intimately coupled with the dynamics of another. The most recent smart grids have a huge number of interconnected zones, each with its generators, loads, and Supervisory Control and Data Acquisition (SCADA) systems as depicted in figure 1-1.

Under the framework of standard communication protocols like IEC-60870 and IEC-61850, system data is collected from Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), integrated remote substations, and local SCADA systems. These data are transferred via an Inter-utility Control Center Communication Protocol (ICCP) via a Wide Area Network (WAN). IEDs are used effectively by SCADA/EMS for remote monitoring and control activities. The IEDs are deployed in remote site/substation control centers as monitoring and control interfaces to the power system equipment and can be integrated utilizing appropriate communication networks. The IEDs and local communication can be accessible via a LAN, while the distant site control center is linked to the SCADA/EMS and other engineering systems via the power system WAN [1].

Wide Area Monitoring, Protection, and Control (WAMPAC) makes use of system-wide data and distributes selected data to remote sites. The Global Positioning System (GPS) drives phasor measurement units (PMUs), which give real-time synchrophasor readings for voltage and current phasors throughout the grid. These metrics supplement typical SCADA measurements by providing a real-time view of the dynamics of the power system. Synchro-phasor networks can provide considerable benefits by delivering quick and precise measurements at rates as high as 60 times per second [2]. Because of low sampling rates and a lack of temporal synchronization, SCADA measurements in Wide-Area Monitoring Systems (WAMS) are unable to offer a timely assessment of the system [3].

WAMPAC has recently been used in a variety of applications due to the availability of PMU measurements. PSSE, AGC, real-time contingency analysis, Remedial Action Schemes (RAS), security-constrained optimal power flow, economic dispatch, unit commitment, phase angle monitoring, power oscillation monitoring, power damping monitoring, voltage stability monitoring, and dynamic line rating are just a few examples of these applications [4]. Generator rejection, load rejection, Under-Frequency Load Shedding (UFLS) schemes, Out-of-Step (OOS) relaying, Under-Voltage Load Shedding (UVLS) schemes, and others are typical remedies for wide-area disturbances.

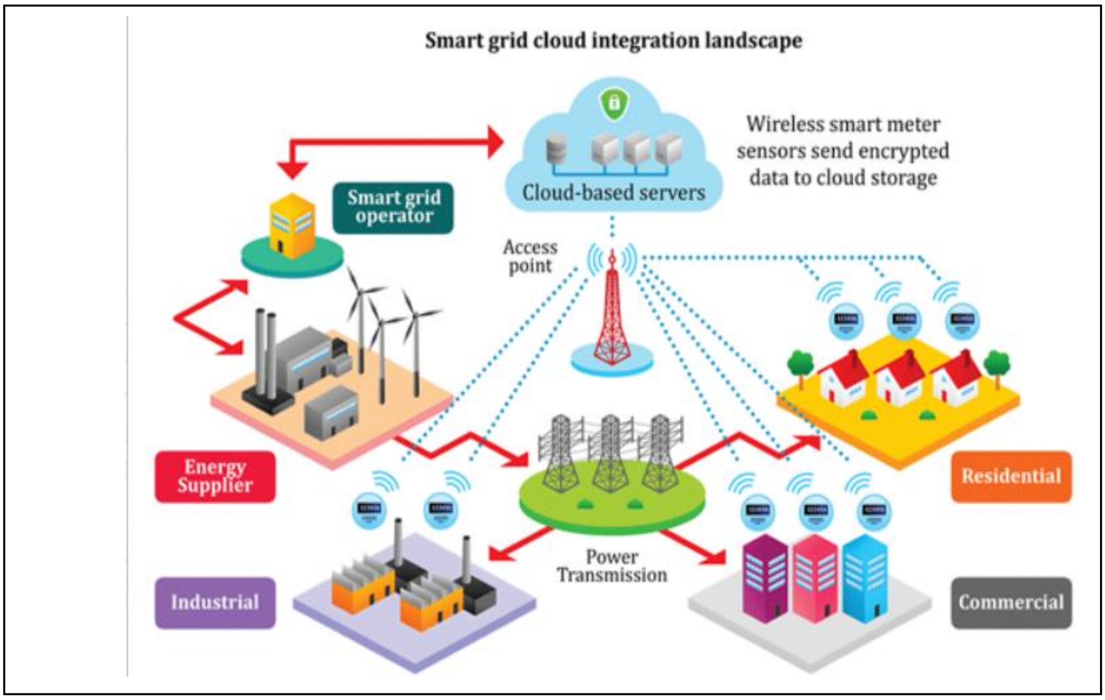


Figure 1-1.The Smart Grid a CyberPhysical System [5]

1.1 The Energy Sector in the Region

Hydropower is the main renewable resource in Africa with over 37GW of installed capacity. The African continent also has the highest untapped hydropower potential in the world, with only 11% utilized. Hydropower amounts to 17% of electricity generation in Africa, with this share potentially increasing to more than 23% by 2040, as part of many African countries' ambitious proposals for creating a lower-carbon energy system, and universal energy access in Africa. Hydropower provides a free and clean fuel source - water, renewed by rainfall. It can supply large amounts of electricity and, when combined with storage (a reservoir), can be dispatched to provide baseload power or to smooth out the intermittency of other renewables in an energy system - meaning it is one of the most flexible and reliable forms of renewable energy [6,7]. In Zambia, energy sources include renewable sources such as water, solar, wind, and biomass; as well as fossil fuels such as petroleum. Given the substantial unexploited reserves of renewable sources, Zambia has the potential to be self-sufficient in energy, except for petroleum, which is wholly imported into the country. Despite the diversity of these energy sources, however, water remains the main energy source in Zambia. It is estimated that Zambia possesses 40 percent of the water resources in the SADC region and has a hydropower potential above 6,000MW out of which about 2,354MW has been developed. The national installed capacity of electricity stood at 2,981.23 MW as of 30th June 2020. With regards to the installed capacity by technology, hydro generation accounted for 80.5 percent followed by coal at 10.1 percent. Further Heavy Fuel Oil (HFO) generation was at 3.7 percent, while Diesel and Solar were at 2.8 percent and 3.0 percent, respectively. The large hydropower projects under feasibility studies are over 2,800MW and situated on the major rivers of Zambia. For this reason, it would be advisable to formulate optimal generation plans that are centered around hydropower [8,9,10].

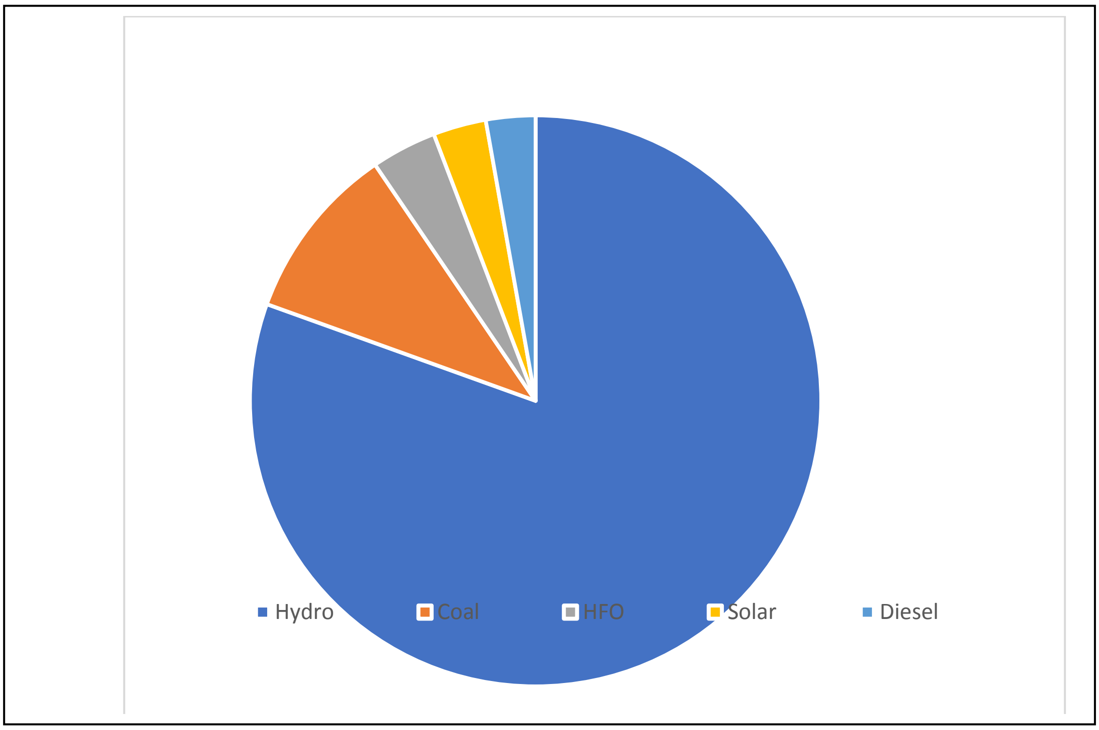


Figure 1-2. The Energy Sources in Zambia

Zambia’s energy sector is dominated by the ZESCO (formerly called Zambia Electricity Supply Corporation). ZESCO is the vertically integrated national utility that generates transmits, distributes, and supplies electricity to national and regional markets. There are two other major players, namely: the Copperbelt Energy Corporation (CEC) which is a transmission company that purchases electricity from

ZESCO at high voltage and distributes it to the mining industry in the Copperbelt region; and the Lunsemfwa Hydro Power Company. There are also two rural concessions: Zengamina Hydro Power Company (ZHPC) which runs a remote rural network in the Northern Province and North West Energy Corporation which distributes electricity to a rural mining community that is not on the ZESCO grid [11]. The regulation of the sector is undertaken by the Energy Regulation Board (ERB). The ERB was created under the Energy Regulation Act of 1995 Chapter 436 of the Laws of Zambia following the issuance of Statutory Instrument number 6 of 1997, the Energy Regulation Act (Commencement Order) of 27th January 1997[11].

1.1.1 Background: Cybersecurity Risks and Models

Industrial control systems (ICS) are an important section of the operational technology sector. It involves monitoring and controlling systems for industrial activities. SCADA systems are industrial systems that use control devices, network protocols, and graphical user interfaces to record and analyze real-time data. SCADA systems are used to monitor and regulate hydropower facilities, telecommunications, water and waste management, oil and gas refining, and energy in general. Cloud computing and the Internet of Things (IoT) are bringing about a paradigm shift that is boosting innovation, allowing for more flexible resources, and cutting operating costs. ICS is shifting to cloud computing and IoT to improve supervision and control operations by exchanging real-time information among machines, industrial chains, suppliers, and customers., ICS is migrating to cloud computing and IoT to improve supervisory and control procedures. SCADA systems feature unique cyber and physical interaction and were originally built as air-gapped or isolated systems, connecting them to the internet potentially creates a security problem [5,12,13,14,15].

Since the first disclosure of Stuxnet, there has been a massive wave of worldwide cyber security events affecting electric grids. In 2011, the industrial control systems (ICSs) of multiple national vital infrastructures in the United States were hacked by Black Energy. At Saudi Aramco, one of the world's largest oil enterprises, Shamoon, a self-replicating computer malware, infected three-quarters of Windows-based corporate PCs [16]. In August 2017, a similar attack on Saudi Aramco was launched. A distributed denial-of-service (DDoS) attack struck JEA in February 2013, causing the online and telephone payment systems to be down for a few days [17] (see Fig. 1-3).

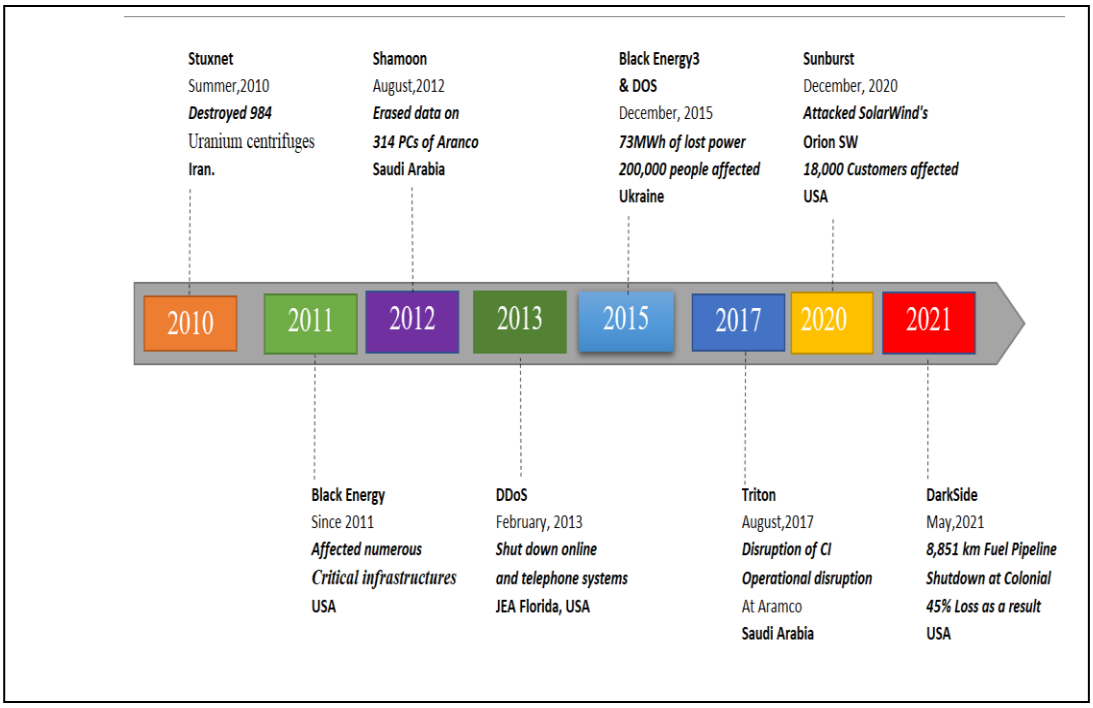


Figure 1-3. A Timeline of cyber attacks on Industrial Control Systems

It is becoming increasingly apparent that intelligent countermeasures at several tiers are required to secure SCADA infrastructure elements and the key applications they enable. Several government evaluations have found substantial cyber security deficiencies in the electric sector, which could have serious ramifications as a result of the rise of Advanced Persistent Threats (APTs) and the urgent need to protect against them [18]. For example, in the United States, the Department of Energy (DOE) created a cyber security Risk Management Process (RMP) for the electric sector in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) [19], National programs such as the NERC Critical Infrastructure Protection (CIP) [20] and the NIST Interagency Report (NISTIR) 7628 [21] guarantee that suitable standards and safeguards are in place to protect the electric power system from potential cyber vulnerabilities and threats.

The Cyber Security Strategy of the European Union, the EU's first comprehensive policy document on cyber security, was adopted in February 2013[22]. The strategy presented in that document serves as the overarching foundation for EU cyber security and cybercrime measures. The EU Parliament enacted the Network Information

Security (NIS) Directive [23] in July 2016, which supports and develops it. Many organizations and groups have also been formed. The European Network and Information Security Agency (ENISA) [24], as well as the Computer Emergency Response Team for EU institutions, support initiatives on network and information security (CERT-EU).

The Directorate-General for Energy (DG Energy) established the Energy Expert Cyber Security Platform (EECSP) in September 2015 intending to assist the Commission with policy and regulatory orientations at the European level, with a focus on the energy sector. The EECSP formed an "informal and temporary Commission expert group" to advise the Commission on policy and regulatory solutions for energy-related cyber security issues. The European Energy Information Sharing and Analysis Centre (EEISAC), founded in 2015, is a public-private partnership that includes four EU energy utilities and other sector stakeholders. The European research project DENSEK, which was supported by the Department of Home Affairs, was used to develop EE-ISAC.

In January 2018, the Executive Council endorsed the decision of the Specialized Technical Committee on ICTs, EX.CL/Dec.987 (XXXII), to establish an Africa Cyber Security Collaboration and Coordination Committee to advise the African Union Commission on cyber strategies and to implement cyber security as a flagship project of Agenda 2063. This committee advises the AUC on issues like cybersecurity, cybercrime, cyber-legislations, online privacy, data protection, and digital policy challenges[24].

From the 10th to the 12th of December 2019, Africa made significant progress in improving its digital environment by hosting the first-ever meeting of the African Union Cybersecurity Expert Group (AUCSEG) in Addis Ababa, Ethiopia. Nonetheless, there are a huge awareness, understanding, knowledge, and competence gap among African Union (AU) member states when it comes to deploying and implementing the requisite strategies, skills, and programs. "As Africans, we need to determine our Philosophy, Ethics, Policy, Strategies, and accountability frameworks for Cyberspace, Cybersecurity, and Cognitive or Artificial Intelligence (AI)," the Experts' Group stated at its first meeting. Cybercrime is getting increasingly common. Furthermore, the group feels that dealing with growing risks like cybercrime and cyber terrorism has become a high issue for all African countries [24]. The group also stated that while information and communication technologies (ICTs) provide Africa with the best possibility to address some of its main development concerns efficiently and rapidly, their widespread use has also resulted in a surge in cyber-criminality. The group also feels that addressing rising dangers such as cybercrime and cyberterrorism has become a high priority for all African nations [24].

According to a study undertaken by the Cyber Security Centre for Southern Africa (C3SA), the SADC area as a whole has a lower degree of cybersecurity maturity than the rest of the globe in all aspects [25]. The bulk of SADC countries is still developing their cybersecurity capabilities. Trust and confidence in online services (Dimension 2), legislative frameworks for cybersecurity (Dimension 4), and national incident response were the most significant variations in maturity between the SADC region and the rest of the globe (Dimension 1).

Dimension 1: Cybersecurity Policy and Strategy,

National cybersecurity plans, incident response, crisis management, CI protection, and cybersecurity in national security and defense are all variables that go into determining the maturity level for this dimension. The Southern African Development Community (SADC) and the rest of the world continue to be separated [25].

Dimension 2: Cybersecurity Culture and Society,

Cybersecurity attitude, trust, and confidence in online services, consumers' comprehension of online personal information protection, reporting methods, and social media are all assessed in Dimension 2. The majority of SADC countries have a poor level of maturity in this area [25].

Dimension 3: Building Cybersecurity Knowledge and Capabilities

Dimension 3 assesses the following factors: initiatives to build cybersecurity awareness, cybersecurity education, cybersecurity professional training, as well as cybersecurity research and innovation. From the assessment it emerged that SADC countries have protocols and strategic plans in place, implying aspirations to develop cybersecurity skills and capacity [25].

Dimension 4: Cybersecurity Legal and Regulatory Frameworks

Dimension 4 assesses the following factors: legal and regulatory provisions; related legislative frameworks; legal and regulatory capability and capacity; and formal and informal cooperation frameworks to combat cybercrime. On average, SADC countries are showing progress in the development of substantive legislation on cybercrime. Most countries have passed specific cybercrime laws or amended their criminal law so that they can address cybercrime [25].

The Zambian government proposes the formation of national cyber security advising and coordinating council (NCSACC**)** in its Cyber Security and Cyber Crimes Act, 2021[26]. For example, the NCSACC is now advising critical infrastructure operators on how to comply with cybersecurity audits. Furthermore, the act requires that the controller of a critical information infrastructure establish mechanisms and processes, per information security standards, as may be required for the detection of a cyber security threat concerning its critical information infrastructure [26]. The National Cyber Security Policy [27] was implemented in 2021 by the Ministry of Transportation and Communications to foster effective mechanisms and a well-coordinated governance framework on cybersecurity by creating a secure, reliable, and trustworthy cyber environment that boosts confidence.

In addition to the above efforts, lots of research efforts are done to assess and address the problem of cyber attacks in power systems. This is where academia can help the most, by doing research and providing feedback on regulations and related recommendations, thereby improving operators' ability to protect against attacks. This, however, is not without its difficulties. Because of the crucial nature of these systems, access is extremely limited, creating a roadblock for anyone looking to do practical research.

1.2 The Problem of Cyberattacks on ICS and SCADA

More digitalization of the electrical system provides many benefits but also introduces security faults and vulnerabilities that could invite attacks. Cybersecurity strives to protect the Confidentiality, Integrity, and Availability (CIA) of information in cyberspace[13].

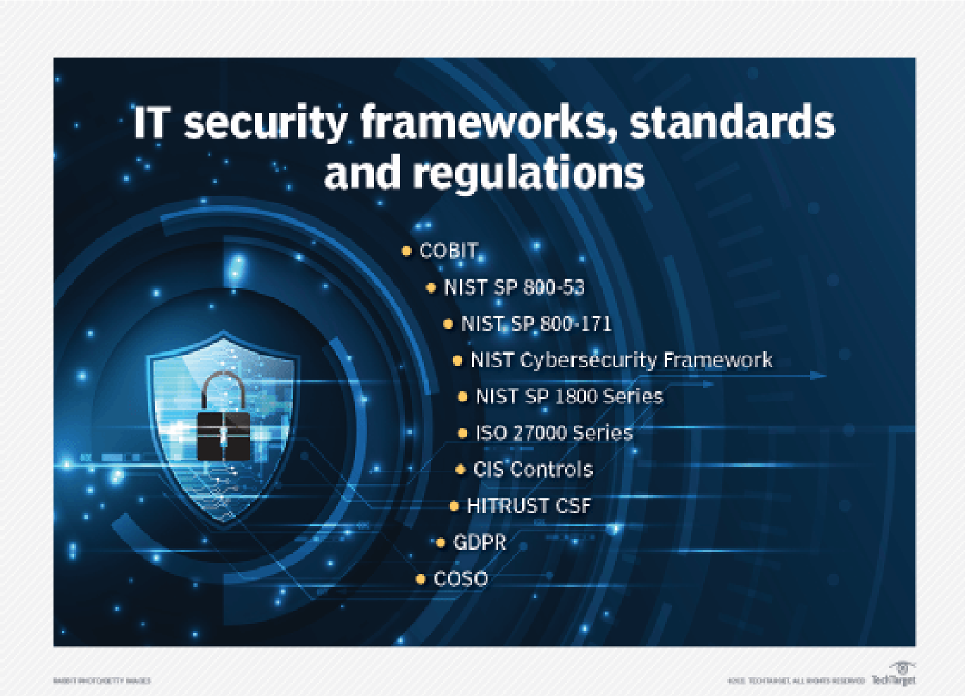
A fundamental security feature for data protection is data confidentiality. Due to the following aspects of cloud computing, that raise the risk of a data breach: remote data storage, a lack of network perimeter, the use of third-party cloud service providers, multitenancy, and extensive infrastructure sharing, offering such a service is crucial. Additionally, because cloud computing, by definition, combines a variety of both old and new technologies, it unavoidably creates new security risks as a result of both implementation and system design flaws. Data security versus usability, system scalability, and dynamics present challenges in offering satisfying security assurance in terms of data confidentiality [28].

Integrity models shield system data from unauthorized or unintentional changes, maintaining the accuracy and reliability of the data [28]. Virtue models aim to achieve three things: preventing unauthorized users from changing applications or data and stopping improper or unauthorized changes from being made by approved users. Ensure that data and initiatives are consistent both internally and externally. Balancing a collection of transactions to ensure that all the data is present and correctly accounted for is an illustration of an integrity check [28].

Data and resources are kept accessible for authorized use by availability models, particularly in times of crisis or catastrophe. Three typical availability issues are typically addressed by information security professionals: Denial of service (DoS) brought on by malicious assaults or by implementation flaws that haven't yet been found (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered) loss of information system capabilities brought on by human error or natural catastrophes (such as fires, floods, storms, or earthquakes) (bombs or strikes) equipment fails while being used normally [28].

Granting access only to authorized personnel, encrypting data being sent over the Internet or stored on digital media, testing computer system security regularly to find new vulnerabilities, building software defensively, and creating a disaster recovery plan are some actions that preserve confidentiality, integrity, and/or availability[13], [28].

It is thought that a general framework that may be utilized to raise the maturity level of cybersecurity in ICS is needed to promote proactive cybersecurity and threat intelligence exchange. A framework is a higher-level abstraction (meta-model) that can be used to clarify and/or combine many concepts, models, processes, and approaches [29]. Thus, a framework provides a structured set of concepts, models, guidelines, and technologies [29].



IT security frameworks, standards and regulations

- COBIT
- NIST SP 800-53
- NIST SP 800-171
- NIST Cybersecurity Framework
- NIST SP 1800 Series
- ISO 27000 Series
- CIS Controls
- HITRUST CSF
- GDPR
- COSO

Figure 1-4. The common cybersecurity frameworks

There is a need for a specific cybersecurity framework for the ICS industry. A review of the state-of-the-art research on the topics revealed the following research gaps [13,92,108,118,165]:

1) The existing work contributes limited efforts to evaluate and estimate cybersecurity maturity levels in ICS.

2) Most organizations do not share cybersecurity information because of reputational issues but there is a need for a standard cybersecurity information delivery system for internal and external cybersecurity communication.

3) Most organizations focus on legacy reactive and detective security technologies ignoring predictive technologies.

4) Most organizations focus on external cybersecurity threats and lack an emphasis on internal cybersecurity threats.

A holistic perspective on cybersecurity is lacking but is urgently needed for ICS and SCADA. This research study proposes a comprehensive cybersecurity framework that takes into account both internal and external threats and integrates existing technologies, standards, and models to communicate cybersecurity information and reduce the risk of cyber threats to close the aforementioned gaps.

1.3 Aim of the Study

The goal of this work is to conduct design research toward the development of a Comprehensive Cybersecurity Defense Framework (CCDF) artifact to enhance the cyber-physical defense of the smart grid (ICS) [13,92,108,118,165]. Figure 1-5 gives a summary of the research purpose.

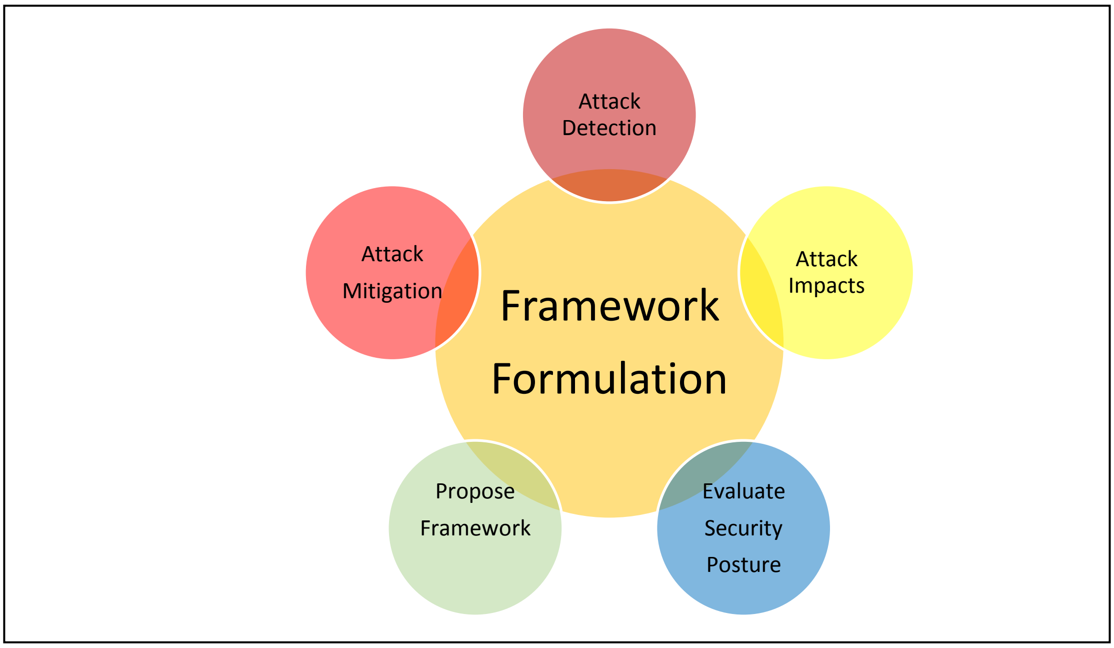


Figure 1-5. A Summary of the research aim

To approach the research problem, a systemic literature review of current cybersecurity frameworks was conducted to outline the gaps in a comprehensive approach to cyber defense[13,92,108,118,165]. A comprehensive cybersecurity defense framework to facilitate understanding of ICS cybersecurity was developed through design science and iterative evaluations of various frameworks. The framework identifies gaps in cybersecurity, risk management, and cybersecurity defense acquisitions. The framework captures operational cyber defense requirements based on ICS stakeholder needs towards the more practical use of security controls and compliance, ultimately providing better defense against cyberattacks. The framework leverages current de facto and de jure frameworks or standards to offer a comprehensive approach to driving cybersecurity defense requirements in large companies, agencies, or organizations. By defining the tasks, what those tasks are trying to achieve, and where best to accomplish those tasks on the network, a comprehensive approach may be reached.

1.4 Research Objectives

General Objective

The objective of the research was to develop a holistic cybersecurity framework for digitalized power grids to enable and operationalize a proactive cybersecurity strategy. The proposed framework can be used to enhance the cybersecurity maturity level and deliver threat intelligence to effectively predict, prevent, detect, and respond to cyber threats in critical national infrastructure.

Specific Objectives

a) Identify the existing cybersecurity maturity levels in industrial control systems;

b) Propose a Stochastic-based risk prediction framework for cyberattacks in the SCADA systems;

c) Determine the impact of cyberattacks on power systems contingency analysis

d) Formulation of a cybersecurity framework to increase the robustness and resilience of the ICS WAN systems

e) Development of a cybersecurity testbed to model attack and mitigation schemes in the smart power grid communications systems

1.5 Research Questions

To achieve the stated purpose and sub-objectives, the following research questions were formulated:

RQ1: What are the cybersecurity issues & challenges and the current level of cybersecurity maturity in critical assets in organizations in Zambia?

RQ2: How can proactive cybersecurity measures be enabled in Industrial control systems?

RQ3: What’s the Impact of cyber attacks on energy markets and contingencies, and how can we model them?

RQ4: How can a cybersecurity framework be developed and how can it enhance cybersecurity resilience in digitalized power?

RQ5: How can network-based state-of-the-art techniques detect and protect against process attacks on ICS?

1.6 Significance of the Study

1. This study contributes to continuing efforts in cyber security by revealing the security posture of the CPS of the electric power system.

2. This study assists in the construction and formulation of sector-specific cybersecurity frameworks to mitigate the effects of cyber attacks on critical infrastructure.

3. This research provides a solution to the present cyber security issues arising from the convergence of the IT/OT networks in critical infrastructure.

4. This research promotes the use of artificial intelligence and machine learning for cyber risk assessment

1.7 Theoretical and Conceptual Framework

1.7.1 Conceptual Framework: Routine Activity Theory

In 1979, Cohen and Felson presented the RAT, which looked at the rise in violent and nonviolent physical crime activity after WWII, concentrating on the role of routine activity in enabling criminal opportunity from the standpoint of the offender [30]. The criminal opportunity theory inspired RAT to depict the meeting of an offender and a target at a time and place where there is little or no supervision [30]. The criminal, a target, and the lack of a guardian are all required for a crime to occur, according to RAT. Cohen, Kluegel, and Land introduced an adaptation of RAT in 1981 to focus on the risks that an individual offender would encounter and use in a decision-making process to help decide whether an opportunity exists for a crime to occur. Cohen and Felson [30] assumed the existence of an offender, and therefore, the location, target, and guardianship become the core considerations. Cohen and Felson examined and debated modification to activity patterns with implications on criminal behavior due to the changes in one or more of the key RAT factors: offender, target, and guardian. A key tenant of RAT is the premise that modification of one or more of the key RAT factors may result in positive implications for criminal activity such as inadequate guardianship and cybersecurity practices [30].

In reaction to growing physical crime in a post-World War II society, Cohen and Felson [30] developed RAT. Many academics have looked into the use of RAT in various sorts of cybercrime, including Leukfeldt and Yar [31], McNeeley [33], Reyns and Henson [32], Vernon-Bido, Padilla, Diallo, Kavak, and Gore [34].

Advances in IT evolved the original RAT factors to adapt to the influences of cyber dependencies in daily online activities, for instance, an offender, cyber user, and lack of appropriate technical or nontechnical controls [32]. Existing research into the adaptation of RAT in response to society's expanded use of modern IT encompasses theories such as the rational choice theory and lifestyle- RAT as outlined by [32]. This adaptation reflects the needed evolution and maturation of RAT to account for situational conformity by an offender, target, and guardian [32, 33, 34].

Technology has evolved significantly since Cohen and Felson [30] first introduced RAT, and therefore, advances in IT have expanded the possibilities of applying the theory in research and analysis of malicious activity in physical and virtual environments [35,31,38]. According to [31] and [36], RAT identified four principal properties composing the acronym VIVA (value, inertia, visibility, and accessibility) that when present hold the potential for a target. Choosing a target may vary based on the motivation(s) and goal(s) of the attacker, and therefore, the four VIVA properties would be measured accordingly to best identify and define a target from the offender's perspective of the VIVA properties. According to Fischer [30], risk management is a basic factor of IT cybersecurity strategy, but one with substantial value and the associated risk assessment process helps to prioritize the possible threat vectors and infrastructure areas based on the criticality of function. An efficient risk management program is in theory a proactive strategic measure used to mitigate or eliminate organizational cybersecurity risks using RAT to help focus attention on the principal factors of threat (offender), vulnerability (target), and implication guardian [35]. My study used the principal factors of offender, target, and guardianship of RAT in a cybersecurity context. Risk management has been seen throughout the literature review noting how important it is for IT cybersecurity professionals to acquire and maintain an awareness and understanding of cyber threat capabilities as well as their infrastructure to best visualize their perception of normal cybersecurity and threat environments.

The use of IT is common and anticipated in modern society, which exposes citizens to cyber threats in the context of routine daily activities. [31] support [30] by reporting an offender might be one or multiple actors, a target could be the data or IT system, and a guardian can take the form of a technical or nontechnical control such as access authentication and system administrator. [35] supports Cohen and Felson's work by describing cybersecurity risks comprising three principal elements: threat (who = offender), vulnerability (what = target), and implication (attack vector = lack of guardianship).

Guardianship was pushed as a key aspect of information security by [31], [32], [35], and [37]. In this study, guardianship is a critical factor to consider. Some instances of guardianship are IT managers and cybersecurity measures. When used in a cyber setting, RAT has been used extensively in the literature to investigate a wide variety of possibilities, allowing for a comprehensive cybersecurity emphasis that includes a greater awareness and understanding of the daily operational environment.

RAT was chosen because it considers the target from the threat's point of view in the context of everyday activities. I used this theory to investigate the context of the offender, target, and preventive (cybersecurity) criteria in repeating, routine tasks and functions in critical infrastructure from a proactive cyber defense standpoint.

1.7.2 The Theoretical Framework

A firm deploying Smart Grid functionality must deal with a wide range of intricate cyber security challenges. As opposed to being a largely closed system, the electric grid is evolving into a complex, highly interconnected environment, or a system of systems. The way that any organization implements its cyber security standards should alter as a result of advancements made in systems and technology as well as in the methods employed by adversaries.

The National Institute of Standards and Technology (NIST) framework [20] serves as the foundation for the study. A consistent approach to cybersecurity is what the NIST Cybersecurity Framework [21] aims to give enterprises. Describe their current cybersecurity state or posture.

1) Describe their desired cybersecurity state.

2) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.

3) Make progress assessment towards the desired cybersecurity state.

4) Make internal or external communication to stakeholders about cybersecurity risks.

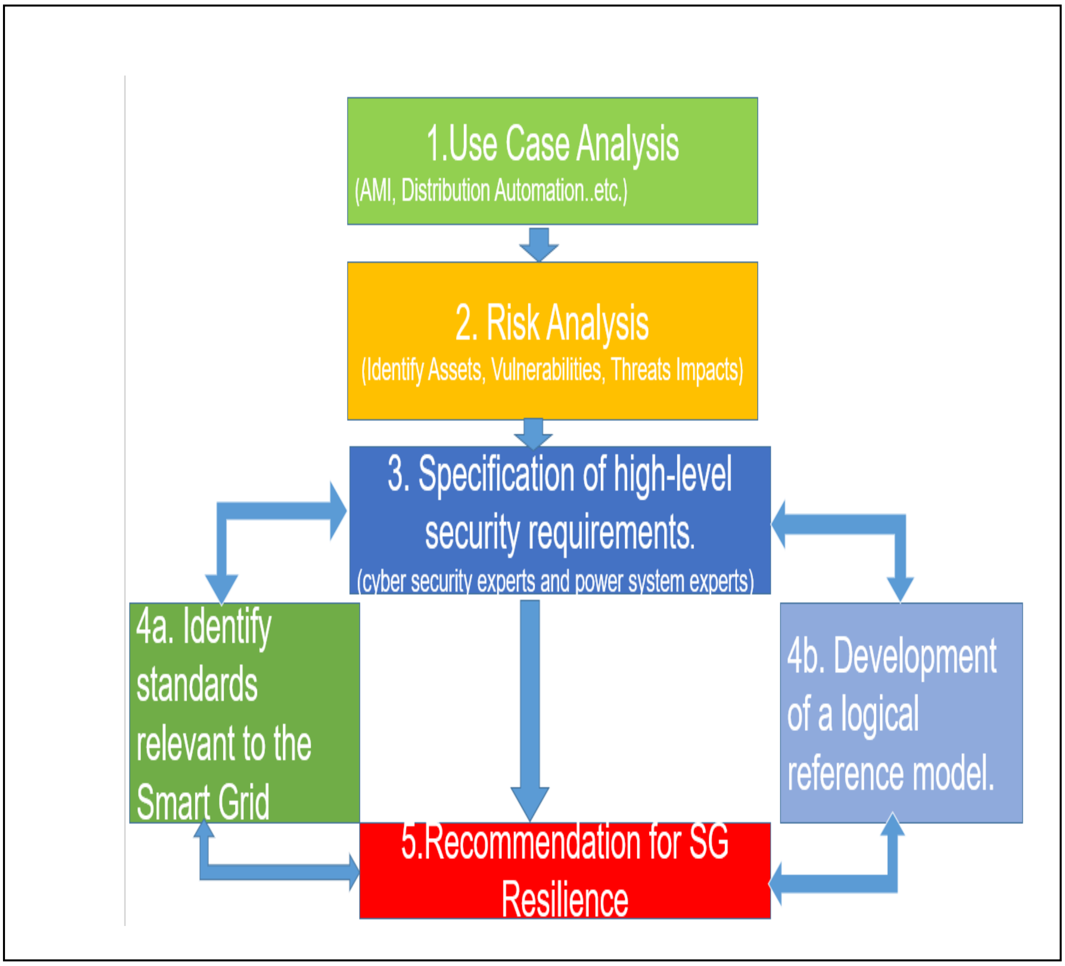

1.Use Case Analysis
(AMI, Distribution Automation..etc.)
2. Risk Analysis
(Identify Assets, Vulnerabilities, Threats Impacts)
3. Specification of high-level security requirements.
(cyber security experts and power system experts)
4a. Identify standards relevant to the Smart Grid
4b. Development of a logical reference model.
5.Recommendation for SG Resilience

Figure 1-6. Theoretical Framework flow diagram

Figure 1-6 depicts the theoretical framework adopted in this study, it consists of five tasks, 1). Selection of use cases, 2). Performance of a risk assessment, 3). Specification of high-level security requirements, 4). Identification of standards relevant to the smart grid, and development of a logical reference model, 5). Recommendation for smart grid resilience.

1.7.2.1 Task 1. Selection of Use Cases with Cyber Security Considerations

A standard framework for performing risk assessments, creating logical reference models, and choosing and customizing security criteria is provided by the collection of use cases [21].

1.7.2.2 Task 2. Performance of a Risk Assessment

The risk assessment has been carried out from a high-level, all-encompassing functional perspective, and includes identifying assets, vulnerabilities, threats, and impacts. The output served as the foundation for choosing the security criteria and identifying any gaps in the related standards and guides [21].

Vulnerability classes: The Open Web Application Security Project (OWASP) vulnerabilities list [40], Common Weakness Enumeration (CWE) vulnerabilities [39], and NIST SP 800-82, among others, were used to create the first list of vulnerability classes[11]. These vulnerability classes will guarantee that the discovered vulnerabilities are addressed by the security controls. To evaluate their systems, Smart Grid implementers, such as vendors and utilities, may also employ vulnerability classes [21].

Bottom-up analysis: The bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation intelligent electronic devices (IEDs), key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems were considered when evaluating the impacts of a cyber security incident. An incident in one infrastructure can potentially cascade to failures in other domains/systems [21].

Top-down analysis: In the top-down approach, logical interface diagrams were developed for the six functional FERC and NIST priority areas that were the focus of the initial draft of this report—Electric Transportation, Electric Storage, Wide-Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management. This report includes a logical reference model for the overall Smart Grid, with logical interfaces identified for the additional grid functionality. Because there are hundreds of interfaces, each logical interface is allocated to one of 22 logical interface categories. Some examples of the logical interface categories are (1) control systems with high data accuracy and high availability, as well as media and computer constraints; (2) business-to-business (B2B) connections; (3) interfaces between sensor networks and controls systems; and (4) interface to the customer site. A set of attributes (e.g., wireless media, inter-organizational interactions, integrity requirements) was defined, and the attributes were allocated to the interface categories, as appropriate. This logical interface category/attributes matrix is used in assessing the impact of a security compromise on confidentiality, integrity, and availability [22].

As with any evaluation, the final result depends on a realistic study of unintentional mistakes, natural disasters, and malevolent threats and their applicability to subsequent risk-mitigation techniques. The Smart Grid is the same. It is advised that all enterprises adopt a realistic perspective on the risks and dangers and collaborate with national authorities as necessary to gather the necessary data, which is projected to be impossible for any one utility or other Smart Grid participants to evaluate independently. The types of information systems' opponents are shown in table 1-1 below. When doing a risk assessment of a Smart Grid information system, these adversaries must be taken into account [21].

Table 1-1. Categories of Adversaries to Information Systems

Adversary	Description
Nation-states	well-financed, state-run, and coordinated. Utilize foreign service agents to collect sensitive or important information from nations that are considered adversarial or to have a political, military, or economic edge.
Hackers	A team of persons who attack networks and systems to take advantage of operating system defects or other weaknesses (such as hackers, phreakers, crackers, trashers, and pirates).
Terrorists/cyber terrorists	People or organizations acting domestically or abroad on behalf of various terrorist or extremist organizations that utilize violence or the threat of violence to sow fear in governments or societies that they will submit to their demands.
Organized crime	Organized criminal behavior, including illegal drug trafficking, gambling, and racketeering, among many other things. a successful and creative criminal enterprise.

Other Criminal Elements	Another facet of the criminal community is normally not well organized or financed. Normally consists of a few individuals, or of one individual acting alone.
Industrial Competitors	Corporate espionage is the illicit collection of information from rival companies or foreign governments by domestic and foreign enterprises operating in a competitive market.
Disgruntled Employees	Potentially harmful persons who are irate and unhappy could harm the Smart Grid network or associated technologies. Depending on the individual's work status at the time and their level of access to the systems, this could be considered an insider threat.
Careless or poorly Trained Employees	Users who put the security of Smart Grid systems at risk due to a lack of training, care, or attention. Another illustration of an enemy or threat from within.

1.7.2.3 Task 3. Specification of High-Level Security Requirements.

For the evaluation of specific security needs and the choice of suitable security technology and methods, experts in power systems, as well as cyber security, were needed. The cyber security specialists brought a broad understanding of IT and control system security technologies, whereas the power system experts brought a deep understanding of conventional power system procedures for maintaining power system reliability.

1.7.2.3.1 Task 4a. Development of a Logical Reference Model.

Logical communication interfaces between actors are identified by the logical reference model. There may be different logical reference model implementations since this is a high-level logical reference model. The logical reference model and the NIST conceptual model can be combined in the future to create a single Smart Grid design. The logical security architecture can then be updated using this Smart Grid design[21].

1.7.2.3.2 Task 4b. Assessment of the Smart Grid Standards.

Task 4b evaluated the standards that the expert teams had identified as possibly applicable to the Smart Grid to ascertain their applicability to Smart Grid security. Gaps in security standards were found during this process, and suggestions are offered for filling these gaps. Additionally, recommendations will be made regarding standards that are in conflict and standards that have security criteria that are not in line with the security needs mentioned in this report. The completion of this assignment will result in the publication of additional materials in the future[21].

1.7.2.4 Task 5. Conformity Assessment.

The last stage is to create a security conformance evaluation program. The actions specified by the testing and certification standing committee of any smart grid operators are coordinated with this program [21].

1.8 Definition of Terms

The following terms are used in this work.

(i) **Critical infrastructure**: Assets are deemed critical to the public's health, welfare, finances, and security [41].

(ii) **Operational technologies:** Industrial systems that operate building infrastructure, utilities, transport, logistics, manufacturing, autonomous vehicles, ships, drones, robotics, and healthcare equipment [42].

(iii) **Cybersecurity in critical infrastructure:** Functions performed to protect IT and OT that comprise the critical infrastructure to include access [43].

(iv) **Cyber-physical systems (CPS):** Transformative technologies for managing interconnected systems between their physical assets and computational capabilities [44].

(v) **Cyber threats:** A threat with malicious intent to cause harm or damage in the cyber domain [45].

1.9 Assumptions

Gergen [46] noted that research is informed by the use of applicable assumptions or presuppositions formed from our informed biases such as in prior experience or through prior research. Berger [47] stated that shared experiences often form challenges for researchers and participants, sometimes resulting in the creation and misapplication of assumptions. Those assumptions are influenced by the perceptions formed during the relevant experiences and, in turn, may impact the ability to make informed decisions because certain data were set aside based on the assumptions [14]. Certain assumptions have been made in this study. We assumed that each of the organizations identified employed at least one IT or compliance professional with prior experience in critical infrastructure protection. We assumed that all employees were expected to comply with the organization's cybersecurity policies and guidance. Another assumption was that participants in the qualitative research interviews are qualified to be part of the study, and each participant was open and truthful in their responses using their relevant knowledge and experience. We also assumed the chosen qualitative research method and conceptual framework for the study was successful in facilitating the analysis of the collected data and providing relevant findings to the research question. To help mitigate the assumptions, semistructured interview questions and member checking were used to allow interviewees to articulate and validate their responses in more depth based on experience rather than providing a simple yes or no answer.

The following assumptions were applied to the simulation for the impact and mitigation of cyber-attacks on smart grid digital communication systems:

1) Contingency analysis and risk assessment are important tasks for the safe operation of electrical energy networks. The knowledge about the possible contingency events in a system can be utilized in the forecast estimation of the system state.
2) A contingency risk assessment performed through load-flow analysis is a tedious and time-consuming operation.
3) The load-flow analysis is a time-consuming approach when a large power system is considered.
4) The statistical approach applied in time-consuming functions of contingency analysis eventually minimizes the computing time of the entire process of contingency analysis.

5) It was assumed that the attacker has access to system measurements through the communication system including frequency and power flow measurements.

1.10 Scope of the Study

We considered single and multi-area power system state estimation. For single-area state estimation, we look at the integrity of measurement data delivered over a wide area communication network. For multi-area state estimation, we look at the integrity of data exchanged between the control centers of neighboring areas in face of a targeted false data integrate attack (FDIA) that compromises an endpoint of the secure communication tunnel.

1.11 Research Contributions and Publications

The research focuses in this thesis lie in main topics relating to FDI attacks in smart grid CPSs including modeling and impacts evaluation of FDI attacks, and novel detection approaches for FDI attacks. Specifically, our main research contributions are summarized as follows:

1. To assess and analyze the system reliability of smart grid CPSs, particularly against topology attacks under system countermeasures, an analytical model based on stochastic Petri nets is created (i.e., intrusion detection systems and malfunction recovery techniques).
2. Risk analysis using a steady-state probability of compromising SCADA and relays: Many of the recent research studies gain their interest in compromising the power system-wide control such as the AGC and the SCADA. “what-if” scenarios are mostly established, and many authors focus on validating the advanced countermeasure against cyberattacks. However, the CPS frameworks require a discussion on how often an event happens from stochastic power of view. The recent articles do not deal with this stochastic process but rather spend more energy on “what-if” approaches. This thesis addresses the hacking process into the SCADA and IEDs (i.e., protective relays) that cause disruptive switching actions on smart grid communication and control systems.
3. Impact analysis using power system dynamic simulation model: Almost all recent research studies adopt a static-based approach, i.e., power flow calculation program-based approach. Although more engineers have increased their interest in

representing cascaded events/attacks, most approaches leverage continuous, multiple power flow snapshots.

4. Implementation of research supported by the Cyber-Physical Security (CPS) laboratory. Integrating the computing, communication, and control that satisfies the needs of physical processes is often referred to as a cyber-physical system. Our contribution to the literature is the principles, which also assist practitioners in several ways, including enhancing the effectiveness of simulations being developed for evaluating cyber-physical artifacts, suggesting remedies for dealing with unanticipated cyber threats posed by emerging artifacts, and offering guidance for cybersecurity assessment.

5. To detect and identify FDI attacks on the power grid, an LSTM-based technique is provided. The model is divided into two stages: (1) attack detection and identification using a multi-class classifier model, and (2) attack mitigation using a regression model after the attacks identified in the first stage.

Table 1-2.Research Contributions

SN.	Peer Reviewed Journals	Conference Paper
1	Petri Net-Based (PN) Cyber Risk Assessment and Modeling for Zambian Smart Grid (SG) ICS and SCADA Systems	Stochastic Edge-Based Anomaly Detection for Supervisory Control And Data Acquisitions Systems: Considering The Zambian Power Grid
2	Cyberphysical Security Analysis of Digital Control Systems in Hydro Electric Power Grids	Assessing the Ramifications of Electric Vehicle Charging Infrastructure on

		Smart Grid Systems in Zambia.
3	Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia	
4	Stochastic Quantification of Cyber Attacks Impact on Smart Grid Contingency Analysis	
5	A Novel Cyber-physical Co-simulation Testbed Development to Assess the Effects of Cyber-attacks on the Wind Farm Operations (Under peer review)	
6	Detection of False Data Injection Attacks in Smart-Grid Systems: Based on Semi-Supervised Learning	
7	False data injection attacks on automatic generation control modeling and mitigation based on reinforcement learning	
8	Detection of False Data Injection Attacks in Smart-Grid Systems: Benchmarking Deep Learning Techniques	

1.12 Ethical Considerations

A research proposal was presented to the Graduate Studies Committee of the School of Engineering, Department of Electrical and Electronic Engineering. Comments and suggestions from the members were noted and incorporated.

Ethical approval for this research was obtained from the University of Zambia Ethics Committee. There was no impact on human dignity. Informed consent from respondents was obtained before they participated to allow them to decide to participate based on adequate knowledge of the study. Any corporate data used in the study were anonymized and names were de-identified to ensure confidentiality and integrity.

1.13 Brief Overview of the Chapters

Chapter Two deals with a review of the literature on the smart grid. Chapter Three considers the method and materials used in the research. That is research design, data modeling, and simulation tools used. Chapter Four presents the modeling of attacks and mitigation results. Chapter Five provides and discusses the results obtained. Chapter Six concludes and gives recommendations for the study.

1.14 Conclusion

Chapter One introduced the background to the research, the problem of cyberattacks on smart grid infrastructure. Also considered are the purpose, significance, justification, and theoretical framework of the research. Lastly, the terms used in the research were defined and the assumptions and scope of the study were stated.

CHAPTER 2: LITERATURE REVIEW

A smart grid can be defined as the incorporation between communication and information technology and the traditional power grid. It utilizes networking techniques to exchange information about the grid conditions and customers' demands. The main target of this integration is to improve the power generation process and reduce electricity losses. In addition, the smart grid merges renewable power resources with traditional power generators to cover the increased electricity demand. Another benefit of the smart grid is assisting in CO2 emissions reduction and environmental protection. Additionally, more distributed generators (DGs) are inserted in the smart grids to satisfy the high electricity demands; they mostly are renewable resources-based generators, such as wind turbines, and solar panels. Furthermore, original techniques, such as microgrids and V2G connection, are utilized in smart grids. The micro-grid offers electrical self-sufficiency for a specific area using one or more DGs and storage units and allows the area to be isolated or connected to the main grid according to the current status of the grid; this feature protects the micro-grid in case of a blackout and assists the self-healing of the grid. In addition, the smart grid utilizes the EVs' batteries as temporary storage units for the extra generated power during low demand periods; V2G networks organize the charging/discharging operations of the EVs' batteries to guarantee a balanced electricity level in the grid [1, 2, 3, 5]. This chapter defines the smart grid's importance, describes its architecture, and briefly introduces its main security concerns.

2.1 Smart Grid Benefits

According to the service provider, i.e., utility companies, smart grid technology can significantly enhance the reliability and efficiency of the power grid. The grid's reliability means reducing the probability of blackouts and guaranteeing the required level of electricity supply to all customers. The electricity company is responsible for providing a specific electricity demand to each customer according to its type, i.e., residential or industrial. In case of an electricity shortage, there will be huge financial and economic losses for the customer, especially industrial ones, and as consequence, the electricity company is obligated to pay a fine to the affected customer [3], [5].

Rearranging users' energy consumption patterns can reduce power losses while increasing grid efficiency. For instance, the electricity supplier can encourage residential customers to use their high-consumption appliances by lowering the price of electricity during periods of low peak load. Implementing a security strategy for the smart grid can also aid in lowering energy theft, a major contributor to energy losses in many countries. As a result, the output of electricity will be planned out and might even be reduced. Additionally, the integration of renewable output resources into the new smart grid can reduce the load on traditional plant generators [2], [3], and [5].

A smart grid can improve the efficiency of the maintenance and replacement operations for the involved devices in the grid. For example, there are many deployed sensors in the smart grid for monitoring purposes; they monitor the performance of the different devices and send an alarm message to the control center in case of an error. Finally, a smart grid is a friend to the environment, as it organizes electricity production and uses renewable generation resources. Accordingly, the smart grid plays a significant role in CO2 emission reduction. To conclude, utility companies are interested in smart grids to assure the optimal usage of electrical power and provide more luxury services to the customers, and consequently, increase their financial profits [1,2,3,5].

2.2 Smart Grid Architecture

The smart grid introduces new components and protocols in the power grid to achieve the smart grid's functions. This section introduces the smart grid's reference model, its different layers and their functions, and then the smart grid's systems.

2.2.1 Smart Grid Reference Model

There are many proposed frameworks to identify the structure of the smart grid. According to [48], the smart grid reference model composes of seven functional domains:

1) Bulk Generation: Electricity is usually generated from non-renewable resources, such as coal and gas generators. In a smart grid, renewable sources, e.g., wind turbines and solar panels, are merged with traditional ones to satisfy the increased demands and reduce CO2 emissions.

2) Transmission: Several substations and transmission lines are utilized to transmit the produced power to consumers.

3) Distribution: The distribution domain spreads the electricity to individual customers and communicates with suppliers and users via communication infrastructure.

4) Operation: This domain controls and monitors the transmission and distribution domains to obtain information about the power system's activities.

5) Market: This domain contains all the parties involved in the electricity-trade operation to sustain the balance between supply and demand.

6) Customer: Customers in the smart grid not only consume electricity but also generate it by distributed generators and store the extra power in rechargeable batteries.

7) Service Provider: The electricity is provided to customers via a service provider that is responsible for services, such as billing and customer accounts management.

2.2.2 Smart Grid Layers

According to [49], a smart grid is composed of five layers that arrange the involved parties in the grid:

1) Application layer: provides smart grid applications for both customers and utilities.

2) Security layer: satisfies the security requirements for all involved parties in the smart grid.

3) Communication layer: provides a two-way reliable and secure data transmission.

4) Power control layer: monitors and controls the power transmission operation using PMUs, sensors, transformers, meters, and storage devices.

5) Power system layer: delivers the electricity to customers through power generation, transmission, and distribution systems.

2.2.3 Smart Grid Systems

The smart grid differs from the traditional power grid in several ways. The most important difference is that the smart grid can exchange electricity and information about the grid conditions between suppliers and end-users in both directions. The main purposes of this communication are to decrease the total consumption of electricity, preserve the electricity demand approximately at the same level all the time, and consequently reduce the overall cost of this service. According to [1], a smart grid is divided into a smart infrastructure system, a smart management system, and smart protection system.

2.2.3.1 Smart Infrastructure System

A smart infrastructure system, which comprises smart energy, smart information, and smart communication subsystems, facilitates the bidirectional movement of data and power [4,5].

The smart energy subsystem: regulates the production, distribution, and use of electricity. In conventional networks, a small number of massive central power units produce electricity. The generated electricity is then sent across the transmission system to substations before being distributed to customers over the distribution grid. As a result, it is a one-way process. A smart grid, on the other hand, is bidirectional and makes use of DGs to improve the grid's consistency, such as solar and wind power. This growth introduces two fresh ideas: A microgrid, a small-scale grid with its own DGs and loads, is self-sufficient in terms of power. As a result, a micro-grid can cut itself off from the main grid in the event of a failure since it believes itself to be a little independent grid that generates its power [5].

However, the communication with the grid did not fully disconnect; microgrids still exchange information with the whole grid to decide when to reconnect with it. The other concept is the V2G connection. EVs' batteries are charged from the grid at low-demand times and work as electrical storage. Still, the charging operation requires efficient scheduling techniques for coordinated charging to conserve the optimal power system performance and keep the peak power demand at a minimum level. The grid restores the power from EVs in high-demand periods, i.e., EVs act as DGs and supply electricity back to the grid [5,13,14].

The smart information subsystem: Measurement of information, grid status monitoring, and user appliance management fall under the purview of the smart information subsystem. To collect energy metering data for analysis and electricity billing reasons, it deploys certain metering and measurement devices, such as smart meters that are a component of the automatic metering infrastructure. The primary objective of a smart meter is to calculate the total amount of electricity consumed by a unit, such as a house, at each predetermined interval and communicate the information to the central control for billing and monitoring. Additionally, smart meters can monitor loads and future demands as well as control appliances, i.e., connect or disconnect them, to lower electricity costs [4,5,13,14].

In addition, smart monitoring and measurement devices, i.e., sensors and PMUs, are utilized. First, sensors are used to monitor the real-time mechanical and electrical conditions of a power system, in addition, to analyzing the failures if happened [4],[5]. Wireless sensor networks are strongly recommended to accomplish this mission because of their effective cost; however, sensors are low-power nodes and vulnerable to attacks or severe environmental conditions. Second, PMUs are secure measurement devices that are based on measuring the phase angle of the power model to determine the power system's state. PMUs are utilized to forecast any failure before happening. A huge amount of information is generated from the metering devices; this data should be stored and analyzed to extract the best benefit. Cloud computing is a good candidate for that huge information storage. However, cloud computing suffers from certain security and privacy threats in addition to the expensive cost of that service [13]-17].

The smart communication subsystem: Utilizing both wired and wireless networks, the smart communication subsystem is in charge of distributing the gathered data across various grid components. With minimal installation costs, the smart grid uses a variety of networks to support dependability, availability, security, and privacy needs while ensuring the appropriate QoS [4,5,28]. Many communication technologies, including wireless mesh networks, cellular communication systems, IEEE 802.15.4-based technologies, satellite communications, fiber optic communications, and PLC, are recommended for the smart grid. The TCP/IP protocol is a promising candidate for controlling the communication subsystem of the smart grid, but it must overcome several difficulties associated with the use of heterogeneous communication networks and low-cost techniques to smoothly transform the current grid into a smart grid [13]-[18].

2.2.3.2 Smart Management System

Modern applications and services in a smart grid are primarily managed and controlled by smart management systems. The major purposes of this system are cost reduction and energy efficiency[4]-[5]. By transferring and rescheduling the loads, a smart management system primarily tries to smooth the demand profile form. As a result, energy losses are reduced, the cost of generation as a whole is reduced, and system dependability is raised. Numerous optimization strategies can be used to achieve these goals [13]-[18].

2.2.3.3 Smart Protection System

A smart protection system protects the grid from threats, which could be user errors, equipment failures, natural disasters, and cyber-attacks, by offering defense mechanisms and preserving the security and privacy of the grid. In a smart grid, DGs with their fluctuant and intermittent renewable resources could threaten the reliability and stability of the grid. Thus, the smart grid uses microgrids. Micro-grid deployment leads to less power flow within the entire grid, as loads are served locally within every microgrid, which consequently reduces the possibility of cascading failures. Another way to guarantee the grid's reliability is to assure the consistency of the measurement system by depending on powerful secured measurement devices. To predict any failure that occurs in the grid, the PMUs' data is utilized to identify the stability region and predicate the weak points in the grid to identify the probability of failures and where they could happen. If the failure happened, the system's knowledge about topology and PMU measurements helps to quickly identify and fix it and prevent cascading events [4]-[5],[13-18].

In other words, the grid satisfies the self-healing feature, which is the ability to prevent the spread of failures and quick recovery of the grid. For micro-grid protection, micro-grid can work in two modes: normal and island modes. In the normal mode, the microgrid connects and exchanges electricity with the main grid. However, if any abnormal conditions, such as power failures, occur, the micro-grid switches to island mode, which isolates the micro-grid and stops the electrical ow with the main grid to protect the micro-grid customers and prevent cascade failure. So, a microgrid with the isolation capability improves self-healing and increases the grid's ability to work well during normal times and outages as well [4]-[5],[13-18].

In addition, cyber security is one of the serious challenges in the smart grid. Cyber adversaries can compromise the power grid via communication systems to perform malicious actions, such as obtaining user private information, gaining access to CC, and altering load conditions to destabilize the grid in addition to new security and privacy issues due to the deployment of smart meters, sensors, and PMUs. For smart meters security, a smart meter is the most vulnerable part of a smart grid; it suffers from many security threats that can falsify the consumed electricity amount; for example, malicious users can compromise their smart meters to reduce their energy meter readings and pay lower electricity bills. Moreover, the extensive deployment of smart meters increases the opportunity for adversaries to inject bad data into the grid. The adversaries' fabricated readings mislead the electric utility and result in wrong decisions about local or regional usage and capacity. The adversaries also can launch an effective DoS attack by forging many demand requests for a smart meter that is requesting a large amount of energy. One of the severe attacks is to target the electricity supply of a country. In traditional grids, this attack is very difficult, as it involves various attacks on generation, transmission, and distribution assets, which are well-protected. However, the emergence of millions of smart meters controlled by a few central controllers in the grid will simplify this attack. The adversary only compromises these controllers and sends a combination of commands to cause supply interruption. As a result, efficient security techniques to guarantee the confidentiality and integrity of the smart meters' readings are essential [4]-[5],[13-18].

According to smart meters' privacy, the major benefit of the smart grid is collecting a huge amount of reading data for various appliances in the household. However, this advantage could turn into a privacy concern, as the information about house energy usage can reveal the personal habits and daily activities of householders. To address the privacy of smart meters, several protection approaches have been proposed, such as employing homomorphic encryption during the data reading aggregation process, compressing the readings and adding random sequences, or deploying anonymization schemes to conceal the real identity of smart meters [4]-[5],[13-18].

The effectiveness of the smart grid for monitoring and measurement unit security depends on the precision of the installed measurement units and PMUs. State estimators, installed in the main CC and used to estimate the status of the power grid by analyzing the results of the measurements, are used to verify the accuracy of the measurements. As a result, the accuracy of the data has a direct bearing on how the grid state is assessed. The FDI assault is a frequent method used to undermine the integrity of measuring data. The intruder in this assault can take advantage of the grid's compromised PMUs and measurement units to modify the state estimation without setting off any bad-data alarms. Many studies concentrate on identifying the attacks by utilizing effective state estimators and optimization strategies [4]-[5],[13-18] to fend off these attacks. Deploying communication networks generally exposes the power grid to security and privacy concerns that are present in these networks as well as introduces additional dangers because of the nature of the power grid [4]-[5],[13-18].

2.3 Smart Grid Networks

The smart grid uses four different types of communication networks: HANs, NANs, V2G connections, and WANs. Each of these networks has a different data rate and coverage area, necessitating the usage of separate communication technology. These networks are used by the smart grid to communicate data on grid conditions and client requests. To link electricity users and the power utility, three networks are used. The first network is called HAN, and it links the smart meter inside the home to smart home equipment. NANs, the second network in use, is in charge of sending the utility company the electricity usage reports for all HANs in the area. In this thesis, we refer to HANs, BANs, IANs, and NANs collectively as "customer-side networks.". For WAN, it is utilized by NANs to forward the electricity reports to the main utility center. The V2G network is utilized to schedule the charging/discharging operations between EVs and the grid. Figure 1-1 shows the power system versus the communication architecture in the smart grid [50], [51], [52].

2.3.1 Home Area Networks (HANs)

HAN, a hybrid local area network, represents the network of communication between smart appliances, electric vehicles, and smart meters. It facilitates communication between smart gadgets within or close to the home. Other networks that fall under the HAN umbrella include building area networks (BANs) and industrial area networks (IANs). BAN connects numerous HANs within a single residential neighborhood, but IAN only connects a few HANs in the same industrial zone [50].

Smart home appliances, such as refrigerators, washing machines, and ovens, are varied in their communication requirements. For instance, the light bulb sends much less data to the smart meter than the air conditioner (AC) so ACs require more communication infrastructure than bulbs. According to their communication needs, smart appliances can be divided into four categories:

Group 1 consists of small-load appliances, such as light bulbs and phone chargers, where an appliance does not significantly impact the total electricity load, and only needs to inform CC whether the appliance is currently connected or disconnected from the grid [50].

Group 2 consists of large uncontrollable-load appliances, e.g., stoves, which operate according to the consumer needs, and their usage cannot be delayed to a later time. The appliances in that group need to send only their power consumption and expected duration of usage to CC[50].

Group 3 consists of controllable large-load appliances, such as ACs and clothes washers. Before any of these appliances are switched on, it should send a request to CC via smart meter, including the appliance's expected electricity requirement, duration of usage, and possible usage times in a day. Based on this information, CC can accept or reject the request according to the dynamic electricity pricing, as well as the agreement between the householder and the utility company [50].

Finally, **Group 4** consists only of EVs, which require an extensive exchange of information with CC to schedule the charging/discharging processes [51]. While a smart meter is an improved electrical meter that primarily aggregates the readings of electricity consumption for a house every specific time interval and forwards the result at least daily to the power service provider for controlling and billing purposes. Smart meter supports the two-way communication feature with CC; whether this CC is a local control unit or the main CC for the utility. HAN/BAN/IANs' applications, such as industrial energy management or computing total electricity costs, require a small data rate of 100 kbps with a short coverage distance of up to 100 m. Thus, technologies, such as ZigBee, PLC, Ethernet, and WiFi, which are low power, low cost, and secure communication, are widely used [50, 51, 52, 56].

2.3.2 Neighbourhood Area Networks (NANs)

NAN is responsible for connecting HANs in a specific area to the main CC. It forwards the electricity consumption reports for the region to the service provider. In addition, it sends the electricity payments' value from the utility to all HANs in the area. NAN's applications, such as smart metering and demand response, need a higher data rate from 100 kbps to 10 Mbps and a larger coverage distance of up to 10 km. Therefore, ZigBee mesh networks, WiFi, PLC, and cellular can be suitable for NAN [50].

2.3.3 Vehicle-to-Grid (V2G) Connections

As known, the optimal utilization of generated power and reduction of electricity losses is one of the major objectives of a smart grid; this objective requires the presence of storage units that save the extra electricity in case of high power generation and provide the electricity back to the grid in case of high power consumption. Many types of energy storage are used as short-term storage devices, such as fuel cells, wheels, and

EVs (as battery electric vehicles (BEVs) or plug-in hybrid electric vehicle (PHEV) batteries). EV batteries consider promising storage media because of the rapid increase in the number of these vehicles soon. As well, the batteries are stable storage units; the losses ratio for the stored power in EVs' batteries is low. In addition, the charging and discharging operations for EV batteries are much faster than increasing or decreasing the generation level of traditional power plants to satisfy the electrical loads. In other words, the vehicles can work as distributed generation resources; they can quickly supply electricity to the grid if the consumers' demands increased, also they can rapidly store the extra power from the grid if the electrical requirements decreased. As a result, EVs supply certain services to the electricity grid, such as providing peak power, spinning reserves, regulation reserves, and storing renewable energy. Consequently, the V2G network term is coined to represent the communication between EVs and the power grid. The communication between the power grid and EVs is bidirectional; when the power transfers from the vehicle's battery to the grid, the connection to manage this operation is called a vehicle-to-grid or V2G connection. While if the power transmits from the grid to the battery of the vehicle, the connection is called the grid-to-vehicle or G2V connection. In the thesis, the term V2G connection is used to refer to both connections. V2G connection suffers from some problems related to scheduling the charging/discharging processes; it also experiences particular security and privacy threats, such as the disclosure of the EV's owner identity or current location, and DoS attacks [50], [51],[52].

2.3.4 Wide Area Networks (WANs)

Additionally, NANs use the WAN, which already exists, to transmit the electricity reports from their local regions to the main CC in the utility business. WAN is used for the charging and discharging activities of the batteries of EVs. Applications that demand a greater data rate from 10 Mbps to 1 Gbps and broad coverage distances up to 100 km include wide-area management, monitoring, and protection. Due to their high capacity, low latency, and broad coverage range, technologies including optical fiber communication, cellular, and WiMAX are most frequently employed between transmission/distribution substations and the utility's CC[50].

2.4 The Power Control System and State Estimation

Fundamentally, the power grid is responsible for the generation, transmission, and distribution of electricity to customers. To achieve these functions, the power grid CC should perform certain auxiliary tasks to guarantee the required quality of service and prevent hazards and disasters, such as blackouts. One of the major tasks is monitoring the grid status using local sensors or measurement units. Therefore, CC should assure the accuracy of these measurements by state estimation operation. The traditional state estimators are based on computing the difference between observed and expected measurements and comparing the residual by a specific threshold. However, this technique is not realistic for the novel smart grid, as the power grid exposure to communication networks leads to a new type of attack that targets the infrastructure of the grid by injecting false measurements; these new attacks are called FDI attacks or stealthy attacks. Accordingly, these FDI attacks can mislead the CC to make wrong decisions for the grid and consequently cause catastrophic results; for instance, on August 14, 2003, a large area of the United States and Canada experienced an electric power blackout, which affected about 50 million people and caused economic losses between $4 billion and $10 billion in the United States and $2.3 billion in Canada [57]. In this section, we describe power system components and services, and then define power system different models, and traditional state estimation processes.

2.4.1 Supervisory Control and Data Acquisition (SCADA) System

An example of an industrial control system is the supervisory control and data acquisition (SCADA) system, which serves as the brain of the power system (ICS). Industrial operations are physically monitored and managed by an ICS, a computer-controlled system. SCADA systems are large-scale systems with several sites and great distances, which sets them apart from other ICS systems. The SCADA system works by transmitting signals through communication channels to control this remote equipment, which comprises a few remote units coupled to various sensors, actuators, and master stations [57]. It is possible to combine the supervisory operation with a data-gathering function by sending signals across communication channels to learn more about the status of the remote equipment [57]. The SCADA system consists mainly of:

1) Remote terminal units (RTUs) that connect to sensors or measurement units that spread in different locations in the grid, convert their signals to digital data, and then send the data to the supervisory system. As well, they receive digital commands from the supervisory system and forward them to the sensors.

2) Telemetry system, which connects the field devices, i.e., RTUs, with CCs via wired or wireless communication media.

3) Data acquisition server that provides some services to the human operator and other parties and allows them to access the field devices' data.

4) Human-machine interface (HMI), displays the data in an interpretable format for the human operator so that he/she monitors and interacts with the grid's status. The operator via HMI can request the data from the data acquisition server.

5) The historian is a software service that records all time-stamped data and events in a database and utilizes them to graphically show the power trends via HMI.

6) The supervisory system, which is the CC, gathers data about the status of different parties in the grid, and also sends control commands to the system via communication infrastructure.

These subsystems allow SCADA to acquire RTU data, aggregate it, and format it to make decision-making by the supervisory system, such as adjusting RTUs, easier. Alternatively, data can be sent to the historian to enable trending and other types of analytical auditing [57].

SCADA systems is used since the 1970s in the power grid but nowadays more devices that provide more functions are attached to them. The modern grid, smart grid, support new tasks, such as automatic generation control and optimal power flow analysis; also new types of sensors, e.g., PMUs, are employed for wide-area monitoring and control systems for the grid. In addition, the SCADA communication network is heterogeneous; it consists of fiber optics, satellite, and microwave connections. Although the traditional SCADA systems are originally designed to be centralized and closed systems, i.e., original SCADA systems have limited connection with open networks like the Internet, SCADA system in a smart grid becomes distributed and connected to different networks. As a result, it is exposed to various cyber security threats. Therefore, SCADA requires protection techniques to provide its services without security risks. Analytical instruments, such as state estimators, are significant in the modern SCADA system. The measurement units that are spread in the grid collect data about the grid's status and forward it to the SCADA system via RTUs. A state estimator is an analytical tool in the SCADA's CC that is responsible for checking the accuracy of the received measurements. Consequently, accurate state estimators are significant for the future smart grid to fulfill its tasks. However, the state estimation operation is threatened by cyber and physical security threats, because the exchanged data is often sent without encryption so that malicious attackers exploit that weakness and launch powerful attacks, such as FDI attacks [58, 59, 60, 61].

2.4.1.1 SCADA-specific Communication Protocols

Standard protocols utilized in data transfer between field controllers and the central server are referred to as SCADA-specific communication protocols. The majority of protocols work on a master/slave basis because of the nature of this data transfer. IEC 60870-5-101/104, DNP3, and Modbus are the three SCADA communication protocols that are most frequently employed. In general, bigger data volumes are employed with the IEC and DNP3 protocols because they are both more functional than Modbus. While DNP3 is frequently used in North America, the IEC protocol is primarily used in European nations [62].

2.4.1.1.1 IEC 60870-5-104

IEC 60870 is a group of standards created by the International Electrotechnical Commission (IEC) for telecontrol (SCADA) in electrical engineering and power system automation applications [65]. The group consists of six main parts plus several companion standards. Part 5 (IEC60870-5) in particular, known as Transmission protocols, provides a communication profile for the transmission of SCADA telemetry control and information [63].

The companion standard IEC 60870-5-101, published in 1995, is typically referred to when IEC 60870, or IEC 870 for short, is addressed concerning SCADA because it was the first document to specify the entire SCADA transmission protocol, allowing it to be utilized in production [63]. As an extension of IEC 60870-5-101, which was initially created for serial communications, the IEC 60870-5-104 standard was later published in 2000. The same serial frames from 101 might be transferred over TCP/IP thanks to IEC 60870-5-104 [64]. An IEC 60870-5-104 packet's data structure, or payload, is seen in Figure 2-1. The Application Protocol Control Information (APCI) and the Application Service Data Unit (ASDU) are the two components of this payload, which is also known as the Application Protocol Data Unit (APDU) [65].

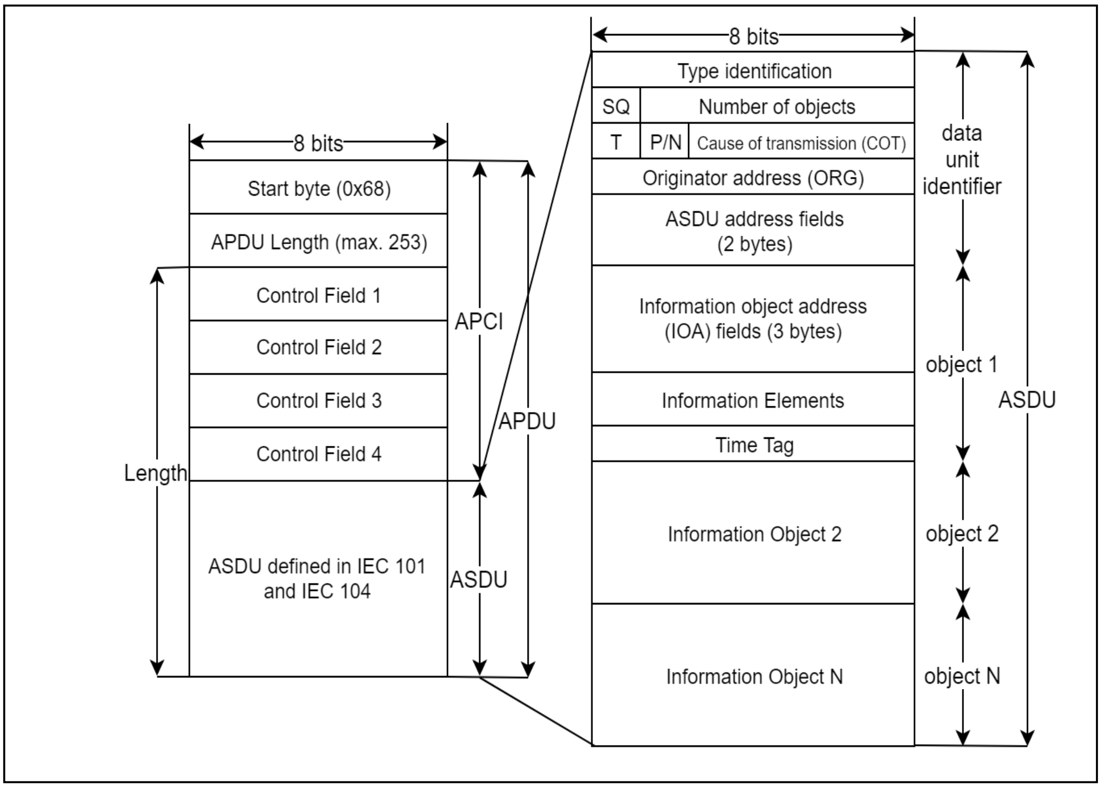


Figure 2-1. The IEC 60870-5-104 APDU Frame Format [64] [65]

The APCI is essentially used as a communication start and stop mechanism for the ASDU. It generally has a length of 6 bytes, which includes a start byte with a value of 0x68 followed by an 8-bit length field (length of the APDU) and four 8-bit control fields. The APDU’s frame format/type is determined by the last two bits of the APCI’s first control field as seen in Figure 2-2, and can be defined as [65]:

- I-format (X0) - Information transfer format;
- S-format (01) - Numbered supervisory functions;
- U-format (11) - Unnumbered control functions.

The ASDU (Figure 2-2), which is only incorporated in the I-format, contains two main sections, the data unit identifier and the data payload of one or more information objects [65]. The data unit identifier in particular defines the specific type and amount of data provides addressing to determine the identity of data and includes additional information such as the cause of transmission (COT) 651]. One of the fields present in the identifier is the Type identification field. This field is responsible for defining the type of data by referring to 8-bit code types.

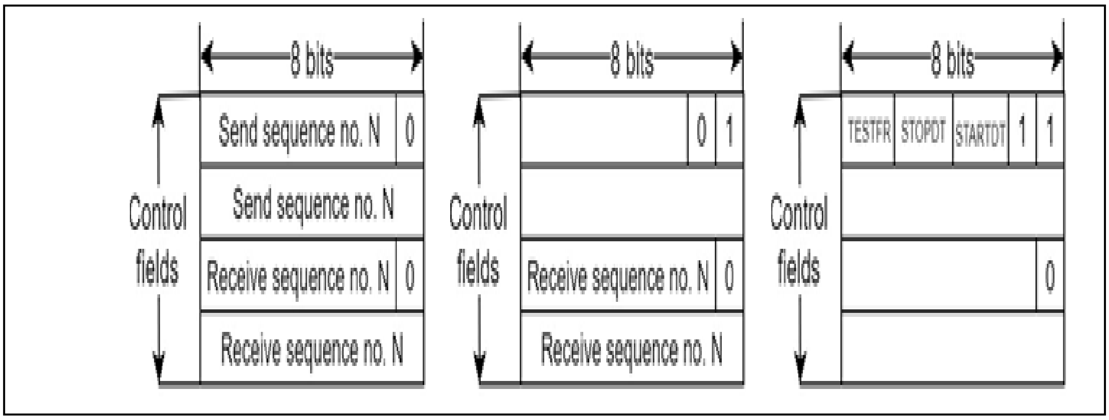


Figure 2-2. The APCI Control Field Information [65]

The types that are currently defined by IEC are shown in Table 2-1 [66]. Another field is the number of objects which indicates the number of information objects contained in the payload and can vary from 0 to 127.

The field labeled "Cause of transmission" indicates the reason why the payload was transmitted and is used to control the routing of messages. Its values vary from 1-47 for standard definitions and 48-63 for special use. Lastly, the ASDU address field, or common address for ASDU, is associated with all objects contained within the ASDU. It is normally interpreted as a station address [65]. Additional information on IEC 104 ASDU types and COT values can be found in Matoušek’s analysis of the IEC 104 protocol [65].

Table 2-1. Code Type Groups [66]

CODE TYPE RANGE	GROUP
1-21,30-40	Process information in the monitor direction
45-51	Process information in the control direction
70	System Information in monitor direction
100-106	System Information in the control direction
110-113	The parameter in the control direction
120-126	File Transfer

After the data unit identifier, each information object will start with an Information object address (IOA) followed by the actual information. This address is used as a destination address in control and as a source address in the monitor direction [65].

IEC 60870-5-104 is generally assigned, by default, to the TCP port number 2404 [65], [66].

2.4.1.1.2 DNP3

The Distributed Network Protocol Version 3 (DNP3) is a communication protocol standard that defines communications between master stations, RTUs, and other intelligent electronic devices. The protocol was designed specifically for SCADA applications and was created as a proprietary protocol by Harris Controls Division to be used solely in the electrical utility industry. It was then later made available for public use as an open protocol standard, when its ownership was transferred to the DNP3 User Group, making it an accepted standard in the electric, oil & gas, waste/water, and security industries [67].

DNP3 is primarily used within SCADA so control centers can communicate with remote substations or outstations in the case of serial communication. It's typically configured in a master-slave configuration, where the DNP3 master would be the control center, and the slaves would be the various RTUs inside a substation [68]. An example of a configuration with one master and multiple slaves (multi-drop) can be seen in Figure 2-3.

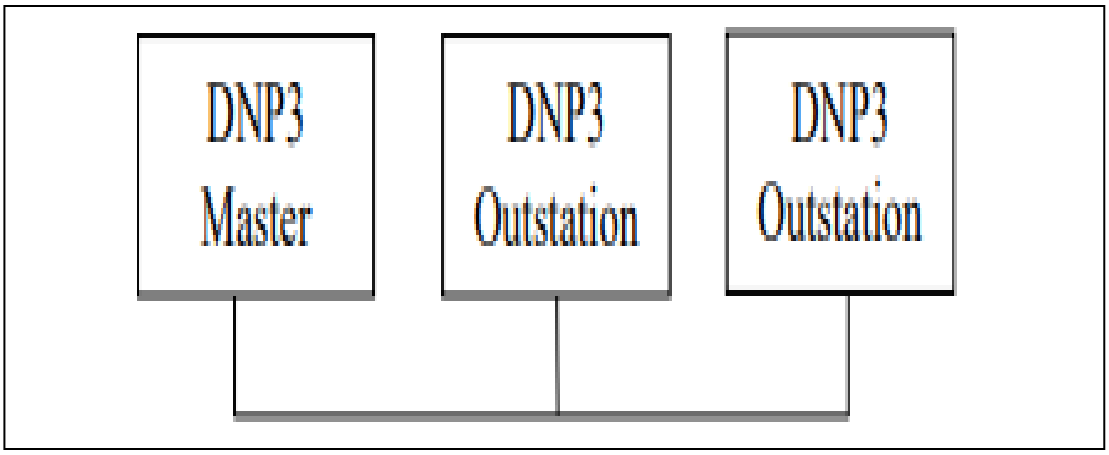


Figure 2-3. The DNP3 Master/Slave Architecture [66]

DNP3 is a four-layer subset of the Open Systems Interconnection (OSI) model in terms of architecture. The application, data connection, physical, and pseudo-transport layers are some of these layers [66]. The architecture of a DNP3 packet is shown in Figure 2-4. The Data Link layer frame is the packet's first part. The two start bytes (0x0564) at the beginning of this frame serve as a starting point for the frame. The Length field, which is the byte after that, indicates how many bytes are left in the frame after the Cyclic Redundancy Check (CRC). The Control field (1 byte) comes next, and it provides details on the contents of the packet. The Source and Destination fields that come after are both 2-byte addresses that specify the receiver and transmitter of the DNP3 device, respectively [68]. Every DNP3 device must have a distinct address to transmit and receive messages to and from other DNP3 devices, and there are over 65500 addresses available utilizing this 2-byte addressing method. Due to the data payload being broken up into blocks, several CRC fields are included with the packet. A pair of CRC bytes are present in every block, except for the final block, per 16 data bytes. The pseudo-transport layer is the layer that follows the data link layer. Long application layer messages must be divided into smaller packets of a size appropriate for transmission by the link layer, and upon receipt, the frames must be reassembled into shorter messages of the application layer size [66].

Finally, we have the Application layer. This layer contains the instructions for the devices, such as confirmation, reads, writes, selects, restarts, responses, and more. The layer starts with an Application Header that contains a control byte, followed by a function code that provides the instruction, and ends with internal indications only if the instruction is a response [67]. Table 2-2 lists the most commonly used function codes when performing a vulnerability assessment and the most enticing ones for attacking the DNP3 protocol.

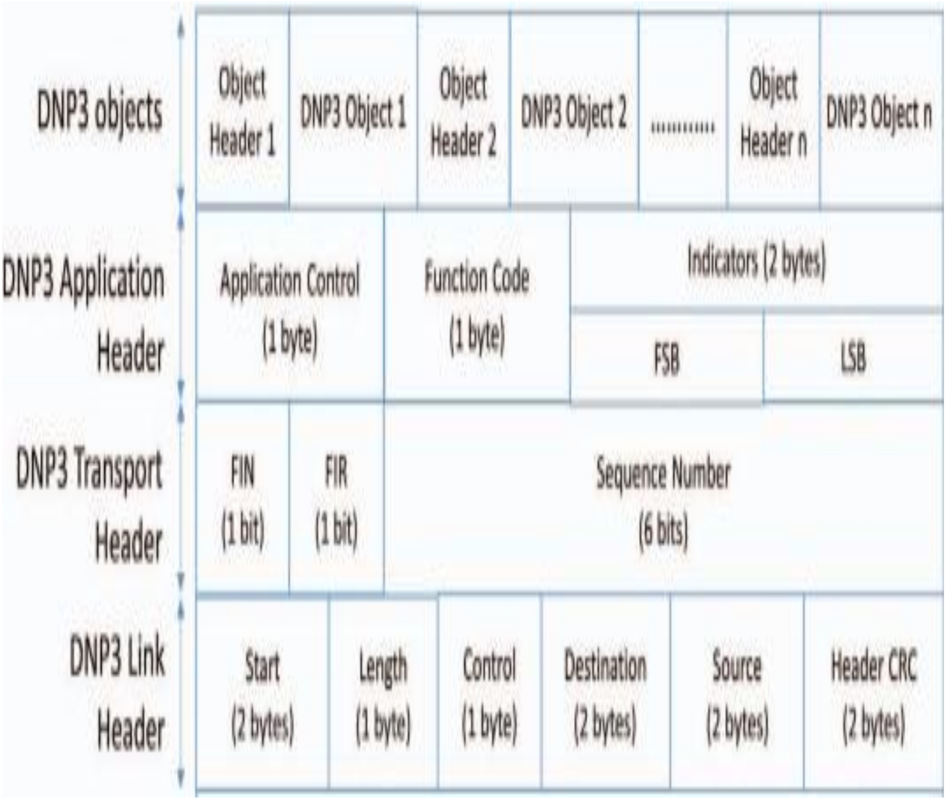


Figure 2-4. The DNP3 Message Architecture[69]

Table 2-2. DNP3 Function Codes

Function Code	Function Code Description
0x00	Confirm
Ox01	Read
0x02	Write
0x03	Select
0x04	Operate
0x05	Direct Operate
0x0d	Cold Operate
0x0e	Warm Operate
0x12	Stop Operate
0x1b	Delete File
0x81	Response
0x82	Unsolicited Response

Like other traditional SCADA protocols, DNP3 was originally designed for serial communications. As in IEC 104, the protocol was extended to allow the use of TCP/IP as a transport mechanism. This extension was done by simply encapsulating the entire DNP3 frame with TCP/IP headers, maintaining the original architecture [69]. DNP3 is assigned, by default, to the TCP port number 20000 [66] [68].

2.4.1.1.3 Modbus

Modbus is a serial-based protocol that was developed in 1979 by Modicon (now Schneider Electric) to be used in industrial automation systems and with their PLCs [70,71]. It's one of the most commonly used protocols in ICS systems due to it being a simple and robust protocol that is open to use without requiring royalties. As in other SCADA communication protocols, Modbus has since been altered to work on Ethernet networks. This was achieved by encapsulating the serial-based protocol inside TCP headers. There are many iterations of Modbus, which include Modbus RTU, Modbus+, Modbus TCP/IP, and Modbus over TCP/IP, which is similar to Modbus TCP/IP, but it has checksums within the payload of the packet, and other less common implementations [68]. In this thesis, we will focus on Modbus TCP/IP which is the encapsulated version of Modbus RTU.

Modbus-enabled devices establish communication with one another by adopting a master-slave (client-server) architecture, where only one device (the master/client) can start transactions or requests. Simply by providing the needed data to the master or carrying out the activities specified in the query, the other devices (slave/server) react [71]. In SCADA systems, Modbus is employed to establish communication between RTUs and the control center (slave/server and master/client, respectively). Figure 2-5 shows an illustration of this client-server architecture over an Ethernet TCP/IP network. Four different message types might be used in this paradigm to express the following [70]:

1) Modbus Request - message sent by the client to initiate a transaction.
2) Modbus Indication - request message received on the server side.
3) Modbus Response - response message sent by the server.
4) Modbus Confirmation - response message received on the client side.

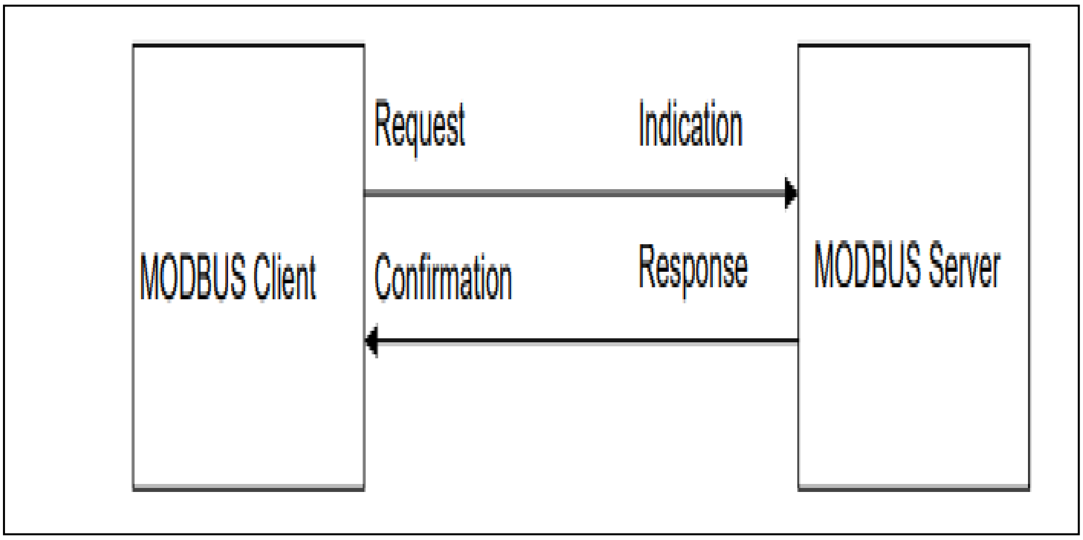


Figure 2-5. The Modbus TCP/IP Client/Server model [5]

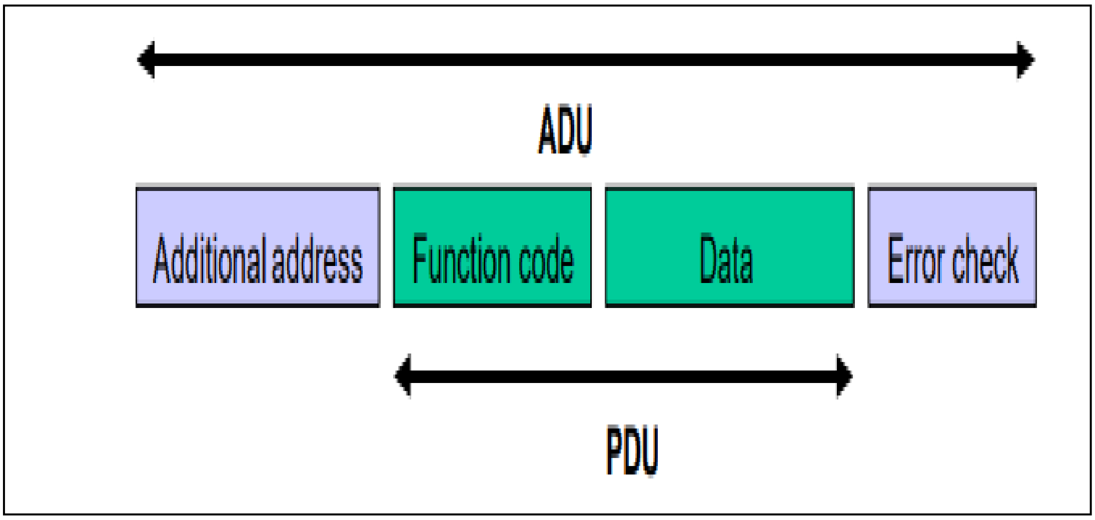


Figure 2-6.General Modbus frame [5]

A fundamental Modbus packet frame is depicted in Figure 2-6 in terms of architecture. The Application Data Unit (ADU) and the Protocol Data Unit (PDU), which the ADU encloses, can be divided into two parts of this packet frame. The PDU, an error-checking technique, and an address field are all included in the ADU. A function code and a data field make up the PDU [68].

Modbus TCP/IP uses a Modbus packet frame that is slightly different from the standard frame. As seen in Figure 2-7, it also consists of an ADU and PDU, but the ADU in this packet frame omits the error-checking technique and is instead made up of a Modbus Application (MBAP) header and the PDU. The Transaction ID, Protocol ID, Length, and Unit ID are all contained in the 7 bytes that make up the MBAP header. For each transaction, the master sets a Transaction ID field with a size of 2 bytes. The two bytes in the Protocol ID field, which is used to specify the protocol, are always set to 0x0000 for Modbus. The Unit ID and data fields are also included in the Length field, which is also made up of 2 bytes and counts the remaining bytes till the conclusion of the ADU. For connecting Ethernet to a serial sub-network, the Unit ID, which is 1 byte long, is used to identify a remote slave on a non-TCP/IP network [70].

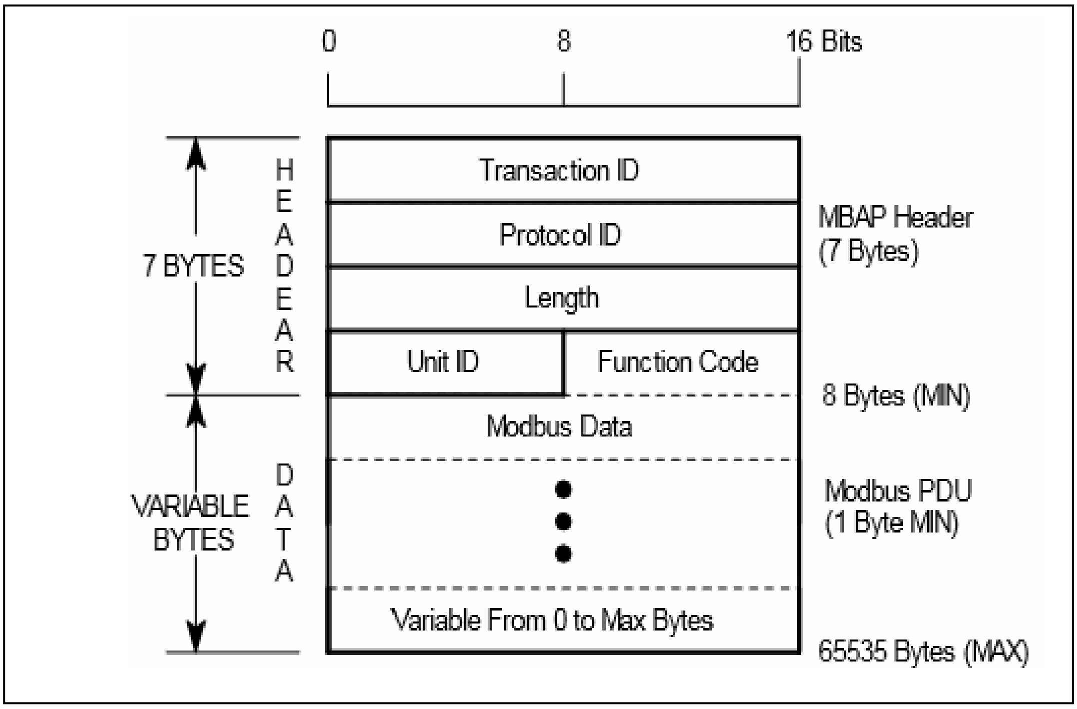


Figure 2-7. A Modbus TCP/IP Application Data Unit (ADU) [6]

The PDU consists of a function code and the actual data of the protocol. The function code field consists of 1 byte that tells the slave what kind of action to take. Function codes can be categorized in three ways: public, user-defined, and reserved. Valid function codes range from 1-255 in decimal, but not all codes will apply to a module. Of these 255 function codes, some are reserved for future use, and others, such as 65-72 and 100-110, are allocated for user-defined services [71]. Some public function codes that most devices will support are shown in Table 2-3.

Table 2-3. Modbus Public Function Codes [11]

Function Code - Function Description (Decimal)	
1 . Read coils	**14.** Read Device Identification
2. Read Discrete inputs	**15.** Write Multiple coils
3. Read Multiple Holding Registers	**16.** Write Multiple Holding Registers
4. Read the Input Register	**17.** Report Slave ID
5. Write Single coil	**20.** Read File Record
6. Write Single Holding Register	**21.** Write File Record
7. Read Exception Status	**22.** Mask Write Register
8. Diagnostic	**23.** Read/Write Multiple Registers
11. Get Com Event Counter	**24.** Read/FIFO Queue
12. Get Com Event Log	**43.** Read Device Identification

Source[11]

Like the other protocols mentioned before, Modbus is assigned a default TCP/IP port when it is configured. Modbus TCP/IP packets are transferred across Ethernet networks over TCP port number 502 [70] [71] [68].

2.4.1.1.4 IEC 61850

In 2004, the IEC61850 global standard for the management and safety of medium and high-voltage switchgear was published. The models of standardization IEC and ANSI are also covered [72]. The new condition ensures:

1) The unified standard for all substations and power plants;
2) Application of a common format for a description of substations and making the design approach easier;
3) Defining the main services required for data transmission using different communication protocols;
4) Interoperability between devices from different manufacturers.

IEC61850 offers a defined framework for integrating functional characteristics, the structure of data packages in devices, standardizing the names of data packages, how applications interface with and control devices, and executing standardized tests. The IEC 61850 standard is divided into 10 parts, totaling around 1200 pages [73].

Table 2-4. General parts of IEC 61850

Part #	Title
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	- Principles and Models

7.2	- Abstract Communication Service Interface (ACSI)
7.3	- Common Data Classes (CDC)
7.4	- Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	- Mappings to MMS(ISO/IEC 9506 – Part 1 and Part 2) and ISO/IEC 8802-3
9	Specific Communication Service Mapping (SCSM)
9.1	- Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link
9.2	- Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

In Fig. 2-8, the relationship between them is made clear. A brief introduction to the ideas, principles, concepts, and terminology of the standard is provided in Parts 1 and 2. The mapping of abstract data classes and services to communication protocols is the main focus of parts 8 and 9, which also provide specifications for serial unidirectional communication and the transfer of sample values [74,75,75]. The client-server communication and engineering tools conformance testing are covered in Part 10 [77]. The next subsections will provide explanations for the other portions, which are more pertinent to electrical engineers.

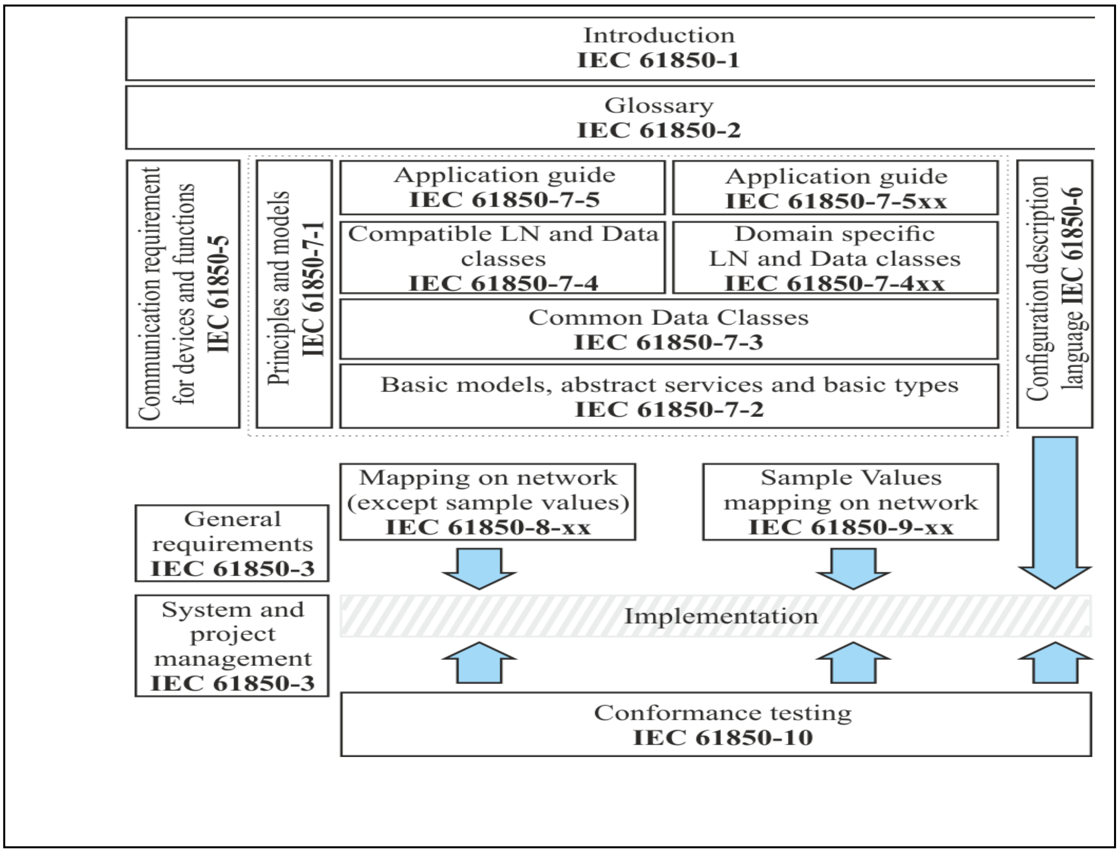

Introduction
IEC 61850-1
Glossary
IEC 61850-2
Communication requirement for devices and functions IEC 61850-5
Principles and models IEC 61850-7-1
Application guide
IEC 61850-7-5
Application guide
IEC 61850-7-5xx
Compatible LN and Data classes
IEC 61850-7-4
Domain specific LN and Data classes
IEC 61850-7-4xx
Common Data Classes
IEC 61850-7-3
Basic models, abstract services and basic types
IEC 61850-7-2
Configuration description language IEC 61850-6
Mapping on network (except sample values)
IEC 61850-8-xx
Sample Values mapping on network
IEC 61850-9-xx
General requirements
IEC 61850-3
System and project management
IEC 61850-3
Implementation
Conformance testing
IEC 61850-10

Figure 2-8. General structure of IEC 61850[77]

A. Part 3: General Requirements

This part focuses on the construction, design, and environmental conditions of intelligent electronic devices (IEDs) [78].

B. Part 4: System and Project Management

The framework for project management of utility automation systems (UAS), including substation automation systems (SAS), is described in this section of the standard [79]. The following elements are often present in the environment where the UAS works (see Fig. 2-9):

1) Telecommunication environment: network control centers, subordinate systems, teleportation;
2) Human as local operator;
3) Process environment: switchgear, power transformers, and auxiliary equipment.

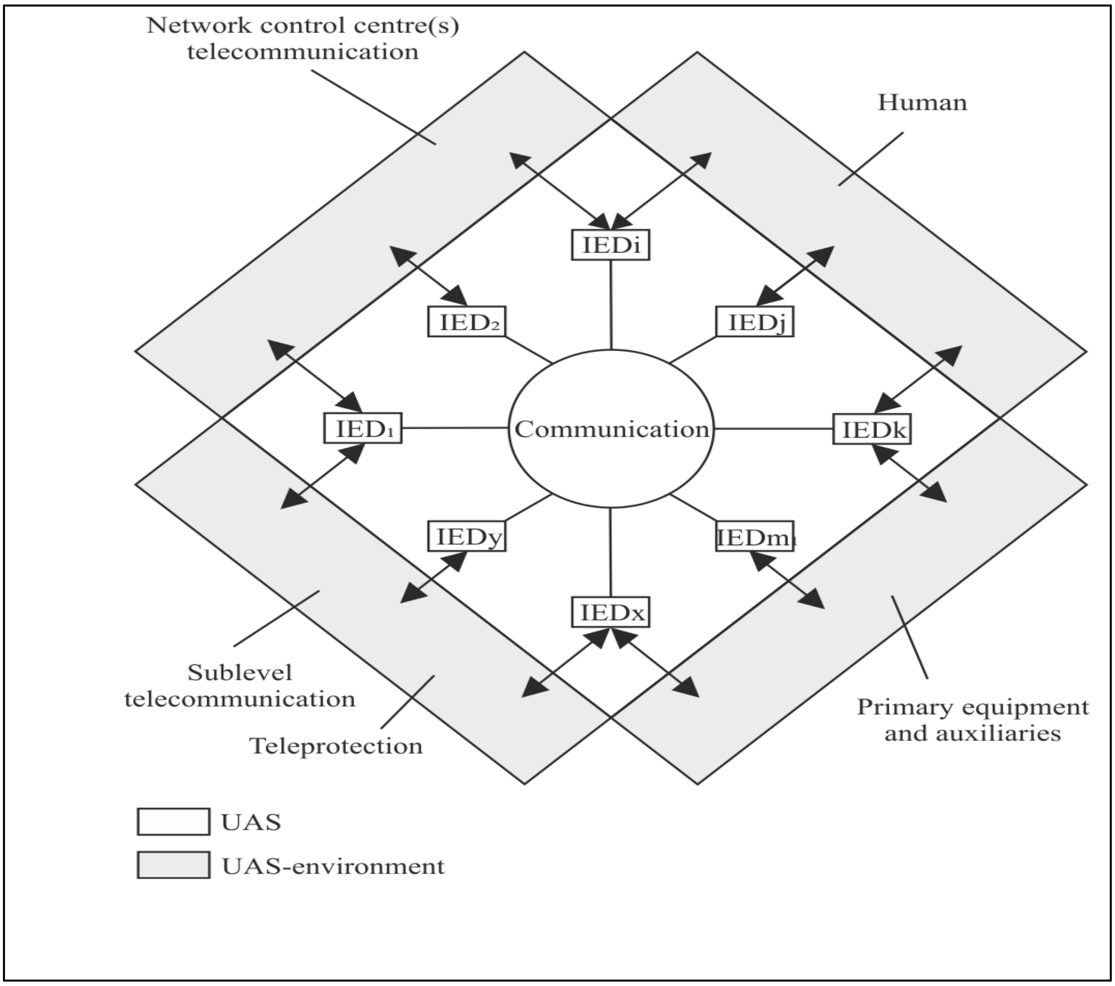

Network control centre(s) telecommunication
Human
IEDi
IED₂
IEDj
IED₁
Communication
IEDk
IEDy
IEDm
IEDx
Sublevel telecommunication
Teleprotection
Primary equipment and auxiliaries
UAS
UAS-environment

Figure 2-9. The Environment of the utility automation system[79]

In terms of UAS, the "process" is used to denote the process of generation, transmission, and distribution of electrical energy [79].

IEDs are the main components of the UAS and could be:

1) For the telecommunication environment: gateways, converters, telecommunication part of RTUs,tele-protection;
2) For human-machine interface (HMI): gateways; personal computers; workstations, other IEDs with embedded HMI;
3) For the process environment: bay control units, relay protection, the process part of RTUs, measurement devices, autonomous controllers, sensors, numerical interfaces of switchgear, power, and instrument transformers.

The engineering process defines the specifications for the design and configuration of a particular power plant or substation based on the operation logic and the needs of the client. The following engineers are jointly responsible[79]:

1. The engineer responsible for the project requirements;
2. The engineer responsible for the system architecture, based on the project requirements;
3. Equipment vendors;
4. System integrators – engineers who ensure the interoperability of the different UAS components and the process environment;
5. IEDs parametrization engineer;
6. Commissioning engineer.

C. Part 5: Communication Requirements for Functions and Device Models

The SAS is the main topic of the fifth section [80]. It harmonizes conditions that must be satisfied and IED-to-IED communication. The IEDs should be able to carry out at least one or more of the SAS's functions, which are divided into categories including protection, control, measurement, etc. The various tasks are standardized. The functions may be divided into distinct parts that carry out particular tasks and may be used by different functions. Logical Nodes are these components (LN). The pieces of information that need to be shared (PICOM) across the various functions and IDEs are contained in the LNs[80].

Fig. 2-10 shows the relationship between LNs, physical objects (PD), and functions (F). Logical connections (LC) connect the LN to the physical devices, whereas physical connections connect the LN to the LN (PC). The image demonstrates how many LNs from a single PD can be included in a single function [80].

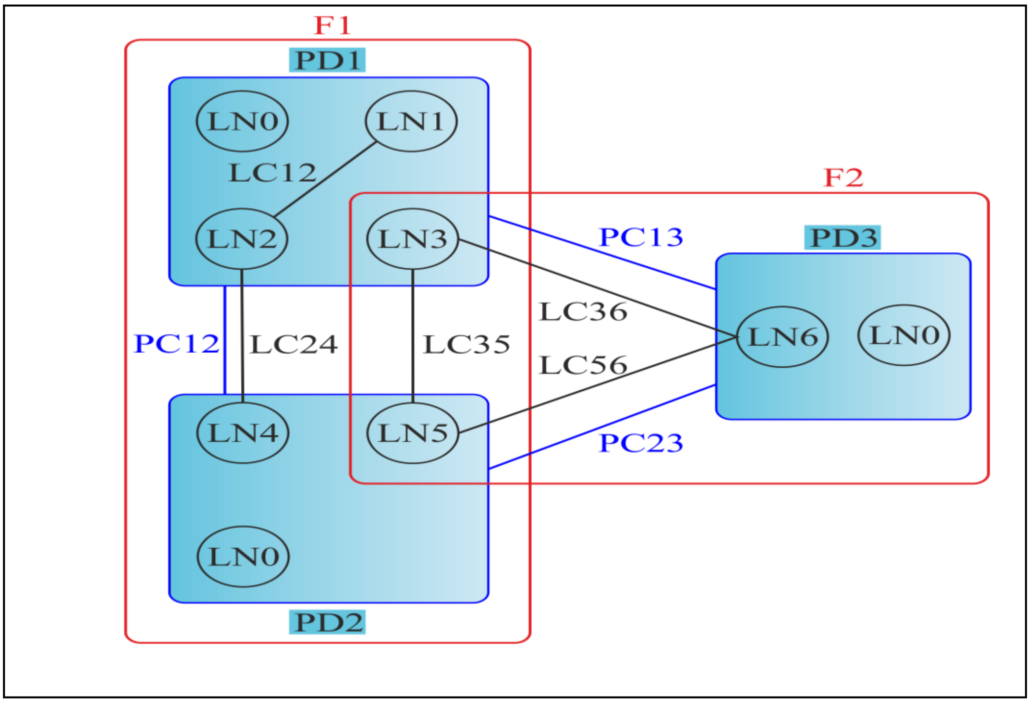


Figure 2-10. The Logical nodes, functions and physical devices

The three tiers into which the functions are divided are called "Station," "Bay/Unit," and "Process" (see Fig. 2-11). The process functions act as an interface to the process itself, including the gathering of sampled data, monitoring and controlling switchgear position, and others. Key pieces of equipment in the bay are primarily impacted by the protection and control features at the bay/unit level. There are two types of station-level tasks: [80]: (i) functions related to the process, which uses information from more than one bay and can act upon all of them; (ii) functions providing an interface to the station operator or a remote control center[80].

Figure 2-11 illustrates the various interfaces between the levels. The numbers enclosed in a circle stand for the following: (1, 2) protection data; (4) analog data; (5, 6) control data; (7) data exchange between substation level and remote engineer's workplace; (3, 7, 8, 9) data exchange; and (10, 11) control data exchange. Interfaces 2 and 11 are exempt from IEC 61850.

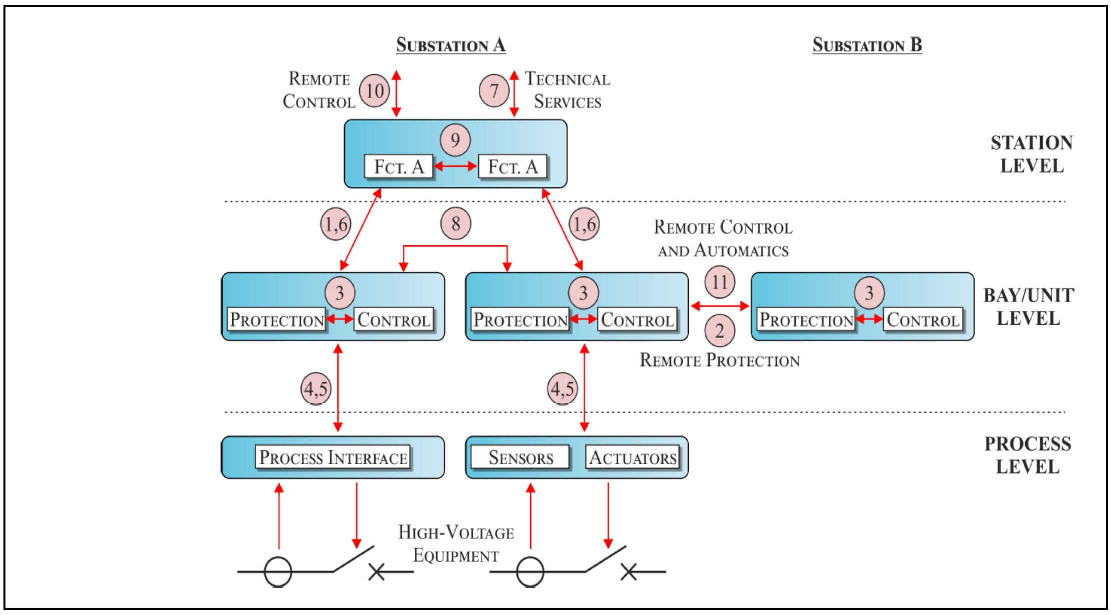


Figure 2-11. The topology of substation automation system[81]

D. Part 6: Configuration Description Language for Communication in Electrical Substations Related to IEDs

System Configuration description Language (SCL) is an object-oriented, XML-based language that is defined in this section of the standard [81]. The description of the main electrical circuit equipment and its connections usually comes first in a configuration file.

The LN, its functions, and its interrelationships are then specified. Every IEC 61850 compatible device should be able to be configured using an SCL code since the SCL code also contains the settings of each unique IED. IED capability description (ICD), instantiated IED description (IID), system specification description (SSD), system configuration description (SCD), configured IED description (CID), and system exchange description are among the file types listed (SED). The functionality of the software tools required for system specification and configuration is described in detail in Clause 10 of this Part [81].

E. Part 7: Basic communication structure

The split of data definition and process specification into data objects and protocol-independent process definitions is the primary structural element of IEC 61850 [82–

87]. As a result, the precise definitions enable the structure of the data objects and processes in line with any protocol that can satisfy their requirements.

Part 7-1 defines the modeling methods, the communication principles, and the information models which are used in the next subparts[82-87].

Part 7-2 standardizes an abstract communication service interface between the client and remote server or between the publishing device and subscribed devices (for sampled values transmission)[82-87].

Part 7-3 defines common data classes used to describe equipment models and functions for substations [82-87].

Part 7-4 introduces compatible LNs for the substation hardware and data classes, which improves the models. It provides comprehensive details for the LNs' commonly used alphabetical designation (relay protection equipment, registering devices, regulators, tap changers, instrument transformers). The guidelines for applying LNs and the information that goes along with them have also been improved. The LNs are organized into groups based on the related functions. Each member of the group has a name that begins with a different letter, such as (A) for automatic control, (C) for supervisory control, (P) for protection, (X) for switchgear, and (M) for metering and measuring, among others [82-87].

2.4.2 Power System Model and State Estimation Process

The master's program known as the energy management system (EMS) is at the core of the power system. EMS is a high-performance critical application that oversees all of the electric grid monitoring control and optimization activities it receives redundant readings from numerous PMUs and SCADA devices field instrument transformers are being sampled for current, voltage, and power flow. When compared to standard SCADA devices the PMUs sample at a rate of 30/60/120/240 messages per second with a substantially higher degree of accuracy and are thus widely used by utilities to improve real-time monitoring [88, 89]. A local phasor data concentrator (PDC) at the substation level receives data packets from PMUs and synchronizes and aligns them. Before sending a report to a data concentrator at the main control center, regional PDCs collect and assemble data from station-level PDCs. Figure 2-12 displays the architecture of the PMU-PDC.

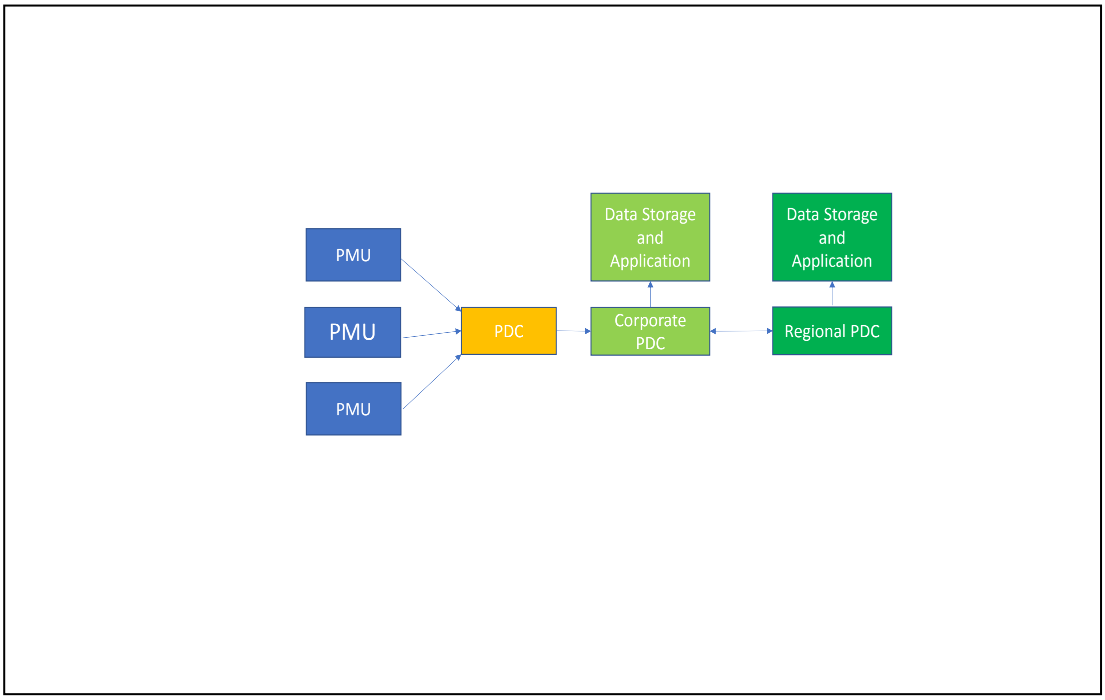


Figure 2-12. The PMU-PDC architecture

2.4.2.1 DC State Estimation

The linear DC state estimate using only traditional SCADA meters is built on the following linear measurement function [90].

$$z = \; Hx + e \tag{1}$$

where e is a m x 1 vector of random Gaussian errors, z is a m x 1 vector of measurements, H is the m x n Jacobian matrix, x is then a n x 1 vector of state variables, and m,n is the total number of measurements and states, respectively. The following presumptions are true for DC state estimation: (1) the voltage magnitudes at all buses in the network are assumed to be constant and equal to 1 per unit (p.u.); (2) the shunt susceptances and series resistances of transmission lines are neglected; (3) the bus angle differences between two buses are thought to be very small; (4) reactive power is entirely neglected, and (5) state variables only consist of bus voltage angles.

The measurement residual arising from the difference between measured and estimated states is defined as,

$$r = \; z - Hx \tag{2}$$

The state variables can be estimated by minimizing the objective function J,

$$J(x) = (z - Hx)^T R^{-1}(z - Hx) \tag{3}$$

Straightforwardly for DC state estimation, the states are estimated as,

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \tag{4}$$

2.4.2.2 AC State Estimation

The oversimplified DC state estimation model might not be suitable for real-time power system state estimation since measurements in power systems are related to their states by a non-linear function. The link between the state variables and the states can be stated as [23] for AC state estimation.

$$z = h(x) + e \tag{5}$$

where z is an m x 1 vector of measurements from SCADA meters and PMUs, h is a set of non-linear power flow functions relating measurements to state variables, x is an n x 1 vector of state variables, e is an m x 1 vector of random Gaussian errors, and m, n is a total number of measurements and states respectively [23].

The non-linear functions h(x) which relate the measurement to the state variables comprise active and reactive power injections at the bus, active and reactive power flow in transmission lines, and branch real and imaginary currents. The real and reactive power injection at bus m is,

$$\mathrm{P}_m = V_m \sum_n V_n \ (\mathrm{g}_{mn} \cos \delta_{mn} + \ \mathrm{B}_{mn} \sin \delta_{mn}) \tag{6}$$

$$\mathrm{Q}_m = V_m \sum_n V_n \ (\mathrm{g}_{mn} \sin \delta_{mn} - \ \mathrm{B}_{mn} \cos \delta_{mn}) \tag{7}$$

The real and reactive power flow from bus m to bus n is,

$$\mathrm{P}_{mn} = V^2{}_m \, \mathrm{g}_{mn} - V_m V_n \, [\, g_{mn} \cos(\delta_m - \delta_n \,) + \mathrm{b}_{mn} \sin(\delta_m - \delta_n)] \tag{8}$$

$$\mathrm{Q}_{mn} = -V^2{}_m \, \mathrm{b}_{mn} - V_m V_n \, [\, g_{mn} \sin(\delta_m - \delta_n \,) - \mathrm{b}_{mn} \cos(\delta_m - \delta_n)] \tag{9}$$

The real and imaginary branch current between bus m and bus n is,

$$\mathrm{I}_{mn}\text{,real} = V_m \left[\, \mathrm{g}_{mn} \cos \delta_m - \mathrm{b}_{ij} \sin \delta_m \right] - \ V_n \left[\, \mathrm{g}_{mn} \cos \delta_n - \mathrm{b}_{ij} \sin \delta_n \right] \tag{10}$$

$$\mathrm{I}_{mn}, \quad \text{imag} \quad = \quad V_m \left[\, \mathrm{b}_{mn} \cos \delta_m + \mathrm{g}_{ij} \sin \delta_m \right] - \ V_n \left[\, \mathrm{b}_{mn} \cos \delta_n - \mathrm{g}_{ij} \sin \delta_n \right] \tag{11}$$

The weighted least squares method is used to minimize the measurement residuals to accurately estimate the states with the objective function defined as [91],

$$J(x) = (z - h(x))^T R^{-1}(z - h(x)) \tag{12}$$

where R is the measurement error covariance matrix. The estimates of the state are found by an iterative process like the Newton-Raphson method,

$$\Delta\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1}(z - h(x)) \tag{13}$$

$$\hat{x}_i + 1 = \hat{x}_i + \Delta\hat{x}_i \tag{14}$$

where H is the measurement Jacobian matrix and is defined as H = $\frac{\partial h(x)}{\partial x}$,

In matrix H, the first and the sixth columns are related to bus voltage magnitude and angle-system states which are directly measured by the PMUs, and hence have an identity relation with the estimated states.

2.4.2.3 Bad Data Detection

Bad PMU and SCADA data can naturally occur as the result of instrumentation errors, thermal degradation of equipment, or random electrical noise. One of the most popular techniques for detecting erroneous measurements is comparing the L2 (norm) of the measurement residuals to a detection threshold τ. For DC state estimation, no bad data is detected when,

$$\|z - H\hat{x}\| < \tau \tag{15}$$

Similarly, for AC state estimation, no bad data is detected when,

$$\|z - h(\hat{x})\| < \tau \tag{16}$$

In general, the threshold τ is determined and obtained from the cumulative chi-square distribution for m - n degrees of freedom [23]. Residuals that satisfy (15) and (16) are assumed to be free of bad data while those that fail to satisfy this condition are excluded from the data set for subsequent calculations. The discarded bad data is often substituted by pseudo-measurements obtained from historical values to ensure that SE converges.

2.5 Smart Grid Cyber Security

2.5.1 The NIST Framework

A smart grid network's vulnerability is the opening via which an attacker could break in and assault the system. The smart grid uses several protocols to interface with various domains, making it susceptible to countless threats. In this section, we look at the circumstances that can make the grid more susceptible to cyberattacks. But first, let's talk about the many kinds of cyberattacks. Attacks can be divided into two categories: passive attacks and aggressive attacks. Active attacks are more harmful than passive attacks because the attacker modifies the data or prevents the receiver from getting it, whereas passive attacks cause no damage to the data and just monitor it [92].

According to the National Institute of Standards and Technology (NIST) [21], the following are the main reasons why the smart grid is vulnerable to cyberattacks:

1. More intelligent electronic devices (IEDs) are being installed: As the number of devices in a network climbs, so do the potential attack points for attackers. The entire network system would be affected even if the security of only one point were to be compromised [21].

2. Installation of third-party components: Installing unrecommended third-party components makes the network more susceptible to hackers. These devices might be infected with Trojans, which spread to other networked devices[21].

3. Insufficient staff training: To use any technology, proper training is required. Staff members could easily fall prey to phishing attempts[21] attacks if they are not properly trained.

4. Using Internet protocols: When it comes to data transmission, not all methods are secure. Unencrypted data is transferred using some protocols. They are therefore prime targets for data extraction using man-in-the-middle attacks.

5. Maintenance: Although the basic objective of maintenance is to maintain things operating smoothly, it occasionally turns into a vector for cyberattacks. Operators frequently disable the security system while performing maintenance so that testing can be done. Eastern European electric power companies reported one comparable incident in 2015 [21], [93].

The following lists the top five objectives for cybersecurity in smart grids. Table 2-5 summarizes the types of attacks and the security objectives they violate.

1. Authentication: The user's identification. The system checks to see if the user-provided credentials are accurate. [94] presents various authentication methods used in the smart grid network.

2. Authorization: When the user enters the correct credentials, he is authorized. The user is now able to access the services and send and receive data packets. In an unencrypted authentication procedure, the attacker can see the credentials that users have entered, and he or she can then use those credentials to appear to be an authorized user.

3. Confidentiality: This guarantees that the data is accessible only to those who are allowed. Sensitive data is widely dispersed throughout the smart grid network. Statistics on client energy use, a customer identification number, and a list of the appliances in use by clients are included in this data. This data can be used by an attacker to look into the customer's energy usage habits. Additionally, an ICMP (Internet Control Message Protocol) flood attack might be initiated and the reading may be tampered with or changed [95] if unauthorized people had access to the data. As a result, utilities can experience serious financial problems or customers might receive exorbitant bills.

4. Integrity: By guaranteeing that the data is not altered or distorted during transmission, this safeguards the recipient from data manipulation. At the receiving end, numerous similar procedures, such as parity check and checksum error, are used to ensure that the data has not been altered. One of the most widely used attack types is the false data injection attack (FDIA). Genuine data is tampered with using an injection attack[96].

5. Availability: Availability guarantees that resources or data are always available whenever the user needs them. The availability may be impacted by several things, including a malfunction in the data center, but in terms of cybersecurity, it is impacted by cyberattacks such as denial of service (DoS) attacks. The attackers commandeer the resources during a DoS assault, making it unable to fulfill user requests[96].

Table 2-5. Summary of the attack category and security goal

Attack Category	Security Goal Compromised	Description	Reference
Flooding attack	Availability	Deterring users from utilizing the resources	[96,97]
Denial of service	Availability	Stop serving users' request	[98-101]
Jamming	Availability	Jamming the network	[102-103]
Buffer overflow,	Availability, Confidentiality	Overwriting the memory of the buffer	[104]
False Data Injection	Integrity	Tampering the real data	[105-108]
Social Engineering Attack	Integrity, Confidentiality	Attacking humans instead of machines or networks	[109-111]

Man-in-the-middle	Confidentiality	Extracting packet information between sender and receiver	[112]
Packet Sniffing	Confidentiality	Analyzing the packet	[113]
Session hijacking attack	Integrity, Confidentiality	Obstructing the user from resources for a particular amount of time	[114]
Data manipulation	Integrity	Data tampering	[115]
Replay Attack	Integrity	Send data, again and again.	[116,117]

2.5.2 Cybersecurity Standards and the Enhanced Cyberphysical Frameworks

An enterprise can implement a cybersecurity risk assessment for the smart grid using one of the various high-level risk assessment frameworks available. These risk assessment techniques are helpful, but they do not offer clear guidance for the unique characteristics of the smart grid. Cyberattacks, for instance, can physically affect the quality of the energy supply or harm electrical equipment in the smart grid. Additionally, attacks may result in safety-related events that cause harm or fatalities. It would be beneficial in this situation to offer detailed instructions on how to evaluate these factors.

2.5.2.1 IEC 62443 (ISA 99*)*

Represents a set of security standards for industrial automation and control systems (IACS) prepared by the IEC technical committee. The goal of these standards is to provide a flexible framework that can address vulnerabilities in IACS and apply required mitigations systematically. The concrete standard that was analyzed is IEC 62443-3-3:2013 System security requirements and security levels [118] which defines the security requirements for control systems related to the seven requirements defined in IEC 62443-1-1 and assigns system security levels to the system constructed. The IEC 62443-3-3:2013 was selected since it represents the system-level standard that can add diversity to the analysis[119].

2.5.2.2 ISO/IEC 27001 and 27002—ISO 27001

Is one of the most well-known and widely accepted IT security standards. ISO/IEC 27001:2013, Information technology—Security methods—Information security management systems—Requirements [120], is the formal name of the standard. In addition to being included in Annex A of ISO 27001, its companion standard, ISO 27002 [121], focuses on the information security measures that businesses may decide to employ. Although adherence to the ISO 27001 standard alone wouldn't be sufficient to secure the ICS ecosystem, it was chosen as a general-purpose security standard since it has standards that may be used in a variety of industries.

2.5.2.3 NIST SP 800-53

Represents the guideline that is published by NIST with the official title: Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems and Organizations (Revision 5). It is intended to be used as a toolbox containing a collection of safeguards, countermeasures, techniques, and processes to respond to security and privacy risks [122]. This guideline is versatile enough to be applied to IT systems as well as ICS systems and even if originally aimed at systems that reside in the US, it is well recognized and applied worldwide. This publication is selected as a guideline representative.

2.5.2.4 NERC CIP

Defines the set of rules that specify how bulk electric systems (BES) can protect themselves from physical and digital threats that might compromise the system's dependability. Critical asset definition, monitoring, configuration changes, and access control all require the use of policies. The Federal Energy Regulatory Commission (FERC) in the US and Canadian government agencies are in charge of monitoring NERC [123]. The NERC CIP standards must be followed by all owners, operators, and consumers of bulk power systems in North America. The publication with the most occurrences throughout the literature review and one of the most reputable representations of the regulatory kind of papers was NERC CIP.

2.5.2.5 Proposed Stochastic Vulnerability Assessment Framework

The combination of sophisticated computer networks with electricity infrastructure significantly increases the surface area vulnerable to cyberattacks, necessitating major improvements in cyber security capabilities. To guarantee that security-based decisions accurately represent a realistic awareness of cyber risk, robust security metrics are required. In response to this need, NIST [122] encourages research into tools and methodologies that offer quantitative notions of risks, i.e., threats, vulnerabilities, and attack outcomes for existing and developing power grid systems.

The main goal of the framework was to depict all possible attack paths in the digital control network (smart grid architectures), evaluate the security level of the smart grid through security metrics, and assess the effectiveness of defense strategies. The proposed framework is shown in Figure 2-13 and can be deployed in layer 3.5 of the Purdue architecture. There are five steps in the framework: i) preprocessing, ii) security model generation, iii) visualization and storage, iv) security analysis, and v) changes and updates. We explain each step as follows:

In step 1, the security decision-maker provides inputs needed to construct a smart network. The inputs required are the total number of nodes, the network topology, and the vulnerability information for each node. The inputs are fed into the SG Generator. The smart grid Generator creates a smart grid network with a specified network topology consisting of levels and nodes with their vulnerability information. The network topology is fixed after the generation. The security decision-maker also selects the security metrics from a pre-defined metric pool which will be used as input into the security analysis phase.

In step 2, the security model generation is performed. Our security model is developed based on the Purdue model in which five layers are used to represent the network reachability information at the uppermost level and the vulnerability information at the lower level, respectively. Specifically, the Security Model Generator takes the constructed network with topology and vulnerability information as inputs and automatically computes all possible attack paths in the SG network.

In step 3, the attack paths generated from the Security Model Generator are visualized in the form of a reachability/coverability graph, depicting the transient and absorbing states.

In step 4, the security analysis is carried out for the SG network. The attack vectors are taken as the input into the Security Evaluator along with the determined security metrics. Based on the metrics, the Security Analysts can perform one of the two options. One is to output the analysis results directly and the other is to generate a text file and import the file into the analytic modeling and evaluation tool named Platform Independent Petri net Editor (PIPE) [124] which computes the security analysis results. The security metric is selected from a pre-defined metric database.

In step 5, any changes caused by the defense strategies are captured to update model inputs. Based on the security analysis results, the security decision-maker knows which part of the SG is the most vulnerable, thus being able to decide on proper defense strategies. The deployment of the defense strategy changes either the vulnerability information (e.g., eliminates a specific vulnerability in a smart grid node or mitigates the effect caused by the vulnerability) or the topology information, which should be updated and taken as the input to the Security Model Generator. When choosing the defense strategies, the security decision-maker can also assess the effectiveness of different strategies via the framework by using security metrics, comparing their effects, and choosing the best one among them.

Analysis

In this part, we described the dependability analysis method that we used to evaluate industrial control systems using the proposed SPN model. We developed three reliability standards and provided a comprehensive algorithm for calculating them. Additionally, we discuss the issue of state-space growth in computing.

Metrics

Metrics are crucial in helping to guide decision-making. Therefore, in this section, we examined the three dependability factors of reliability, availability, and maintainability for digital control networks in smart grids.

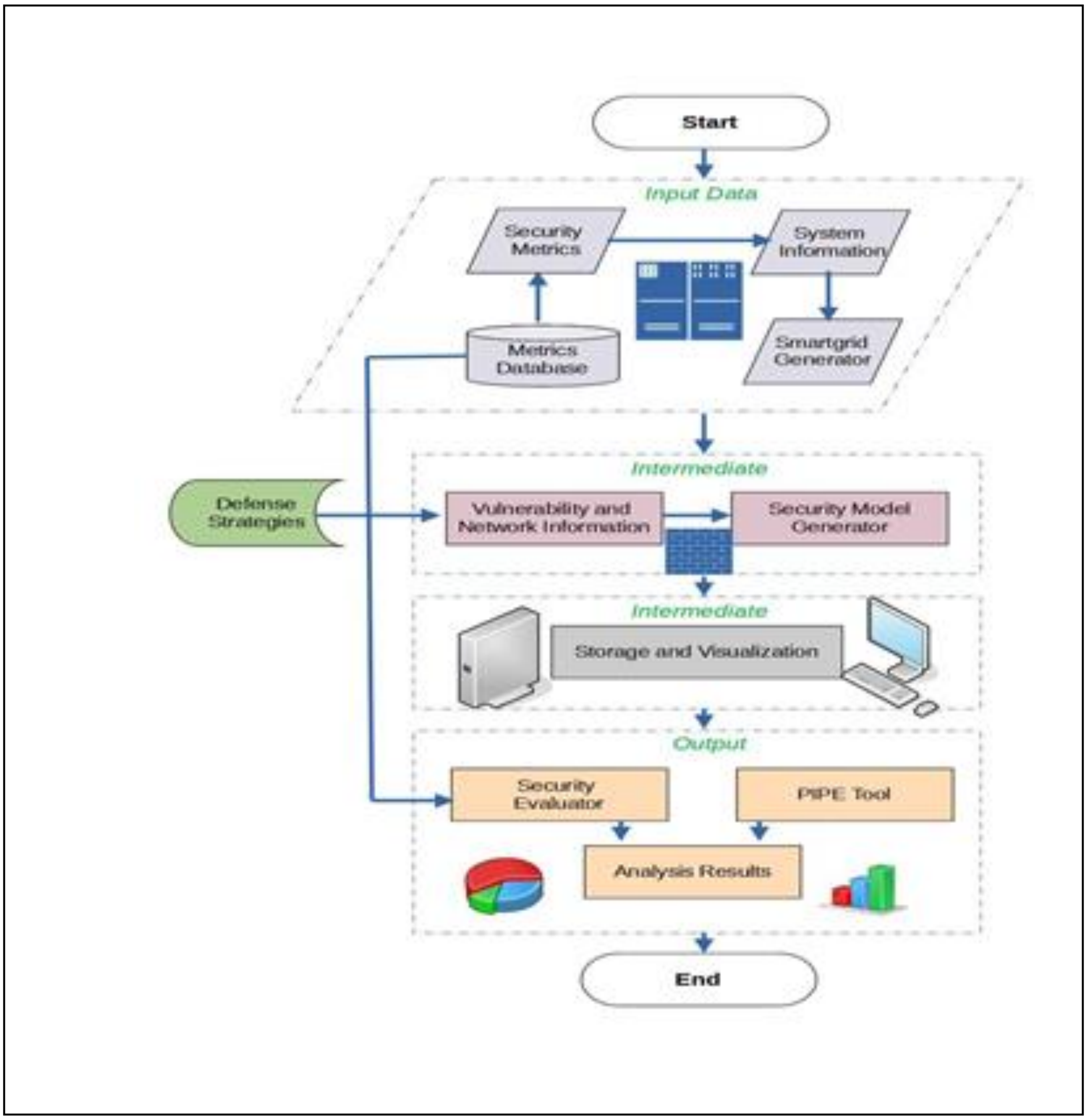


Figure 2-13. The proposed framework

2.6 Evaluating the State of the Industrial Control Systems

2.6.1 Industrial Control Systems (ICS) Cyber Security: Critical and Exposed

According to TXOne [125], cyber attackers' techniques shifted dramatically in 2021, with more advanced and devastating supply chain attacks than ever before. These new cybercrime developments have created a climate of dread, which is pushing cyber defense research and the discovery of ICS-related Common Vulnerabilities and Exposures (CVEs). Current cybercriminal operations have progressed to the point that a service industry has evolved with a similar business model – ransomware-as-a-Service, according to a timeline of the year's major OT and ICS cyber events (RaaS). Users who want to carry out illicit projects might use a customized platform provided by RaaS service providers. They market their services using a variety of payment schemes, including affiliate programs that provide special offers - for example, if the provider generally takes 25% of the ransom, they might agree to take a reduced amount if the client requests a much greater ransom. RaaS organizations have increased ransom demands in this fashion.

Maze, Lockbit, REvil, and DarkSide are known recently active ransomware gangs, however, their activity levels can fluctuate. For example, the Maze ransomware gang announced its retirement in November 2020 [126]. REvil and DarkSide landed on the wrong side of the US government in the middle of 2021 when their service was used to launch two of the year's most severe ransomware assaults, the Colonial Pipeline cyber disaster, and the Kaseya supply chain attack.

DarkSide's RaaS platform [127] was used in the Colonial Pipeline attack [128], which resulted in a $4.4 million payoff to attackers. REvil's service was used to launch the Kaseya supply chain assault, which exploited CVE-2021-30116 [129], a "zero-day authentication bypass" vulnerability. The REvil organization claimed to have infected over a million machines when they demanded a $70 million ransom [130]. Following these two attacks, both DarkSide and REvil went silent, with REvil reappearing in October as a result of increasing government and law enforcement attention. However, further RaaS development, including new RaaS platforms that incorporate capabilities from prior systems, is possible. The Darkside, REvil, and LockBit 2.0 ransomware families, for example, use tools and strategies from the BlackMatter ransomware [131]. Our investigators suspect, but cannot confirm, that BlackMatter is the DarkSide rebranding. Emotet and Conti resurfaced in December 2021, this time with a stronger exploit of the Log4Shell vulnerability to achieve their objectives.

According to Trend Micro, supply chain attacks will continue to be a major trend in 2022, with attackers employing "quadruple extortion," in which they "hold the victim's critical data for ransom, threaten to leak the data and publicize the breach, threaten to go after the victim's customers, and attack the victim's supply chain or vendors" [132].

2.6.2 Case Studies of Known Incidents in ICS

In this section, some of the risks associated with the cyber-security aspects of the current industrial manufacturing industry will be put into perspective. These risks are unique in the sense that although the OT platforms typically utilized in the industry are widely familiar, they pose certain cyber-security risks that are different from those encountered in an IT environment. Consequently, these risks have not been considered as such until recently. First, a few case studies of historic cyber-physical attacks were briefly introduced to put into perspective the true nature of such attacks on industrial control systems networks. A comprehensive study into the details of how these attacks work is given in the following chapters, some key aspects in terms of the associated security vulnerabilities can still be identified to formulate more clearly defined cyber-physical security problem statements. Putting these security aspects into perspective, they can be contextualized to identify and formulate solutions to the problems.

2.6.2.1 Colonial Pipeline: The DarkSide Colonial Pipeline Strikes

The Colonial Pipeline Company [125] reported on May 8, 2021, that a ransomware attack had caused it to cease running its pipelines, halting the East Coast's vital supply of gasoline and other refined products. This incident resembled a pipeline ransomware assault in 2020 that similarly caused the pipeline to be shut down [125].

According to the investigation [125], hackers used a password for a VPN account that had been made public to access the Colonial Pipeline network. To provide safe, encrypted remote access to their corporate network, many firms use virtual private networks (VPNs). According to the report[125], a Colonial Pipeline employee who was not publicly named during the hearing allegedly used the identical VPN password at another site.

2.6.2.2 Destructive Industrial Control System Malware Targeted at Saudi Arabia Energy Infrastructure in 2017

In December 2017, FireEye revealed [133] that it had dealt with an industrial operator whose facility had been targeted by a new type of ICS malware known as TRITON (also known as TRISIS or Hatman by other groups) [134]. The hack reprogrammed the facility's SIS controllers, causing them to reach a failed condition and forcing the industrial process to shut down automatically. The hacking effort was discovered during the inquiry that followed the shutdown.

The SIS that was attacked was a Triconex Safety Instrumented System from Schneider Electric, and the target location was later identified as a Saudi Arabian petrochemical manufacturing complex [134]. This form of SIS is frequently used and is commissioned in a consistent manner across numerous sectors [134].

TRITON is one of just a few malware strains capable of interrupting the physical processes of an industrial control system. The attack began with a network breach that was carried out using well-documented and easily detectable attack methods. To get access to the OT (Operational Technology) network, the attackers employed systems that were available in both environments [135].

After gaining access to the OT network, the threat actors were able to infect the SIS system's engineering workstation, which was typically placed in a separate network segment. The infection was most likely spread via social engineering, with the engineer obtaining or downloading a program with a genuine file name, such as "trilog.exe." The dropper file (TRIconex LOGging filename) [135] is a basic program that interacts with Triconex and its logging capabilities, as the name implies.

The main goal of the dropper file was to deliver the malicious script to the target, in this case, the SIS controller. Shortly after the execution, the dropper attached to the targeted Triconex and injected the legitimate malware code into its memory [135].

The malware payload was stored in two binary files called inject.bin and imain.bin. Reading, injecting, and executing these files into the Tri-memory conex's were among the dropper's actions [135].

1) inject.bin contained code that exploited a specific zero-day vulnerability to execute the contents of the file "imain.bin."

2) imain.bin contained the final code that allows a remote user to entirely operate the SIS device.

The dropper, which was written in Python, was compiled using the trilog.exe application. It comprises a reverse-engineered version of the TriStation protocol, which is used to communicate with the targeted device [135].

2.6.2.3 Attack on the Ukraine Distribution System Operator in 2015

The electric power sector was forced to take a more aggressive approach to cybersecurity following the 2015 attack on the Ukrainian power grid, affecting 27 substations and approximately 225,000 end customers. The target was the Ukrainian electricity distribution company Kyivoblenergo. The attack can be classified as an advanced persistent threat (APT) and resulted in a disruption of service and blackout [136].

The attackers used targeted emails carrying weaponized visual basic for application (VBA) Microsoft Word and Excel attachments. Opening the files by employees installed a specific remote access tool (RAT) / malware, BlackEnergy3, on the workstations [136].

From there the attackers got access privileges for at least 6 months until they fully deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations. Finally, they were able to open a series of breakers of multiple substations, triggering the blackout. Seven 110 kV and twenty-three 35 kV substations were disconnected. This incident received global attention and helped spread public awareness of the vulnerabilities of electric power systems. A subsequent attack in December 2016 further exasperated industry concerns, with the country’s power grid quickly becoming a testbed of sorts for cyberattacks [136].

2.6.2.4 Self-inflicted Information Overload of the Austrian Control center due to Cross-Border Miscommunication in 2013

A single counter-value inquiry from the Bavarian gas system caused an overload or temporary non-availability of the Austrian control center's critical operations in 2013, due to a misconfiguration in the Austrian electrical transmission grid operator's control system. The incident was caused by a misinterpretation of a data signal at the intersection of two domains in two different energy sectors, which resulted in the temporary non-availability of critical system functions [136].

More specifically, a status request command packet, which was broadcast from a German gas company as a test for their newly installed network branch, found its way into the systems of the Austrian energy power control and monitoring network. Due to misinterpretation, the data message from the gas system generated thousands of reply messages in the power system, which generated even more data packages, which in turn flooded the control network. To stop this self-inflicted Distributed-Denial-of-Service (DDoS) ‘attack’, part of the monitoring and control network had to be isolated and disconnected. Fortunately, the situation was resolved without any power outages [136].

2.6.2.5 Shamoon (Saudi Aramco and RasGas)

On August 15, 2012, harmful spyware infiltrated Saudi Aramco's computer systems, making it the world's largest energy business. The attackers meticulously chose the one day of the year when they knew they could do the greatest damage: the day that more than 55,000 Saudi Aramco employees remained home from work to prepare for Lailat al Qadr, or the Night of Power, which commemorates the revelation of the Quran to Muhammad [137].

When the Shamoon spyware was turned on, an image of a burning American flag was rewritten in the files of more than 30,000 PCs. Shamoon was malware that included a destructive component as well as the ability to steal information. Shamoon renders infected systems worthless by overwriting the Master Boot Record (MBR), the partition tables, and the majority of the files with random data. It is impossible to restore information that has been overwritten [137].

Symantec described the malware on their social media blog on August 16, 2012 [138]. On August 27, 2012, the Shamoon malware hit its second target, the Qatari natural gas company RasGas, which is one of the world's largest liquefied natural gas (LNG) firms [137].

There was no evidence that Shamoon had any direct impact on ICS or SCADA systems at either Saudi Aramco or RasGas. Once a system is infected with the Shamoon malware, it attempts to spread itself to other devices on the local network. C2 communications are used to control the operation of the attack but are not necessary if the threat actor has programmed a time for disk destruction before delivering the malware [137].

To spread the infection or download more tools on the victim's device for network traversal, Shamoon provides the ability to download and execute arbitrary executables from the C2 server [137].

2.6.3 Selection of Cyber Threats in the Industrial Control Systems

The danger landscape for utilities has grown to include a wider range of threats from a wider range of players. Infrastructure providers have been increasingly targeted by nation-state actors and other smart players as part of bigger campaigns. Furthermore, fraudsters profit from utilities and other vital infrastructure players. This section examines some recent criminal operations that have targeted ICS. Because the target of such attacks is no longer limited to IT networks [2-3], a paradigm shift in the content eminent risks that cyberattack pose to ICS systems is required. Table 2-6 gives a summary of the threats to energy systems.

Table 2-6. Threats in the energy system

SN	Title	Description	System Impacted
1	Infection through intrusion detection system (IDS)	To infect the general ICT protection systems of power system equipment enables the attacker to get access rights for all crucial elements and subsystems of the infected system, e. g. substation or generation unit. A threat agent exploits the security vulnerability in out-facing interfaces of a protection measure	ICT System

		(e.g. firewall or IDS) to gain access to the internal network. Access then is extended laterally throughout the distribution or transmission grid operators' enterprise network. This scenario is an instance of a general type of scenario where the (often necessarily) higher access rights of protection software and devices make them an interesting entry vector to compromise the control system of the system operator	
2	Virus/Trojan infiltrates industrial control system	In this scenario, the attacker infiltrates the equipment using a virus, worm, or trojan. An existing virus,	IT/OT System

		worm, or trojan that isn't built for industrial control systems (ICS) infects the system, disrupting or threatening to disrupt the process and seize control of the targeted equipment.	
3	Social engineering: phishing employees on enterprise-level propagates to field-level manipulation or introducing a remote access tool kit to the human-machine interface	In this indirect attack, the attacker first infiltrates the general office ICT-System of the network operator or manufacturer and secondly gets access to the control systems of the attacked organization. This attack does not address individual power system equipment but allows access to all control systems of the organization. Remote Access Toolkits (RAT) are injected into	Office ICT System (affecting OT-System)

		workstations in the Enterprise Zone through spear-phishing employees through emails carrying weaponized attachments (e.g. scripts embedded in text processor macros). The attacker then laterally extends its foothold in the Enterprise Zone and collects intelligence on access codes and the structure of the company network. This information is then used to vertically extend access by deploying RAT in the Operations and Field Zone using legitimate credentials. The threat agent operates an external command and control service to execute control	

		on the infected devices. The gained access is then used to change the behavior of field devices, e.g. to disrupt power or gas distribution or to damage equipment.	
4	Malicious update to firmware in the field to influence single substation	This scenario focuses on the security of the manufacturers/supply chain and affects all equipment having regular firmware updates. A threat agent uses access to the update service for OEM firmware to inject malicious code to influence, by injection of communication to the field bus, the behavior of other devices at the substation of the power system. The	Substation OT-System

		attacker may aim at damaging individual devices by blocking (i.e. jamming) communication for protection functions or disrupting service by issuing single commands.	
5	Cross-sector, cross-border message flooding	A misconfiguration in the control system of the electricity transmission grid operator can lead to a situation where a single counter-value query from the gas system triggers a domino effect and an overload or temporary non-availability of the crucial services of the control center. The incident misinterpretation of a data signal at the interface of	Control Centre (TSO,DSO)

		two domains in different energy sectors can result in the temporary non-availability of relevant system functions	
6	Compromise equipment through SCADA apps	This scenario focuses on the security of regular maintenance via so-called SCADA apps (business clients) and smart home applications (end consumers). Most generation units are affected in this scenario. A threat agent exploits the established relationship between a (legitimate) SCADA app on a dual-use (private and business) smartphone of a control room engineer to gain privileged access to a distribution	IT/OT System

		SCADA system (e.g. of a generation unit or transformer station) and establishes persistent remote access there.	
7	Advanced persistent threat (APT) to DSO flexibility management system	A threat agent performs reconnaissance of utility communications and electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. The threat agent gains access to selected elements of the utility distribution management system (DMS) - which includes all distribution automation systems and equipment in control rooms, substations, and on	DSO (IT/OT Convergence threat)

		pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, possibly causing automated tripping of distribution level generation sources due to power and voltage fluctuations. A blackout of varying degrees and potential equipment damage ensues. Remote connections to the DMS might be established using a variety of methods or a combination of methods.	
8	Plant tripped off-line through	This scenario focuses on the security of the	Generation

		a compromised vendor (software update by manufacturer) and remote connection to generation unit or equipment	communication channel of the manufacturer to upload software updates on power system equipment in the field (in general generation units) per remote access. A threat agent uses compromised authorization credentials to access a secured remote maintenance network interface. The interface provides access to a vendor-maintained asset controllable through a distributed control system (DCS). The network access must correlate with a separate call from the vendor to the utility to open a conduit to the interface. The threat agent then	

		drops a modified system file that further attacks the local DCS network, either by flooding the network or by compromising further devices within the network. To affect a large area, multiple similar attacks have to be executed in parallel. The threat otherwise affects only a single DCS and all attached assets. A variant of the scenario establishes a foothold in a DCS and uses this access to further progress into different parts of the system. The elevated trust potentially assigned to a utility's "own" devices is exploited and used	

		to access larger control structures, for example through an uplink to a control room. The threat might also be the first stage of a coordinated load-changing attack that potentially affects the whole system.	
9	Compromised distribution grid management through supply chain vulnerabilities	Lifecycle attacks against equipment (in general generation units) during development, production, shipping, and maintenance can introduce deliberate errors that will fail under special conditions. For example, a threat agent might upload modified firmware in a relay during production that introduces a back door for	Supply Chain

		changing relay settings and set points. This could render the relay inoperable or cause it to operate unexpectedly. The functional integrity of digital systems is based on functional assumptions of the whole hardware and software stack. This implies, that the whole supply and maintenance chain, starting from the design process, is protected against code injections. Any modification potentially has a catastrophic impact that not be detected for a long time. The recently publicized vulnerabilities "Meltdown" and "Spectre", which affected the whole design series of	

		microcontrollers, provide an example of the possible scale of the number of involved devices in case of such issues. Large-scale industrial installations are considered vulnerable if they rely on a very limited number of manufacturers of parts and sub-parts of the system.	
10	Unauthorized Mass Remote Disconnect Through Firmware update	A threat agent prepares smart meter firmware containing malware and manually installs it on a target smart meter in each neighborhood. The single insertion point in each neighborhood becomes the botmaster for a smart meter-based botnet. The	Smart Meter

		botmaster acquires the IP address for the neighborhood’s headend at the utility and spoofs that address. As other smart meters attempt to connect to the headend, the botmaster sends a firmware update command to the smart meters and transmits the malicious firmware to each victim. Individual bots propagate the malicious firmware throughout the neighborhood and use them to achieve a mass remote disconnect scheduled at the same time.	

Source:[136]

2.7 Unified Extended Cyber Kill Chain and ICS Cyber Kill Chain

The Smart Grid (SG) is converging Information and Communication Technology (ICT) with Operational Technology (OT), so adversaries can compromise and gain control of a digital asset in the OT environment through the IT environment. For example, data historians can be accessed within the OT environment [139]. Cyberattacks need to be detected in both environments. The Cyber Kill Chain (CKC) model is one of the most widely used models to detect cyberattacks in an ICT environment [140]. The European Network and Information Security Agency (ENISA) identified the two main trends of adopting the philosophy and methods of Military Intelligence and introducing Artificial Intelligence into technologies for counteraction to cyber-attacks. The first was the qualitative transition to new cyber defense tools involving the use of artificial intelligence methods to analyze information exchanged, network flows, and sources of threats, and to plan effective impact measures, including proactive ones [141].

The second avenue was the application of Kill chains, which are traditional military science and military intelligence methodologies and methods, to cyber defense. The concept of a kill chain was first applied to an attack's organizational structure in the military. The goal is to successfully thwart or neutralize the adversary during each stage of the attack lifecycle [142, 143, 144].

The CKC model is focused on malware-based intrusions and APTs and can be applied in complex technical systems. It has been expanded and improved for use in Industrial Control Systems (ICS) and the detection of internal threats (Assante and Lee, 2015) [145]. A combination of both types of kill chains can be applied in the ICS as a unified extended cyber kill chain and an ICS cyber kill chain (Figure 2-14).

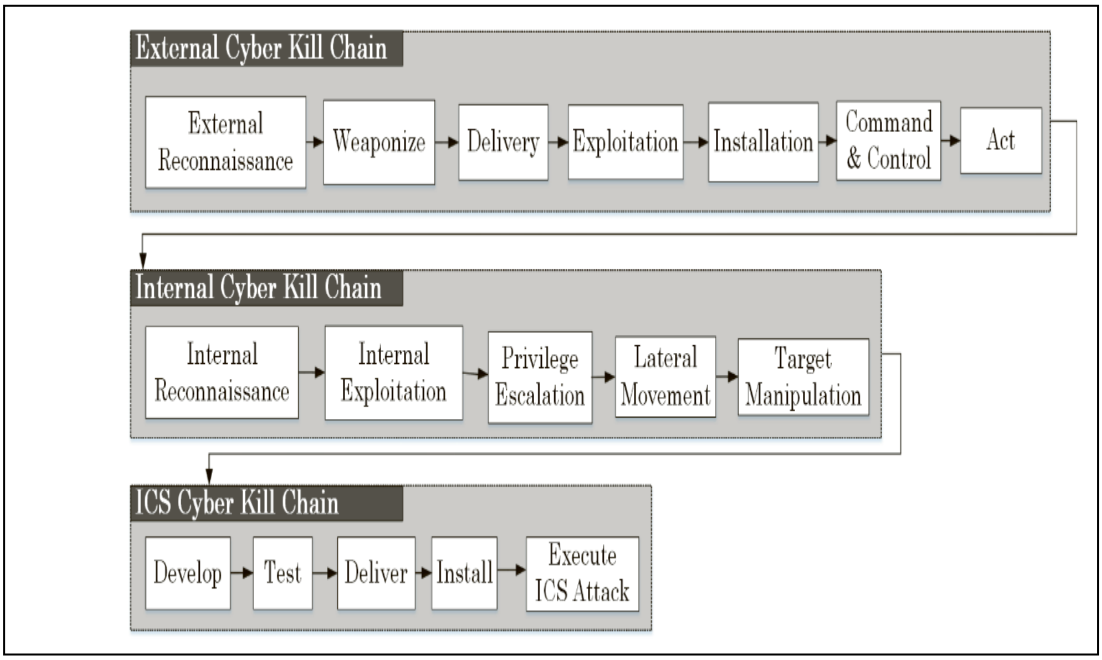


Figure 2-14. The unified extended cyber kill chain[140]

2.7.1 External Cyber Kill Chain Model

Lockheed Martin produced the original CKC model [140; Cloppert, 2009[141]]. This model's seven phases are:

Reconnaissance: From the standpoint of security monitoring, the planning stage of a cyberattack is one of the hardest to spot. The adversary uses social media platforms, conferences, blogs, mailing lists, and other network tracing tools to look up and collect data on the target. Later on, when delivering the payload—the actual intended message that carries out the malicious action—to the target system[140,141], the information gathered will be helpful[140,141].

Weaponize: The operation planning stage makes up the second step of the model. In the weaponizing stage, a Remote Access Trojan (RAT) and an exploit are combined to create a deliverable payload, generally via an automated tool (weaponizer) (Hutchins et al.,2011[146]). Yadav and Rao (2015)[147] provide a thorough explanation of the specific details relating to RAT and an exploit. Botnets, Distributed Denial of Service (DDOS), and malware are often employed cyberweapons. The effectiveness and quantity of the adversary's first-stage reconnaissance provide the foundation for the cyber attack operation. Therefore, it's crucial to restrict how much of the organizational profile is made publicly available.

Delivery: The third stage of the concept, called the operation launch stage by Velázquez (2015)[148], is when an organization might deploy technology as a mitigating control. Now the weapon is in its place, where it belongs. Websites, USB portable media, and email attachments were the three most often used delivery vectors for weaponized payloads by advanced persistent threat actors between 2004 and 2010 according to the Lockheed Martin Computer Incident Response Team (LM-CIRT) (Hutchins et al., 2011)[147]. One of the first technologies that could be deployed at this stage is a Network Intrusion Detection System (NIDS).

Exploitation: At this stage, the exploit is triggered to silently install/execute the delivered payload. The most common exploits are operating system, network, and application/software level vulnerabilities (Yadav and Rao, 2015)[147]. One of the most popular viruses, Wannacry, uses operating system exploits. One of the best mitigation technologies to increase the difficulty of the exploitation phase is patching. Therefore, security patches should be installed on all systems.

Installation: This stage involves the installation of the back door RAT and stays persistent inside the targeted environment. Techniques used by malware authors for installations include anti-debugger, anti-antivirus, rootkit and bootkit installation, targeted delivery, and host-based encrypted data exfiltration (Yadav and Rao, 2015)[147].

Command & Control (C2): After successfully installing the back door, the adversary seeks to establish a two-way communication channel so that they may take remote control of the targeted environment. This is known as command and control (C2). The attacker has "hands on the keyboard" access inside the targeted environment after the C2 channel has been established. In the literature, methods used by malware writers to transfer data to and from a target computer have been discussed (e.g., Yadav and Rao, 2015)[147].

Act on Objective: The model's final stage is to implement the objective. The enemy completes the planned attack objectives in this phase. These objectives may involve compromising the assets' availability, integrity, or secrecy. APT threat actors may remain undetected for years in an organization, according to Velazquez (2015)[128].

2.7.2 Internal Cyber Kill Chain

The internal cyber kill chain, which is a part of the extended cyber kill chain and has almost identical procedures to the exterior kill chain, is described by Zhou et al. (2018)[148]. The internal cyber death chain must first pass through several stages before it may penetrate the Industrial Control system (ICS), advance from workstations to servers via privileged escalation, migrate laterally inside the network, and control certain targeted devices (Zhou et al., 2018) [149]. The stages of the internal cyber death chain are as follows:

1) Internal Reconnaissance: At this point, the adversary has access to each user's workstation and can learn about its security flaws [149].
2) Internal Exploitation: During this phase, the adversary takes advantage of data and security gaps in the internal network[149].
3) Privilege Escalation (Zhou et al., 2018)[149]: During this phase, the adversary uses the compromised accounts to obtain a high level of privilege to change security settings and configuration files and attempt to steal passwords.

4) Lateral Movement: This stage involves the adversary moving between systems to penetrate the system's restricted region to obtain sensitive data and critical data[149].

5) Target Manipulation: During this phase, the antagonist assaults particular targets (Zhou et al., 2018)[149].

2.7.3 ICS Cyber Kill Chain

The adversary begins designing a particular attack tool for the ICS system and validates it for effective impact after learning information from the corporate network (internal kill chain) and the ICS system (external kill chain) of the target company. The opponent distributes the tool, installs it, and carries out the attack after successful testing (Assante and Lee, 2015)[145] (Figure 2-14). The ICS cyber death chain has the stages listed below:

1) **Develop:** This is the stage where the adversary begins with an attack tool based on ICS-specific vulnerability information (Assante and Lee, 2015[145]; Zhou et al., 2018[149]).

2) **Test:** This is the stage where the adversary validates a specific attack tool for reliable impact.

3) **Delivery:** This is the stage where the adversary delivers the attack tool to the ICS system.

4) **Install:** This is the stage where the adversary installs the attack tool, such as malware or a Trojan, into the target ICS system.

5) **Execute:** This is the stage where the adversary launches an attack on a specific production process to damage the physical equipment (Assante and Lee, 2015[145]; Zhou et al., 2018[149]).

2.8 Multistage Cyberattack in Smart Grid SCADA System

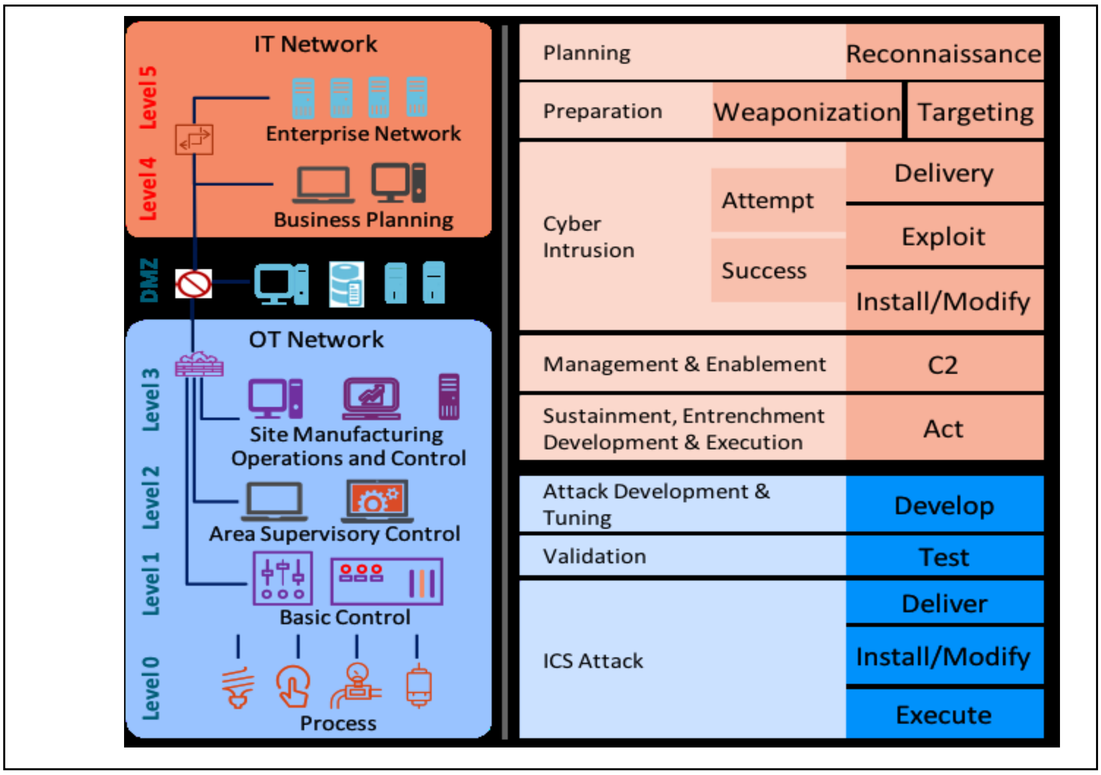


Figure 2-15. The IIoT zoned architecture [150] (left) and cyber kill chain for ICS[145]

In general, the target in industrial attacks can be an asset in either the IT, the DMZ, or the OT zone, however, the ultimate target in most ICS incidents was shown to be a host/device in the control zone (levels 0-2). As observed in the recent APT patterns in IIoT [151], the main attack vector focuses on gaining entry through IT systems and traversing the OT infrastructure by launching multiple low and slow attacks. Therefore, APTs in IIoT are most likely multi-domain, multi-step attacks that require one or more recurring sets of phases explained above. In other words, an actionable attack reference model for IIoT must take the architectural levels (or zones) into consideration.

ICS Kill Chain published by SANS [151] is developed based on CKC and the zonal architecture of industrial networks. As shown in Figure 2-15, the ICS kill chain is a two-stage attack model where the first stage (shown in pink) consists of the same phases as CKC in IT; implying that an adversary needs to first compromise the IT network, gain knowledge about business and operational information, and finally target OT components. Upon gathering sufficient information about the cyber-physical systems and processes in the OT, the attacker needs to develop and test a capability (e.g., a PLC configuration in [1]) for attacking it meaningfully (i.e., stage two shown in blue). For example, it may take a few weeks/months for the attacker to learn what controller is used in the target control zone, acquire a similar component to play with, develop a malicious code for it, and finally install and execute it on the target. Note that all of these steps are taken outside the defender's field of view, and relying on the detection of the install/modify phase might be too late for preventing the attacker from damaging a critical asset.

The ICS kill chain is the first IIoT attack model that includes the reference architecture of IIoT networks. However, it does not provide details regarding post-compromise and recurring phases and how an attacker may move laterally from IT to DMZ or DMZ to levels 3 or 2 in OT. In fact, in this model, stage two (and its five phases) only applies to level 1 and level 0 of IIoT reference architecture that includes controllers and physical processes.

Thus, all pre-and post-compromise phases and recurring steps certainly take place in the upper levels; the attacker first compromises internet-facing levels (e.g., corporate or enterprise networks) and then moves laterally within the IIoT network towards lower levels in the OT zones. Very recent research on ICS cyber defense triage process [152] shows this concept is based on the Mandiant attack model and IIoT reference architecture. However, the researchers did not elaborate on how to map security alerts to each phase and architectural level.

2.9 Related Works

In this section, we critically evaluate the related works on the topic of industrial control systems (ICSs) and their security, arguing that more research is needed.

2.9.1 The Stochastic Modelling Framework

This research, written by Pen et al. [153], focuses on a comprehensive security understanding of the SGs framework, assault scenarios, detection/protection mechanisms, estimation, and control tactics from both the communication and control perspectives. In addition, several potential obstacles and solutions for dealing with SG threat issues are presented. Finally, some findings are offered, as well as future study directions. The authors of [154] look at the design goals and functionalities of the smart grid communication system, as well as the communication requirements in depth. There are also discussions on some of the most current innovations in smart grid communication technologies. In this paper [155], Mrabet et al. summarize the cyber security requirements and the possible vulnerabilities in smart grid communications and survey the current solutions for cyber security for smart grid communications. However, both these works lack a survey based on primary data which is the main focus of this current research.

Authors in [156] review state the art of cybersecurity risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. Knowles et al.[157] have surveyed the cyber-security of ICSs and the risk management aspects of it. The related standard in this domain is discussed as how the current systems lack built-in security considerations.

Kriaaa et al. [158] conducted a thorough investigation into the safety and security of industrial control systems. The distinction between these two ideas (ICS safety and security) has been established. Different methods for these difficulties proposed in the literature are also classified as generic or non-generic. A review by Sajid et al. [159] focuses on the security challenges of cloud-based ICS systems. Additional issues following cloud integration, as well as the general security flaws of SCADA systems, are mentioned. However, a more thorough security examination is required, particularly for the applicability of the machine learning methodologies that we will develop in later papers.

Authors in [160] have provided a survey on the developed distributed filtration and control of ICSs using mathematical methodologies The differential dynamic models are the main focus, with a short component dedicated to security controls. For the security of these systems, it is necessary to design mod-el-based techniques. Molina and Jacob [160] examined existing cyber-security techniques for industrial settings based on software-defined networking solutions. However, they are more concerned with the general concept of cyber-physical systems than with ICSs in particular[161].

The available approaches for intrusion detection systems (IDSs) deployed in ICSs were investigated by Zeng and Zhou [162]. There is also a taxonomy of the relevant vulnerabilities in these systems. They explore machine learning-based solutions as well as various forms of intrusion detection systems.

Control system availability and reliability are frequently seen to be at odds with efforts to safeguard those systems, and this topic has recently attracted attention. With the growing use of IP-based technologies in control system contexts, well-known security concerns have arisen. Unfortunately, in the ICS environment, the methodologies and technologies that have been in use for a long time in IT can be extremely disruptive. New technologies and solutions are being developed in response to the requirement for nondisruptive approaches to safeguard control systems without having to wait for their rare shutdowns[163].

Numerous research has talked about the dependability of power systems and cyber-physical security in the literature. In [164], they used a Modular Petri Net Approach to model one actual use case and two anticipated extensions of a factory setting. Their approach allowed for the simulation and study of threat dissemination and represented information-based interdependence inside smart industrial networks. A new model called Susceptible-Exposed-Infectious-Recovered-Delayed and the Susceptible-Exposed-Infectious-Recovered-Recovered (SEIR) model Stochastic Petri Nets and Continuous Time Markov Chains were used to investigate the hybrid quarantine strategy together with the quarantined(Susceptible/Recovered) (SEIDQR(S/I)) method that was proposed in [165].

The authors in [166,167,168] suggested using Petri nets rather than attacking trees to depict the behaviors of concurrent attackers in industrial control systems and smart grids because Petri nets give greater expressiveness and flexibility. According to Mahmoudi and Payam [169], the capacity to specify the attacks in an adjustable fashion in a parametric model is the first step in assessing the different types of cyber-attacks. This allows one to explicitly test various attack types and then provide solutions to deal with them. Their work involved extracting and modeling a multi-stage attack using a colored Petri net (CPN) and a timed Petri net (TPN) and comparing the outcomes to those of papers that were similar to their own[170].

The security concerns of the IEC 60870-5-104 (IEC-104) protocol, which is widely used in the European energy sector, were the focus of the study SCADA Systems [171]. Specifically, a Coloured Petri Net (CPN)-based SCADA threat model was offered, and four types of assaults against IEC-104 were simulated. Last but not least, the danger level that each of these cyberattacks poses to the suggested system was assessed using AlienVault's risk assessment approach [172]. Malicious software, sometimes known as malware, is the main source of cyber risks that target end users and terminals. Either comparing their digital signatures or examining their behavioral models can be used to discover malware. The behavioral analysis must be used in conjunction with traditional signature-based anti-virus solutions because obfuscation techniques virtually render malware invisible. Based on colored Petri nets, the suggested method for simulating malware behavior [172,173,174]. Our research strategy adopted that of [173], who suggested that steady-state probabilities of the power communication infrastructure based on current cybersecurity technologies be derived. The development of steady-state probability is based on newly generated models on digital relays that represent the authentication method, (ii) changed models on password models and (iii) models for honeypots/honeynets inside a substation network. The precise statuses and transitions of components included in a cyber-net are formulated using a generalized stochastic Petri net (GSPN). Both quantitative and qualitative steady-state probabilities are computed.

Authors in [170] advocated the use of a program model based on fuzzy interpreted Petri nets (FIPN) to regulate DES in contrast to [172,173,174] and the method for creating this model using the graphical representation of the net. Comparing FIPN to discrete PNs, improved visibility is provided, and through the use of a simulator called FIPN-SML, program code may be created quickly. A graph-based dynamical system model that was simulated in MATLAB/Simulink using the fourth-order Runge-Kutta method [175] evaluated the risk of cyberattacks for hazardous liquid loading operations, and [176] demonstrated how cause-and-effect relationships can be conveniently expressed for both analysis and extension to large-scale smart grid systems. By employing a case study of the Western Electricity Coordinating Council 3-machine, a 9-bus system, and simulations in MATLAB and PSCAD to validate the method, the authors in [177] also reevaluated the prior framework in [178].

However, the literature study shows that each framework made an effort to solve a few issues relating to the numerous significant components of the smart grid infrastructure framework. The proposed cyber architecture was modeled using the Platform Independent Petri Net (PIPE) [124]. We use a method to decrease the state space because it expands exponentially as the number of components rises. To demonstrate that the plan is successful, we then examined the suggested framework's steady-state availability [179-182].

2.9.2 The stochastic Impact Modelling Approach

The stochastic hybrid system (SHS) is a mixture of the linearized differential-algebraic equation (DAE) model and the CTMC, as described in [183]. They claim that active/reactive power injections are governed by a continuous-time Markov chain (CTMC), while power system dynamics are governed by the standard DAE model. To linearize the DAE model, a hypothetical set of active/reactive power injections is used. The authors of [184] suggested solving the resulting bilinear programming model using the big – M technique and giving the decomposition method. Both the advantages of RO and stochastic programming are combined in the suggested technique. Zhou and his associates. [185] investigated the application of the stochastic response surface method (SRSM) to small-signal stability analysis of coupled solar and load systems with probabilistic uncertainty. The impact of false data integration attacks (FDIA) on power systems was investigated in [186].

In [187-188], the authors described an integrated operational simulation tool that includes different stochastic unit commitment (SUC) and economic dispatch models that take stochastic loads and variable generation into account across multiple operational timescales. The program included customizable sub-models for day-ahead security-constrained unit commitment (SCUC), real-time SCUC, real-time security-constrained economic dispatch (SCED), and automatic generation control (AGC).

Milano and Minano [189] present a broad and systematic framework for modeling power systems as continuous stochastic differential-algebraic equations. This was accomplished in the paper by providing a theoretical background on stochastic differential-algebraic equations and advocating for the use of stochastic models in power system research. Similarly, [190], [191], [192], and [193] recommended the use of stochastic differential equations (SDEs), a sort of power system model. [190] looks at quasi-Hamiltonian power systems with losses and SDEs in the first section. Second, an unique analytical method for studying the stability of the power system with losses under SDEs is proposed, based on the stochastic averaging method. [191] examines the stability of the quantity of uncertainty in a power system using the noise-to-state stability (NSS) and NSS Lyapunov function (NSS-LF).

[192] designs Dynamic Load Altering Attacks to counter smart grid demand response algorithms (D-LAA). The D-LAAs are described in great depth. Open-loop vs. closed-loop assaults, single-point vs. multi-point attacks, feedback type, and attack controller

type are all examples of D-LAAs. The attacker uses feedback from the power system frequency to manage changes in the victim load, which is defined and assessed, in a closed-loop D-LAA against power system stability. Zhang et al [193], proposed a forced outage rate (FOR) model to study the reliability of the generators and transmission lines. Authors in [194], used the Bayesian networks to model the attack propagation process and inferred the probabilities of sensors and actuators being compromised. The probabilities were fed into a stochastic hybrid system (SHS) model to predict the evolution of the physical system being controlled. [195, 196,197], also attempted to study the impacts of cyberattacks on the physical components of the power systems such as circuit breakers.

Several methods to model cascading failures in power systems have been proposed in the literature review; however, the strategies proposed do not include overloaded lines based on hypothesized substation outages, or a Semi-Markov Process (SMP) to model the impact of cyberattacks on power system contingency analysis.

2.9.3 The Real-time Simulator Modelling Approach

When we place an actual physical system in a hazardous state, testing in the energy sector can be practically unfeasible and difficult. In that regard, a Real-Time Simulator (RTS), which is a computer model that operates at the same speed as the real-world physical system, would aid in accelerating development. Additionally, it would assist in simulating various cyberattack situations in a physical system and offer scripts to address those events. Thus, RTS has been extensively utilized in the energy industry [198]. The majority of RTS literature, however, focuses on technical aspects of energy-related cyber security issues rather than, for instance, guidelines for developing cybersecurity simulations of cyber-physical artifacts in real-time simulation [199], power systems themselves [200], or regulations and standards [199]. Thus, our research fills this gap and offers guidelines for creating simulations of cyber-physical objects.

Numerous universities and U.S. national laboratories have created internal testbeds for research as well as for training and education due to the significance of cybersecurity research for CPS and key CPES infrastructures [201]. Hardware-assisted testbeds are intended to formally examine CPS and typically include many real-world physical elements. For example, CPES hardware-assisted testbeds use actual hardware like generators, relays, switchgear, energy storage systems (ESS), solar panels, wind turbines, etc. The Idaho National Laboratory (INL) of the U.S. Department of Energy

(DOE) is an example of a hardware-assisted research lab that uses actual working equipment to carry out CPES security research [202]. Using real hardware and data generating procedures, INL's Power and Energy Real-Time Laboratory [203, 204], Nuclear Laboratory [205, 206], and Microgrid (MG) testbed [207, 208] enable the modeling of realistic scenarios.

Researchers can develop complex scenarios involving power hardware devices that are interfaced with real-time simulation environments using HIL methodologies such as controller hardware-in-the-loop (CHIL) and power hardware-in-the-loop (PHIL) thanks to INL's testbeds' real-time simulation capabilities [202]. Before being fully integrated into the main grid, HIL enables comprehensive testing of controllers (CHIL) and components of EPS (PHIL) [208]. Hardware-assisted testbeds are also a part of DOE's National Renewable Energy Laboratory (NREL) [209]. The Flatirons campus of NREL is an expert in developing precise simulation models for hydrokinetic generation facilities, hydropower plants, and wind turbines [210]. Their distinctive facilities promote the advancement of their high-fidelity simulation models, which are cross-referenced to real assets and offer priceless tools for power engineers doing system studies combining dispersed hydro and wind generation or off-shore generation [211]. It is possible to investigate the potential effects of component failures or cyber-attack incidents using the actual power system assets of wind turbines and hydroelectric plants as well as their simulation models for very little money and, most importantly, without jeopardizing the actual EPS operation.

Hybrid testbeds are viewed as a viable alternative to fill the gap between the hardware- and software-assisted CPS testbed approaches. HELICS [212, 213] is an excellent illustration of a hybrid CPES testbed infrastructure. Another hybrid testbed that makes use of the benefits outlined above is available at the Pacific Northwest National Laboratory (PNNL). A hybrid testbed configuration is also part of the facilities of Florida State University's Center for Advanced Power Systems (CAPS).

In addition to testbeds, a wide range of methodologies has been used to assess the cyber security of the smart grid system. [214] offers and studies a comprehensive overview of the most recent analysis tools and their smart grid applications. Recently, several methods for simulating attacker behavior have been put forth. These methods aimed to comprehend the socio-technical perspective of the system and investigate how an intrusive party might affect the system's operation. In the study of Shama et al. [215], the components of a smart grid system, including IoT-enabled devices and crucial communication protocols, are assessed for security and safety issues. A model of adaptive Bayes-based network security has been created from the "multiarmed bandit" problem in detail. This innovative approach to cyber security investment looks at how network defenders could effectively allocate cyber defense teams among nodes.

2.9.4 The Approach to Modeling FDIA on the AGC

A threat analysis structured method was proposed by Beckers et al. [216] and involved mapping the attacker's strategy (described in an attack tree) to specific system vulnerabilities (represented as an attack graph). They showed how to extract a section of a complex graph relevant to a certain target in the attack tree. The study's findings indicated that the complexity of analyzing attack graphs had much decreased. This research also suggested an approach to determine the likelihood that an attacker will successfully reach the target overall.

The authors of [217] suggested a framework for the security graphical modeling and assessment of the Internet of Things. (IoT). The five steps of the framework include data processing, security model construction, security model analysis, security visualization, and model updates. An IoT Generator, a Security Model Generator, and a Security Evaluator were created as a result of this research. Building an IoT network using knowledge about node vulnerability and network reachability is one component of the IoT Generator's task. Additionally, based on the chosen IoT network, the Security Model Generator generates the extended Hierarchical Attack Representation Model (HARM). The Security Evaluator, on the other hand, uses a variety of security criteria to assess the network's security.

Attack graph visualization is a useful approach for cybersecurity professionals and non-experts to investigate the system's suspicious activities and examine all possible hacking attempts. The likelihood of an attack, which strongly enhances the risk evaluation process, can be defined. Unfortunately, the development of accurate trees is a difficult process when attacker capabilities and objectives are not well known.

In recent years, several cyber-attack incidents have been reported. A detailed survey of different cyber-attack incidents was provided in [218], [219],[220], [221]. A detailed elaboration on cyber-attack incidents in power networks appears in [222]. Little work has been conducted concerning attack-resilient measures that are used to detect, identify, and mitigate corrupted real-time measurements in the feedback loop of automatic generation control (AGC)[223]. The accuracy and reliability of real-time measurements have a significant impact on the system's real-time operation. In smart power grids, real-time measurements for AGC are transmitted using computer networks[224].

A major concern in AGC security is false data injection (FDI) attacks [225]. An FDI attack is when an adversary gains access to the communication between the components of an AGC and injects data packets that are intentionally inaccurate. AGCs are inherently not resilient to unforeseen patterns. A successful FDI attack can cause the state estimation component of an AGC to generate erroneous values, which may lead to unpredictable and unstable responses, disrupting a system's operation. In recent years, FDI attacks have been the focus of significant research studies[226]. Therefore it is of vital importance to protect the AGC from cyber attacks.

Model-based methods [227]–[230],[231],[232] and learning-based methods [233]–[236][237],[238],[239] can be used to categorize FDI attack detection strategies in AGCs. Model-based techniques for FDI detection use an observer to gauge a system's dynamics such as Kalman filter [233], [236], weighted least square observer [234], and principal component analysis (PCA) [235], [238]. To detect and react to attacks on the states and sensing systems of agents, the authors of [232] suggest an adaptive sliding mode observer with online parameter estimation. The research in [233], [236] develops a Euclidean detector, a 2 detector, and a Kalman filter estimator for cyberattacks. In [234], the authors develop a least-cost defense tactic to defend power systems from FDI assaults.

Results like [235] use PCA to guarantee data integrity when estimating the condition of power grids. Model-based approaches may have some benefits, such as real-time anomaly identification and cheap processing complexity, but because of how heavily they rely on precise mathematical models, they are susceptible to model uncertainties and disturbances.

To detect system states, learning-based FDI detection systems generally employ neural networks (NN) and machine learning techniques [233]–[236][237],[238],[239] from the field of artificial intelligence. Learning-based techniques are the best option for studying complex dynamical systems because they provide a framework for estimating nonlinear systems.

Modern power systems' complicated operations have been successfully solved by machine learning models. Particularly, new research on Deep Learning (DL) methods using data sequences like Recurrent Neural Networks (RNN) has demonstrated considerable promise when used with time-series data like observations from power systems. Multi-input RNN is used to perform adaptive identification and control signal protection in power systems [233-237]. Using a Long-Short Term Memory (LSTM) architecture, active distribution networks' complicated topologies and dynamic activity are represented in [237-238].

Several research publications on cyber-physical security have discussed the use of DL approaches to identify and counteract various threats. In [239], stacked auto-encoders are used to extract nonlinear and non-stationary power system features, and a proposed interval-based state estimation to identify cyber-attacks is presented. [239] presents a framework that protects both security and privacy.

2.10 Industrial Control Systems and Cybersecurity in Zambia

The numerous connected works, governance and security frameworks for ICS, cyber-security incidents involving ICS and related systems, and risks and vulnerabilities specific to ICS/SCADA environments are covered in this area.

2.10.1 SCADA Implementations in Zambia

According to [240] Currently, Zesco has over 90% visibility of the Lusaka Division and Kitwe Region Substations and Distribution network via a somewhat aged SCADA/Demand Management System (DMS) system branded as Micro SCADA and Opera ++ installed in 2002. The Micro SCADA solution monitors and controls over 52 substations in Lusaka Division and 13 substations in the Kitwe Region whilst the Opera ++ (DMS) covers a radius of 150km in Lusaka.

They added that the SCADA/DMS is not integrated with the enterprise-wide outage management Information Management System (IMS), which is a system that is a key component of an integrated enterprise-wide Business Information System (BIS) that was put in place in 2004. The Customer Management System (CMS), Design and Construction System (DCS), Plant and Equipment Maintenance System (PEMS), Stores and Procurement Management System (SPMS), Transport Management System (TMS), Payroll and Human Resource Management System (PHRIS), and Oracle

Financials are additional applications that make up the Business Information System (BIS) [240].

Apart from ZESCO, ICS/SCADA systems implemented in Zambia include Copperbelt Energy Corporation (CEC), the mining and mineral processing industry, the sugar industry, and the water treatment and recycling plants country-wide. Other ICS/SCADA environments include the petrochemical industry Indeni and Tazama, and breweries [241,242].

2.10.2 Zambian Legislation and Governance Related to ICS/SCADA

A variety of regulations that Zambia has passed ensure an environment that is efficient, safe, and suitable for using electronic communications. The primary laws in Zambia governing data privacy and protection are the Electronic Communications and Transactions Act No. 4 of 2021 (the "ECT Act")[243], the Data Protection Act No. 3 of 2021 (the "Data Protection Act")[244], the Cyber Security and Cyber Crimes Act No. 2 of 2021 (the "CSCC Act"), and the Information and Communications Technologies Act No. 15 of 2009 (the "ICT Act")[245]. The aforementioned legislation is comprehensive and outlines the legal criteria for domain name registration, the processing of personal data, the recognition of authentication service providers, and the exchange of data messages. The law also contains rules that make it illegal to intercept communications, reveal messages that have been retained, decode communications without authorization, or release a decryption key and disclose records or other information by the key holder. The law also establishes guidelines for cyber audits, cybercrimes, and the security of electronic communications.

Notably, the Minister of Transport, Works, Supply, and Communications directed that the commencement orders for the Data Protection Act, the CSCC Act, and the ECT Act be published in the Government Gazette on April 1, 2021. (hereinafter referred to as "the Minister"). Per Section 1 of the relevant Acts, this led to the three Acts becoming operative on that date.

ICS/SCADA systems will need to be adequately governed to comply with the requirements. The acts discussed in this section may not be obliviously applicable to ICS/SCADA environments, however as is evident, under certain conditions they are applicable. Therefore, IT governance and security functions may in the future be required to have more oversight of ICS/SCADA systems.

2.11 Challenges

Because of the antiquated systems, especially the unsupported Windows XP, patching is hard, leaving vulnerabilities that are challenging to fix. Additionally, the time frame for doing this is limited because patching and security methods frequently cannot be implemented in a live production environment. Only one or two days a year, depending on the environment, do the company's operations or factory not run.

Because ICS/SCADA is frequently the domain of engineers, not IT, IT security has less of an impact on the systems. Therefore, there are additional difficulties in getting buy-in from all stakeholders, especially in light of the other difficulties and the business consequences mentioned above.

2.12 Conclusion

In general, controls and dangers related to information security were examined. Cybercrime has become more prevalent globally, and millions of people have become victims. There was a discussion of the dangers and vulnerabilities specific to ICS/SCADA. The instances that have already happened show that the ICS/SCADA environment is susceptible to attack and can result in serious disruption.

They must be protected because Zambia like any other country has multiple ICS/SCADA implementations in infrastructure that are vital to the country's economy. The SCADA environment presents many difficulties for security. International control frameworks that are structured using a defense-in-depth strategy may be able to overcome these obstacles and offer these ICS/SCADA systems an adequate level of security. Also highlighted was the process for creating a control framework for ICS/SCADA. The next chapter discusses the research methodology.

CHAPTER 3: MATERIALS AND METHOD

3.1 Introduction

In this thesis, we've concentrated on learning new information and using it to address a particular need. We worked with Texas Technical University (TTU) Wind Energy Laboratory, Arkansas State University, Nebraska University, and an industrial partner (ZESCO) throughout the entire research process to take into account the limitations of current systems where our ideas could be implemented and assessed.

We employed design science research in our contributions, see figure 3-1. Design science research is focused on developing new knowledge through the design of inventive or original artifacts (things or processes) and the examination of the artifact's performance and/or use through reflection and abstraction [246].

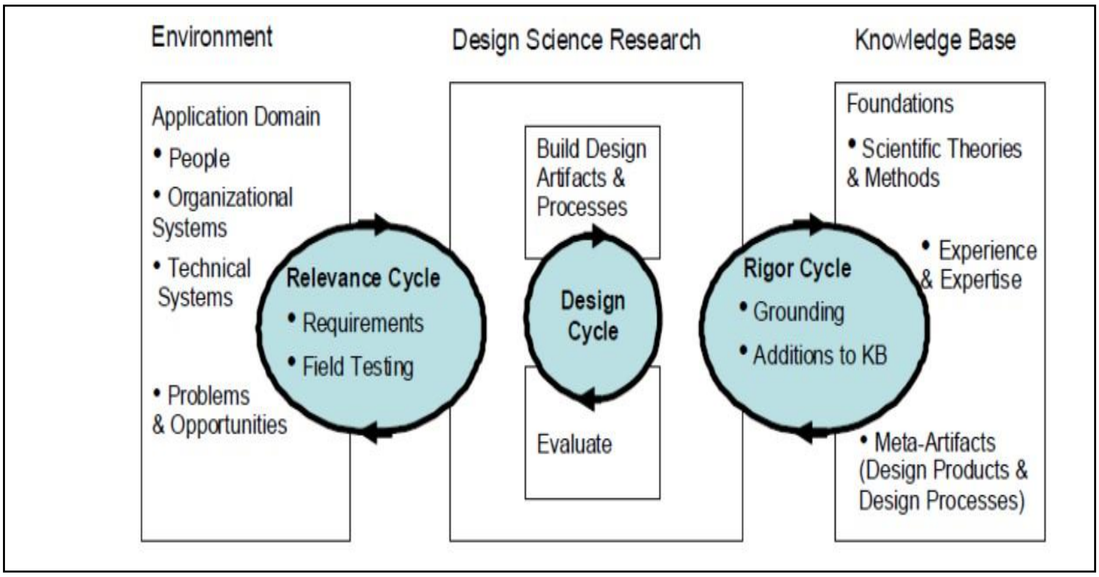


Figure 3-1. The Design Science Research Cycle [248]

"Knowledge in the form of constructs, procedures, and methodologies, models, and/or well-developed theory for conducting the mapping of the know-how for building products that satisfy specified sets of functional requirements" is what is meant by "design science."

Through the interchange between a knowledge base and an environment, the environment is improved by applying design science [247].

We used the process model by [248] which consists of six activities:

1. Define the specific research problem and justify the value of a solution.

2. Define the objectives for the solution

3. Create the artifactual solution which could be constructs, models, methods, or instantiations, and determine the artifact's desired functionality

4. Demonstrate the effectiveness of the artifact to solve the problem involving its use in experimentation, simulation, a case study, proof, or other appropriate activity

5. Evaluate how well the artifact solves the problem

6. Communicate the problem, its importance, the artifact, and its effectiveness to researchers and other relevant audiences.

Relevance Cycle. Through three cycles of the design science research approach, as described by [249], we carry out these six actions. Based on this methodology, a research context is established during a Relevance Cycle that specifies the needs for the study in terms of the issue to be resolved as well as the standards for approving the research findings. The first two steps of Peffers et al [249] activities cover this cycle, which also serves to determine the criteria applied in steps 4 and 5. Whether the relevance cycle needs to go through additional iterations depends on the findings of these steps.

The **Rigor Cycle.** By giving previous information to the research project based on the experiences and expertise that define the state-of-the-art in the application domain of the research, the rigor cycle combines the design science findings with the knowledge base. Additionally, it makes sure that the knowledge base is expanded by the research contribution. This includes any modifications to the current theories and methodologies, new design products and procedures, as well as all research-related learnings [248]. Step 3 of the Peffers et al. activities initiate this cycle, which is followed by Step 6 to complete it.

The central **Design Cycle** Until a good design is obtained, which is done in steps 3 to 5, the primary Design Cycle iterates between the fundamental activities of creating design alternatives and evaluating the alternatives against requirements.

In the relevance cycle, which defines the need for an approach to enhance software security during software development, we specified our study topics. We offered new artifacts to help software developers during the software lifecycle using the knowledge base of known vulnerabilities and security best practices, and we evaluated the proposed artifacts against the needs we had specified in the relevance cycle. We will refine the artifacts during iterations between their design and development to meet new needs, take into account real-world effects in industrial settings, and be pragmatic.

We contended that the development of ZICSCSF would help improve the knowledge and understanding of the cyber security and crime domain and the actual framework can be used as a guide to address some of the current shortcomings in the Zambian context. Table 3-1 shows how the design science principles are being applied in this research.

Table 3-1. Design Science and its applications to ZICSCSF

Steps	Guidelines (Hevner et al., 2004)[248]	Application of Design Science: **ZICSCSF**
Guideline 1: Design an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, or an instantiation.	The research project will produce a viable artifact, a cyber-security framework, ZICSCSF
Guideline 2: Problem Relevance	The objective of design science research is to develop technology-based solutions to important and	ZICSCSF is formulated to address the current lack of formal national cyber-security strategy and guide. The current state increases Zambia’s

	relevant business problems.	vulnerabilities to cyberattacks and crimes due to a lack of formal guidance and control mechanisms. ZICSCSF seeks to address this gap.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	ZICSCSF is evaluated for its viability and usefulness by the utilization of the descriptive approach. A scenario is used to demonstrate the utility of the artifact.
Guideline 4: Research Contribution	Effective design science must provide clear and verifiable contributions in the areas of design artifacts, design foundations, and or design methodologies.	The research and the artifact, ZICSCSF provide both research and practical contributions to Zambia and other developing countries. It establishes a platform from which controls and proactive mechanisms can be

		used to manage cybercrime. The research also seeks to extend the knowledge base in cyber-security through the examination of the phenomenon in a currently underrepresented context: developing countries such as Zambia.
Guideline 5: Research Rigor	Design science research relies upon the application of rigors methods in both the construction and evaluation of design artifacts.	Strict research guidelines are used in the development of ZICSCSF through the reliance on multiple established sources to inform its development.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the	Multiple sources are used to guide the development such as feedback from officials in government and businesses and established global

	problem environment.	benchmarks such as ISO 23072.
Guideline 7: Communication of Research	Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The research will be communicated through various publication mediums including the thesis. The work will also be presented to government officials and business executives.

3.1.1 The Empirical Evaluation Methods

To verify that the suggested artifacts meet the requirements, the study described in this thesis employs surveys [250], expert opinions [252], and case studies [253] (or a mix of these methods).

When the phenomena of interest must be researched in their natural environment and when they occur in the present or recent past, surveys are used [250]. "The distinguishing characteristic of survey research is the selection of a representative sample from a well-defined community, and the data analytic procedures used to generalize from that sample to the public, usually to answer base-rate questions," according to Easterbrook et al. [251]. Survey research requires a specific research question to be defined by inquiring about the characteristics of the target group. Survey research has been performed to assess vulnerability modeling and to confirm the proposed framework and model's integration into the ICS control bus.

Using expert opinions is one of the four kinds of methods listed by [252] for empirical validation in design science research when researchers want to generalize from validation studies to future practices. The other three are single-case mechanism experiments, technical action research, and statistical difference-making experiments [252]. Expert opinion can be elicited before the artifact is tested on models or in the field to gather early information about the possible usability and usefulness of the artifact in a real-world context [252].

When studying contemporary phenomena—which are challenging to investigate in isolation—a case study is utilized as a research tool for software engineering because it allows for the study of these phenomena in their real-world context [253].

When running a case, there are five stages to be taken. An extensive number of revisions may be made to a case study's steps. The procedures are [253]:

1. Case study design to define objectives and plan

2. Preparation for data collection

3. Collect evidence on the studied case.

4. Analysis of collected data

5. Reporting

According to [254], case studies can have a single-case design, i.e., one single context and one case within the boundaries of that context, or a multiple-case design where multiple contexts and cases within their boundaries are used.

We have used case studies in our research for two purposes:

1) To address step 4 of the design science process and demonstrate the efficiency of the artifact to solve the problem: e.g., by applying a vulnerability modeling method to publicly reported software vulnerabilities by security experts in a software development organization. Note that we will use expert opinions to validate the results.
2) To evaluate how well the artifact solves the problem and address step 5 of the design science process: e.g., to evaluate how a large enterprise implements the cyber security framework.

3.2 The Study Area or Site

The study baseline was Lusaka (ZESCO), Kitwe (CEC and ZESCO), and Namalundu (Kafue Gorge Regional Training Centre, Kafue Gorge Upper, and Lower Hydro Power Plants).

3.3 The Study Population

According to [255] studies, the term "population" refers to the entire group of people (subjects or events) who have the traits that the researcher is interested in. Based on a system of purposeful sampling, the study's population was established. The population in this context refers to all of the ICS security experts and workers from ZESCO, CEC, Kafue Gorge Lower, and Kafue Gorge Upper, and ICS operators, who made up the population.

3.4 The Study Sample and Sampling Techniques

There are numerous approaches, incorporating many different formulas, for calculating the sample size for categorical data. We used Yamane's finite equation [256]

$$n = \frac{N}{1+Ne^2} \qquad (17)$$

Where:

n is the required sample size, N is the percentage occurrence of a state or condition, and e is the percentage maximum error required.

Taking the population of specialized personnel to be 200 across all the targeted organizations and precision be 95%,

Then, $n = \frac{200}{1+(200x0.05^2)}$

n = 170

The Sample size for the participants was anticipated to be a minimum of 170 people across various professional organizations and companies running ICS/SCADA systems to help elicit requirements for the model.

The sample study included Chief Information Security officers, information security professionals, Cybersecurity professionals, Network Administrators, IT Auditors, Computer Engineers, End Users, and other related professionals who are directly involved in the administration and management of cybersecurity, Top Management, Finance, Legal, and Training.

3.5 The Data Collection Methods

Data collection is one of the key elements of the research technique. When selecting a data-gathering method, a study purpose or question should be taken into account [257].

The level of the researcher's involvement in the data-gathering process is one of the most important elements to consider when choosing the data collection method. We used a range of data collection strategies in this thesis, depending on the setup for the empirical evaluation and the goal of the data collection.

3.5.1 The Questionnaire

Questionnaires are sets of questions administered in a written format [257]. Questions can be closed-ended or open-ended. For example, multiple-choice questions are closed-ended and free-text answers are open-ended. We used questionnaires:

In a survey ask experienced developers about how a trusted node fits into the development process and how much value it adds. It will help us to gather input from subjects during the performed survey in a structured and targeted way.

In a case study to get feedback from experienced requirements engineers in a large enterprise on using security risk assessment. The benefit is gathering input from a relatively large number of subjects in a cost-effective way to easily quantify the results.

We will use the Goal-Question-Metric (GQM) technique to develop and build the surveys in both scenarios. GQM is a framework for specifying and evaluating software metrics [258]. A goal, along with the thing to be measured, the rationale behind the measurement, and the vantage point from which the measurement is carried out, are the first things a GQM model states (Basili et al., 1994). The use of goal-oriented measurement techniques, such as GQM, for data collection, is covered in [259].

3.5.2 The Interviews

Interviews utilize questions, which may be open-ended or closed-ended, similar to surveys. Interviews have the advantage that questions can be clarified and strange responses can be looked into [260].

Depending on the interviewer's major area of interest, interviews can be structured with preplanned questions, semi-structured with preplanned questions that can be adjusted in language and sequence, or unstructured [261].

We used semi-structured interviews as a follow-up to both questionnaires and went through the answers provided by the subjects to possibly get elaboration on the answers they had provided. This helped us to validate our interpretations of the answers provided in the questionnaires. The interviews were either face-to-face or telephone meetings when the subject was not geographically located in the same place as the researcher.

3.5.3 The Focus Group

Focus groups are meetings where participants concentrate on a single subject under the direction and supervision of a moderator [257].

This method is a cost-effective way to gain expertise from practitioners and users and is especially suitable for gathering initial comments on new ideas or producing questionnaires [262]. It follows a predetermined format and lasts two to three hours on average. The advantage of holding a focus group depends on the members' understanding and perspective of the study's objective [262].

One of the surveys in our study included a focus group to see how well participants understand the vulnerability modeling method and get their reflections on our proposed method.

3.5.4 Content Analysis and Analysis of the Statistics

Content analysis is a method of collecting data from written documents [261] and can be used when qualitative data are expressed in words and there is no statistical analysis to interpret the data. Lethbridge et al. classify this method as a "*Third Degree Technique*" which is about the analysis of work artifacts, e.g., source code, documentation, and reports documentation generated by software engineers, including comments in the program code, as well as separate documents describing a software system [257].

Analysis of statistics is used when there is quantitative data available in an empirical study. Statistical methods are used for the interpretation, analysis, organization, and presentation of data when researchers would like to ascertain that their findings are statistically significant [261].

3.6 Modeling and Simulation

Table 3-2 below summarizes the procedures that were employed to meet the research objectives.

Table 3-2. Procedure for Data Collection

No	OBJECTIVE	RESEARCH METHOD	RESEARCH TOOLS
1	Identify the existing cybersecurity maturity levels in industrial control systems;	Literature review, survey	Simulation, modeling,
2	Enable the prediction of cyberattacks in the SCADA systems;	Literature review, case studies, DSRM	Simulations
3	Determine the impact of cyberattacks on power systems contingency analysis.	Literature Review, Case study, DSRM	Simulations, Modeling, Cybersecurity Standards
4	Formulation of a cybersecurity framework to increase the	Literature Review	Simulations, Modeling,

	robustness and resilience of the ICS and SCADA systems	DSRM, Case study	Cybersecurity standards
5	Development of a cybersecurity testbed to model attack and mitigation schemes in the smart power grid communications systems.	DSRM	Simulation, Modeling

3.6.1 Characterizing Intrusion Process - Stochastic Processes

A stochastic process (also known as a chance or random process) is a group of random variables that are indexed by a parameter like time[263].

X(t) | t ∈ T, defined on a certain probability space, indexed by the parameter t, where t fluctuates over an index set, T[263], is a family of random variables that make up a stochastic process.

States are the values that the random variable X(t) assumes, and the state space of the process is the set of all possible values. The letter i [263] will stand in for the state space.

A stochastic process is referred to as a discrete-state process, often known as a "chain," if the state space is discrete. The state space in this situation is frequently thought to be

{0, 1, 2, . . .} etc. As an alternative, we have a continuous-state process if the state space is continuous. Similar to this, we have a discrete-time (parameter) process if the index set T is discrete; otherwise, we have a continuous-time (parameter) process. The symbol for a discrete-time process, commonly known as a stochastic sequence, is $\{X_n|$ n ∈ T} [263]. As indicated in Table 3-3, this results in four different kinds of stochastic processes.

Table 3-3. Categories of Stochastic Processes

Time Parameters	Index set T (state space)	
	Discrete-time Stochastic chain	Continuous state
Discrete-Time	Discrete-time Stochastic chain	Discrete-time Stochastic process
Continuous Time	Continuous Stochastic chain	Continuous Stochastic process

3.6.1.1 Classification of Stochastic Processes

For a fixed time $t = t_1$, the term $X(t_1)$ is a simple random variable that describes the state of the process at a time t_1. For a fixed number x_1, the probability of the event $[X(t_1) \leq x_1]$ gives the CDF of the random variable $X(t_1)$, denoted by [263]

$$F(x_1; t_1) = FX(t_1)(x_1) = P[X(t_1) \leq x_1].$$

$F(x_1; t_1)$ is known as the *first-order distribution* of the process $\{X(t) \mid t \geq 0\}$. Given two-time instants t_1 *and* t_2 , $X(t_1)$ and $X(t_2)$ are two random variables in the same probability space. Their joint distribution is known as the *second-order distribution* of the process and is given by $F(x_1, x_2; t_1, t_2) = P[X(t_1) \leq 1, X(t_2) \leq x_2]$.In general, we define the *n*th-order joint distribution of the stochastic process $X(t)$, $t \in T$ by

$$F(x; t) = P[X(t_1) \leq 1, \dots X(t_n) \leq x_n] \tag{18}$$

for all $\boldsymbol{x} = (x_1, \dots., x_n)$∈ $\Re^n$ and $\boldsymbol{t} = (t_1, \dots., t_n)$)∈ T^n such that $t_1 < t_2 < \cdots < t_n$. Such a complete description of a process is no small task. Many processes of practical interest, however, permit a much simpler description. For instance, the *n*th-order joint distribution function is often found to be invariant under shifts of the time origin. Such a process is said to be a strict-sense stationary stochastic process[263].

Definition (Strictly Stationary Process). A stochastic process $\{X(t) \mid t \in T\}$ is said to be stationary in the strict sense if, for $n \geq 1$, its nth-order joint CDF satisfies the condition:

$F(\mathrm{x}; \mathrm{t}) = F(\mathrm{x}; \mathrm{t} + \tau)$

for all vectors $\mathbf{x} \in \mathfrak{R}^{\boldsymbol{n}}$and $\in T^n$, and all scalars τ such that $t_i + \tau \in T$. The notation $\mathbf{t} + \tau$ implies that the scalar τ is added to all components of vector **t**.

We let $\mu(t) = E[X(t)]$ denote the time-dependent mean of the stochastic process. $\mu(t)$ is often called the **ensemble average** of the stochastic process. Applying the definition of strictly stationary process to the first-order CDF, we get $F(x; t) = F(x; t + \tau)$ or $F_{X(t)} = F_{X(t+\tau)}$ for all τ. It follows that a strict-sense stationary stochastic process has a time-independent mean; that is, $\mu(t) = \mu$ for all $t \in T$.

By restricting the nature of dependence among the random variables $\{X(t)\}$, a simpler form of the nth-order joint CDF can be obtained.

The simplest form of the joint distribution corresponds to a family of independent random variables. Then the joint distribution is given by the product of individual distributions[263].

Definition (Independent Process). A stochastic process $\{X(t) \mid t \in T\}$ is said to be an **independent process** provided its nth-order joint distribution satisfies the condition:

$F(\mathrm{x}; \mathrm{t}) = \prod_{i=1}^{n}(xi; t1)$

$$= \prod_{i=1}^{n} P[(X(t_1) \leq x_1] \tag{19}$$

As a special case, we have the following definition.

A **renewal process** is defined as a discrete-time independent process {Xn| n = 1, 2, . . .} where $X_1, X_2, \ldots$, are independent, identically distributed, nonnegative random variables.

As an example of such a process, consider a system in which the repair (or replacement) after a failure is performed, requiring negligible time. Now the times between successive failures might well be independent, identically distributed random variables $\{Xn \mid n = 1, 2, \ldots\}$ of a renewal process. Though the assumption of an independent process considerably simplifies analysis, such an assumption is often unwarranted, and we are forced to consider some sort of dependence among these random variables. The simplest and the most important type of dependence is the first-order dependence or **Markov dependence** [236,264].

3.6.1.2 Markov Chain

The stationery distribution is often discussed in the Markov chain. To obtain a clearer picture, let's assume that substation attacks consist of three states, as shown in Fig 3-2 depicted by [265].

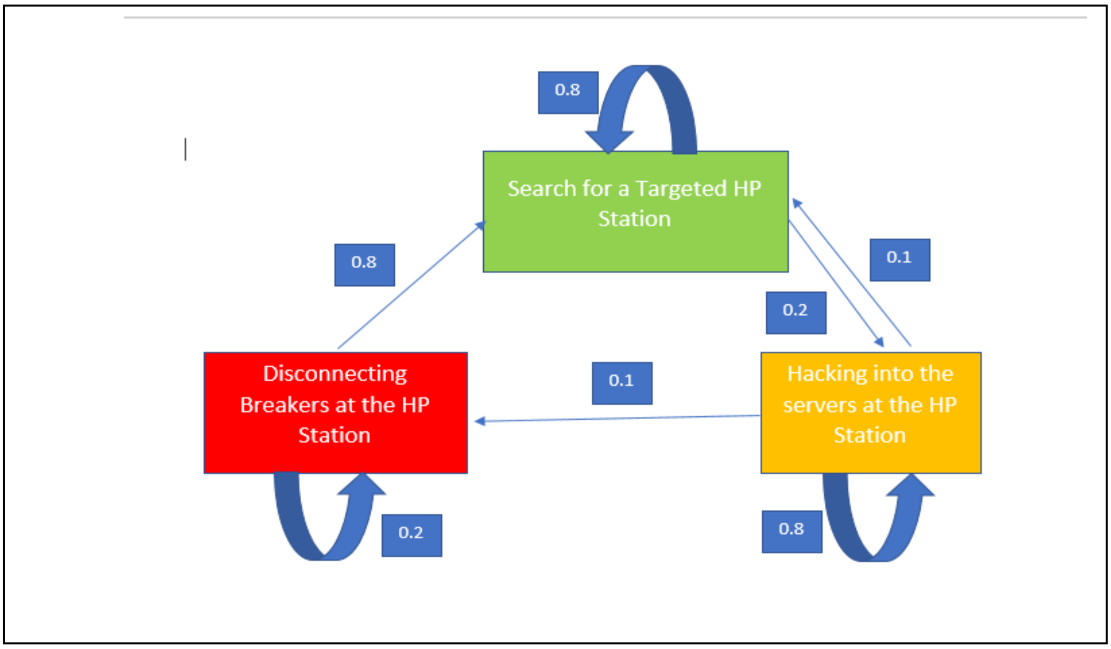

0.8
Search for a Targeted HP Station
0.8
0.1
0.2
Disconnecting Breakers at the HP Station
0.1
Hacking into the servers at the HP Station
0.2
0.8

Figure 3-2. Example of attack transitions to Hydro Power station network

In this example, the state space is represented as $S = \{S_1,S_2,S_3\}$ where,

S_1**:** Search for a Targeted Hydro Power station

S_2**:** Hacking into Servers at the Hydro Power station

S_3**:** Disconnecting Breakers at the Hydro Power station

When the state at time m is defined as $\{X_m\}$, the probability of this state, and the transition probability from one state to another is expressed as $P(X_m)$ and $P(X_{m+1}|X_m)$, respectively. In this example in Fig.3-2, $P(X_{m+1} = S_2|X_m = S_1) = 0.1$ and $P(X_{m+1} = S_2|X_m = S_2) = 0.8$.

The Markov chain is defined as Equation (20) using a state at time m, $\{X_m\}$.

$$P(X_{m+1}|X_m,...,X_1,X_0) = P(X_{m+1}) \tag{20}$$

The meaning of this equation can be summarized as two bullet points:

- X_{m+1} is determined by X_m only
- X_{m-1},X_{m-2},X_{m-3}... are nothing to do with X_{m+1}

In this example, it can be stated that disconnecting breakers is nothing to do with searching for the targeted HPstation but has much to do with cracking the server at the Hydro Power station only. These characteristics shown in Equation (20) are called Markov properties. When the Markov chain and its relevant theorems are used, the Markov property for the created Markov chain model needs to be tested first. If the Markov property is not justified, the Markov chain model needs to be further updated, and segmentalizing the states, *i.e.* increasing the number of states is known as a general countermeasure. Therefore, the Markov chain can be utilized, especially when the action flow or procedure is clarified.

3.6.1.3 Homogeneous Markov Processes

A Markov process {x(t)} is said to be homogeneous or stationary if the following condition holds[264].

$$\mathrm{P}[\mathrm{X}(\mathrm{t} + \mathrm{s}) = \mathrm{x}|\ \mathrm{X}(t_n + \mathrm{s}) = x_n] = \mathrm{P}[\mathrm{X}(\mathrm{t}) = \mathrm{x}|\mathrm{X}(t_n = x_n] \tag{21}$$

The equation expresses that a homogeneous Markov process is invariant to shifts in time.

In the case of a homogeneous Markov process, the particular instant t_n in Eq. (21) does not matter either so the future of the process is completely determined by the knowledge of the present state. In other words[264],

$$P_{ij}(\mathrm{t} - t_n) :=\mathrm{P}[\mathrm{X}(\mathrm{t}) = \mathrm{j}|\mathrm{X}(t_n) = \mathrm{i}] \tag{22}$$

Worse than that, an important implication is that the distribution of the sojourn time in any state must be memoryless. A hacker does not know how long he has been on the HPstation network! If you think about it, if the future evolution depends on the present state only, it cannot depend on the amount of time spent in the current state either [264].

When time is continuous, there is only one probability distribution $f_x(y)$ of the time y spent in a state which satisfies the property

$$P[X \geq y + s|X \geq s] = P[X \geq y] \tag{23}$$

and that is the negative exponential function

$$f_x(y) = \lambda e^{-\lambda y}, y \geq 0 \tag{24}$$

In other words, the sojourn times in a Continuous Time Markov Chain (CTMC) have an exponential probability distribution function. Similarly, for a Discrete Time Markov Chain (DTMC), the sojourn time η in a state must be a geometrically distributed random variable [264]

$$p_\eta(n) = P[\eta = n] = q^{n-1}(1 - q), n = 1,2,3, . . . ; 0 \leq q < 1. \tag{25}$$

with cumulative distribution function Fη (n)

$$F_\eta(n) = \sum_{k=1}^{n} Pn(k)$$

Note that when a process has an interarrival time distribution given by F_η (n) it is said to be a Bernoulli arrival process. Moreover, let η = nδ for n an integer and δ the basic unit of time[264]. Then the meantime is given by δ

$$\sum_{k=1}^{\infty} Kp\eta(k) = \frac{\delta}{(1-q)} \tag{26}$$

from which the mean arrival rate is $\frac{1-q}{\delta}$.

To decide whether a particular process is a Markov process, it suffices to check whether the distribution of sojourn times is either exponential or geometric and whether the probabilities of going from one state to another only depend on the state the process is leaving and on the destination state[264].

3.6.1.4 Discrete-Time Markov Chains

The case where the time spent in a Markov state has a discrete distribution whence we have a Discrete Time Markov Chain (DTMC). The stochastic sequence $\{X_n$|n = 0,1,2, . . .} is a DTMC provided that[264],

$$P[X_{n+1} = X_{n+1}|X_n = x_n, X_{n-1} = x_{n-1}, . . . , X_0 = X_0] = P[X_n+1 = x_n+1|x_n = x_n] \tag{27}$$

for n ∈ N.

The expression on the right-hand side of this equation is the one-step transition probability of the process and it denotes the probability that the process goes from state x_n to state x_{n+1} when the time (or index) parameter is increased from n to n + 1. That is, using the indices for notating the states [264],

P_{ij} (n,n + 1) = P[X_{n+1} = j|X_n = i]

The more general form of the sth step transition probabilities is given by

P_{ij}(n,s) = P[X_s = j|x_n = i]

which gives the probability that the system will be in state j at step s, given that it was in state i at step n where s ≥ n.

Note that the probabilities P_{ij} (n,s) must satisfy the following requirements:

0 < p_{ij} (n,s) ≤ 1, i,j = 1,2, . . . ,N; n,s = 0,1,2, . .

$\sum_{j \in S} p_{ij}$(n,s) = 1, i = 1,2, . . . ,N; n,s = 0,1,2, . . .

If the DTMC is homogeneous which will be the case in all of our discussions, the probability of various states m steps into the future depends only upon m and not upon the current time n; so that we may simplify the notation and write[264]

p_{ij}(m) = p_{ij}(n,n + m) = P[X_{n+m} = j|X_n = i]

for all m∈N. From the Markov property, we can establish the following recursive equation for calculating

p_{ij}(m) = $\sum_k p_{ij}$(m-1) p_{ij}(1), m = 2,3, . . . , (28)

We can write Eq. (29) in matrix form by defining matrix P = [p_{ij}], where $p_{ij} := p_{ij}(1)$, so that

$P^{(m)} = P^{(m-1)}$ P (29)

Where $P^{(0)}$ = I is the identity matrix.

Note that

$P^{(1)} = P^{(0)}$ P = IP

$P^{(2)} = P^{(1)}$ P = P^2

$P^{(3)} = P^{(2)}$ P = P^3

and in general

$P^{(m)} = P^{m}$, m = 0,1,2, . . . (30)

This equation enables us to compute the m-step transition probabilities from the one-step transition probabilities.

Next, we consider a very important quantity, the probability $\pi_j^{(m)}$ of finding our DTMC in state j at the m^th^ step:

$\pi_j^{(m)} = P[X_m = j]$ (31)

or, alternatively

$\pi_j^{(m)} = \sum_i \pi i^{(0)}\, pij^{(m)}$ (32)

That is, the state probabilities at time m can be determined by multiplying the multistep transition probabilities by the probability of starting in each of the states and summing over all states[264].

The row vector formed by the state probabilities at time m is called the state probability vector $\Pi^{(m)}$. That is,

$\Pi^{(m)} = (\pi_0^{(m)}, \pi_1^{(m)}, \pi_2^{(m)}\ldots\ldots)$

With this definition, Eq. (32) can be written in matrix form as follows

$\Pi^{(m)} = \Pi^{(0)} P^{(m)}$ m = 0,1,2, . . . (33)

To obtain a clear image, let's use the previous example in figure 3-2. In the transition probability matrix, P is expressed as Equation (28). It can be realized that the summation of each row is always one. In other words, the summation of the probabilities from one state to another (including the same state) needs to be always one. This is an important property that the Markov chain owns.

$$P = \begin{bmatrix} 0.9 & 0.1 & 0 \\ 0.1 & 0.8 & 0.1 \\ 0.8 & 0 & 0.2 \end{bmatrix} \quad (34)$$

Assume that our hacker starts at state (search for the target HPstation). In other words, the initial distribution is $\Pi^{(0)} = (1,0,0)$. From discovering the hydropower station the hacker can go to hacking the server at the HPstation and further disconnect circuit breakers at the HPstation with equal probability, i.e.,

$$\Pi^{(1)} = (1,0,0) \begin{bmatrix} 0.9 & 0.1 & 0 \\ 0.1 & 0.8 & 0.1 \\ 0.8 & 0 & 0.2 \end{bmatrix} = (0.9,0.1,0)$$

from Eq. (34) and so on.

If we analyzed further, the vector Π(m) of state probabilities tends to a limit of $m \to \infty$. Even more, one can show that for specific DTMCs the effect of Π(0) on the vector Π(m) completely vanishes.

Steady-State Distribution

The most interesting DTMCs for performance evaluation are those whose state probability distribution $\pi_j^{(m)}$ does not change when of $m \to \infty$. or to put it differently, a probability distribution π_j defined on the DTMC states j is said to be stationary (or have reached a steady-state distribution) if $\pi_j^{(m)} = \pi_j$ when $\pi_j^{(0)} = \pi_j$, that is, once a distribution π_j has been attained, it does not change in the future (with m)[263].

The steady-state probability distribution { π_j; $j \in S$} of a DTMC by

$$\pi_j = \lim_{m \to \infty} \pi_j{}^m$$

In an irreducible and aperiodic homogeneous MC the limiting probabilities π_j always exist and are independent of the initial state probability distribution. Moreover, either[263]

1. all states are transient or all states are recurrent null. In both cases $\pi_j = 0 \ \forall$ j and there exists no steady-state distribution, or

2. all states are recurrent nonnull and then $\pi_j > \forall$ j, in which case the set $\{\pi_j\}$ is a steady-state probability distribution and

$$\pi_j = \frac{1}{M_j} \tag{35}$$

Where M_j is the mean recurrence time of state j, given by equation 37,

$$M_j = \sum_{m=1}^{\infty} m f_j^{(m)} \tag{36}$$

The mean recurrence time is thus the average number of steps needed to return to state j for the first time after leaving it. $f_j^{(m)}$ is the probability of a Markov process leaving a state j and first returning to the same state j in m steps[264].

In this case, the quantities π_j are uniquely determined through the following equations

$$\sum_i \pi_i = 1 \tag{37}$$

$$\sum_i \pi_i p_{ij} = \pi j \tag{38}$$

A recurrent nonnull DTMC is also referred to as an ergodic MC and all the states in such a chain are ergodic. The limiting probabilities πj of an ergodic DTMC are referred to as equilibrium or steady-state probabilities. It should be clear that if we observe an ergodic MC for a fixed time T, the average sojourn time spent in state i by the DTMC during T can be computed from [264]

$$\bar{\tau} = \pi_i \text{ T} \tag{39}$$

Another quantity that will be useful to us is the average time v_{ij} spent by the DTMC in state i between two successive visits to state j in steady-state. This quantity is also known as the visit ratio or mean number of visits and can be computed from [264]

$$v_{ij} = \frac{\pi_i}{\pi_j} \tag{40}$$

3.6.2 Petri Nets and GSPNs

A PN also called a place transition net, is a pictorial mathematical model of information flow named after its developer, Petri [264].

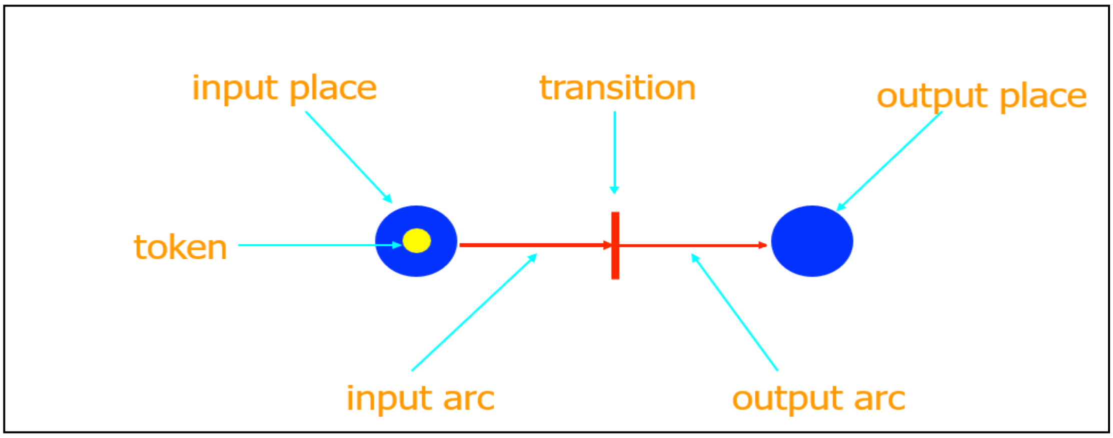


Figure 3-3. Basic Components of a Petri Net before firing

The parts of a PN are depicted in Figure 3-3 as a collection of locations represented by circles, a collection of transitions represented by bars, and a collection of directed arcs. Places and transitions are connected by arcs that run from one to the other. Tokens can be obtained in various locations and are graphically depicted as dots residing in circles. Each position in a marking may have zero or more tokens. The model's status is represented by marking at a particular time. This notion serves as the basis for PNs[263],[264].

A transition is deemed enabled when each of its input places has at least as many tokens as the multiplicity of the corresponding input arc. See figure 3-4 for an illustration of a token being fired[263],[264]. When a transition is enabled, it can execute. When a transition executes, some tokens equal to the input arc's multiplicity are taken from each of the input locations and some tokens equal to the output arc's multiplicity are deposited in each of the output places.

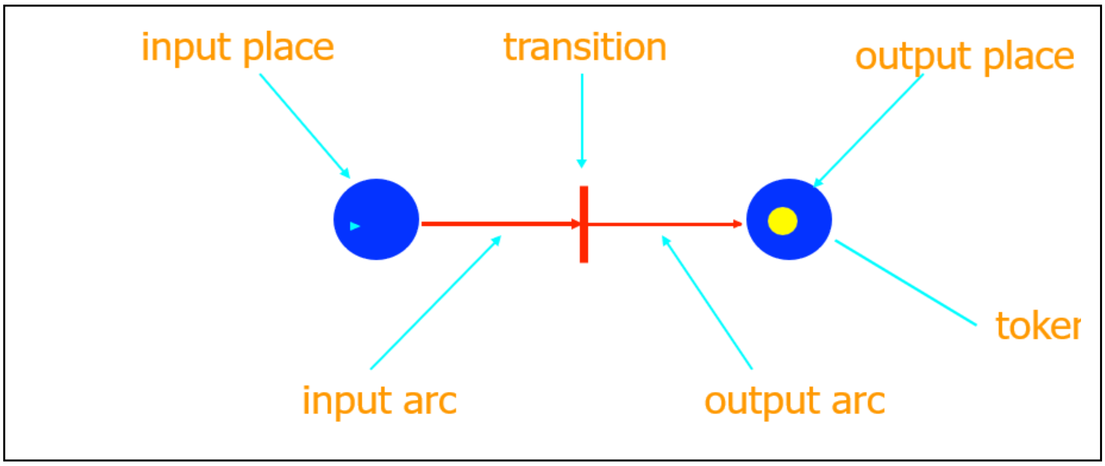


Figure 3-4. The basic components of a Petri Net after firing

In PNs, firing order is a significant problem. When two transitions are enabled in a PN marking, they cannot be fired "at the same time"; instead, a decision must be taken regarding which transition to fire first, with the other transition able to do nothing more than remaining enabled. A transition firing may change a PN's marking from one to another. The set of all markings that can be reached from a given initial marking, M0, through any firing sequences of transitions is known as the reachability set. The reachability graph of a PN, in which each marking in the reachability set is a node and the arcs indicate potential marking-marking transitions, can fully characterize the history of a PN [266, 267]. Arcs are labeled with the name of the transition whose firing caused the associated changes in the marking.

An enabled transition fires by removing one token in each input place and generating one token in each output place. The execution of a PN is controlled by the movement of tokens, while the distribution of tokens over places is denoted by a marking corresponding to the notion of a state in a Markov chain. A PN is defined as follows [263].

Definition 1*:* A PN is a four-tuple (P, T, A, and M_0), where:

1) P = $\{P_1, P_2, \ldots, P_n\}$ is a set of places;

2) T = $\{t_1, t_2\}, \ldots, t_n\}$ is a set of transitions;

3) A ⊆ {P × T} ∪ {T × P} is an arc set;

4) M_0 = $(m_{01}, m_{02}, \ldots, m_n)$ is the initial marking.

A GSPN defines two different classes of transitions: 1) immediate transitions (drawn as boxes) and 2) timed transitions (drawn as bars). In a GSPN, an enabled immediate transition fires immediately, whereas an enabled timed transition fires after an exponentially distributed firing time. The state space is then divided into two subsets, one containing vanishing states (markings), which enable at least one immediate transition, and the other containing tangible states (markings), which enable only timed transitions. A GSPN is said to be k-bounded if, for any marking, the maximum number of tokens in any place is less than or equal to k. Therefore, a k-bounded GSPN is isomorphic to the continuous-time Markov chain and the quantitative analysis of GSPNs can be transferred to that of Markov models [263]. The definition of a GSPN is given as follows.

Definition 2: A GSPN is a four-tuple (P_N, T1, T2, and λ), where:

1) P_N = (P, T, A, M_0) is the underlying place transition net;

2) $T_1 \subseteq$ T is a set of timed transitions;

3) $T_2 \subset T$ is a set of immediate transitions;

4) $T_1 \cap T_2 = \varphi$, $T_1 \cup T_2 = T$;

5) $\lambda = (\lambda_1, \lambda_2, \ldots \lambda_k)$ is a set of nonnegative real numbers:

a) λ_1 denotes a firing rate if $t_1 \in T_1$

b) λ_2 denotes a firing weight if $t_2 \in T_2$

PNs and GSPNs are versatile and hence, find them applicable in a variety of systems engineering. The locations stand in for the system's statuses or resources. The transitions stand in for the occasions that permit state transfer in the system. The arcs show how the locations and transitions relate to one another. The SPN is more effective at preserving resources like time and energy than alternative plans like prototype design. In light of this, we opt to use the SPN in the system modeling and analysis.

1. The target system's performance evaluation model needs to be built first. Depending on the system being studied. As a result, we provide an example model immediately, as seen in Figure 3-5.

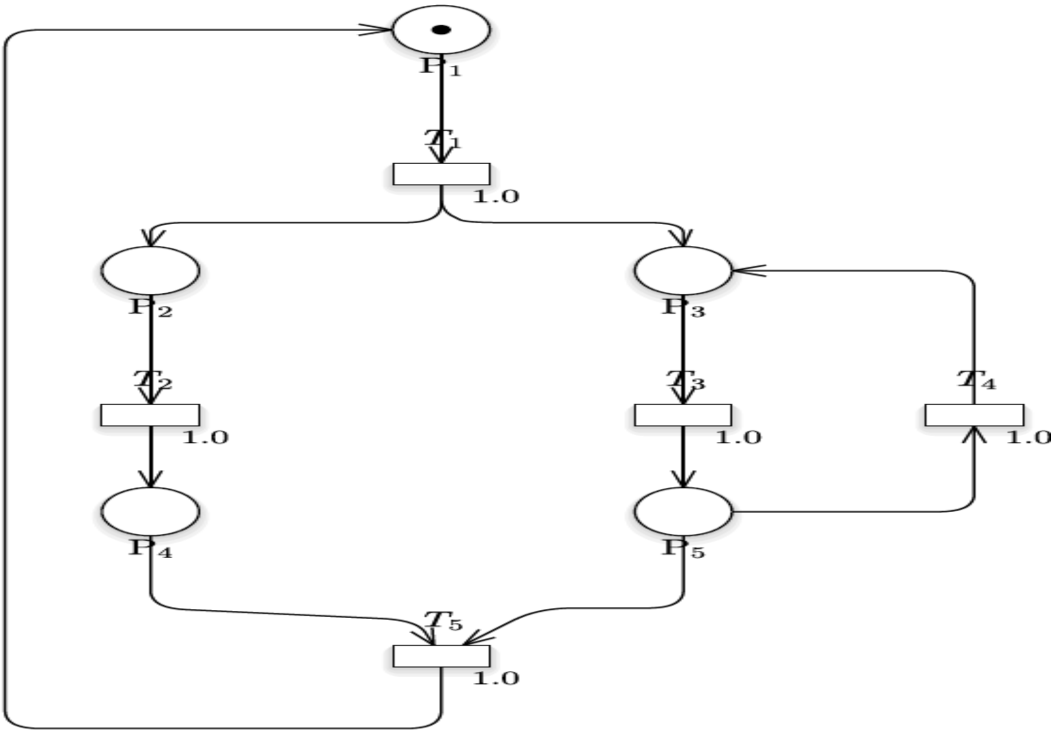


Figure 3-5. A sample of the Stochastic Petri Nets (SPN) model

2. The target system's performance evaluation model needs to be built first. Depending on the system being studied. As a result, we provide an example model immediately, as seen in Figure 52. $\lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}$. Lastly, we get the MC by replacing the transition t_i with the corresponding λ_i. The reachable markings set and the MC of the simple SPN model above are shown in Table 3-4 and Figure 3-6.

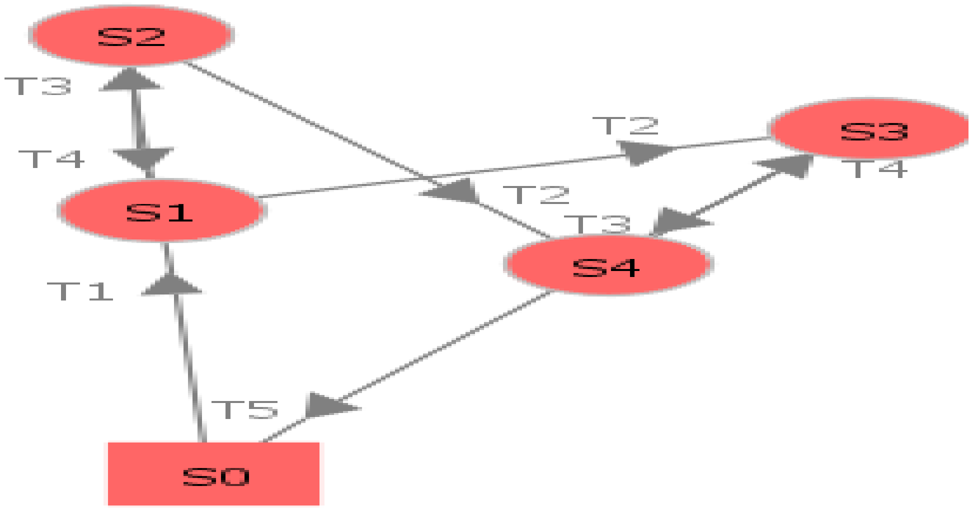


Figure 3-6.The reachability graph of the sample SPN

Table 3-4. Reachable markings' set of the sample.

	P1	P2	P3	P4	P5
M0	1	0	0	0	0
M1	0	1	1	0	0
M2	0	1	0	0	1
M3	0	0	1	1	0
M4	0	0	0	1	1

3. Thirdly, we can work on the system performance evaluation with the steady-state probability based on the MC. Some formulas help the theoretical inference. They are as follows.

We can get the steady probability of each state by resolving the system of linear equations derived above.

Ulteriorly, we can get further parameters, such as:

(1) Residence time in each state M:

$$\tau(M) = (-r_{i,j})^{-1} = (\sum_{tj \in H} \lambda j)^{-1} \tag{41}$$

Where H is the transitions' set that can be enforceable at M.

(2) Token density function:

$$\mathrm{P[M(P) = i] = \sum_j P[M_j]} \tag{42}$$

Where, $M_{j\in}[M(p) = i], M_j(p) = i$

(3) Average number of tokens in a place:

$$\bar{u}_i = \sum_j x\, P[M(p_i) = j \tag{43}$$

The average number of tokens of a place set P_i is the sum of each place's average number of tokens.

It can be expressed as:

$$\bar{N} = \sum_{Pi \in Pi} \bar{u}_i \tag{44}$$

Where the place is $P_i \in P_j$.

(4) Utilization rate of the transition:

$$U(t) = \sum_{M\in E} PM \tag{45}$$

There, E represents the set of all reachable markings that make t enforceable.

(5) Token velocity of the transition:

$$R(t,s) = W(t,s)xU(t)x\lambda \tag{46}$$

There, λ stands for the average transition firing rate of t. Based on all the performance parameters mentioned above, we can do further research on the system response time and so on.

3.6.3 Representation of System States (State of each Unit)

An industrial system is made up of several subsystems or units $(U_1, U_2, \dots U_n)$. The domino effect analysis framework divides each unit into four stages:

1. State1, Normal state (N),
2. State2, Vulnerable state (V),
3. State3, Failure state (F)
4. State4, Restored state (R).

Masked compromised state, undiscovered compromised state, triage state, fail-secure state, and graceful degradation state are examples of intermediate stages between Normal and Restored. The intermediate phases are merged into the failed state for the sake of simplicity.

3.6.3.1 The transition between the System States

Considering two units, the transitions may take place from state 1 to state 2,3, and/or state 4.

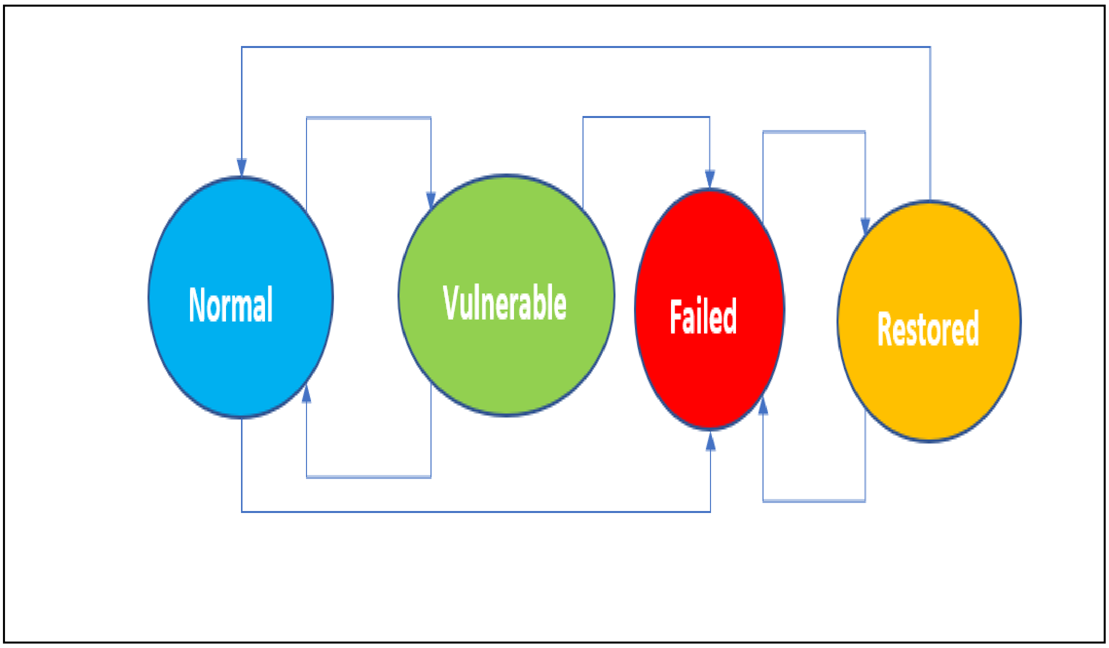


Figure 3-7. Description of system states

Given the stochastic nature of attacks, a transition into state V can be characterized as an exponential distribution with the rate λ_{NV} when the system is in state N. (commonly referred to as zero-day attacks). This is because once the system's security is compromised (state V), the chances of a serious attack increase, and the system goes to state F. To replicate the duration spent in state V, which simulates a generally increasing rate of failure, a Weibull distribution (shape parameter θ, scale parameter β) with θ_{VF}, $\beta_{VF} > 1$ is utilized.

The unsuccessful attacks mimic a decreasing failure rate, and the transition from V to N is modeled as a Weibull distribution with θ_{VF}, $\beta_{VF} < 1$. The change from N to F reflects an insider assault based on past system information, which is likewise considered to be stochastic and described using exponential distributions with λ_{WF}. When system operators uncover malicious attempts, they disconnect the systems and install fixes to address the vulnerabilities. The system now enters the recovery phase. Transitions from F to R or R to F are considered stochastic for both successful and unsuccessful patch installations.

Given the sophistication and novelty of zero-day attacks, a rapid mitigation method may not be easily available. An exponential distribution is used to modify the transition from R to W. The fundamental idea is to use non-exponential distributions to model activities involving increasing or decreasing the rate of failures, and exponential distributions to model stochastic actions.

Table 3-5 summarizes the cumulative distribution functions (CDF) of time spent in various states. The steady-state probability π_i is derived using the state transitions.

Table 3-5. The cumulative distribution functions (CDF) of time spent in various states.

CDF	**Distribution**	**Parameters**	**Expression**
$\boldsymbol{P_{NV}}$	Exponential	λ_{NV}	1- $e^{-\lambda_{NV}t}$
$\boldsymbol{P_{NF}}$	Exponential	λ_{NF}	1- $e^{-\lambda_{NF}t}$
$\boldsymbol{P_{VN}}$	Weibull	θ_{VN}, β_{VN}	1- $e^{-(\frac{t}{\beta_{VN}})\theta_{VN}}$
$\boldsymbol{P_{VF}}$	Weibull	θ_{VF}, β_{VF}	1-$e^{-(\frac{t}{\beta_{VF}})\theta_{VF}}$
$\boldsymbol{P_{FR}}$	Exponential	λ_{FR}	1- $e^{-\lambda_{FR}t}$

$\boldsymbol{P_{RF}}$	Exponential	λ_{RF}	1- $e^{-\lambda_{RF}t}$
$\boldsymbol{P_{RN}}$	Exponential	λ_{RN}	1- $e^{-\lambda_{RN}t}$

The steady-state probabilities describe the fraction of time the system spends in different states over the whole assault horizon, i.e. The semi-Markov Process is then meticulously mathematically modeled.

Starting with the failure of at least one unit as the starting event, one can study the domino effect sequence. At least one unit, according to the assumption, has failed.

3.6.3.2 Sojourn Time and Transition Probability of Semi-Markov Process

The semi-Markov Process is then meticulously mathematically modeled. The steady-state probabilities describe the fraction of time the system spends in different states over the entire assault horizon.

The domino effect sequence can be studied by starting with the failure of at least one unit as the initiating event. According to the presumption, at least one unit has failed.

(1) J = (J_m)m ∈ N where (J_m) is the system state at the mth time,

(2) S =(S_m)m ∈ N where (S_m) is the mth transition time and

(3) X = $(X_m)m \in N$ where (X_m) = (S_m) $-$ (S_{m-1}) is the sojourn time in the state (J_{m-1}). The chain (J_m, S_m)n ∈ N is a Markov renewal chain if ∀ m ∈ N,

$$P((J_{m+1}) = j,\ S_{m+1} - S_m = k|J_0, S_0,\ldots, J_m, S_m)$$

$$P((J_{m+1}) = j,\ S_{m+1} - S_m = k|J_m) \tag{47}$$

Equation ten shows that the next transition state and time spent in the current state are completely dependent on the system's current state. The semi-Markov chain is a type of Markov chain. Z = (Z_k)k ∈ N associated with the Markov renewal process (J, S) is $Z_k = J_{N(k)}$. N represents the number of transitions that occur during time k. The average sojourn period for the SMP in each state is derived using the formula[263]:

$$t_i = \int_0^{\infty} (1 - P_{ij(k)})\ (1 - P_{ik(k)})\, \mathrm{dk} \tag{48}$$

where j; k is reachable states from i and ($1 - P_{ij(k)}$) is the duration of the sojourn in the state i's survival function.

With an exponential distribution, the sojourn time in state N can be expressed as, for example, using equation (49).

$$t_i = \int_0^{\infty} (P_{NV}) \; (P_{NF}) \, \mathrm{dt} = \int_0^{\infty} (e^{-(\lambda_{NV}+\lambda_{NF})\mathrm{t}} \, \mathrm{dt} \tag{49}$$

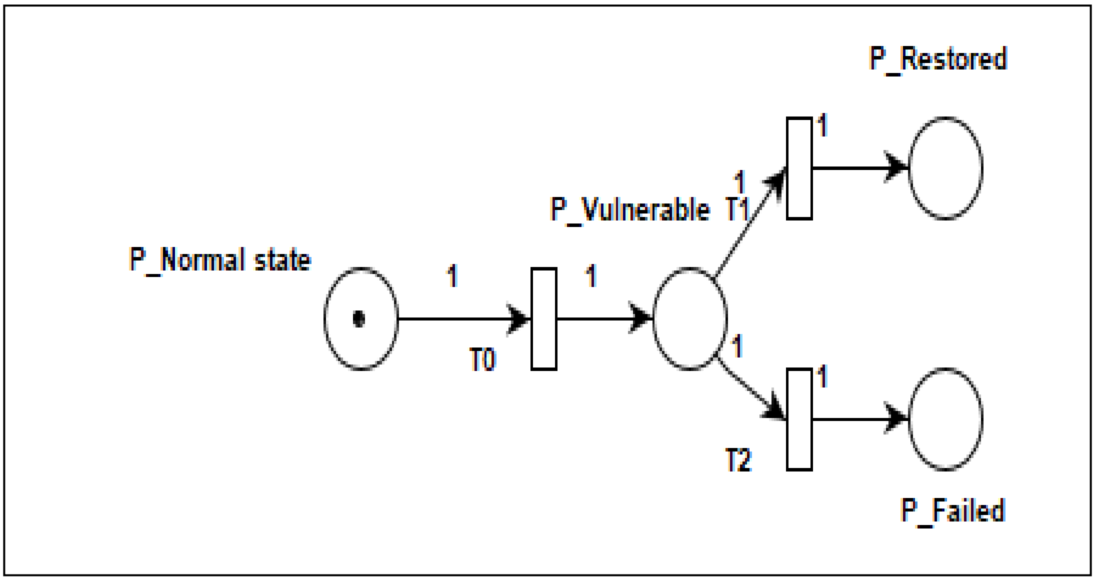


Figure 3-8. The GSPN for the unit states

A transition probability matrix Q is defined for the evolution of this SMP. The elements of Q = Q_{ij}(k) are defined as, and they indicate the likelihood of transitioning from a state i to a state j within time k [263].

$$Q_{ij}(k) = \mathrm{P} \; (J_{n+1} = \mathrm{j}, \, X_{n+1} \leq \mathrm{k} | J_n = i) \tag{50}$$

The constituents of the kernel Q can be evaluated as P_{ij} signifies the cumulative distributions of the sojourn time in state I corresponding to the following state j.

$$Q_{ij}(k) = \int_0^{k} (1 - P_{ik(k)}) \; \mathrm{d}P_{ik(k)} \tag{51}$$

where j; k is reachable states from I and (1 - P_{ij}(k)) is the sojourn time survival function in state i. The transition probability matrix Q can be written as, as seen in equation 52.

$$\mathrm{Q} = \begin{vmatrix} 0 & QNV & QNF & 0 \\ QVN & 0 & QVF & 0 \\ 0 & 0 & 0 & QFR \\ QNV & 0 & QRF & 0 \end{vmatrix} \tag{52}$$

The one-step transition probability matrix in the steady-state analysis of the SMP is computed as M = Q (∞), assuming state transitions are time-independent. After that, by solving the set of linear equations with M, the steady-state probability vector of the embedded Markov chain v = $\{v_1, v_2, ---- v_n\}$ may be obtained.v = v_M with $\sum_{i=1}^{n} v_i = 1$. The steady-state probabilities π_i are then evaluated as [263];

$$\pi_i = \frac{v_i t_i}{\sum_\delta v_i t_i}, \mathrm{i} \in \delta \tag{53}$$

Unit States

Each unit can be described by a state graph represented by basic (elementary) Stochastic Petri Nets as a result of the preceding procedures. The units in place P1 are in normal operation. The vulnerable buses are housed in P2. P3 is where the buses that have been recovered are kept. P4 is the location of the failed buses, and it is a source of hazard for the adjacent apartments (see Figure 3-8).

Firing conditions

According to the preceding procedures, a primary scenario resulted in the catastrophic failure of one bus, which may have generated a system disruption that impacted other nearby units. The firing of transitions simulates the evolution of system behavior, with each transition firing matching the occurrence of an event. Similarly, an event alters the system state, causing transition fires and, eventually, changes to the Stochastic Petri Net marking.

Failure probability/mitigation probability

According to figure 3-8, the failure probability ($\boldsymbol{P_{CFi}}$) for each bus may be calculated as the firing probability of the transition T2. The mitigation probability of the unit Bi is the firing probability of the transition T1 knowing that the transition T0 is fired.

Domino scenario probability

While the failure probability, PBi, is known for each unit, The chance of a domino effect can be computed for the entire system. The likelihood of each domino scenario (domino sequence) can be calculated as follows:

$$\boldsymbol{P_{CF} = \prod_{j=1}^{n} P_{Bi}} \tag{54}$$

P_{CF} is the joint probability that each unit in sequence i fails, and n is the number of failed units in the domino sequence, where n is the number of failed units in the domino sequence.

3.7 Modelling False Data Injection Attacks

3.7.1 FDIA on the Communications System

In a wind power plant, there are multiple points of vulnerability where the external intruder will gain access using physical and cyber means. This is a huge concern in wind farms as they are housed in remote locations and each turbine in a ring is a part of the same broadcast domain. The Modbus/TCP, Ethernet/IP, ICCP DNP3 protocol, and IEC 61850 are commonly used in a transmission control network [266]. The network is separated from the operations network, and the SCADA (DNP3 or other) protocol is not encrypted and has limited authentication and authorization. The wide area control network is vulnerable to multiple network intrusions such as Man-in-the-Middle (MitM), signal jamming, sniffing, spoofing, and Denial-of-Service (DoS) [267-270]. Having control over a single communication infrastructure inside the domain will expose the entire power infrastructure network. A cyber breach in a single turbine opens the channel to intercept command and control messages throughout the network. The effect can escalate from the failed operation of a single turbine to hundreds of wind turbines within the network. The attacker can obtain information about devices, protocols, network topology, and control architecture; can manipulate the control operations; and key physical components of power systems like turbines, relays, breakers, transformers, and other metering equipment. The attacker can use the same access point to gain access to the substation control network and disrupt the operation of the entire power grid. The attacker with physical access to a substation can connect to the transmission control network and alter the electric power collection, configuration, and delivery.

The mathematical representation of the physical and cyber layers for these cases follows the following relation.

$$(t+1) = G * x(t) + B * u(t) \tag{55}$$

$$(t) = C * x(t+1) + e \tag{56}$$

$$(t+1) = H * y(t) \tag{57}$$

Where (t) represents the state variables, $u(t)$ represents the control variables, $y(t)$ represents the system measurements at time t and e is the measurement error. G, B, C, and H are namely system matrix, input matrix, output matrix, and control matrix. The attack scenario is represented in state equation form as follows,

$$(t+1) = G * x(t) + B * [u(t) + \Delta u(t)] \tag{58}$$

$$(t) = C * [x(t+1) + B * \Delta u(t)] + e \tag{59}$$

Fig. 3-9 shows the diagrammatic representation of the above-stated variables of the system. The presence of the cyber intruder will intend to modify the control variables and system measurements. Besides modifications, the control signals can also be delayed or fabricated with dummy variables.

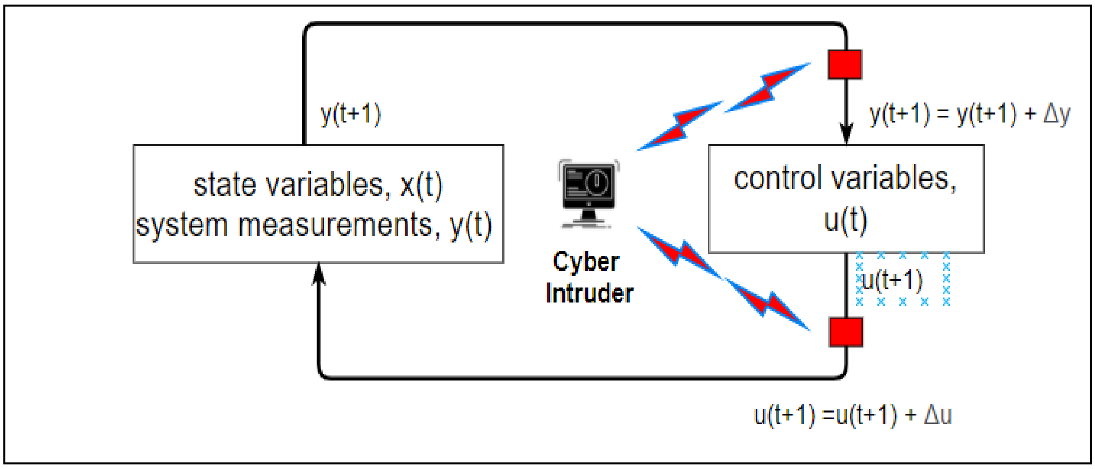


Figure 3-9. Presentation of the variables used

1) Denial of Service (DoS) Attacks

The DoS attack is the intentional act of targeting the memory and/or computational resource of the victim device by overwhelming the device with a large volume of traffic. It aims to disrupt the service to authorized users by feeding a large number of fake service requests and consuming the operating resource of the target device [271]. For example, the excessive flow of packets into the control node will pause/stop the inflow or outflow nodes impacting time-critical events. The attack affects the wide area of voltage stability, monitoring, and control application of the modern power grid. The impact of DoS attacks on the stability of dynamic systems can be represented using non-linear differential equations. The attack occurs mainly in the path between the controller and the actuator. The measurement vectors for controller nodes (C) and actuator nodes (A) can be represented as y(t) and u(t). The DoS on a subset of these nodes is given as:

$$U = \begin{cases} 0, \ \forall\, t \in A \\ u(t), \ \forall\, t \notin A \end{cases} \tag{60}$$

$$Y = \begin{cases} 0, \ \forall\, t \in C \\ y(t), \ \forall\, t \notin C \end{cases} \tag{61}$$

With the attack, the arbitrary signals (Δ) are sent, and the DoS on each of these nodes are:

$$U = \begin{cases} \Delta, \ \forall\, t \in A \\ u(t), \ \forall\, t \notin A \end{cases} \tag{62}$$

$$Y = \begin{cases} \Delta, \ \forall\, t \in C \\ y(t), \ \forall\, t \notin C \end{cases} \tag{63}$$

Consider α(t) to be the attack schedule at time t, where η is the success probability factor and α is 1 for a DoS attack and 0 for no attack.

$$\alpha(\mathrm{t}) = \begin{cases} 1, \ \forall\, t \in A, C \ with\, probability\, of\ 1 - \eta \\ 0, \ \ \forall\, t \notin A, C \ with\, probability\, of\ \eta \end{cases} \tag{64}$$

2) **Man-in-the-Middle (MitM) Attack**

The attack exploits the security vulnerabilities of the network by intercepting the data traffic transmitted between two nodes. It is active eavesdropping where the attacker compromises the communication between two endpoints and relays false information between them. In MitM attacks, the attacker maliciously intercepts and modifies (delays, blocks, and/or injects data) flow between communication nodes in CPS. In the real world, utilities use UDP protocol following IEEE C37 to exchange PMU data which increases the vulnerability to the MITM attack [272 and 273]. The MitM attack can be represented as the polynomial under some conditions on the parameter set. If false data injected $\dot{z}$ gets successful in MitM attacks with $(\dot{a}, \dot{b}, \dot{z}) = (0, 0, \dot{v})$, the error vector $\dot{v}$ introduced in the input signal (a, b, z) by sending $z + \dot{v}$ instead of z. The final consequence of the attack is an m-bit message manipulated by a noise vector in which each bit has the probability of η of being 1. For successful false data injected in each bit with a probability of $P(m - n)$, the n-bit positions not in support of the error vector are manipulated with a probability of [274],

$$\eta_n = \frac{\sum_{i=0}^{t}(i\binom{n}{i}\eta^{i}(1-\eta)^{n}\sum_{j=0}^{t-i}\binom{m-n}{j}\eta^{m-n-j}(1-n)^{j})}{n*P(m-n)} \tag{65}$$

The other bit positions in support of the error vector are manipulated with the probability of,

$$\eta_{m-n} = \frac{\sum_{i=0}^{t}(\binom{n}{i}\eta^{i}(1-\eta)^{n-i}\sum_{j=0}^{t-i}\binom{m-n}{j}\eta^{m-n-j}(1-n)^{j})}{(m-n)*P(m-n)} \tag{66}$$

3) **Modify Packets Attack**

The attack works by compromising the device node within the network and modifying the live data streams passing through the node. This will cause the system to operate abnormally. The modification parameter includes the message payload and delivery time of application packets.

a) Add-Offset: It adds a targeted increment of bytes within the payload. With the attack, the arbitrary signals at time t, $\alpha(t)$ are sent, and the packet modification on measurement vectors of the controller and actuator nodes are:

$$U = \begin{cases} u(t) + \alpha(t), \ \forall\, t \in A \\ u(t), \ \forall\, t \notin A \end{cases} \tag{67}$$

$$Y = \begin{cases} u(t) + \alpha(t), \ \forall\, t \in C \\ y(t), \ \forall\, t \notin C \end{cases} \tag{68}$$

b) Compress/Multiply: It compresses or multiplies the packet stream by dropping a specified fraction of packets. For a given factor of α,

$$\alpha = \begin{cases} \alpha > 1, \ \rightarrow Multiply \\ 0 < \alpha < 1, \ \rightarrow Compress \end{cases} \tag{69}$$

The packet modification on measurement vectors of the controller and actuator nodes are:

$$U = \begin{cases} \alpha * u(t), \ \forall\, t \in A \\ u(t), \ \forall\, t \notin A \end{cases} \tag{70}$$

$$Y = \begin{cases} \alpha * u(t), \ \forall\, t \in C \\ y(t), \ \forall\, t \notin C \end{cases} \tag{71}$$

c) Delay: It delays the delivery time of application packets by a specified time. For a given time delay factor of δ, the packet modification on measurement vectors of the controller and actuator nodes are:

$$U = \begin{cases} u(t-\delta), \ \forall\, t \in A \\ u(t), \ \ \forall\, t \notin A \end{cases} \tag{72}$$

$$Y = \begin{cases} u(t-\delta), \ \forall\, t \in C \\ y(t), \ \ \forall\, t \notin C \end{cases} \tag{73}$$

δ represents a discrete constant delay or a time-varying delay function.

d) Invert: It inverts the sequence of bytes within the payload. The packet modification on measurement vectors of the controller and actuator nodes are:

$$U = \begin{cases} 0, \ \forall\, t \in A \\ \overline{u}(t), \ \ \forall\, t \notin A \end{cases} \tag{74}$$

$$Y = \begin{cases} 0, \ \forall\, t \in C \\ \overline{y}(t), \ \ \forall\, t \notin C \end{cases} \tag{75}$$

Where the overhead bar for vectors represents the inverted sequence of bits.

e) Replace: It replaces the bytes of the payload with different values. The packet modification on measurement vectors of the controller and actuator nodes are:

$$U = \begin{cases} \overline{(u \oplus x)(t)}, \ \forall\, t \in A \\ u(t(, \ \ \forall\, t \notin A \end{cases} \tag{76}$$

$$Y = \begin{cases} \overline{(y \oplus x)(t)}, \ \forall\, t \in C \\ y(t), \ \ \forall\, t \notin C \end{cases} \tag{77}$$

3.7.2 Modeling the FDIA on the Control System – Laplace Domain Attack Model

To derive the attack impact model, we use Fig. 3-10 to incorporate more details. Several symbols in Fig.3-10 are defined as follows. For an N-area grid, denote by ℓij a virtual tie-line from area i to area j. The power flow over ℓij is the sum of power flows over all the real tie-lines from area i to area j. For instance, Fig. 3-10 (c) illustrates the virtual ie-lines of the three-area grid in Fig. 3-10. Denote by Δωi and Δpi the frequency deviation and the change of load in area i, respectively; Δω the average of the frequency deviations of all the areas; Δp = [_$\Delta p_1, . . . ,\Delta p_N]^T$. Suppose there are a total of L virtual tie-lines. Let T represent an L×m matrix (m is the number of power flow sensors) that consists of −1, 0, and 1, and aggregates the real tie-line power flows in z as virtual tie-line power flows. That is, an element of Tz is the power flow over a virtual tie-line. Following existing approaches [275], we model the two sets of generators under and out of AGC in an area as two virtual generators, respectively. Fig. 3-10 shows a block diagram of a widely adopted Laplace-domain model [275] for the two virtual generators. Other symbols in Fig. 3-10 are briefly explained in the figure caption.

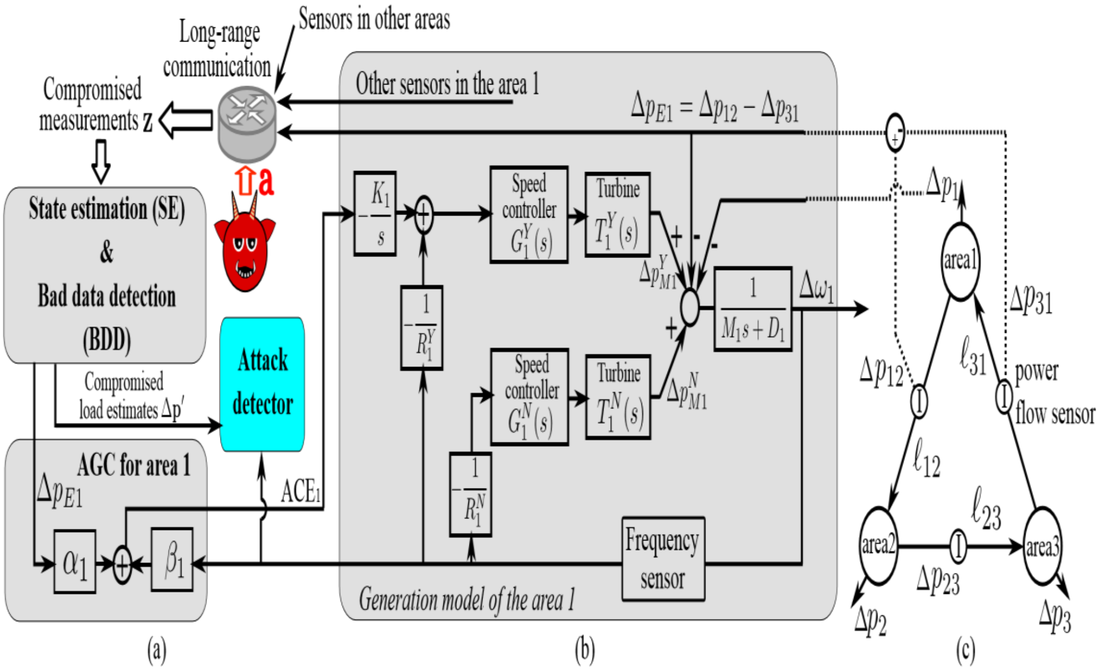


Figure 3-10. The attack model for the AGC

(a) SE, BDD, AGC programs, and attack detector discussed in Section VI; (b) Block diagram of the generation model for area 1; (c) Virtual tie-lines of the three-area grid in Fig. 1. Notation explanation: Δp_{ij} is the deviation of the power flow over ℓij from its scheduled value; Gi(s) and Ti(s) are transfer functions of the speed controller and the turbine of a generator, respectively; ΔpM_{ij} is a change of input mechanical power; gain Ki; droop constant Ri; total generator inertia Mi; load-damping constant Di; superscripts 'Y ' and 'N' modify the symbols for the generators under and out of AGC, respectively.

From a control-theoretic perspective, in the presence of FDI attacks, an AGC system can be viewed as an open-loop system with the load change Δp and the FDI attack vector a as the inputs, and the frequency deviation Δω and the area power export deviations as the outputs. In this section, we treat $\breve{a}$ as a vector of continuous-time variables. Denote by s the Laplace coordinates and $\breve{x}$ the Laplace transform of x. Based on the model in Fig. 3-10, the output ω is given by the following equation (a detailed derivation can be found in Appendix A):

$$\widehat{\Delta\omega} = \theta^{\intercal}\mathbf{\Phi}^{-1}\widehat{\Delta p} + \theta^{\intercal}\mathbf{\Phi}^{-1}\mathbf{\Lambda\Psi T a}e, \qquad (78)$$

(Let T represent an L × m matrix (m is the number of power flow sensors) that consists of −1, 0, and 1, and aggregates the real tie-line power flows in z as virtual tie-line power flows, $\mathbf{\Psi}$ is an $N \times L$ matrix consisting of −1, 0, and 1; $\mathbf{\Phi}$ is an $N \times N$ matrix and its elements are expressions of the generators' transfer functions, $\mathbf{\Lambda}$ = diag($s \cdot n_1 - 1$,...,$s \cdot n_N - 1$)

We proposed a linear regression model based on a key observation from Eq. (78). Based on the additive property, we propose a linear regression-based attack impact model. Let Δω(k), Δpk, and a_k denote the grid frequency deviation, the load change vector, and the attack vector in the kth AGC cycle, respectively. The model is given by

$$\Delta\omega(k) = \sum_{h=0}^{H-1} U_h^T \,\Delta p_{k-h} + \, V_h^T \, T_{a_{k-h}} \tag{79}$$

where H is the horizon of the regression, $\mathbf{u}_h \in \mathrm{R}^{N\times1}$ and $\mathbf{v}_h \in \mathrm{R}^{L\times1}$ are the coefficients that "encode" the coefficients $\theta^\intercal\mathbf{\Phi}^{-1}$ and θ⊺Φ−1ΛΨ in Eq. (78). Eq. (79) preserves the additive property of Eq. (78).

The MSE is a commonly used loss function for regression problems, where the goal is to predict continuous values

$$MSE = \frac{1}{N}\sum_{k=1}^{N} e_k^2 \tag{80}$$

3.8 Modeling the Impact of Cyber Attack on the Power Grid

3.8.1 Review of the Four-Bus Test System

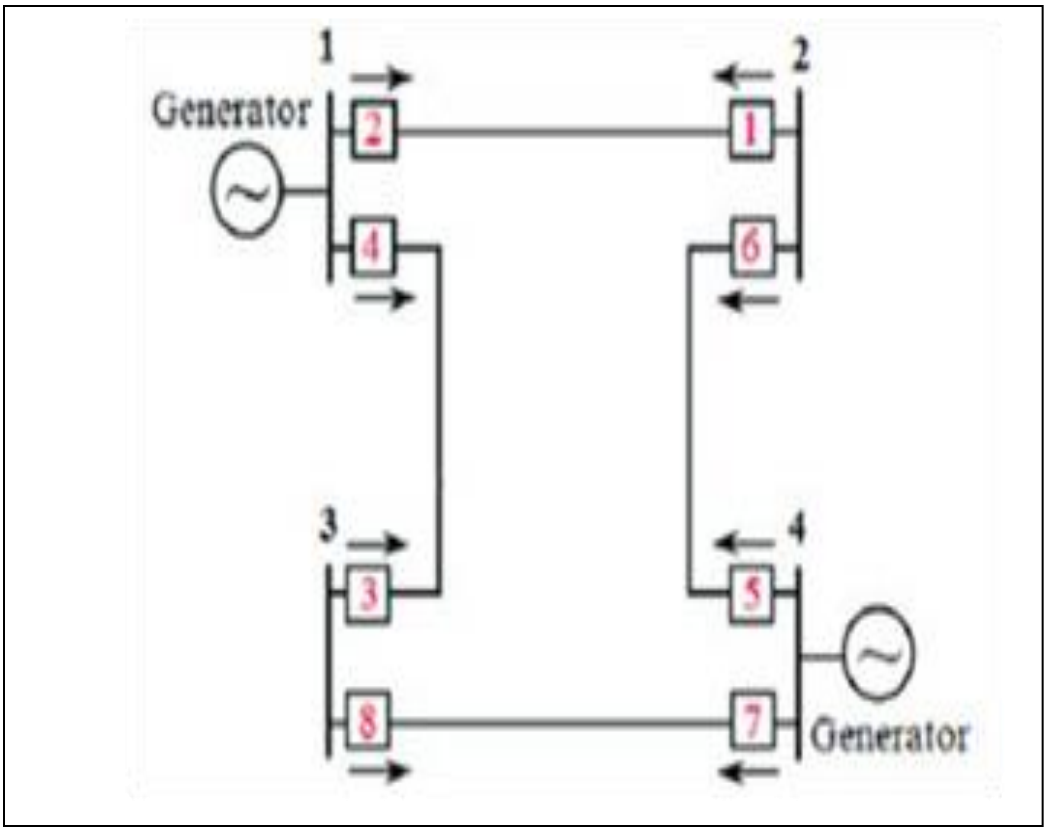


Figure 3-11. The IEEE four Bus system

The basic equation for power-flow analysis is derived from the nodal analysis equations of the power system: Take, for example, the four-bus system shown in Figure 3-11.

$$\begin{bmatrix} Y11 & Y12 & Y13 & Y14 \\ Y21 & Y22 & Y23 & Y24 \\ Y31 & Y32 & Y33 & Y34 \\ Y41 & Y42 & Y43 & Y44 \end{bmatrix} \begin{bmatrix} V1 \\ V2 \\ V3 \\ V4 \end{bmatrix} = \begin{bmatrix} I1 \\ I2 \\ I3 \\ I4 \end{bmatrix} \tag{81}$$

where Y_{ij} are the elements of the bus admittance matrix, V_i is the bus voltages, and I_i is the currents injected at each of the nodes. The node equation at bus *i* can be written as

$$\boldsymbol{I_i} = \sum_{j=1}^{n} \boldsymbol{Y_{ij} V_j} \tag{82}$$

The per-unit real and reactive power provided to the system at bus i and the per-unit current injected into the system at that bus has the following relationship:

$$S_i = V_i \, I_i^* = P_i + \mathrm{j} Q_i \tag{83}$$

where V_i is the per-unit voltage at the bus; I_i^* - the complex conjugate of the per-unit current injected at the bus; Pi and Qi are per-unit real and reactive powers. Therefore,

$$I_i^* = (P_i + \mathrm{j}Q_i)/V_i \qquad (84)$$

$$I_i = (P_i - jQ_i)/V_i^* \qquad (85)$$

$$P_i - jQ_i = V_i^* \sum_{j=1}^{n} Y_{ij} V_j$$

Let $Y_{ij} = |Y_{ij}| \angle \theta_{ij}$ and $V_i = |V_i| \angle \delta_i$

$$P_i - jQ_i = \sum_{j=1}^{n} |V_j|\,|Y_{ij}||V_i| \angle(\theta_{ij} + \delta_j\text{-}\delta_i) \qquad (86)$$

$$P_i = \sum_{j=1}^{n} |V_j|\,|Y_{ij}||V_i| cos(\theta_{ij} + \delta_j\text{-}\delta_i) \qquad (87)$$

$$Q_i = -\sum_{j=1}^{n} |V_j|\,|Y_{ij}||V_i| sin(\theta_{ij} + \delta_j\text{-}\delta_i) \qquad (88)$$

Each bus is associated with its respective variable:

(i) P, (ii) Q (iii) V (iv) δ

In the meantime, each bus is linked to two power flow equations. In a power flow study, two of the four variables are known, while the other two are unknown. As a result, the number of equations equals the number of unknowns. The known and unknown variables differ depending on the bus type.

Each bus in a power system is classified into one of three types:

1. Load bus (P-Q bus) – a bus with defined real and reactive power for which the bus voltage will be computed Load buses are those that do not have generators. V and δare unknown in this case.

2. Generator bus (P-V bus) – a bus on which the magnitude of the voltage is defined and maintained by modifying the synchronous generator's field current. According to the economic dispatch, we also assign real power generation to each generator. Q and δ are unknown in this case.

3. Slack bus (swing bus) – As the reference bus, a dedicated generator bus is used. The magnitude and phase of its voltage are presumed to be fixed (for instance, 1∠0˚ per unit). Here, P and Q are unknown.

Formulation of power-flow

Because the power flow equations are non-linear, they are impossible to solve analytically. Solving such equations necessitates the use of a numerical iterative procedure. The following is a standard procedure:

1. For the power system, create a Ybus bus admittance matrix;

2. Calculate the voltages (both magnitude and phase angle) at each bus in the system;

3. Plug in the power flow equations and calculate the deviations from the answer.

4. Use several well-known numerical procedures to update the estimated voltages (e.g., New-ton-Raphson or Gauss-Seidel).

5. Repeat step 5 until the deviations from the solution are as small as possible.

3.8.2 Flow Diagram for Impact Assessment

Figure 3-12 depicts the method employed in this experiment. The failure of a target unit in a power system domino effect research is determined by the dynamic properties of the escalation vectors (physical effects), threshold values, target unit category, system parameters, and the robustness of the mitigation/intervention systems. Following a successful breach into a substation network, attackers can use their domain-specific abilities to produce traffic manipulation. To maximize the impact of an attack, important cyber-physical security understanding between established communication protocols and the interface with physical equipment is critical. The attacker would need to understand software settings and how device addresses in power control centers correspond to user interfaces. The most obvious manipulation is to add a delay to each signal, which has an impact not only on the protection system but also on the SCADA capability of the control center. The breaker in a damaged part of the transmission line is delayed when a trip signal is blocked for a specified period, which might cause a system failure. This section contains a collection of credible clever attack strategies that have successfully penetrated a substation network.

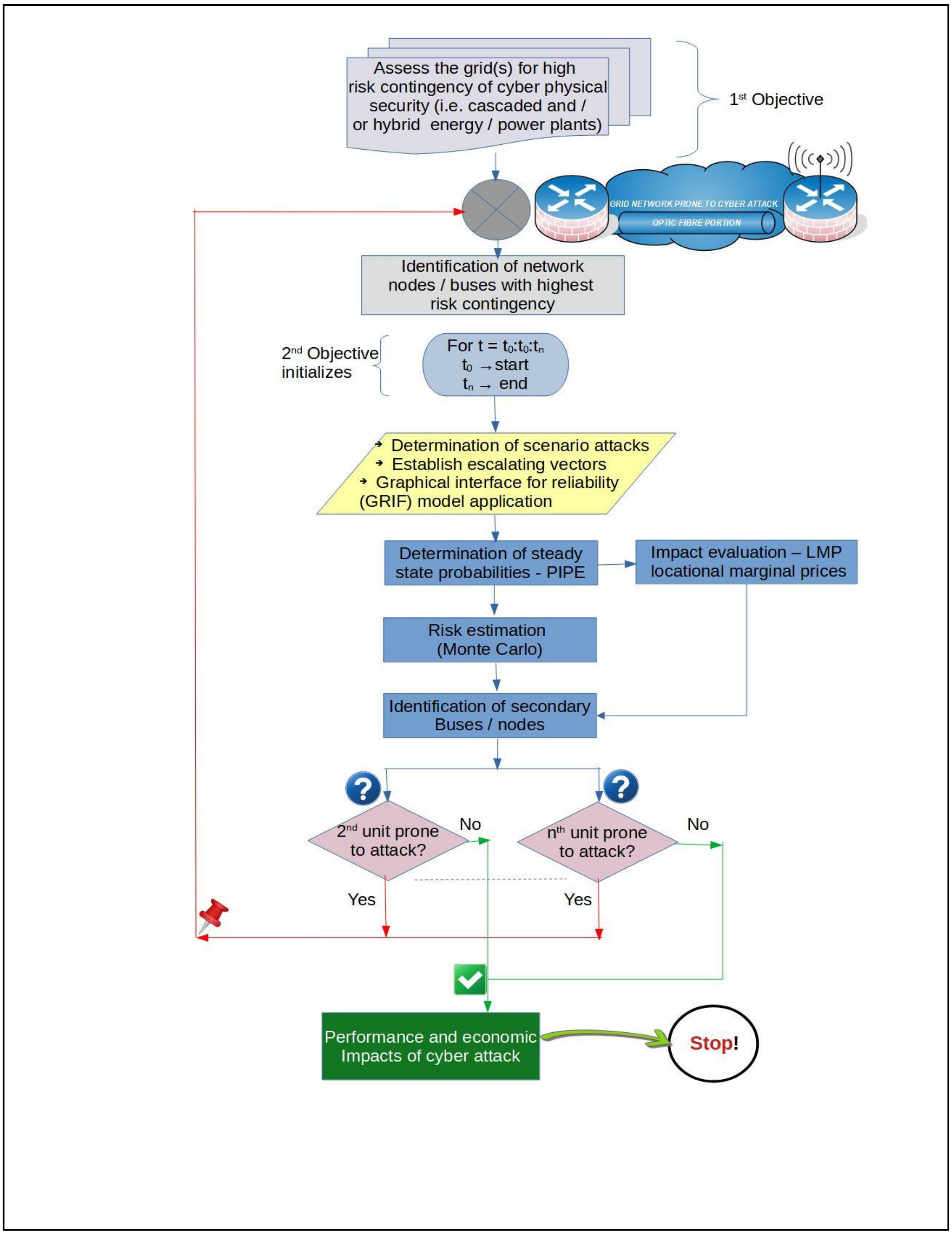

Assess the grid(s) for high risk contingency of cyber physical security (i.e. cascaded and / or hybrid energy / power plants)
1st Objective
GRID NETWORK PRONE TO CYBER ATTACK
OPTIC FIBRE PORTION
Identification of network nodes / buses with highest risk contingency
2nd Objective initializes
For t = t0:t0:tn
t0 → start
tn → end
Determination of scenario attacks
Establish escalating vectors
Graphical interface for reliability (GRIF) model application
Determination of steady state probabilities - PIPE
Impact evaluation – LMP locational marginal prices
Risk estimation (Monte Carlo)
Identification of secondary Buses / nodes
2nd unit prone to attack?
No
Yes
nth unit prone to attack?
No
Yes
Performance and economic Impacts of cyber attack
Stop!

Figure 3-12. Methodology flow graph

3.8.3 Performance and Economic Impact of Attacks

The power system reliability worth evaluating in this study is the monetary loss. We adopted the formulation proposed in [276,277,278,279,280,281], letting C_0 be the optimal operating cost of the system under normal conditions (no cyber-attack). Let C_{Ln} denote the optimal cost of the system under the n^{th} (N-1) line outage due to a cyberattack. Then, deviation from optimal cost under this condition is given by ΔC_{Ln}. Mathematically, we can write it as follows

$$\Delta C_{Ln} = C_{Ln} - C_0 \tag{89}$$

The average cost deviation due to the (N-1) line an outage is given by ΔC_L. Mathematically,

$$\Delta C_L = \sum_{n=1}^{NL} \Delta C_{Ln} \,/\, N_L \tag{90}$$

Let σ denote the net economic impact due to both (N-1) lines by cyber-attack. Then:

$$\sigma = \Delta C_L \tag{91}$$

Further letting R_i denote the risk due to outages, the Risk is;

$$R_i = P_i \text{ x } \sigma \tag{92}$$

where P_i denotes the probability of a cyber-attack (on single bus i).

3.9 Modeling and Mitigation of False Data Injection

3.9.1 Long Short-Term Memory (LSTM) Model

The fundamental concept behind the implementation of machine learning techniques in attack detection is that normal data and modified data tend to have a certain distinction in the projected space. This data together with the historical data can be used to develop the learning model to detect the anomaly. But the challenge remains due to the vast volume and the larger dimension of data to be trained. As the power grid is growing and the dimension of measurement variables has increased tremendously, the selection of the data learning techniques is largely dependent on the computational complexity, convergence rate, training loss, and training duration. LSTM is a unique technique to facilitate the data learning process. A multilayered LSTM framework as shown in the figure can capture the uncertainty of the modern grid and can successfully detect the presence of cyber anomalies [282].

LSTM networks support input data with varying sequence lengths. When passing data through the network, the software pads truncate or split sequences so that all the sequences in each mini-batch have the specified length (cells). Figure 3-13 below illustrates the architecture of a simple LSTM network for regression. The core of the LSTM network is the input sequence layer and an LSTM layer. The input layer feeds the time series data into the network and the LSTM layers learn the long-term dependencies between the input time steps of the sequence data[282],[283].

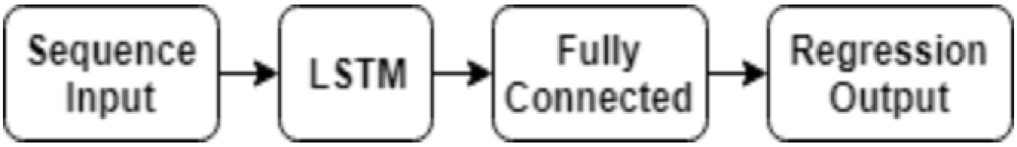


Figure 3-13. The LSTM network for regression

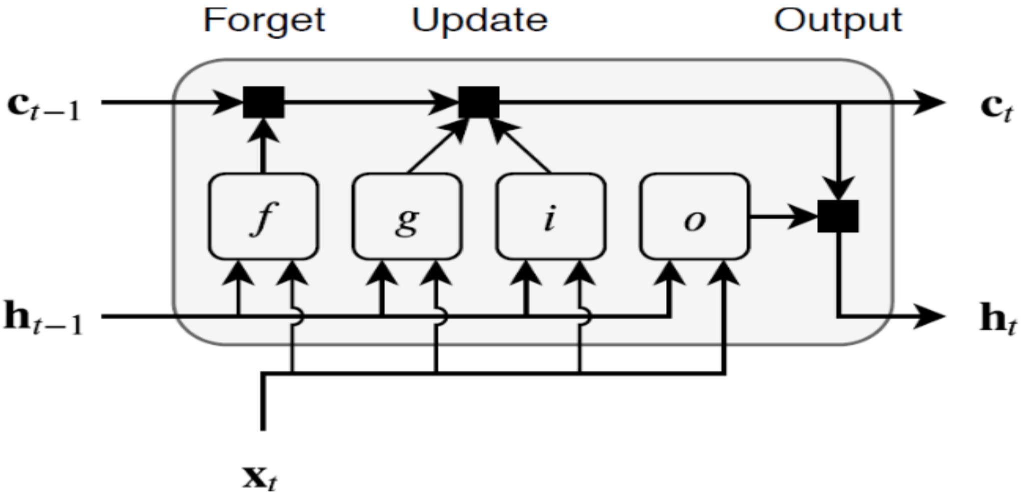


Figure 3-14. The Flow diagram of the LSTM block at time step t

At every time step, the input measurements vector $x = [x_1, x, \dots . x_N]$, is passed through the LSTM block. There are three inputs to the LSTM cell: h_{t-1} previous timestep (t-1) hidden state value, c_{t-1} previous timestep (t-1) cell state value and x_t current timestep (t) input value. The learnable weights of an LSTM layer are the input weight W, the recurrent weight R, and the bias b. The matrices are concatenated as follows[284]:

$$W = \begin{bmatrix} W_i \\ W_f \\ W_g \\ W_o \end{bmatrix}, \quad R = \begin{bmatrix} R_i \\ R_f \\ R_g \\ R_o \end{bmatrix}, \quad b = \begin{bmatrix} b_i \\ b_f \\ b_g \\ b_o \end{bmatrix},$$

There are four dense layers: Input gate (i), Forget gate (f), Cell candidate (g), and Output gate (o). The model uses a multi-class classifier model with four output labels.

The output state of the LSTM block at every time step is used as input to the model for the next time cycle. The block applies a cell policy to limit the number of time steps and data points. The cell consists of an input gate, forget gate, and a control gate. The input gate is responsible to decide which values to be updated. The forget gate decides the number of data points to be used in the calculation and the control gate outputs the control variable using the output function. The cell state at time step t is given by element-wise multiplication as[283],

$$c_t = f_t * c_{t-1} + i_t * g_t \tag{93}$$

$$h_t = o_t * s_t(c_t) \tag{94}$$

Where, $s_t(c_t)$ is the state activation vector which is a function of cell state time. Every four dense layers are expressed as the function of t as,

$$i_t = \theta_t(W_i * x_t + R_i * h_{t-1} + b_i) \tag{95}$$

$$f_t = \theta_g(W_g * x_t + R_g * h_{t-1} + b_g) \tag{96}$$

$$g_t = \theta_g(W_g * x_t + R_g * h_{t-1} + b_g) \tag{97}$$

$$o_t = \theta_o(W_o * x_t + R_o * h_{t-1} + b_o) \tag{98}$$

The θ_o gate activation vector can be expressed using the sigmoid function as $\theta_o = (1 - e^{-x})^{-1}$. The measurement matrices and the adjustable weight matrix are trained with the LSTM model for attack surface detection. The training of data is based on different input parameters: input layers, hidden layers, hidden units, dropout, sequence length, batch size, learning rate, optimizer, FC layers, and output layers. We can stack each LSTM layer on top of the other so that the output of the first LSTM layer is the input to the second LSTM layer. The hidden layer defines the number of LSTM layers stacked on top of each other. The dropout parameter controls the data fitting sequence. Sequence length defines the number of samples that follows the current in the sequence[283].

The prediction from the classifier model is studied for four possible outcomes of output labels.

i) True Positive (TP): positive prediction with positive ground truth,

ii) True Negative (TN): negative prediction with negative ground truth,

iii) False Positive (FP): positive prediction with negative ground truth,

iv) False Negative (FN): negative prediction with positive ground truth

The outcomes of the classification model are observed using four key metrics.

i) Accuracy metrics: These represent the correctness of the positive and negative classification.

ii) Precision metrics: These represent the correctness of the positive classification.

iii) Recall metrics: These indicate the ability to predict positive cases.

iv) F1 score: This metric correlates between precision and recall.

3.9.2 Attack Detection and Mitigation

For challenges involving classification and regression, LSTM structures can be used. The type of output—continuous (prediction) or discrete—is determined by the last layer activation function (classification). Attack detection is carried out by using the softmax function in the output layer to provide discrete outputs (labels) [284]. First, we train the $LSTM_{detection}$ model, a multi-class classifier model with four output labels (normal state (NS), $\Delta f_1, \Delta f_2$, and Δp), to identify the attacks. The predictions of a classification model are evaluated for each of the four possible outputs, by considering an output l as positive and all other outputs as negative:

i) True Positive (TP): positive prediction with positive ground truth,

ii) True Negative (TN): negative prediction with negative ground truth,

iii) False Positive (FP): positive prediction with negative ground truth, and

iv) False Negative (FN): negative prediction with positive ground truth. Accordingly, the following four statistical metrics are used:

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \tag{99}$$

$$\text{Precision} = \frac{TP}{TP+FP} \tag{100}$$

$$\text{Recall} = \frac{TP}{TP+ FN} \tag{101}$$

$$f_1 = \frac{2\ x\ Precision\ x\ Recall}{Precision+Recall} \tag{102}$$

where accuracy serves as a general metric of model success by estimating the chance of accurate classifications (both positive and negative); Recall estimates the likelihood that all positive labels will be correctly classified, and it serves as a gauge of the capacity to forecast positive cases. The precision and recall are balanced out by the f_1 score. The accuracy metric assesses the likelihood of correctly classifying positive cases and serves as a gauge of confidence in the anticipated positive cases.

3.9.3 Regression-based Attack Impact Model

We use the regression-based attack impact model to train the output of the LSTM detection and to mitigate the effects of the detected attacks. The mitigation model is employed only when the FDIA attack is detected by the first stage of the LSTM model. The application of regression-based attack analysis has been investigated in many works of literature. [285] proposes a unique method of FDIA detection based on vector auto-regression (VAR) and tested on the IEEE 14-bus system. For the linear state estimation [286], consider the voltage phase angle of the state estimation vector $x(t)$ is θ and the unity voltage amplitude ϋ. The prediction model of the system state is represented as:

$$\theta_{k+1} = T_k * \theta_k + \epsilon_{k+1} \tag{103}$$

θ_{k+1} and θ_k represents the state voltage phase angle at $k+1$ and k sampling time. T_k is the parameter matrix and ϵ_{k+1} is the gaussian random noise with normal distribution and zero mean. We obtain the state prediction error matrix using the parameter matrix from the above equation as,

$$R_{\theta_{k+1}} = T_k * R_{\theta_k} * T_k^T + R_{\epsilon_{k+1}} \tag{104}$$

The predicted value of measured active power at sample time $k+1$ can be calculated from the prediction error matrix and parameter matrix as,

$$P_{k+1} = H * \theta_{k+1} \tag{105}$$

The residual of the measured and predicted values follows the gaussian distribution with a mean value of 0 and covariance matrix of N which is given by,

$$N = R + H * R_{\theta_k} * H^T \tag{106}$$

$$\sigma_N = diag(N) \tag{107}$$

The regression-based attack impact model is a method of predicting the severity of an attack using a regression model. The model is based on the characteristics of the attack, such as the type of attack, the target, and the amount of data compromised. The model uses the L2 norm to calculate the distance between the predicted value and the actual attack severity and then adjusts the attack severity to account for any potential errors in the model. Measurement residual analysis method based on the L2 norm is proven and widely used for bad data detection and FDIA attack detection method [287]. It is a method of analyzing the residuals of a model based on the L2 norm. It is used to assess the accuracy of a model by calculating the sum of the squared residuals and is an important tool for determining the quality of the model and whether further refinement or improvement is needed. The L2 norm is a measure of the overall distance between the predicted values and the actual values [288]. A model with a low L2 norm indicates that the model is more accurate than one with a large L2 norm.

Using the measurement residual analysis method, we can identify potential sources of bias or errors in the system and can be used to adjust the parameters of the model or system to improve its accuracy [289]. The analysis method based on $\infty\ Norm\ and\ L\ Norm$ can be expressed as,

$$Z(k) = \begin{cases} 1, & FDIA\ ATTACK \\ 0, & NO\ FDIA\ ATTACK \end{cases} \tag{108}$$

This method uses two threshold detectors, $\tau 1\ and\ \tau 2$. $\tau 1$ is used for attack detection while $\tau 2$ is used to detect the performance of the detector. When $Z(k) = 1$,

$$\|P - H * \theta\|_{L2\ Norm} \geq \tau 1 \tag{109}$$

$$\left\|\frac{residue}{\sigma_N}\right\|_{\infty\ Norm} \geq \tau 2 \tag{110}$$

The evaluation index for the attack detection scheme is based on the mean square error (MSE) [288]. The MSE is a commonly used loss function for regression problems, where the goal is to predict continuous values [290]. It is the function of the difference between the observed state and the predicted state variable and is expressed as,

$$MSE = \frac{1}{N}\sum_{k=1}^{N} e_k^2 \tag{111}$$

$$e_k = \theta_{k\_o} - \theta_{k\_p} \tag{112}$$

where N is the number of time points, θ_{k_p} is the predicted state and $\theta_{k_o}$is the observed state. Another performance metric is the Receiver Operating Characteristic (ROC) curve, which is a graphical representation of the performance of a binary classifier system as its discrimination threshold is varied. The ROC curve is created by plotting the True Positive Rate (TPR) against the False Positive Rate (FPR) at various classification thresholds. The TPR is the ratio of true positive instances to all positive instances, while the FPR is the ratio of false positive instances to all negative instances.

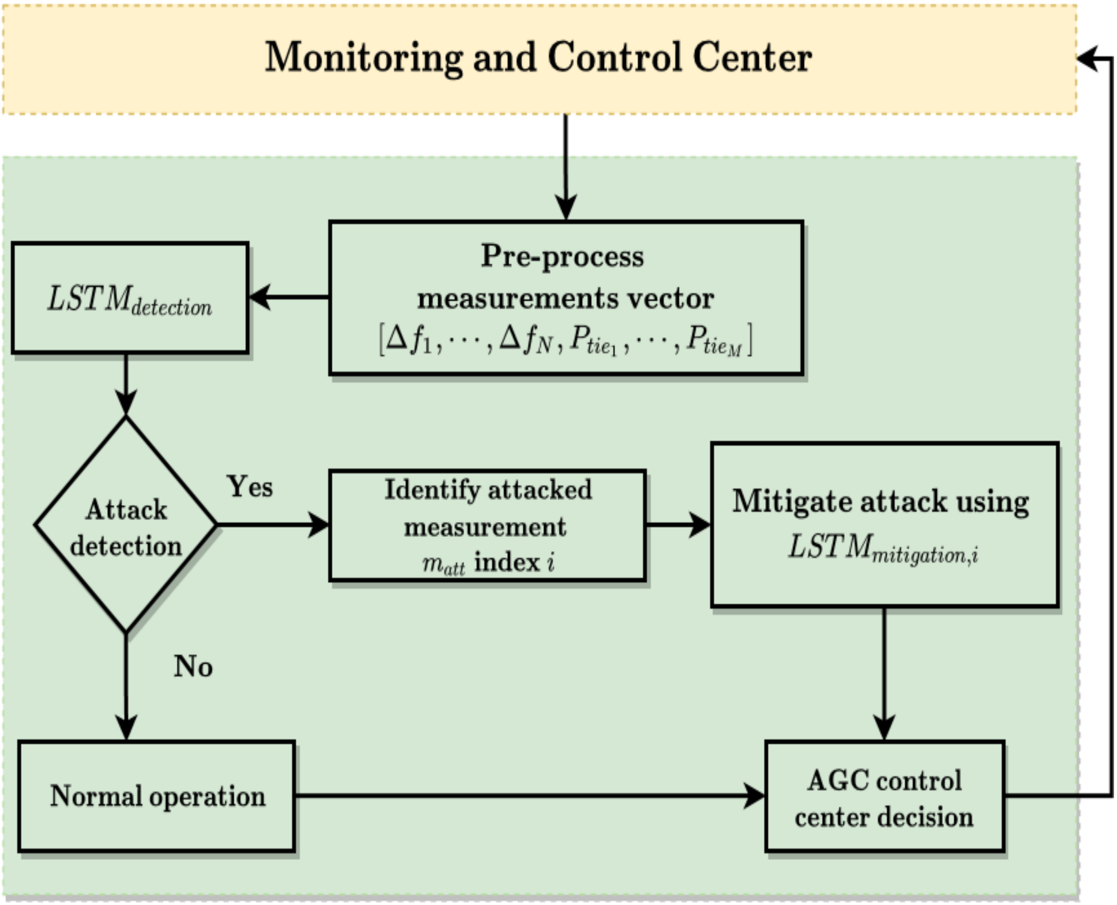

Monitoring and Control Center
Pre-process measurements vector $[\Delta f_1, \cdots, \Delta f_N, P_{tie_1}, \cdots, P_{tie_M}]$
$LSTM_{detection}$
Attack detection
Yes
No
Identify attacked measurement m_{att} index i
Mitigate attack using $LSTM_{mitigation,i}$
Normal operation
AGC control center decision

Figure 3-15. Attacks detection and mitigation flowchart

The flow of figure 3-15 illustrated the attack detection and mitigation we developed. Second, we developed the $LSTM_{mitigation}$ regression model to reduce the impact of attacks that are detected. To forecast the proper signal values based on the other uncompromised signal data, we built and train a model for each of the system signals.

When the system is in operation, only attacks that have been detected by the $LSTM_{detection}$ model caused the appropriate mitigation model to be triggered. Since $LSTM_{mitigation}$ is a regression model that forecasts the attack measurement's continuous value to lessen the impact of the attack, its $LSTM_{mitigation}$ is assessed using the attack mitigation plots and the root mean square error (RMSE) metric.

The control center processes frequency deviation and tie-line power readings from the N-Area AGC to compute the AGC signals that are delivered back to the areas. The deviation frequency measurements $[\Delta f_1, \cdot\cdot\cdot, \Delta f_N]$ from the N areas and the M tie-line measurements$[P_{tie1}, \cdot\cdot\cdot, P_{tieM}]$ are included in the input features vector. Second, the $LSTM_{detection}$ model receives these input properties to detect any attacks. If an attack event is discovered, the attacked measurement is located, and the associated LSTMitigation model is applied to lessen the impact of the attack on the attacked measurement. As a result, we will have (N + M + 1) models for a control center that monitors N locations with M tie-line power interconnections: a single LSTM detection model, $(N + M)$ $LSTM_{mitigation}$ models (one for each measurement). Based on the trusted and corrected signals, the control center calculates and sends back the new operation (OP) to each area.

3.10 Comparison of Results with Other Studies Conducted by Other Researchers

The results obtained were later compared with findings from other studies. Learning points were shared with other programs and projects. Of these the following are notable:

1. PRIME [291] (PNNL cybeR physIcal systeMs tEstbed): the testbed that integrates a real-time transmission system simulator with commercial industry-grade energy management system (EMS) software and remote hardware-in-the-loop (RHIL). PRIME is an end-to-end, modular testbed that allows high-fidelity RHIL experimentation of a power system.
2. They developed a novel edge-based multi-level anomaly detection framework for SCADA networks named EDMAND. EDMAND monitors all three levels of network traffic data and applies appropriate anomaly detection methods based on the distinct characteristics of data. Alerts are generated, aggregated, and prioritized before being sent back to control centers. A prototype of the framework is built to evaluate its detection ability and time overhead of it [292].

3. A real-time, cyber-physical co-simulation testbed utilizing a Real-Time Digital Simulator (RTDS) for simulating the power system, a Common Open Research Emulator (CORE) for emulation of the communication network, and a TCP/IP-based interface is used in this work. The testbed is used to simulate an Army microgrid-based model for validation. Cyber-physical system simulation results demonstrate the ability of the testbed to implement cyber attacks and analyze the impact on microgrids [293].

4. The proof-of-concept examples that make up this study's proof-of-concept are carried out based on dynamical simulations that use the IEEE-14 bus system. To describe the relay tripping and its cascading effects by the initial event of switching attacks based on observation of other places of relaying, relay models and associated control methods are offered. The simulated statistics for the small power system's anticipated results have demonstrated the grids' cascading effects between the initial event and the network topology. The cascade impacts of relay models are recognized by the local measurements from other substations based on the electrical quantity, such as frequency and voltage of substations as well as the rotor angle of generators, to exhibit spatiotemporal breaker trippings [208].

3.11 Conclusion

The research methods used in the study and study constraints were all covered in this chapter. Mixed methodologies were used in this investigation, and were explored. There were descriptions of the target population, sampling techniques, modeling, and simulation analyses. Additionally, a design science research (DSRM) methodology was covered.

CHAPTER 4: MODEL SETTING AND ANALYSIS

4.1 Introduction

This chapter outlines the modeling and simulations that were conducted to meet the research objectives. The modeling and simulation principles guiding these experiment has been explained in chapter 3.

4.2 The Steady-State Probabilities

4.2.1 The SPN Model of Scenario I: Firewall Model

We constructed the SPN model for Defense Scenario I, using a single server and depicting a substation interface with another remote SCADA substation network shown in Figure 4-1.

We denote :

$\lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8, \lambda_9, \lambda_{10}\}$ as the average transition triggering rate and

$P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$ as the places.

We can get the set of reachable markings as $M = \{M_1, M_2, M_3, M_4, M_5, M_6, M_7\}$.

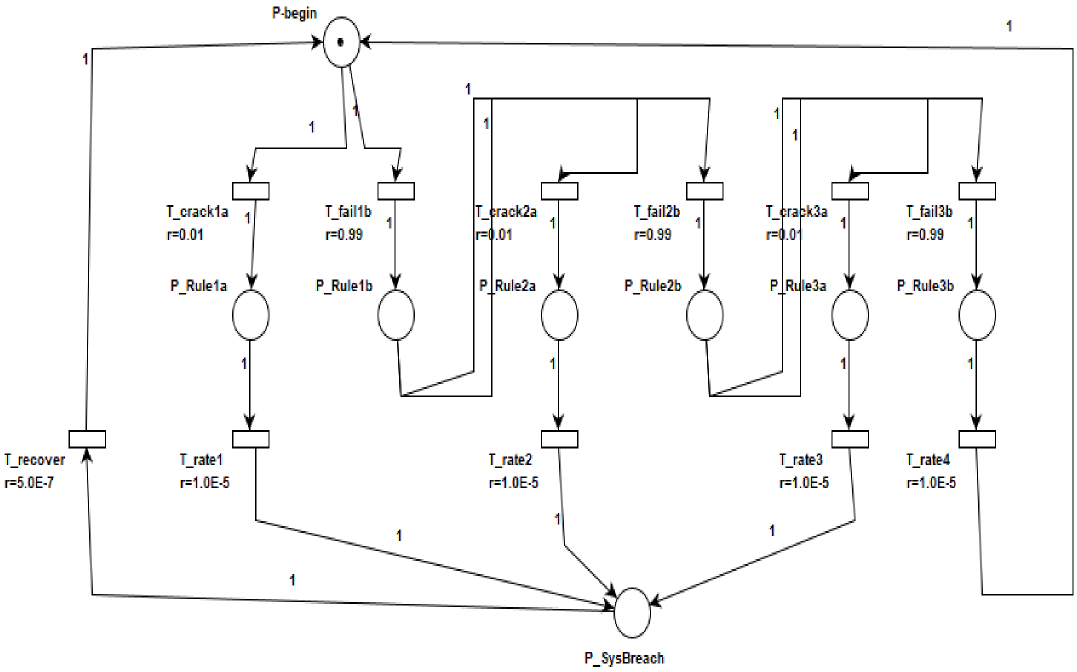


Figure 4-1. The SPN Model of Scenario I: Firewall model.

Table 4-1. Places and transitions for the GSPN model

Places	Description	Rates
Po	Intrusion attempts begin P_Begin	
P1	Intruder cracks rule 1 P_Rule1a	
P2	Intruder fails rule 1 P_Rule1a	
P3	Intruder cracks rule 2 P_Rule1a	
P4	Intruder fails rule 2 P_Rule1a	
P5	Intruder cracks rule 3 P_Rule1a	
P6	Intruder fails rule 3 P_Rule1a	
P7	The system is breached P_SysBreach	

Transition	**Description**	**Rate**
T0	Crack rule number 1 T_crack1a	λ_a (0.01)
T1	Fail Firewall rule number 1 T_fail1b	λ_b(0.99)
T2	Crack Firewall rule number 2 T_crack2a	λ_c(0.01)
T3	Fail Firewall rule number 2 T_fail2b	λ_d(0.99)
T4	Crack rule number 3 T_crack3a	λ_e(0.01)
T5	Fail Firewall rule number 3 T_fail3b	λ_f(0.99)
T6	Firewall execution rate1 T_rate1	$\lambda_g(10^{-6})$
T7	Firewall execution rate2 T_rate2	$\lambda_h(10^{-6})$
T8	Firewall execution rate3 T_rate3	$\lambda_i(10^{-6})$
T9	Firewall execution rate4 T_rate4	$\lambda_j(10^{-6})$
T10	Firewall recovery rate T_Recover	λ_k(0.5E-6)

Table 4-2. Reachable markings' set of the Firewall model

	P_Begin	P_Rule1a	P_Rule1b	P_Rule2a	P_Ru1e2b	P_Rule3a	P_Rule3b
	1	0	0	0	0	0	0
	0	0	1	0	0	0	0
	0	1	0	0	0	0	0
	0	0	0	0	1	0	0
	0	0	0	1	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	1

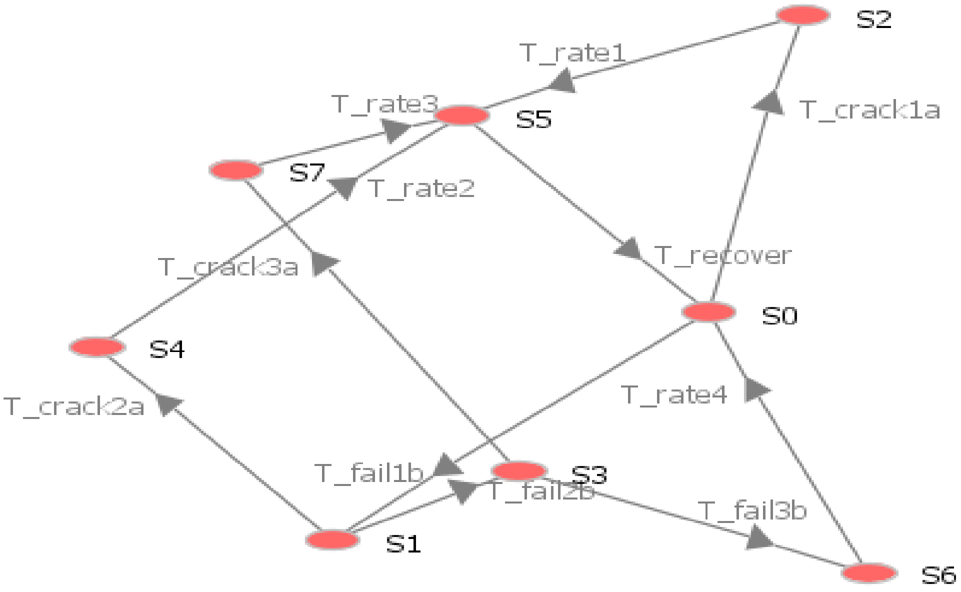


Figure 4-2. The Reachability graph for the firewall model

Starting from the initial marking shown (S0) in Fig. 4-2, a possible evolution of the GSPN state may be evaluated. As shown in Figure 4-1, and table 4-1 the places $P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$ represent the system states and the transitions T_0 to T_{10} represent the events that enable the transfer of the system state. Initially, the system is in a normal state. When the transition T_crack1a is enabled, the system transfers to the state P_Rule1a indicating that an intrusion attempt is in progress and rule number 1 is being circumvented. T_fail1b to T_fail3b indicates failed attempts to breach firewall results. A successful attack is achieved if any or all the transitions T_rate1, T_rate2, or T_rate3 are enabled. A system recovery is achieved through enabling transition Trecover, thereby enabling the initial marking P_0 (in our case S0, since that's the default nomenclature in PIPE). According to the definition of the transition matrix and other performance metrics, we can estimate the SPN model as follows. The transition matrix Q is obtained by solving the Markov Chain equivalent of the reachability graph in figure 4-2. Q is thus, an 8 x 8 matrix presented in equation 113. Furthermore, we solved equation 38; that is multiply Q x vector $\pi = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6, \pi_7\}$ to get the steady-state probability.

$$[Q =]\begin{bmatrix} 0 & \lambda b & \lambda a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda d & \lambda c & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda g & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda f & \lambda e \\ 0 & 0 & 0 & 0 & 0 & \lambda h & 0 & 0 \\ \lambda k & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda j & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda i & 0 & 0 \end{bmatrix} \tag{113}$$

Substitution of the values for all rates (i.e. λa to λk) from Table 4-2, and normalize the sum of each row to one. Applying equation 39 described above; gives the steady-state probability as:

$$\pi\{\pi_0, \pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6, \pi_7 \qquad) \qquad x$$

$$\begin{bmatrix} 0 & 0.99 & 0.01 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.99 & 0.01 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.99 & 0.01 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (114)$$

Steady-state probabilities are as follows: $\pi_0 = 0, \pi_1 = 0, \pi_2 = 0, \pi_2 = 0.0049, \pi_3 = 0, \pi_4 = 0.0048, \pi_5 = 0.95109, \pi_6$=0.0475, $\pi_7 = 0.00048$

4.2.2 The SPN Model of Scenario II: Password Model

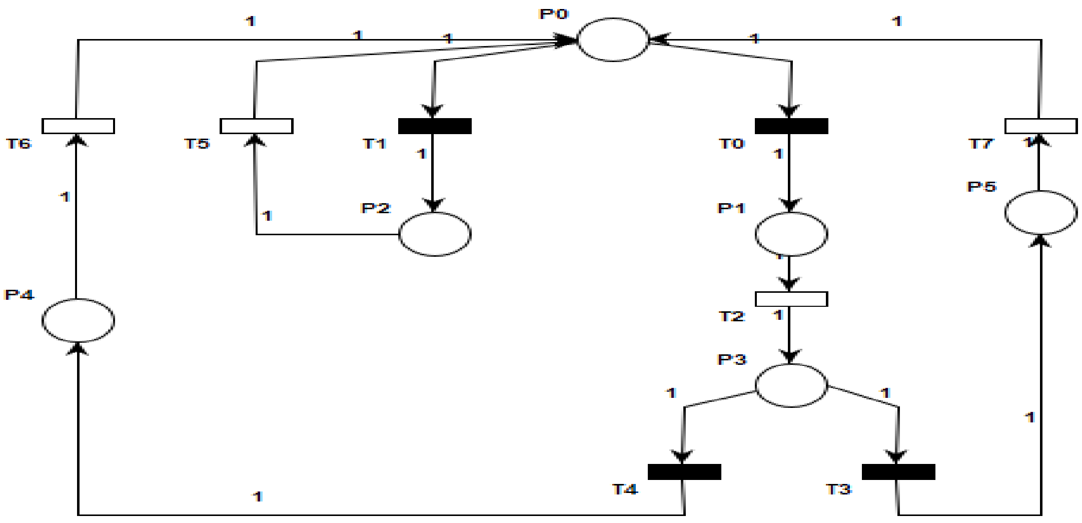


Figure 4-3. The SPN Model of Scenario II: Password Model [208]

a. The place, P0 denotes the initiation of the password cracking of local SCADA systems.

b. The place, P1 denotes the successful login.

c. The place, P2 denotes the failed login to the local SCADA.

d. The place, P3 denotes the knowledge discovered from the SCADA.

e. The place, P4 denotes the executed sequence of disruptive switching attacks from the SCADA.

f. The place, P5 denotes the failure to sequentially execute switches due to interlocking blocks.

Variables, T0, T1, T3, and T4 denote the transition probabilities of the successful login to the SCADA, failure to login to the SCADA, failure to execute, and successful execution of the sequential switching in the targeted substation, respectively.

Variables, T2, T5, T6, and T7 denote the transition rates of learning to discover the cyber-physical relation, the response to attackers indicating the failed login, the response to attackers about successful switching attacks, and the response to attackers indicating the failure of the sequential switching due to interlock rules, respectively.

Table 4-3. Transitions descriptions and rates for the password model (II)

Transition	Description	Rates
T0	Failure to crack the password	λ_a (0.01)
T1	Successful cracking of password	λ_b (0.99)
T2	Successful login to SCADA	λ_c (0.0000001)
T3	Failure to execute an active attack	λ_d (0.9987)
T4	Success in executing a sequential attack	λ_e (0.0013)
T5	Response to failed login	λ_f (0.00001)

T6	Response after a successful attack	λ_g (0.0000005)
T7	Response to failed executing of sequential attack	λ_h (0.001)

Table 4-4. Reachability markings' set of the password model.

	P0	P1	P2	P3	P4	P5
M0	1	0	0	0	0	0
M1	0	0	1	0	0	0
M2	0	1	0	0	0	0
M3	0	0	0	1	0	0
M4	0	0	0	0	1	0
M5	0	0	0	0	0	1

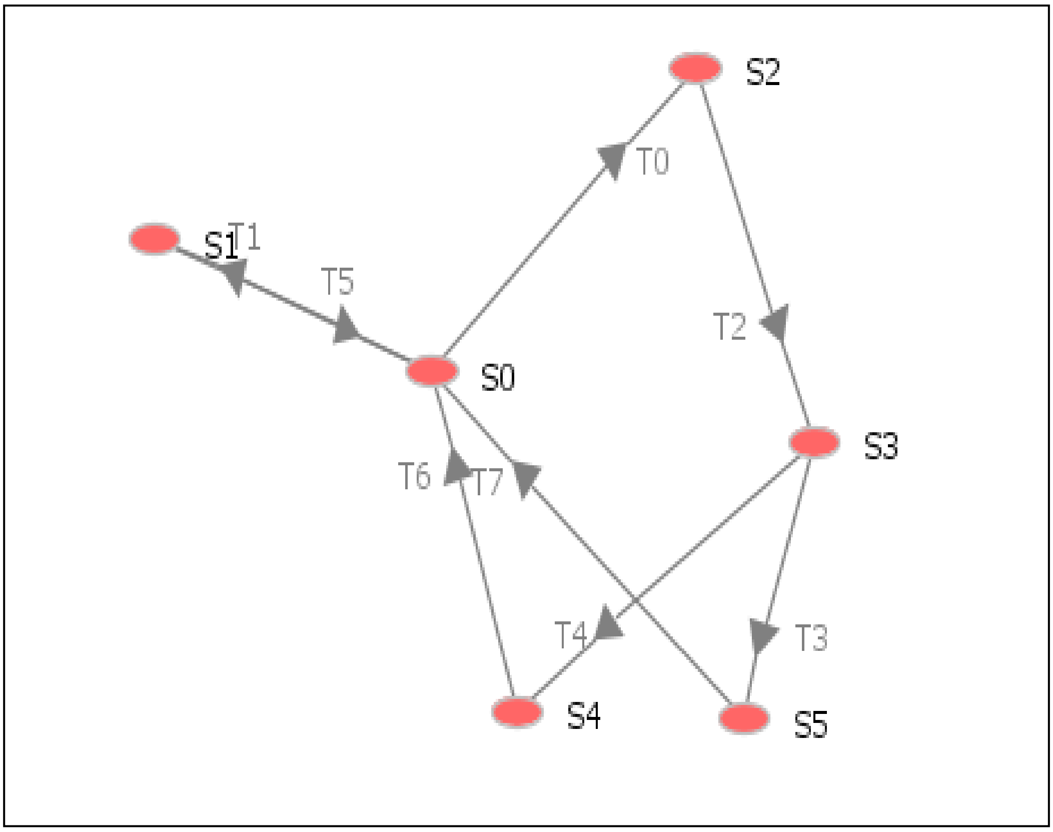


Figure 4-4. The reachability graph of password model

Using a similar argument as above, the steady-state probability is derived as follows:

$$\pi_0 = 0.00001, \pi_1 = 0.00966, \pi_2 = 0, \pi_2 = 0.95592, \pi_3 = 0.00001, \pi_4 = 0.02485, \pi_5 = 0.00955$$

4.2.3 The SPN Model of Scenario III: Combined Firewall and Password models within a Substation

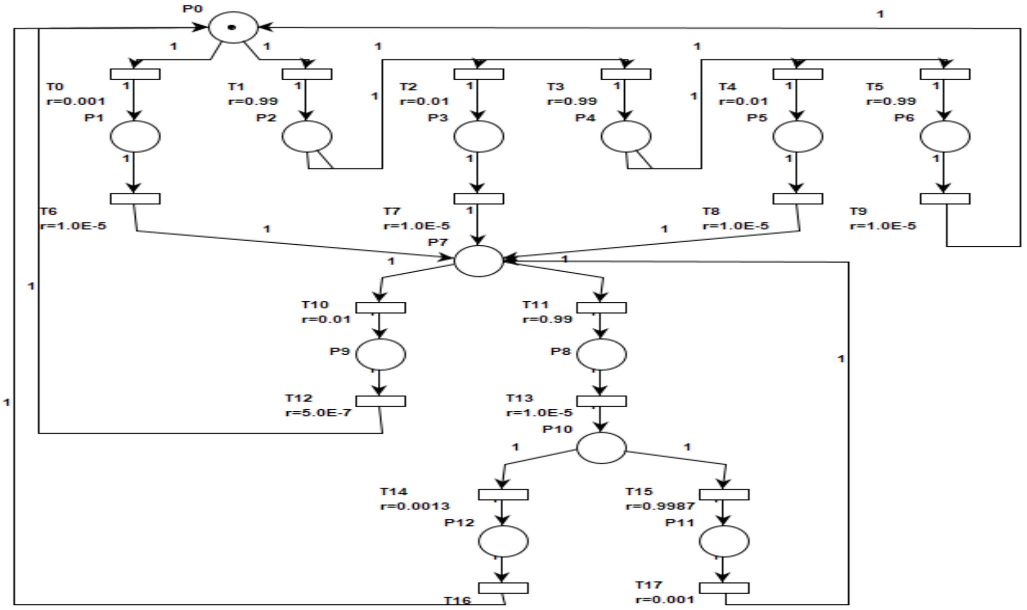


Figure 4-5. Scenario III: Combined Firewall and Password models

The third scenario (Fig. 4-5) is modeled by combining the firewall and password models depicted in figures 4-1 and 4-3. The description for transitions and places remains as defined in the preceding sections. As from the previous arguments, the reachability set and graph are obtained in figure 4-6 and table 4-5. Further, the steady-state probability is calculated.

Table 4-5. The reachability set for scenario III

	P0	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
M0	1	0	0	0	0	0	0	0	0	0	0	0	0
M1	0	0	1	0	0	0	0	0	0	0	0	0	0
M2	0	1	0	0	0	0	0	0	0	0	0	0	0
M3	0	0	0	0	1	0	0	0	0	0	0	0	0
M4	0	0	0	1	0	0	0	0	0	0	0	0	0
M5	0	0	0	0	0	0	0	1	0	0	0	0	0
M6	0	0	0	0	0	0	1	0	0	0	0	0	0
M7	0	0	0	0	0	1	0	0	0	0	0	0	0
M8	0	0	0	0	0	0	0	0	1	0	0	0	0
M9	0	0	0	0	0	0	0	0	0	1	0	0	0
M10	0	0	0	0	0	0	0	0	0	0	1	0	0
M11	0	0	0	0	0	0	0	0	0	0	0	1	0
M12	0	0	0	0	0	0	0	0	0	0	0	0	1

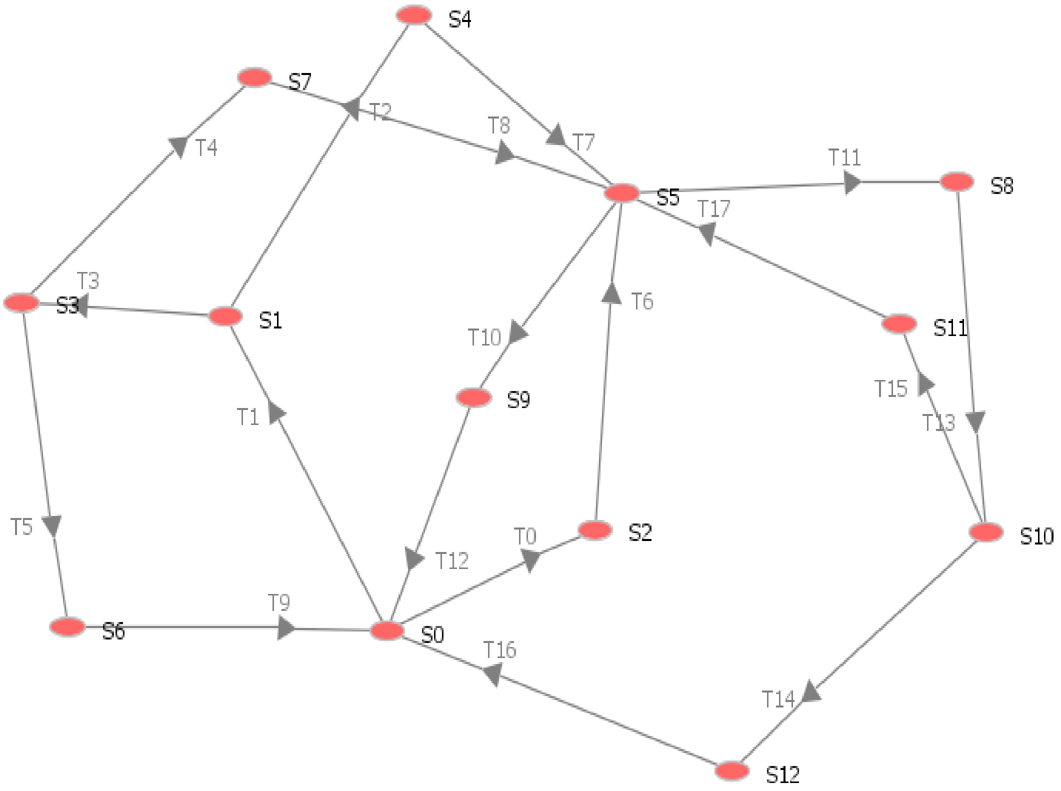


Figure 4-6. The Reachability graph of Scenario III

Using a similar argument as in the Sections above, and the rates in tables 4-1 and 4-3 the steady-state probability, were derived as follows:

π0 = 0, π1= 0, π2= 0.0022, π3= 0, π4= 0.00218, π5= 0.00001, π6= 0.21379, π7=0.00216, π8=0.64737,π9=0.13078,π10=0.00001,π11=0.00065,π12=0.00084

4.2.4 Modeling Intrusions into the Wide Area Control Networks

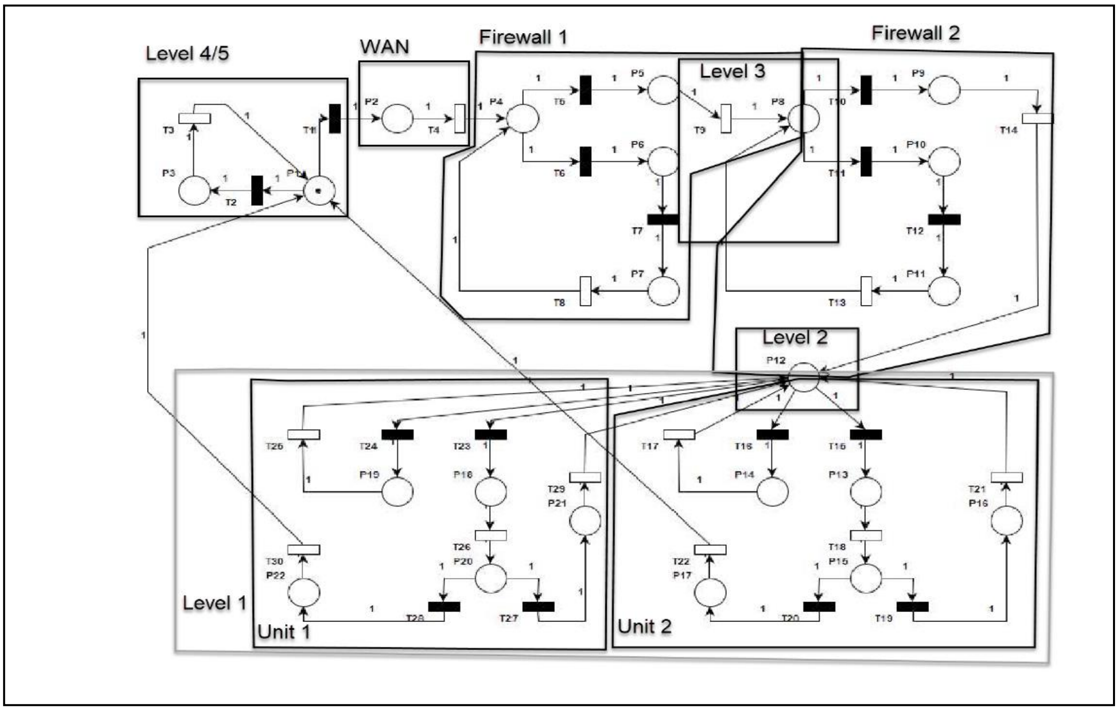


Figure 4-7. The GSPN Model for ICS Architecture

4.2.4.1 Modeling Intrusions Into the Control Networks

Motivated by the cryptography and Firewall (FW) protection against cyber intrusions proposed models in [208], in section, scenarios to model intrusions into the digital control networks in HPPs: the cyberattacks launched from level 4 and level 5 are modeled. As described in Section II, the cybersecurity level of the ICS architecture is five. The application workstation in level 3 can connect the terminal server (TS) residing in the plant's main control room through the remote desktop connection. However, if the malicious attacker intrudes into the supervisory control from the internet or external network and successfully logs into the TS, i.e., cracks the correct password, he can immediately penetrate the plant control networks and do severe damage. The intrusion scenario is thus illustrated in Fig. 4-7 by using a GSPN. The attacker from the Internet can intrude into the corporate WAN through the DMZ, if the attacker guesses the correct password then the attacker penetrates the corporate WAN successfully. Communications between WAN and LAN as well as between LAN and Control networks are protected by FWs.

4.2.4.2 Quantitative Analysis of Scenario

To quantitatively evaluate the intrusion probability of control networks launched from the enterprise network, we need to define the GSPN:

GSPN_1 = (PN_1, T_1, T_2, λ)

PN_1 = (P, T, A, M_0)

P = $\{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}, P_{16}, P_{17}, P_{18}, P_{19}, P_{20}, P_{21}, P_{22}\}$

T = $\{t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9, t_{10}, t_{11}, t_{12}, t_{13}, t_{14}, t_{15}, t_{16}, t_{17}, t_{18}, t_{19}, t_{20}, t_{21}, t_{22}$

$t_{23}, t_{24}, t_{25}, t_{26}, t_{27}, t_{28}, t_{29}, t_{30}\}$

M_0 = (1, 0, 0, 0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)

T_1= $\{t_3, t_4, t_8, t_9, t_{13}, t_{14}, t_{17}, t_{18}, t_{21}, t_{22}, t_{25}, t_{26}, t_{29}, t_{30}\}$

T_2 = $\{t_1, t_2, t_5, t_6, t_7, t_{10}, t_{11}, t_{12}, t_{15}, t_{16}, t_{19}, t_{20}, t_{23}, t_{24}, t_{27}, t_{28}\}$

λ = $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8, \lambda_9, \lambda_{10}, \lambda_{11}, \lambda_{12}, \lambda_{13}, \lambda_{14}, \lambda_{15}, \lambda_{16}, \lambda_{17}, \lambda_{18}, \lambda_{19}, \lambda_{20}, \lambda_{21}, \lambda_{22}$

$\lambda_{23}, \lambda_{24}, \lambda_{25}, \lambda_{26}, \lambda_{27}, \lambda_{28}, \lambda_{29}, \lambda_{30}\}$ (115)

Where P1 denotes the initiation of the password cracking of local SCADA systems, P2 denotes the successful login, P3 denotes the failed login to the local SCADA, P4 denotes the initiation of cracking of FW rule of DMZ , P5 denotes the success of cracking DMZ Firewall, P6 failure to crack DMZ FW , P7 denotes denial of attack on FW attack, P8 denotes the initiation of cracking of FW rule of levels 3 LAN, P9 denotes the success of cracking FW rule of level 3 LAN,P10 failure to crack FW rule of level 3 LAN, P11 denotes denial of attack on FW attack, P12 denotes initiation of the password cracking of local SCADA systems of units 1 to units N, P13,and P18 denotes the successful login to the local SCADA, P14, and P19 denotes the failed login to the local SCADA,P15 and P20 denotes the knowledge discovered from the SCADA, P17 and P22 denotes the executed disruptive sequence of switching attacks from the SCADA, and P16 and P21 denotes the failure to execute switches due to sequentially interlocking blocks.

We assumed that the probability to guess the correct password is 0.01. The firing weights of λ1 = 0.01, λ2 = 0.99, We also assign the firing rates λ3 = λ4 = 10−6 and λ6 = 0.5×10−6 representing response delay times the rest of the rates are depicted in table 4-6, and as proposed in [208]. From the initial marking M0 (S0 in our case) and by a sequence of transition firings, we obtained the reachability graph, as shown in Fig. 4-8. The GSPN is one-bound and contains 22 markings. Among these markings, S0, S3, S4, S7, S8, S11, S16, and S17 are vanishing, whereas S1, S2, S5, S6, S9, S10, S12, S13, S14, S15, S18, S19, S20, and S21 are tangible. Therefore, the transition matrix P can be composed of four submatrices for the set of vanishing markings (V) or adsorbing states (n_a) and the set of tangible markings (T) or transient states (n_t) for immediate and timed transitions respectively.

Table 4-6. Transition firing rates

λ1	λ2	λ3	λ4	λ5	λ6	λ7	λ8	λ9	λ10
0.01	0.99	10E-6	10E-6	0.01	0.99	1	0.5E-6	10E-6	0.01
λ11	λ12	λ13	λ14	λ15	λ16	λ17	λ18	λ19	λ20
0.99	1	10E-6	0.5E-6	0.01	0.99	10E-6	10E-6	0.9987	0.0013
λ21	λ22	λ23	λ24	λ25	λ26	λ27	λ28	λ29	λ30
10E-6	0.5E-6	0.01	0.99	10E-6	10E-6	0.9987	0.0013	10E-6	0.5E-6

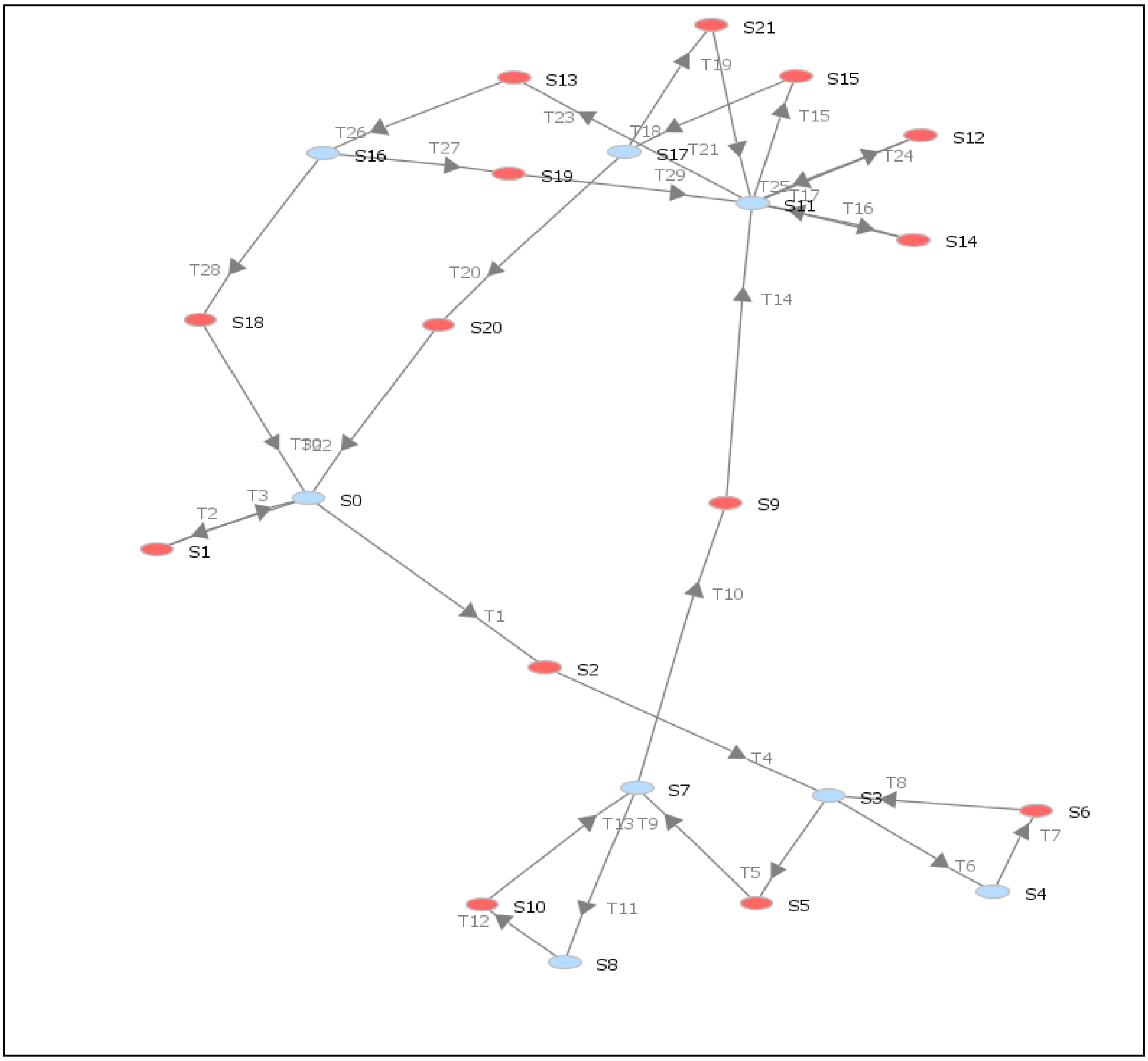


Figure 4-8. The Reachability graph of modeling intrusions launched from the Enterprise Network

We began our analysis by numbering the states in the MC such that the $\mathbf{n_a}$ absorbing states occur first and writing the transition probability matrix P as

$$\mathrm{P} = \begin{bmatrix} \mathrm{C} & D \\ E & F \end{bmatrix} \tag{116}$$

Where;

$C := (c_{ij})$, c_{ij} = Prob$[M_i \rightarrow M_j]$ $M_i \in$ V and $M_j \in$ V;

$D := (d_{ij})$, d_{ij} = Prob$[M_i \rightarrow M_j]$ $M_i \in$ V and $M_j \in$ T;

$E := (e_{ij})$, e_{ij} = Prob$[M_i \rightarrow M_j]$ $M_i \in$ T and $M_j \in$ V;

$F := (f_{ij})$, f_{ij} = Prob$[M_i \rightarrow M_j]$ $M_i \in$ T and $M_j \in$ T;

and T denotes the set of tangible states and V the set of vanishing states. C describes the transition probabilities between vanishing states and F specifies the probabilities between tangible states.

Once in an absorbing state, the process remains there, so C is the identity matrix with all elements $p_{ii} = 1$, $1 \leq i \leq n_a$. E is the $n_t \times n_a$ the matrix describing the movement from the transient to the absorbing states, and F is the $n_t \times n_t$ the matrix describing the movement amongst transient states. Since it is not possible to move from the absorbing to the transient states, D is the $n_t \times n_t$ zero matrices. By using the values described in Table 4-6 above, the transition matrix P formed is a 22 x 22 matrix. The dimensions of C, D, E, and F are 8 × 8, 8 x 14, 14 × 8, and 14×14, respectively.

$$E =$$

$$\begin{vmatrix}
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0
\end{vmatrix}$$

The steady-state distribution $\tilde{\boldsymbol{\pi}}$ of the embedded Markov chain (EMC) is given by equation 38.

$\tilde{\pi}P = \tilde{\pi}$ and $\sum_{Mi\in T\cup V} \tilde{\pi}_{\imath} = 1$

Since an enabled immediate transition fires immediately, it is obvious that the time spent by each vanishing marking is zero. The matrix P can be reduced to a smaller matrix P’ where only tangible markings for timed transitions are considered. The reduced matrix P’ is thus obtained as follows [263]:

$$P' = F + E \times (I - C)^{-1} \times D. \tag{117}$$

Therefore, we formulate this problem with the continuous Markov chain instead of the semi-Markov chain. The steady-state distribution, π of the continuous-time Markov chain is expressed by the reduced EMC given by [263]:

$$\tilde{\pi} P' = \tilde{\pi} \text{ and } \textstyle\sum_{\mathrm{Mi}\in\mathrm{T}} \tilde{\pi}_{\mathrm{i}} = 1 \tag{118}$$

The steady-state probability π_j can be calculated by the mean time spent in marking M_j divided by the mean cycle time [263]. The steady-state solution π_j is given as

$$\pi_j = \begin{cases} \dfrac{\{\tilde{\pi}_j\, X\, (\sum_{k:tk\in ENT(Mj)} \lambda_k\ )^{-1}}{\{\sum_{Ms\in T}\quad \tilde{\pi}_s\, X\, (\sum_{k:tk\in ENT(Mj)} \lambda_k\ )^{-1}} \text{ if } M_j \in \mathrm{T} \end{cases} \tag{119}$$

where $t_k \in \mathrm{EN}(M_j)$ denotes that the transition t_k is enabled in marking M_j.

The steady-state distribution, $\tilde{\pi}$, for the tangible markings after solving equations (118) and (119) as follows:

$\tilde{\pi}$ = (π_1 = 0.00998, π_2 =0.00181, π_5 = 0.00544, π_6 = 0.19958, π_9 = 0.23587, π_{10} = 0.00544, π_{12} = 0.02109, π_{13} = 0.02207, π_{14} = 0.02207, π_{15} = 0.02339, π_{18} = 0.01055, π_{19} = 0.21092, π_{20} = 0.01104, π_{21} = 0.22075).

The ability to constantly supply services without interruptions is assessed using reliability [294]. It can be specifically described as the likelihood that the digital control networks function correctly across the period [0, t], that is,

where the system is operational at time zero and the failure distribution is exponentially distributed with a constant failure rate λ. The steady-state probability of reliability (Rel) and mean time to failure (MTTF) are given as follows:

$$\mathrm{Rel} = \mathrm{R}(\infty) = 0 \text{ and } \mathrm{MTTF} = 1/\lambda \tag{120}$$

Maintainability is defined as the probability that a failed system will be restored to an operable state within a specified downtime t and is given by [295]

$$\mathrm{M(t)} = 1 - e^{-\mu t} \tag{121}$$

where t denotes the downtime (i.e., time to repair) and the repair distribution is exponentially distributed with a constant repair rate μ. The probability of maintainability (Mnt) as t approaches infinity and the mean time to repair (MTTR) is given by

$$\mathrm{Mnt} = M(\infty) = 1 \text{ and } \mathrm{MTTR} = 1/\mu \tag{122}$$

Availability is defined as the fraction of time that the system provides correct services during an observation period, and is dependent on reliability and maintainability [296]. MTTF reflects how good the reliability of each component is and MTTR reflects how good the maintainability is. To achieve high steady-state availability, the MTTF should be designed as high as possible and the MTTR as low as possible. Therefore, we are interested in the steady-state availability analysis that the system provides correct services of data transmission from the plant network to the enterprise network or vice versa. The steady-state availability is given as:

$$\mathrm{AVL} = \sum_j \boldsymbol{\pi_j} \tag{123}$$

Where πj is the steady-state solution corresponding to the state j where the system is available, i.e., providing correct services. The steady-state solution π can be calculated by using the definition above.

4.3 The Impact of Cyber Attacks

The case study to assess the domino effect in the case of an IEEE 4 Bus system is depicted in this section.

4.3.1 Scenario 1: Bus 1 to Bus 2 cascade propagation Considering both Physical and Cyber Failures

Figure 4-9 depicts the layout that was evaluated during the analysis. We suppose that the breakdown of generator number 1 was caused by both a physical failure and a cyberattack scenario, affecting bus 1. The latter can cause escalation vectors, which can affect nearby units. For buses 1 and 2, convert the IEEE 4 Bus into a state-space graph or generalized stochastic model.

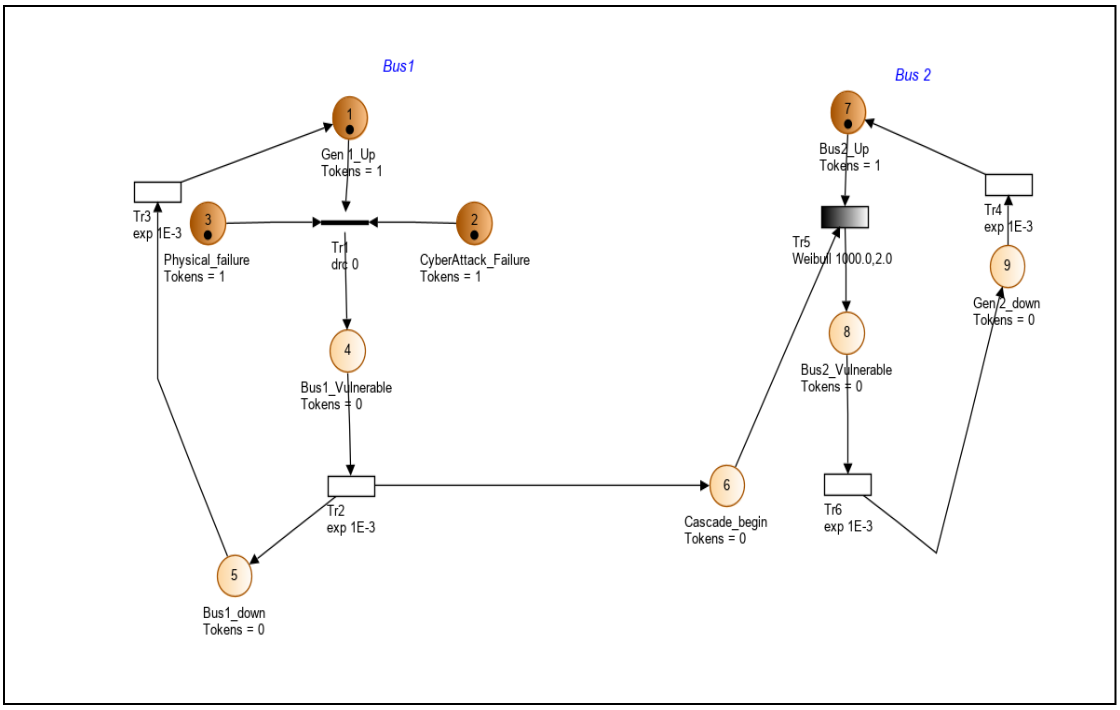


Figure 4-9. Considering both physical and cyber failures

In its initial state, there is a token each in the places Gen1_Up, Physical_failure, CyberAtack_Failure, and Bus2_Up. The transition Tr1 once enabled changes the state of bus 1 from normal to vulnerable without any delay based on the protection settings of the transmission line intelligent electronic device (IED). The vulnerability of bus 1 has a cascading or domino effect on bus 2 if the vulnerability is sustained, and Tr2 which is an exponentially distributed transition is enabled, then bus 1 fails. The failure propagates an effect on bus 2 which falls into a vulnerable state once Tr5 gets enabled. Similarly, if no action is applied bus 2 equally fails when the CDF transition Tr6 is enabled. The transitions Tr3 and Tr4 are restoration transitions for bus 1, and bus 2 respectively.

4.3.2 Scenario 2: Bus 1 to Bus 2, Bus 3, and Bus 4 Cascade Propagation

The final scenario depicted in figure 4-10, is a GSPN model for the entire 4-bus system. Tokens in places Bus1_Up, Bus2_Up, Bus3_Up, and Bus4_Up indicate that the four buses are in their normal operating state. The presence of tokens in places 2, and 3 introduce vulnerabilities in the form of physical and cyber failures. Firing or enabling of the transition Tr2 initiates a failure in Bus 1, and propagates cascaded effects to mostly buses 2 and 3, bus 4 is reliant mostly on power supply from generator 2 but it's equally vulnerable to a domino effect due to the loss of loads on the other busses if load curtailment is not initiated.

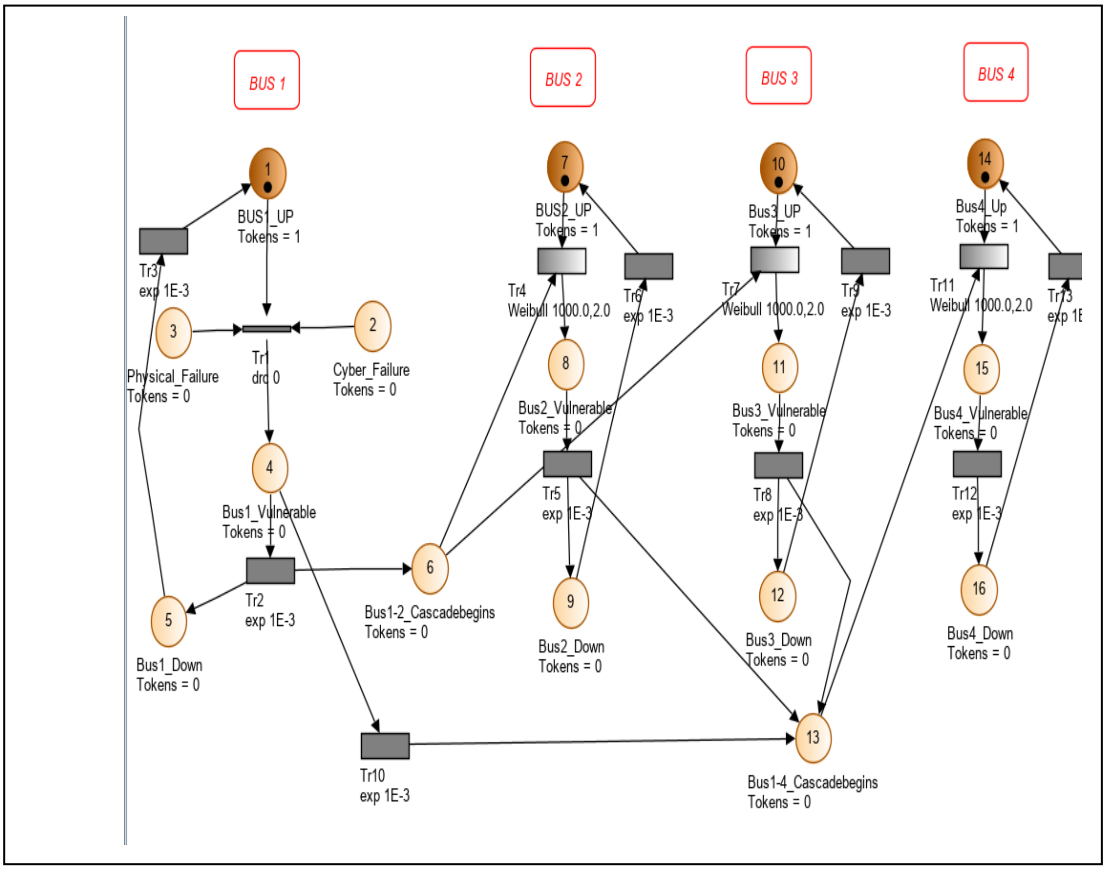


Figure 4-10. A four Bus complete model

4.4 Wind Farm Security Risks, Cyber Architecture, and Testbeds

From the perspective of functionality and security, a wind farm can be envisioned as having two interconnected, cooperative infrastructures: (i) power infrastructure; and (ii) communications infrastructure. Figure 4-12 presents a schematic diagram of a wind farm infrastructure showing an electrical and control network. The electrical network consists of wind turbines, transformers, power lines, relays, and circuit breakers while the control network consists of programmable logic controllers, remote terminal units

(RTUs), IEDs, and communication equipment. For larger wind farms, wind turbines are arranged in a fiber ring for IP-based communications and are connected to an operations control system in a substation. In the substation, equipment's categorized into the operations control system and the transmission control system. These remote substations are connected to the control station located via a wide area network. Thus, the modern wind power plant is made up of mainly three parts: information technology, industrial control, and physical assets.

Access to the virtual private network (VPN) by the suppliers of hardware or software service providers is another vulnerability in cybersecurity. An attacker may utilize a VPN that employs out-of-date and unencrypted protocols to remotely access the LAN that manages the wind farm. Real-time command and measurement data can be modified on the workstation. Both the remote control for the wind farm and the control center is open to penetration via a VPN. If the SCADA server and Inter-Control Center Communications Protocol (ICCP) server are compromised, an attacker will have an access to prevent the operation of wind farms. The attacker may alter the wind turbine's output, insert bogus data, or cause an emergency shutdown, which could result in a hard halt that causes undue wear and tear on vital mechanical parts. In this study, the likelihood of cyberattacks was modeled as the outcome of a competition between exploiting and repairing cyber vulnerabilities. On the system dependability evaluation, the next operating and physical states of wind turbines were projected.

4.4.1 The Architecture of the Testbed

The OPAL-RT offers a cost-efficient, scalable, and flexible real-time platform with a highly incorporated Linux-based real-time operating system for extreme performance [297]. The co-simulation of the communication network on the network emulation software EXATA CPS along with the electric power network simulated with HYPERSIM provides the real-time simulation platform to observe the response of the power system under different cyberattack scenarios. EXATA CPS [298] is integrated with OPAL-RT's HYPERSIM simulator on the same hardware to offer a complete real-time cyber-physical situation for the development, testing, and assessment of electrical grids with communication networks [298]. They can employ low-latency communications at layer 2 to analyze cyber threats that can be injected at these lower layers in the physical system. The testbed, shown in fig 4-11, fig 4-12, and fig. 413 was developed on three different layers: 1) the electrical grid and substation layer; 2) the communication layer; and 3) the application layer, where the electrical and substation layer is modeled in HYPERSIM, the communication layer in EXATA CPS and application layer in Survalent SCADA [299].

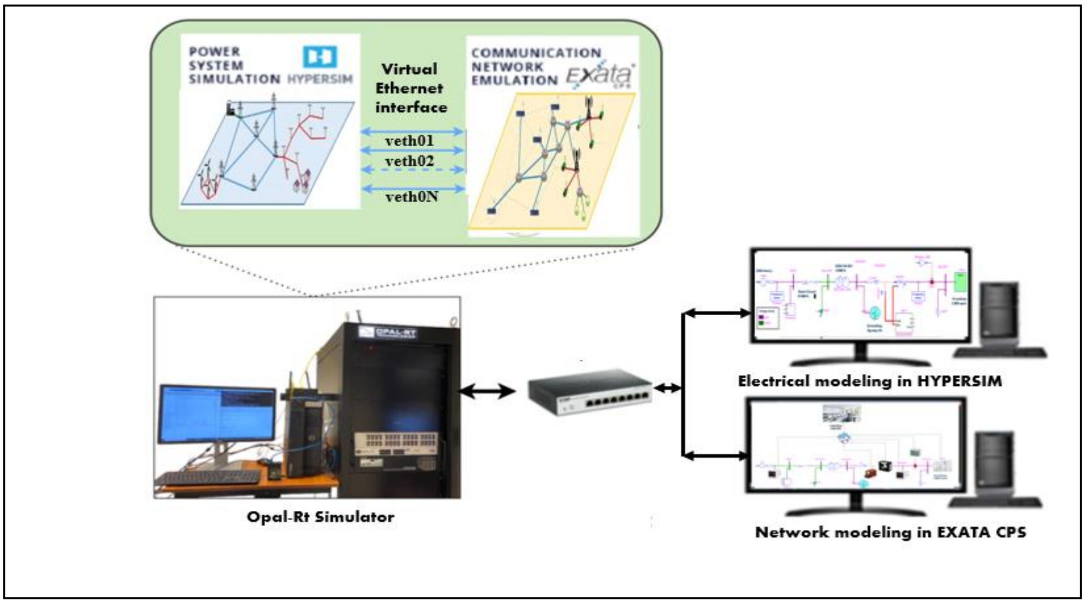

POWER SYSTEM SIMULATION HYPERSIM
Virtual Ethernet interface
veth01
veth02
veth0N
COMMUNICATION NETWORK EMULATION Exata CPS
Opal-Rt Simulator
Electrical modeling in HYPERSIM
Network modeling in EXATA CPS

Figure 4-11. The co-simulation testbed of the wind farm

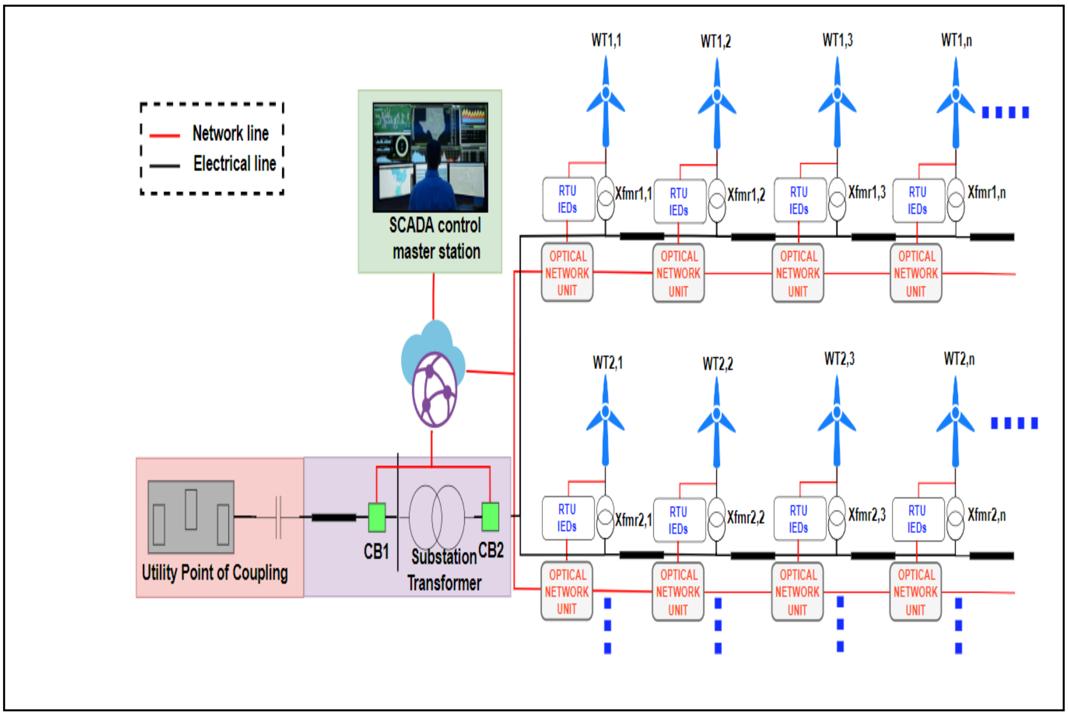


Figure 4-12. The Wind Farm Cyber Architecture

4.4.2 Case Studies

The physical system layer representing the Wind Power Plant (WPP) is developed with 50 equivalent wind turbines, each producing 2 MW, connected to the 230kV line-line voltage distribution system through a 230kV/34.5kV, 125 MVA sub-station transformer. The turbine is a 425V current source direct drive-based generation block connected to a 34kV collector system through a saturation transformer. The network layer is modeled with multiple wind turbine nodes connected to the SCADA node and employs DNP3 (Distributed Network Protocol-3) and IEC 61850 protocol. The physical and network layers are mapped using virtual ethernet ports within the OPAL simulator. Information from each turbine is mapped to the Survalent SCADA database by creating DNP3 clients, which emulate virtual RTU and are visualized using SMART VU. The communication between the wind farm and the control center is through the gateway. Different cyber-attack scenarios are simulated in EXata CPS, and the impact of a cyber-attack is visualized in Hypersim. Also, the implementation of the situational control algorithm in wind farm SCADA system is studied with and without cyber-attacks.

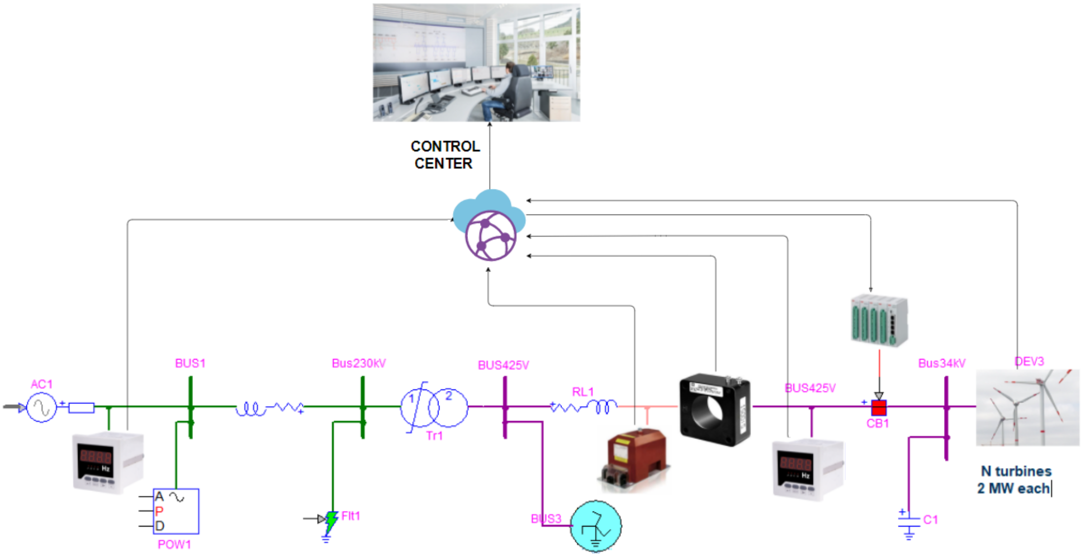


Figure 4-13.The Wind farm cyber-physical modeling

4.5 Attack Modeling and Mitigation

4.5.1 LSTM Models Training for the AGC Model

The two LSTM models are created and trained based on the formulation in chapter 3. To train and test the LSTM models, 2400 cases of attack scenarios (ramp, pulse) and normal operations are created and used as input data. Each case is composed of 1000 time steps vectors of the Δf_1, Δf_2, and ΔP_{tie} signals. Out of these 2400 cases, 70% were used for training and validation, and 30% were used for testing. The two models had one input layer, five hidden LSTM layers, and one output layer.

During training, the model performance is optimized by finding the optimal hyper-parameters. Hyperparameters include the number of hidden layers, the number of neurons per layer, and the learning rate. In this paper, we used the grid search technique [300] to tune the hyperparameters and to systematically search for the optimal number of hidden layers and nodes per layer. The optimal parameters are five hidden layers with 100 neurons per layer, the Adam optimizer [301] with a learning rate of 0.008. The grid search parameters and selected values are outlined in Table 4-7. The training of the models required 10,000 iterations for both the detection and mitigation models.

Table 4-7. The grid search parameters for tuning hyperparameters

Hyper-parameter	Search values	Optimal value
# of hidden layers	[3,5,7]	5
# of neurons per layer	[10,100,1000]	100
Optimizers	Adam, SGD	Adam
Learning rate	[0.001,0.004,0.008,0.01]	0.008

4.5.2 IEEE 118-Bus Test Benchmark

In this section, we present the origin and the preparation of the data set for the LSTM model, followed by the implementation of the LSTM techniques and the performance metrics.

4.5.2.1 Data Preparation

For the implementation of the FDIA attack, we generate the load data set by simulating the real-world load measurements on each bus. The power grid was assumed to operate under normal conditions and the scaled aggregated 5-min load data is used. The obtained input load data follows the normal distribution whose mean is equal to the base load and the variance is 16.67% of the base load. We index the line flow from meters located at each bus and measure the flow from adjacent buses. The dataset consists of data from the IEEE 118-bus power test system with the following statistics (shown in table 4-8):

Table 4-8. The topologies of the IEEE 118-bus test benchmark

Parameters	Number
Buses	118
Lines	186
Measurements	180
Injected measurements	70
Flow measurements	110
Unmeasured lines	7

For the cyber layer, network performance testing measures the performance of a network in terms of packet loss, throughput, delay, and output. This can be done by using tools such as iperf, ping, traceroute, and others. Packet loss, throughput, delay, and output are all important performance metrics for networking systems.

- Packet loss: Packet loss refers to the percentage of packets that are not successfully delivered to the intended destination. High packet loss can indicate a problem with the network, such as congestion or a faulty link.

- Throughput: Throughput is a measure of the amount of data that is successfully transmitted over a network in each period. It is typically measured in bits or bytes per second. High throughput is desirable, as it indicates that the network can handle a large amount of data.

- Delay: Delay refers to the amount of time it takes for a packet to travel from its source to its destination. High delay can indicate a problem with the network, such as congestion or a long distance between the source and destination.

- Output: Output refers to the amount of data that is successfully received by the destination. It is typically measured in bits or bytes. High output is desirable, as it indicates that the destination can receive all of the data that is being transmitted.

4.5.2.2 LSTM Implementation

We use the preprocessed data consisting of all the above-mentioned variables and we divide the data into the training and the testing sets. The training set contains 10000*180 measurements while the testing set contains 2000*180 measurements. For the implementation of the FDIA attack, we generate the compromised data set by performing optimum attack formulation using the weighted directed graph. We construct the graph by removing the unmeasured lines and assigning weights to the other lines. An attacking node is added which connects all the target nodes with infinite edge weight. We introduce the error variable which is added to the meter measurements in the target node.

The number of target meters follows the discrete uniform (2,10) distribution in the IEEE 118-bus systems. The added noise follows the random Gaussian distribution. The true label of the meter i at time t is determined as given by equation 124.

The code was set up as a Sequential model with two LSTM layers, a Dense layer, and a Flatten layer. The first layer had 64 neurons, with a '*ReLU*' activation function. The unroll parameter was set to True, and '*return_sequences*' was set to True, which meant that the layer will return a sequence of output for each input. The second layer has 64 neurons, with a '*ReLU*' activation function. The activation function maps the first $(i = 1)$ convolution layer generated from the input data, and is expressed as,

$$c_{q,j} = RELU(z * h_{q,j} + b_{q,j}) \tag{124}$$

where, $c_{q,j}$ is q feature map at j^{th} layer of convolution layer, $h_{q,j}$ is q feature map at j^{th} convolution kernel, and $b_{q,j}$ is the corresponding scalar bias. The '*return_sequences*' parameter is set to True, which means that the layer will return a sequence of output for each input. The third layer is a dense layer with 32 neurons and a '*ReLU*' activation function. The hidden features generated on the previous layer are then used as the input to the successive layers and processed similarly.

The fourth layer is a Flatten layer that flattens the input. The fifth and final layer is a Dense layer with 180 neurons and a sigmoid activation function. The sigmoid activation function is applied to the fully connected nodes in the dense layer and provides the output to distinguish the nature of the measurement variables. For the weights and biases of the dense layer, w_d, b_d, the true label of measurement is obtained for equation 125 as,

$$Z(i,t) = sigmoid(w_d * c_{q,j} + b_d) \tag{125}$$

Finally, the model is compiled with a '*binary_crossentropy*' loss function and the '*Adam*' optimizer, with accuracy as the metric for optimal learning. The loss function calculates the difference between the actual output and the predicted output for each epoch. Once enough training samples are provided, the LSTM learns from the features and updates the weight at different layers by minimizing the cross-entropy loss function. The binary cross-entropy loss function is commonly used for binary classification problems, where the goal is to predict a binary outcome. It is defined as follows:

$$Loss = -(y * \log(p) + (1 - y) * \log(1 - p)) \tag{126}$$

where "y" is the true label (0 or 1), "p" is the predicted probability that the example belongs to class 1, and the log is the natural logarithm. The binary cross-entropy loss measures the dissimilarity between the predicted probabilities and the true labels.

The Adam optimizer is an adaptive optimization algorithm that updates the model's parameters based on the gradient of the loss function and historical gradient information [301]. The algorithm computes an exponential moving average of the gradient and squared gradient, and updates the parameters based on these averages. The algorithm's update rule for a parameter "w" can be written as follows:

$$w = \frac{w - learning_{rate} * m}{\sqrt{v} + \epsilon} \tag{127}$$

where "m" is the moving average of the gradients, "v" is the moving average of the squared gradients, " $learning_{rate}$ " is a hyperparameter that controls the step size of the optimization, and "ϵ" is a small constant added for numerical stability.

The output from the modeling and fitting of the LSTM model is evaluated from a precision-recall curve which uses the evaluation metrics defined in chapter 3. The precision and recall values can then be calculated from the values in the confusion matrix. A confusion matrix is a table that is used to evaluate the performance of a classification model. In the case of an LSTM model for binary classification, the confusion matrix would contain 4 values: true positives (TP), false positives (FP), false negatives (FN), and true negatives (TN). The values can be calculated based on the predictions made by the LSTM model on the test data. The values in a confusion matrix are used to calculate various performance metrics such as precision, recall, F1 score, and accuracy. These metrics provide insight into the performance of a model and help in understanding the strengths and weaknesses of the model.

CHAPTER 5: RESULTS AND DISCUSSIONS

5.1 Introduction

This chapter discusses the results of the experiments and case studies outlined in chapters 3 and 4.

5.2 The Steady-State Probabilities

We used PIPE (Platform-Independent Petri Net Editor) [199] and Great Stochastic Petri nets [209] to model and analyze the GSPN attack model of the SCADA network. Both tools are open-source tools that support creating and analyzing Petri Nets. They have an easy-to-use graphical user interface that allows a user to create standard Petri Net and Stochastic Petri Net models. It also allows a user to animate the model with the random firing of transitions or interactive user manipulations. The analysis environment in these tools includes different modules such as steady-state analysis, steady space analysis, and GSPN analysis [210].

First, we implemented the DoS model in PIPE as shown in the previous chapters. Next, we assigned a weight to each of the transitions. The designed GSPN model of the DoS attack was simulated fifty times using a different number of initial random firings: 100, 300, 500, 700, 1000, and 1200. The variation of the token distribution with the same number of initial random firings is recorded. The transition triggering rates of the Défense Scenario's firewall, password, and combined SPN models respectively (models I, II, and III). SPN models are shown in Table 0-1 in the appendix.

In the evaluation process, we obtained the transition triggering rates (shown in Table 0-1 in the appendix). Then, we conducted the simulations, to get the reachable markings' set of the three scenarios respectively. We obtained the steady-state probability (shown in table 0-2 in the appendix) for further performance evaluation.

5.2.1 The Combined Firewall, and Password Models

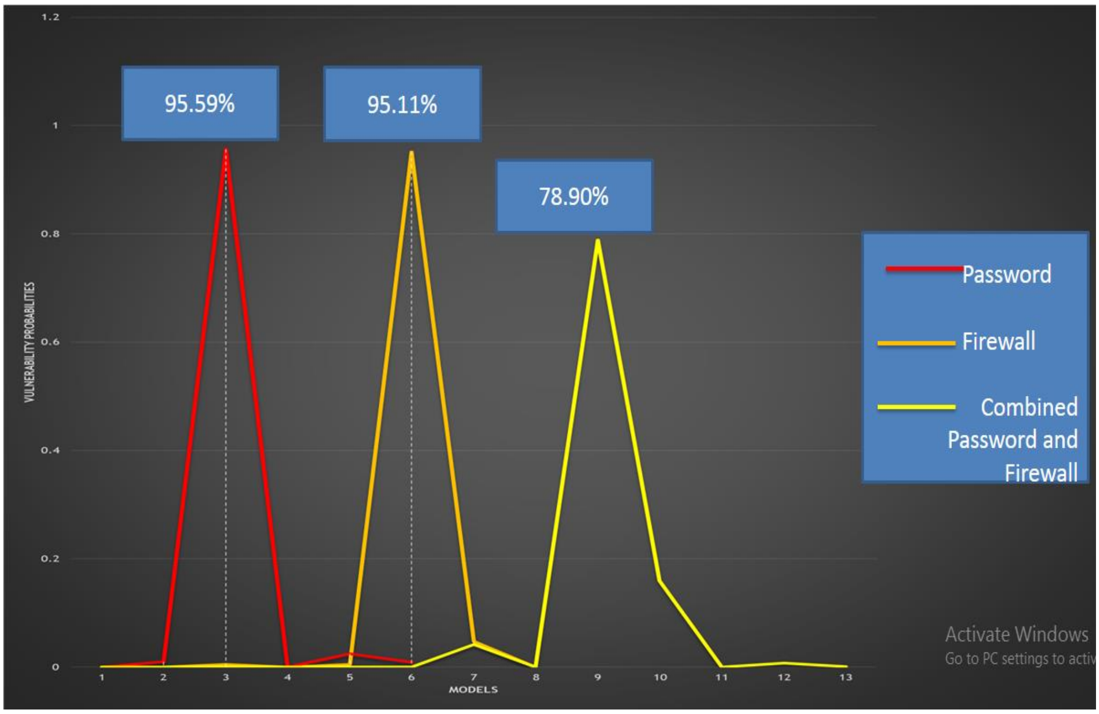


Figure 5-1. The performance comparison for all models

Performance Comparison

With the data, we got from the simulations in chapter 4 and the equations of the three scenarios in chapter 3, we can figure out the system breach probability (Psysbreach), failure rate to crack the password, and several parameters. Scenario I target state is Psystem breach which is achieved by circumventing any or all of the three firewall rules. The number of successful attempts to open a port relative to the total attempts to open the port is based on operating system event logs, while response times are based on the specification of server performance and security events logs of servers. In our case, a 10 percent for success rate and a 90 percent fail rate were applied. Cybersecurity audits or vulnerability assessments are not frequently conducted in Industrial Control Systems (ICS/SCADA) as compared to IT infrastructures due to availability issues.

By analyzing the data, we can deduce that the probability of breaching the system in scenario I was 0.48% and after adding the password mechanism, the security probability of the system and the defense level are both increasing gradually. The probability of the system being intruded on when secured by the password was assumed at 1% and this resulted in a steady-state probability of a system attack of 2.485%.

Indicating that a password is not an ideal defense mechanism to secure a SCADA system.

From figure 5-1, it can be deduced that the net probability of being attacked with only a password as an intrusion protection mechanism was higher at 95.59% compared to the firewall model at 95.11%, and a combined model gave 78.902%. This indication demonstrates that given a firewall and a password as a combined intrusion protection mechanism then the probability of being hit by a cyber attack was relatively very high.

5.2.2 WAN Model

The steady-state distribution, $\tilde{\pi}$, for the tangible markings after solving equations (37) and (38) as follows:

$\tilde{\pi}$ = (π_1 = 0.00998, π_2 =0.00181, π_5 = 0.00544, π_6 = 0.19958, π_9 = 0.23587, π_{10} = 0.00544, π_{12} = 0.02109, π_{13} = 0.02207, π_{14} = 0.02207, π_{15} = 0.02339, π_{18} = 0.01055, π_{19} = 0.21092, π_{20} = 0.01104, π_{21} = 0.22075).

Having calculated the steady-state probabilities, we then computed the reliability and availability. For reliability, it can be seen that only the initial state is reliable, and the rate of leaving the reliable state M_o is λ_1. Thus, we can have the steady-state reliability as R = $e^{-0.99t}$

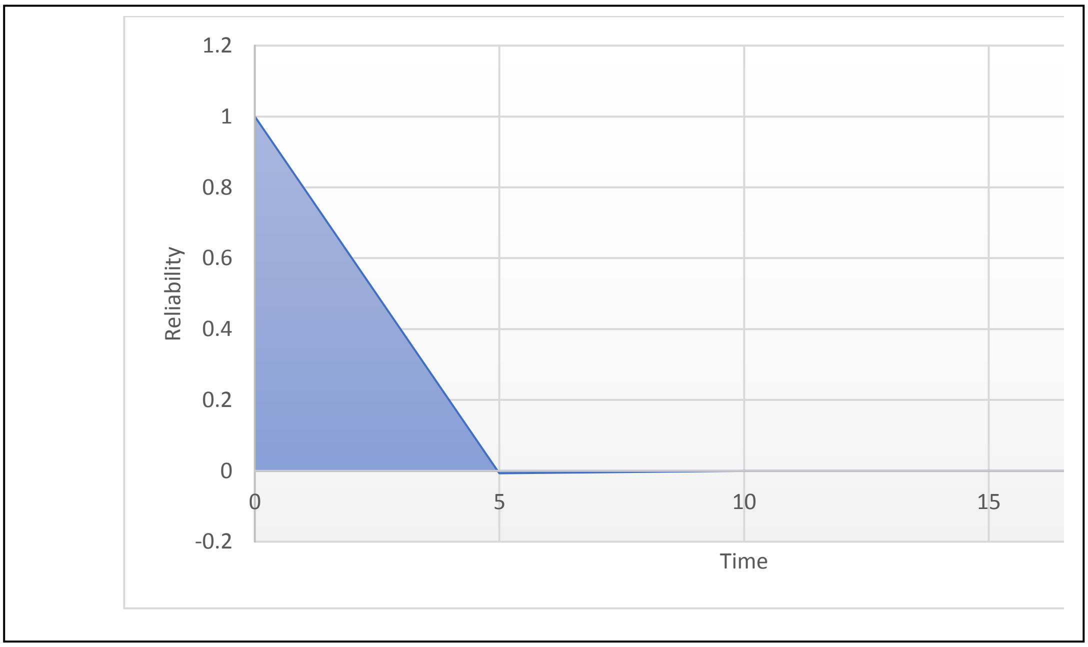


Figure 5-2. The steady state availability

Assuming that the initial state (M0) is reliable and not susceptible to any intrusion, then:

Ava = 1 – (0.00181 + 0.00544 + 0.19958 +0.23587+ 0.00544 + 0.02109 + 0.02207 + 0.02207+ 0.02339 + 0.01055 + 0.21092+0.01104+0.22075)

Then steady-state availability is 0.99002. Therefore, we have demonstrated that the proposed framework is highly applicable for dependability and reliability analyses. We can further improve steady-state availability by improving cybersecurity and maintenance policies.

5.3 The Stochastic Impact of Cyber Attacks

5.3.1 Scenario 1: Results

To model the domino effect, GRIF's PN module [302] was used to model the stochastic impact of the cyberattacks on the power systems contingencies. The results show that generator number 1 or bus 1 has a higher probability of being in a running state compared to bus 2. Conversely, a probability of 0.1497 compared to 0.112 shows that bus 1 is highly likely to be in a failed state. The sojourn times for the places depicting the escalation vectors are zero, and hence the steady-state probabilities for places CyberAttack_Failure and Physical_failure are zero. See figure 5-3 for a detailed view of the results.

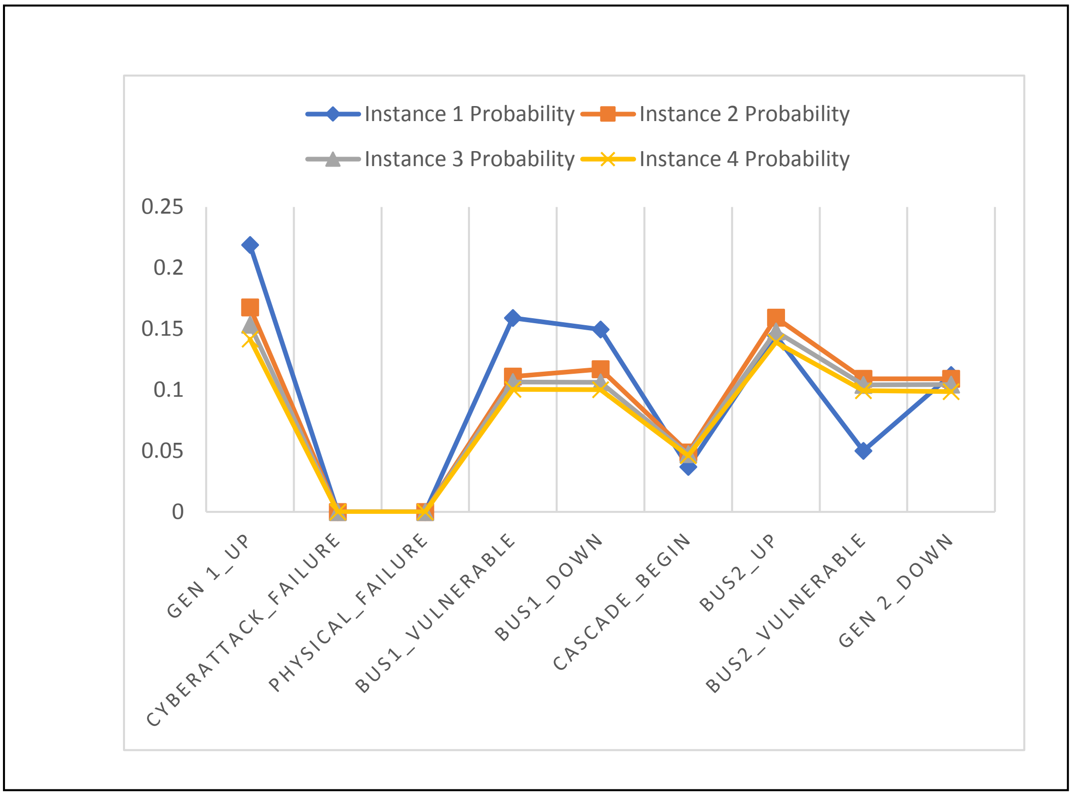


Figure 5-3. The comparison of instance probabilities

5.3.2 Scenario 2: Results

Maintaining the argument introduced in chapter 4.3, the steady-state probabilities for scenario 2 are depicted in figure 5-4 below.

The result suggests that the probability of buses being in the running state is higher for bus 1, seconded by bus 2, third is bus 4 and last is bus 3. Concerning cascaded vulnerabilities; bus 2 has a higher likelihood is falling due to escalating vectors emanating from bus1, while bus1 is less likely to be affected by a cascaded vulnerability. States Bus1-2_Cascadebegins and Bus1-4_Cascadebegins depict the initiation of the cascading effects with steady-state probabilities of 0.0471 and 0.0456 respectively.

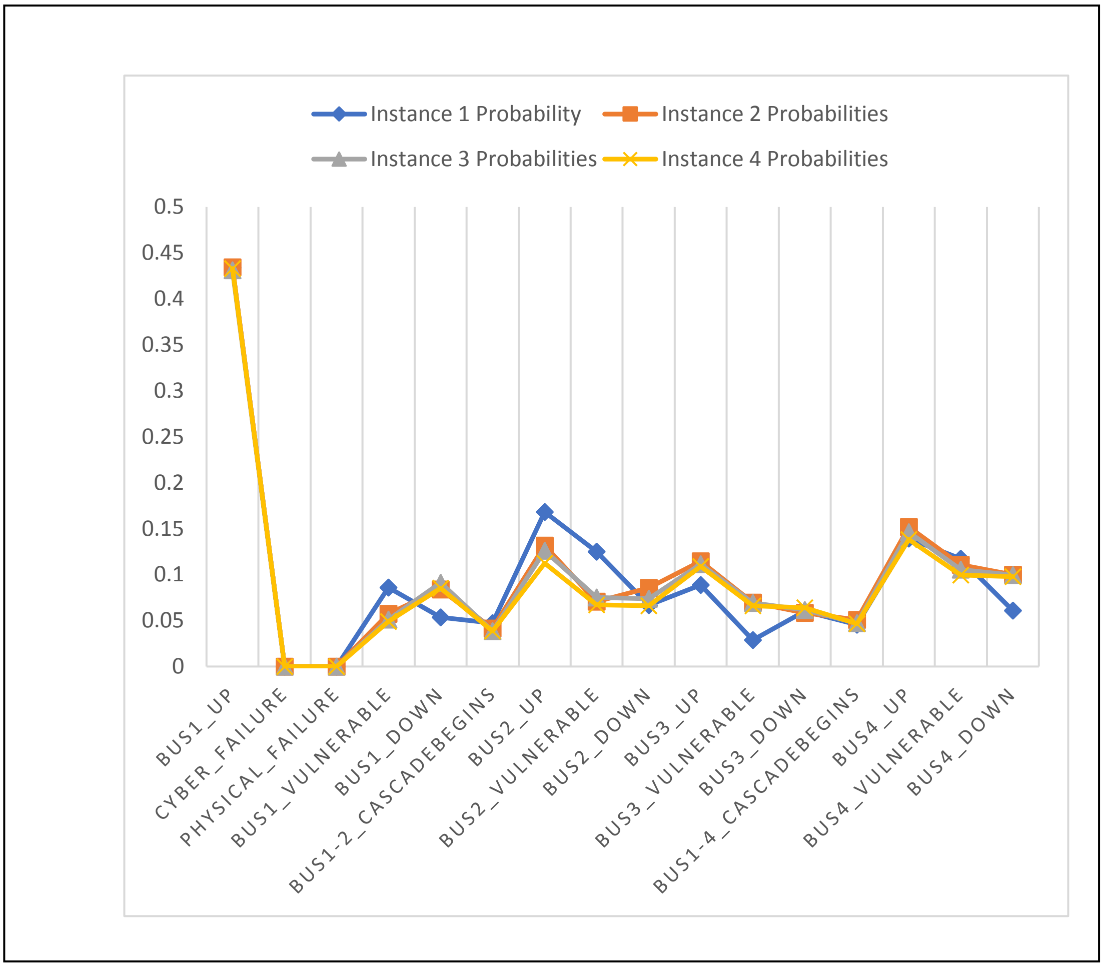


Figure 5-4. The comparisons of instances

5.3.3 Numerical Analysis of Performance and Economic Impact of Attacks on a 24-Bus System

Based on the computation procedure described in chapters 3 and 4 applied to the IEEE 24 bus. The corresponding Locational Marginal Pricing (LMP) tabular results are shown in Table 0-6 (see appendix). In this case, a data integrity attack on the transmission line and buses was modeled.From table 0-6 it is determined that buses 14, 11, and 6 have the highest LMP As a result, these three elements are regarded as the most important when estimating the consequences of a cyber-attack. System designers must pay special attention to these components so that suitable rules and procedures may be developed to safeguard their integrity and make the system as dependable as possible. Evaluation of the economic impact is based on the LMP given in table 0-6 in Appendix B and the average vulnerability probability. As a result, the cyber-net attack's risk owing to bus outages (line) is calculated using equations 91 and 92.

R_{14} = 0.060 x 67.3583 = \$ 4.041/hr (128)

R_{11} = 0.060 x 61.6508 = \$ 3.939/hr (129)

R_6 = 0.060 x 60.5628 = \$ 3.633/hr (130)

5.4 The Real-Time Simulation Testbed Results

The control station has two basic functionalities: a SCADA system for real-time monitoring and a control system for controlling and defending against cyber-attacks. The mathematical formulation of the cyber-physical model is generated based on the available measurements, and an attack detection study is performed in real-time. The control involves a real-time data-driven adaptive learning technique for accurate estimation of the behavior of the system. The control center monitors power production and can send active and reactive power setpoints to wind turbine generators. In the presence of any abnormalities, the attack detector must detect and identify the manipulated measurement and take appropriate measures, such as active power control, VAR support, optimal power flow, and reliability analysis, among others.

5.4.1 Case 1: Modify Packets Attack.

To validate the modeling defined in the preceding chapters, we used the real-time simulation testbed. For this case study, a vulnerability in the protection mechanism of wind turbine control was tested, and the results were observed before and after the cyberattack. First, the system was run in a normal, attack-free environment. Figure 5-5 shows the behavior of the system under normal operation. The wind speed measurement for the turbine (in blue) and the measurement received by the control center (in red) matches since we do not have any cyber-attack. The frequency at the POC is 60 Hz, and the turbine is generating output based on the available wind speed measurements. A cyber-attack to manipulate the wind speed measurement of the wind turbine was performed at the wind turbine actuator node. The goal of this attack is to modify the wind speed measurement signal going into the control center. Figures 5-6, and 5-7 show the behavior of the system in the presence of a cyber-attack. We observed the difference between the actual wind speed (in red) and the measurement received by the control center (in blue). As the wind speed measurement was seen going above the cut-off wind speed, the control center sent the false trip command to the wind turbine circuit breaker. The impact of the cyberattack is mainly seen in frequency deviation, voltage oscillation, and loss of generation output. The false information given to the controller forces it to make false decisions like curtailing the output power, increasing the load demand, shutting down the turbine, or even shutting down the entire wind farm. The random turning on and off of the turbine creates oscillation at the point of coupling. The oscillation can go beyond the acceptable values, which creates instability in the grid.

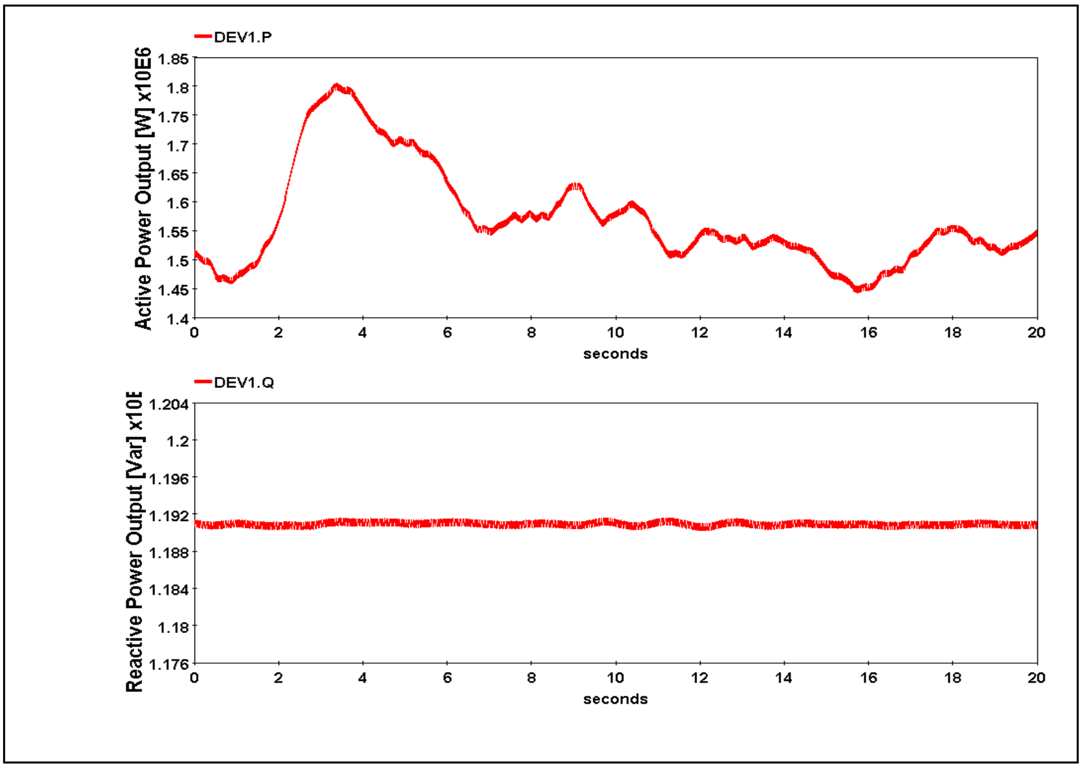


Figure 5-5. The Active Power and Reactive Power before a cyberattack

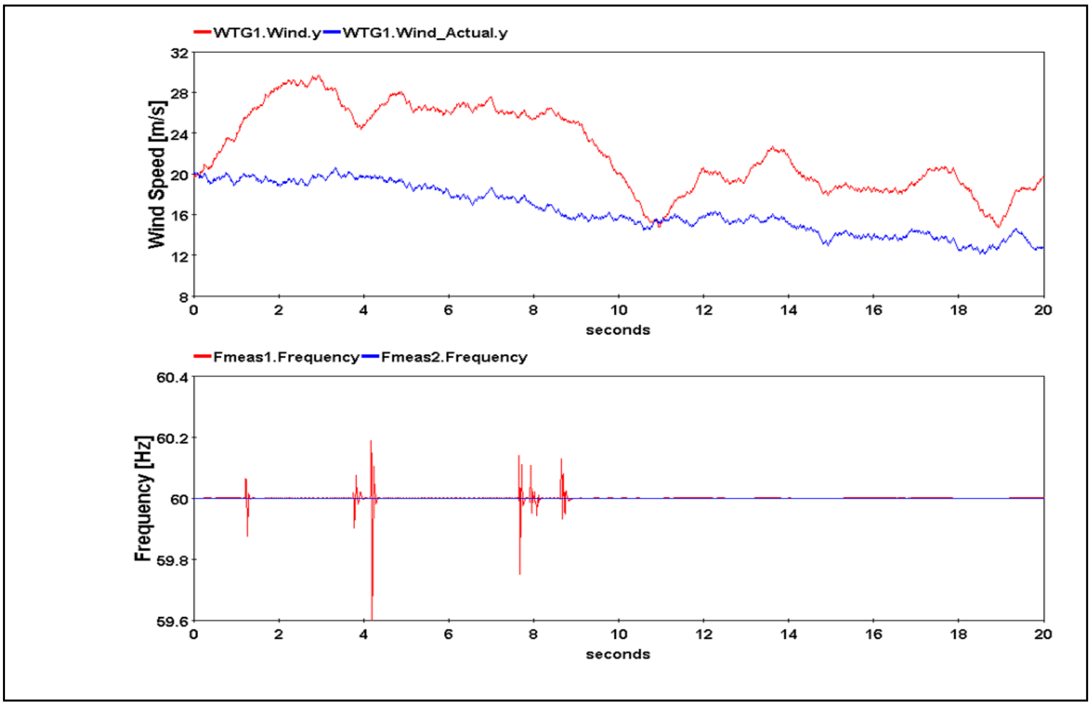


Figure 5-6. The wind speed and the frequency graphs after a cyberattack

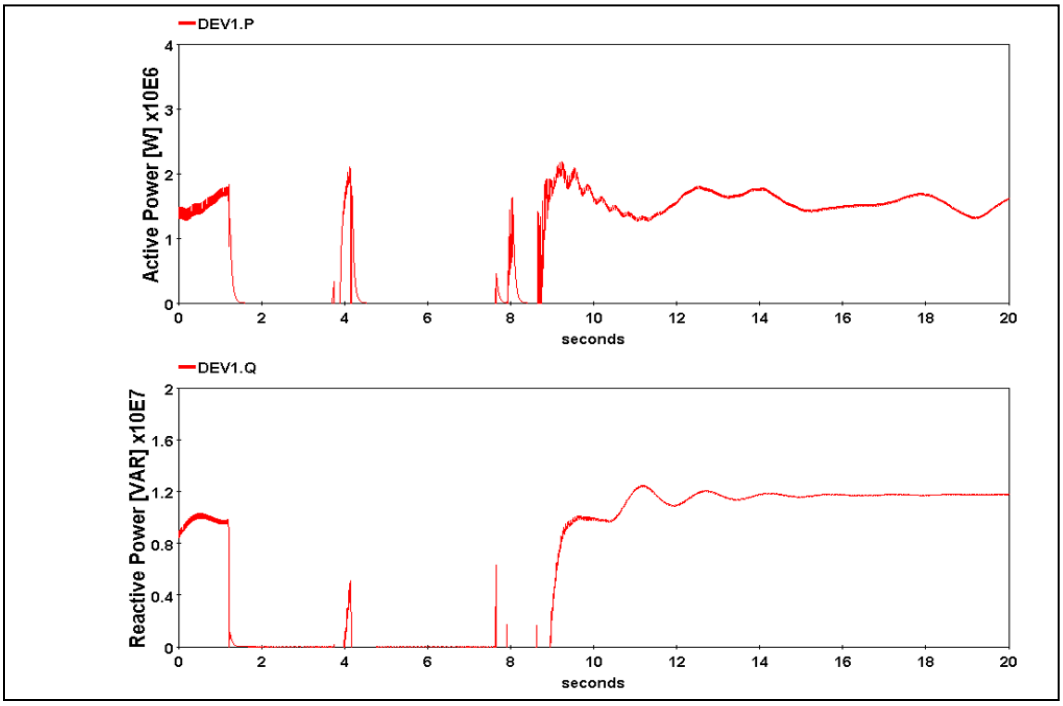


Figure 5-7. The Active Power and Reactive Power measurement after a cyberattack

5.4.2 Case 2: Distributed Denial of Service (DDoS) Attack.

For our second user case, the DDoS attack was performed at the wind turbine nodes. The DDoS attack is the simplest and most popular in the cybersecurity field. However, it can be significantly devastating as it overwhelms the resources of the victim's device and takes it out of service. The failure of enough critical devices may result in a cascading effect and cripple the entire power system. A DDoS attack approach may include: a) flooding a channel/device with data traffic, b) flooding a channel or device with TCP SYN packets. c) Sending IP fragments to devices When any devices are flooded with UDP traffic, it consumes the buffer memory and CPU resources of the devices. If the devices are flooded with TCP SYN packets, the transport layer memory is overloaded. In contrast, if the devices are swamped with a large number of IP fragments, the network layer buffer memory is compromised. All of these attacks effectively render a device incapable of performing legitimate operations. Successful initiation of a DDoS attack requires an attacker to possess or take over a network of computers, also known as a botnet, and perform the activities mentioned above.

.

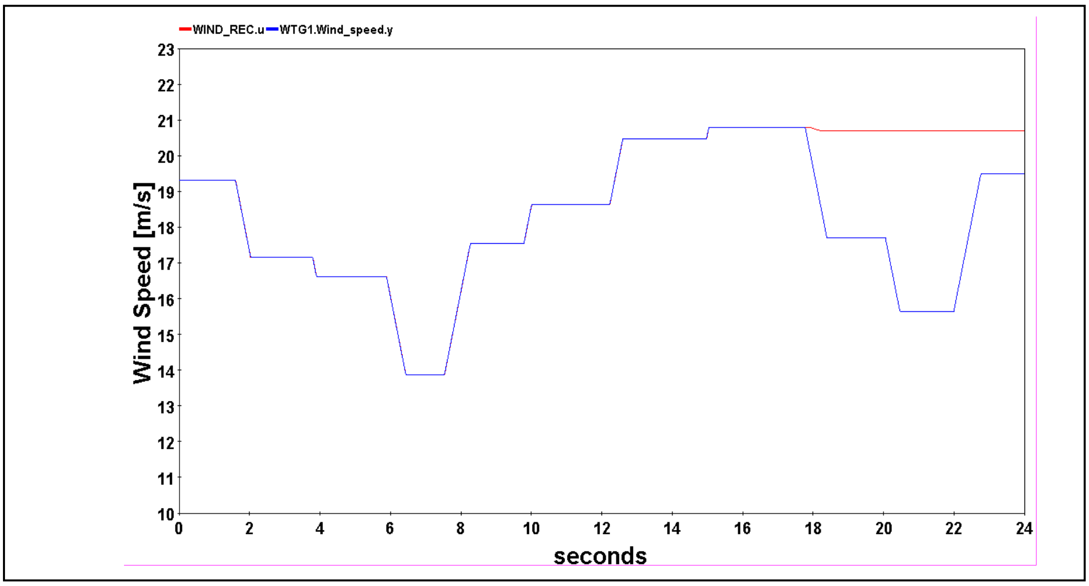


Figure 5-8. The Wind Speed graph under a DDos attack

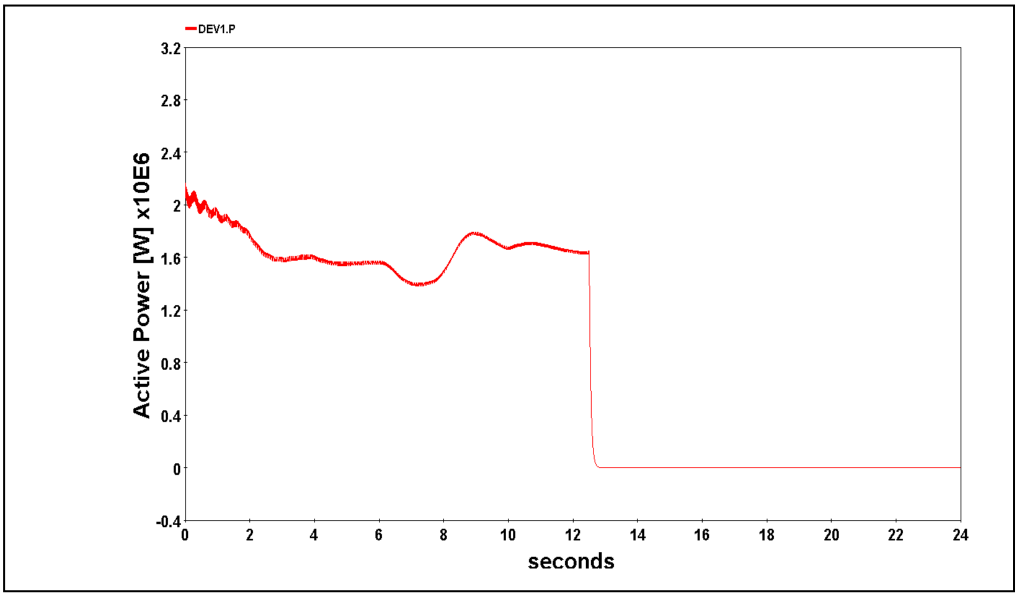


Figure 5-9. The Active Power graph under a DDoS attack

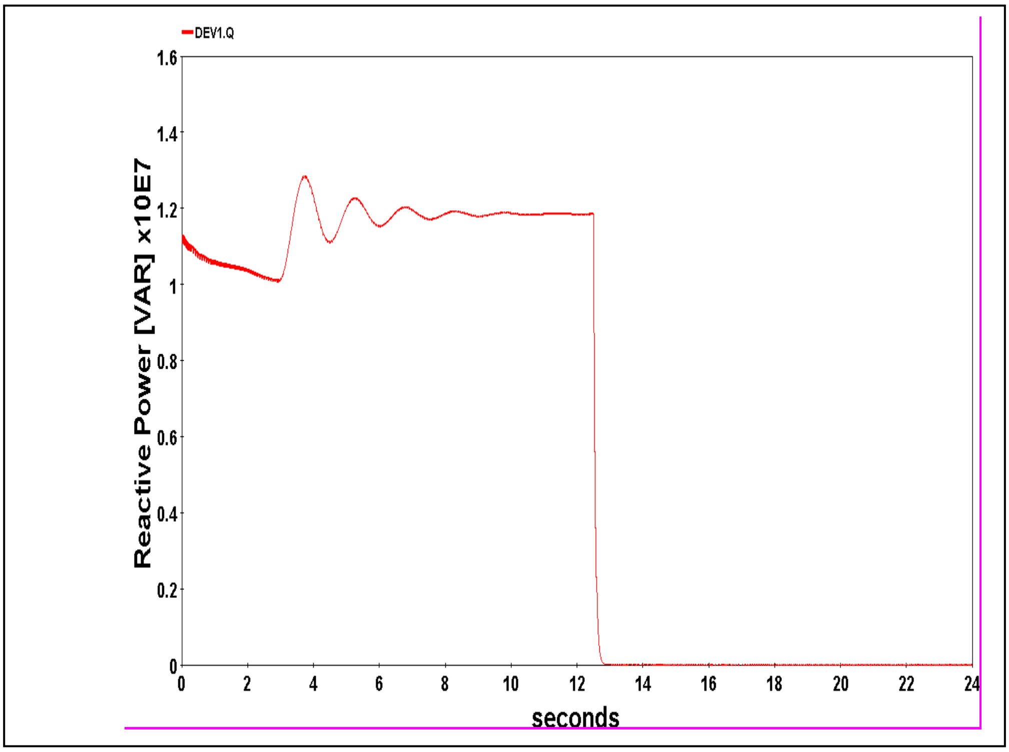


Figure 5-10. The reactive power graph under a cyberattack

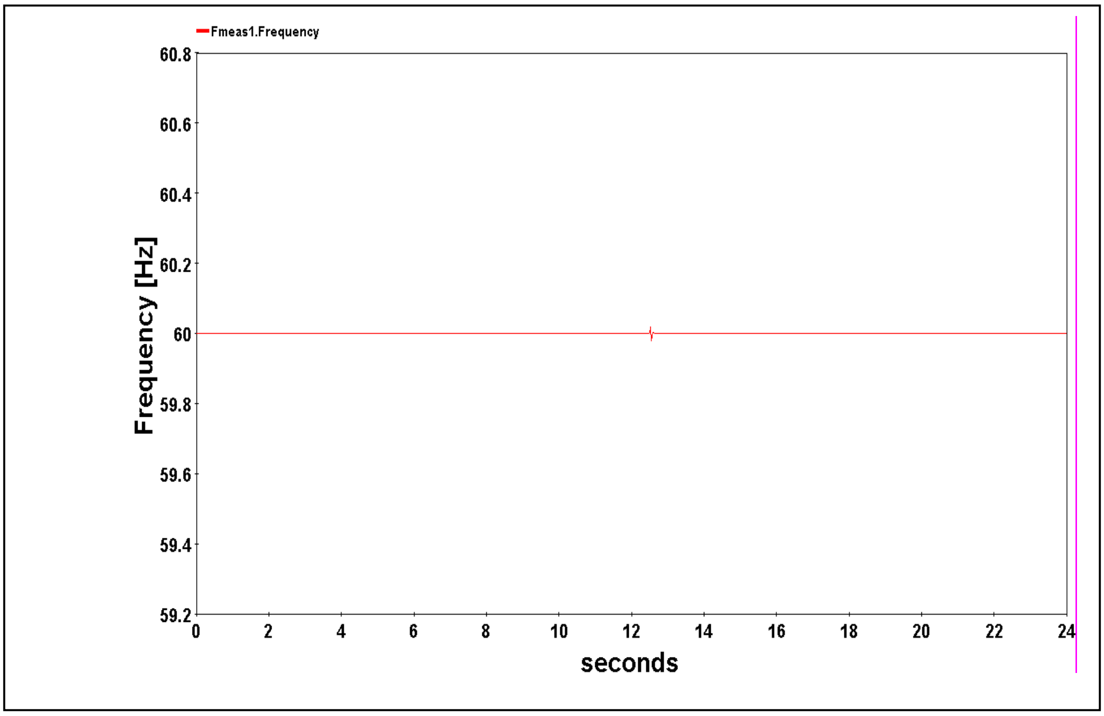


Figure 5-11. The frequency graph

In our case study, the attacker has succeeded to infiltrate the three machines in the network. During simulation, the botnet continuously floods the controller with massive data packets at the beginning of each 15s. The control center receives the wind speed from the field-deployed sensors before the start of a DDoS attack. The controller functions in zones from Zone I to Zone IV depending on the wind speed. It is not practical to run the WT for power production if the wind speed is less than the WT's cut-in speed. Hence, WT is not in use (Zone I). The WT works at partial power operation if the wind speed is between the cut-in speed and the rated speed. At this zone, the WT produces less power than the rated power. At Zone III, the wind speed lies in between the rated speed and cut-out speed; the wind farm can produce the rated power. If the wind speed exceeds the cut-out speed (20m/s), also known as Zone IV, the wind turbines are deliberately taken out of operation to avoid any mechanical damage on a wind turbine. After the onset of the DDoS attack at 15s, the buffer memory and CPU resources are overloaded, and the controller is unable to receive the actual wind speed and perform the control operation. As a result, the controller fails to operate the wind turbine even after the wind speed drops below the cut-out speed. The effect of DDoS is reflected in reactive power and active power generation, as shown in figures 5-8, 5-9,5-10, and 5-11 respectively.

5.5 The AGC Results

Fig. 5-12 depicts the training progress for four models: one $LSTM_{detection}$ model and three $LSTM_{mitigation}$ models, one for each signal. The improvement for the detection model is measured by the increase in model accuracy performance on the testing data, while the improvement of the mitigation models is depicted by the decrease in root-mean-square error (RMSE) value for the testing data.

5.5.1 LSTM Models Evaluation

Table 5-1 shows the confusion matrix for the $LSTM_{detection}$ model. The confusion matrix is an important tool to measure the effectiveness of classification models, whether binary or multi-class models. The confusion matrix combines the actual outputs (ground truth), represented in the matrix rows, and the model predictions, represented in the matrix columns. For the $LSTM_{detection}$ model, there are four output possibilities: No attack (NS), attack on Δf_1, attack on Δf_2, or attack on ΔP_{tie}. The diagonal elements correspond to the correct predictions, while the off-diagonal are incorrect predictions. For example, the model correctly detected and classified 93.25% of attacks on Δf_1, and the remaining 6.75% were flagged as attacks but incorrectly classified. However, the model did not miss any attack case (i.e., flag an attack as NS), which is of greater importance to the system operator from a security perspective. The incorrect classifications are of small percentages compared to the correct classifications for all signals. In addition, Fig. 5-13 reveals the precision, recall, and f_1 score statistical metrics for each location output. The high scores in all three metrics (all above 90%) indicate that the $LSTM_{detection}$ is a strong and balanced classifier.

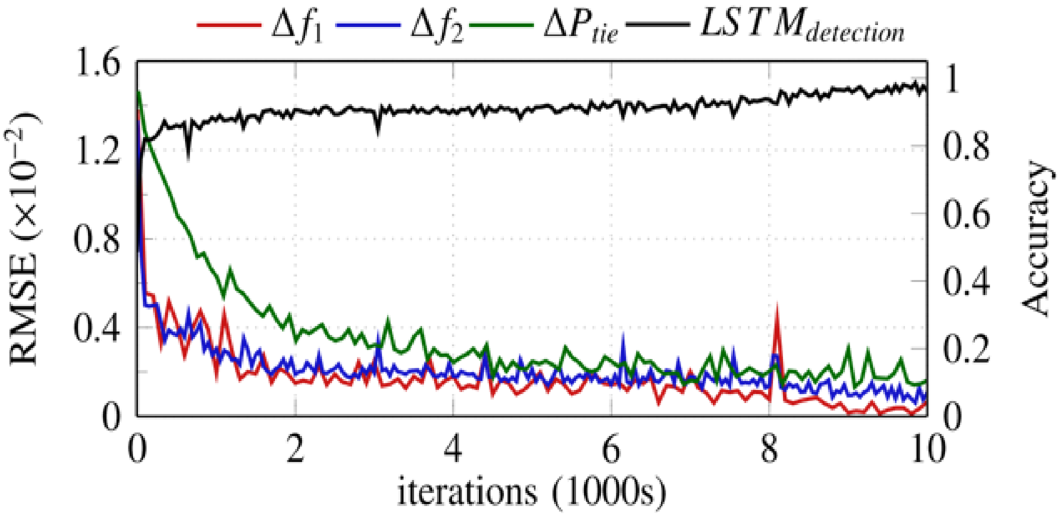


Figure 5-12. The RMSE of the 3 LSTMmitigation and accuracy of the LSTMdetection

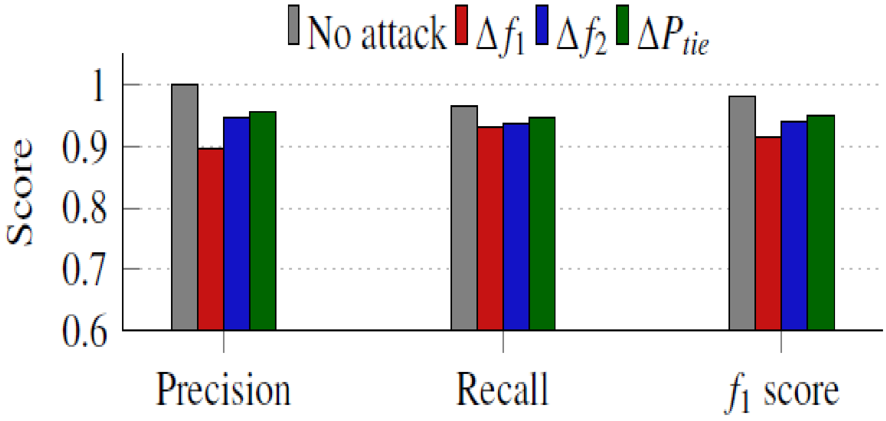


Figure 5-13. The performance of the LSTMdetection model

Table 5-1. The confusion matrix for the LSTMdetection model

Actual	Predicted			
	NS	Δf_1	Δf_2	ΔP_{tie}
NS	96.67%	0.0%	3.33%	0.0%
Δf_1	0.0%	93.25%	3.37%	3.38%
Δf_2	0.0%	4.0%	93.77%	2.23%
ΔP_{tie}	0.0%	3.89%	1.56%	94.55%

The evaluation of the $LSTM_{mitigation}$ performance is achieved by analyzing the mitigated signals in comparison with the original signal as well as the attacked signal. Fig. 5-14 depicts a test case with an attack on Δf_1. The graph shows how closely the LSTM prediction follows the actual signal, in contrast with the attacked signals as perceived by the system operator. Similarly, Fig. 5-15 and Fig. 5-16 depict a similar analysis of the Δf_2 and ΔP_{tie} signals, respectively. Therefore, these signals obtained from the *LSTM* model can be used in case an attack is detected. The RMSE comparison between the magnitudes of attacked signals and the mitigated signals for all testing data is depicted in Fig. 5-17. As shown in the figure, the $LSTM_{mitigation}$ model has significantly reduced the error in measurements.

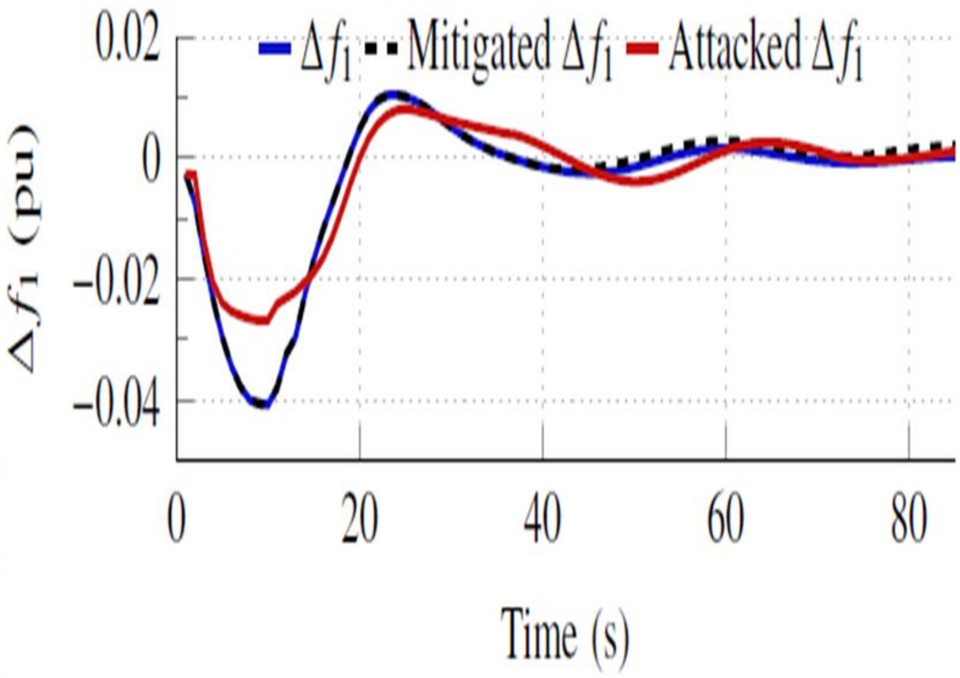


Figure 5-14. Attack mitigation on Δf1

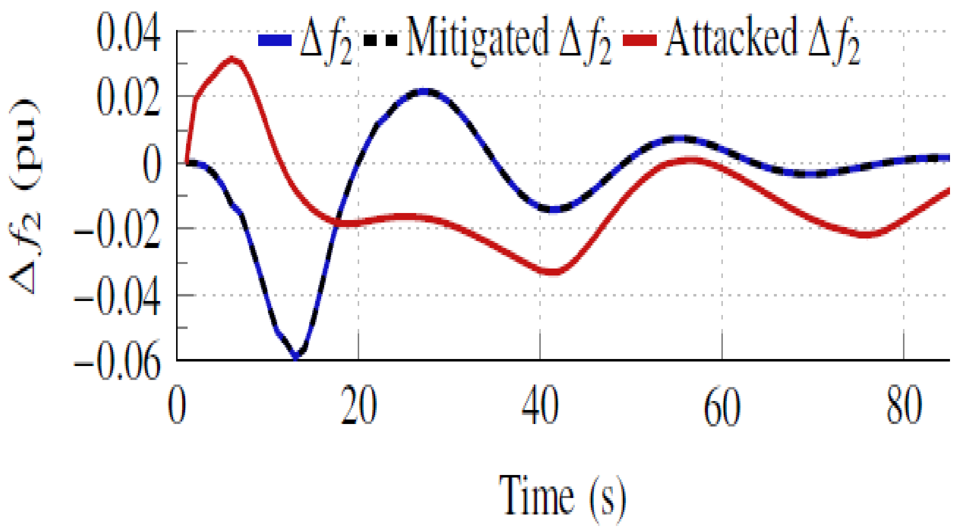


Figure 5-15. The attack mitigation on Δf2

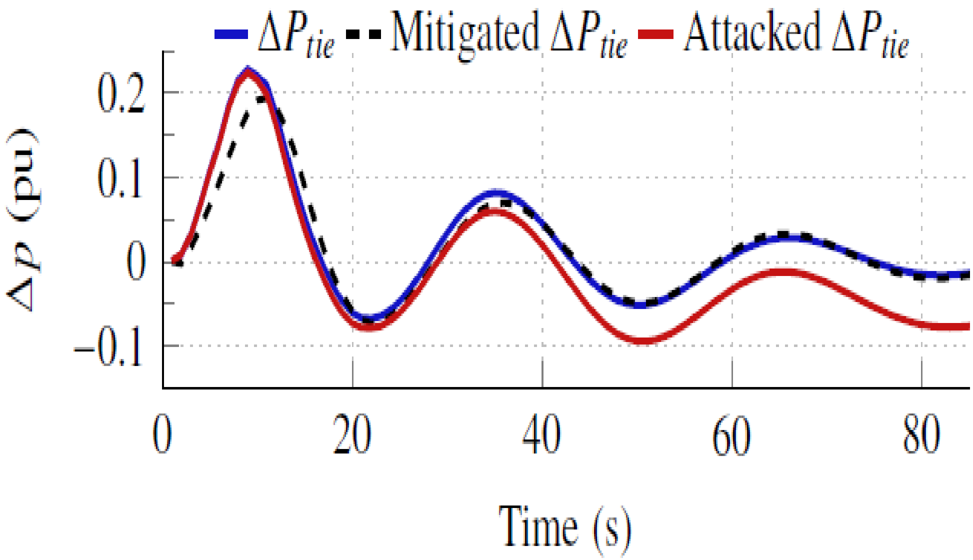


Figure 5-16. The attack mitigation on ΔPtie

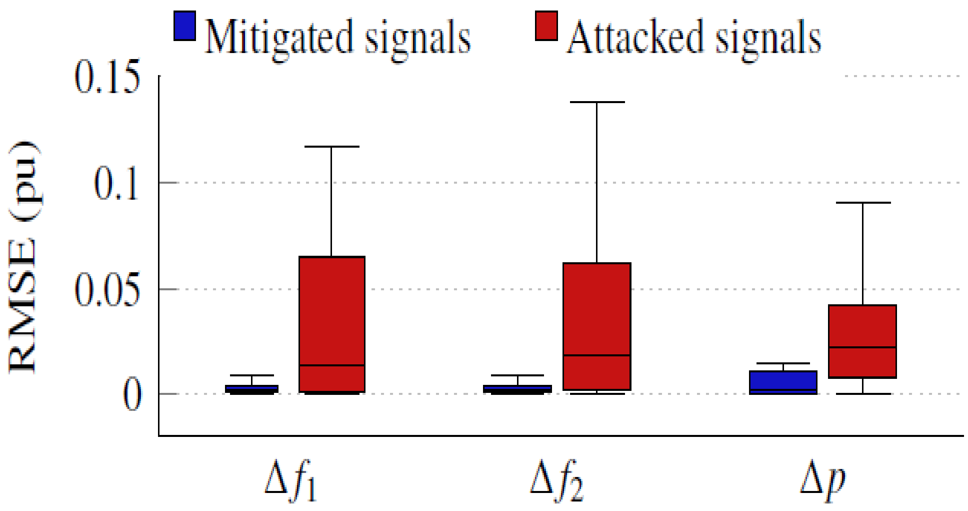


Figure 5-17. The RMSE of mitigated and attacked signals

Fig. 5-17 depicts the training progress for four models: one $LSTM_{detection}$ model and three $LSTM_{mitigation}$ models, one for each signal. The improvement for the detection model is measured by the increase in model accuracy performance on the testing data, while the improvement of the mitigation models is depicted by the decrease in root-mean-square error (RMSE) value for the testing data.

5.6 Detection and Mitigation of FDIA on the IEEE 118 Bus System

To evaluate the performance of an LSTM model under an FDIA attack, we needed to first train the model on a clean dataset, then evaluated it on a dataset with an FDIA attack. Once the network was trained for 32 epochs, we estimated the performance of the model on the train and test datasets. This will give us the point of comparison between trained and validated datasets. Figure 5-18 shows the accuracy of the validated data to trained data with and without the FDIA attacks. The validation accuracy measures how well the model generalizes to new data that it has not seen before. From the results, we can observe that the validation accuracy and training accuracy of the data without an FDIA attack is higher. It means that the LSTM model is well-fit to learn the pattern and make the prediction. In contrast, the dataset with an FDIA attack shows a higher difference between the training and validation accuracy. Figure 5-19 shows the training and validation loss with and without an FDIA attack which has an inverse relationship with the accuracy of the model. That means the higher the accuracy of the model, the lower the loss. The training loss is calculated by evaluating the model on the training data and measuring the difference between the predicted outputs and the actual outputs. The validation loss, on the other hand, is calculated by evaluating the model on a validation dataset and measuring the difference between the predicted outputs and the actual outputs.

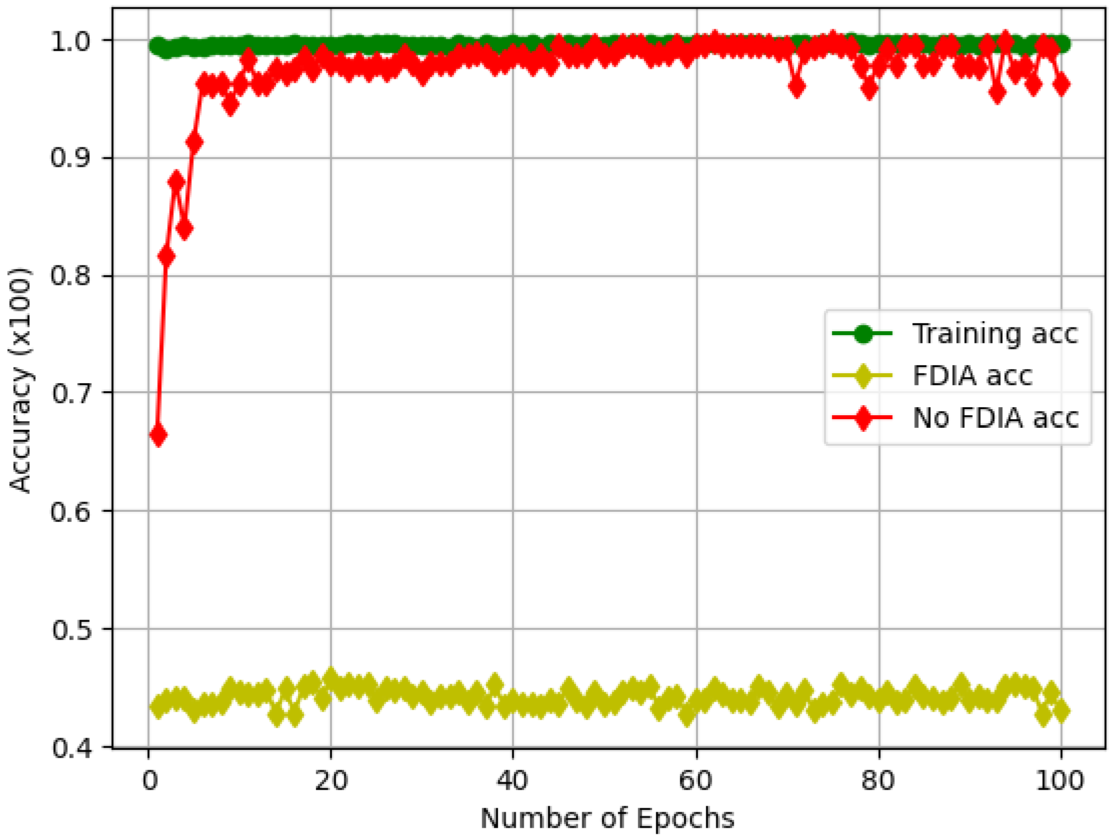


Figure 5-18. Training and validation accuracy with and without FDIA

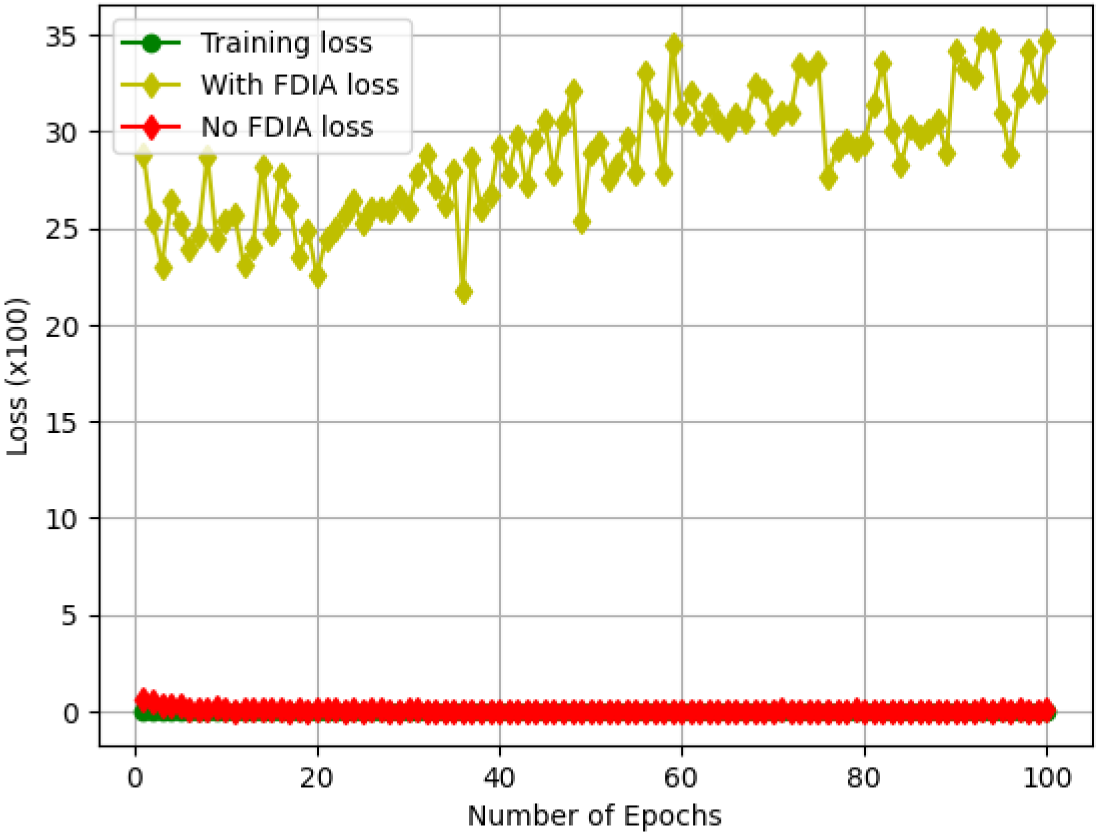


Figure 5-19. Training and validation loss with and without FDIA.

The confusion matrix summarizes the number of correct and incorrect predictions made by the LSTM and provides a visual representation of the performance of the algorithm. It is used to evaluate the performance of a classification algorithm by comparing the true labels of the samples to the predicted labels. With FDIA the accuracy and misclassification rate of the model can be impacted, therefore the confusion matrix would show a difference between the results with and without FDIA. The matrix would display the number of true positive (correctly predicted as trusted), false positive (incorrectly predicted as trusted), true negative (correctly predicted as not trusted), and false negative (incorrectly predicted as not trusted) results. Fig 5-20 shows the confusion matrix with and without the FDIA attack. This shows that the accuracy of the proposed model to predict the attack variables is higher.

Table 5-2. Accuracy vs Misclassification

Accuracy	0.9888
Misclassification	0.0112

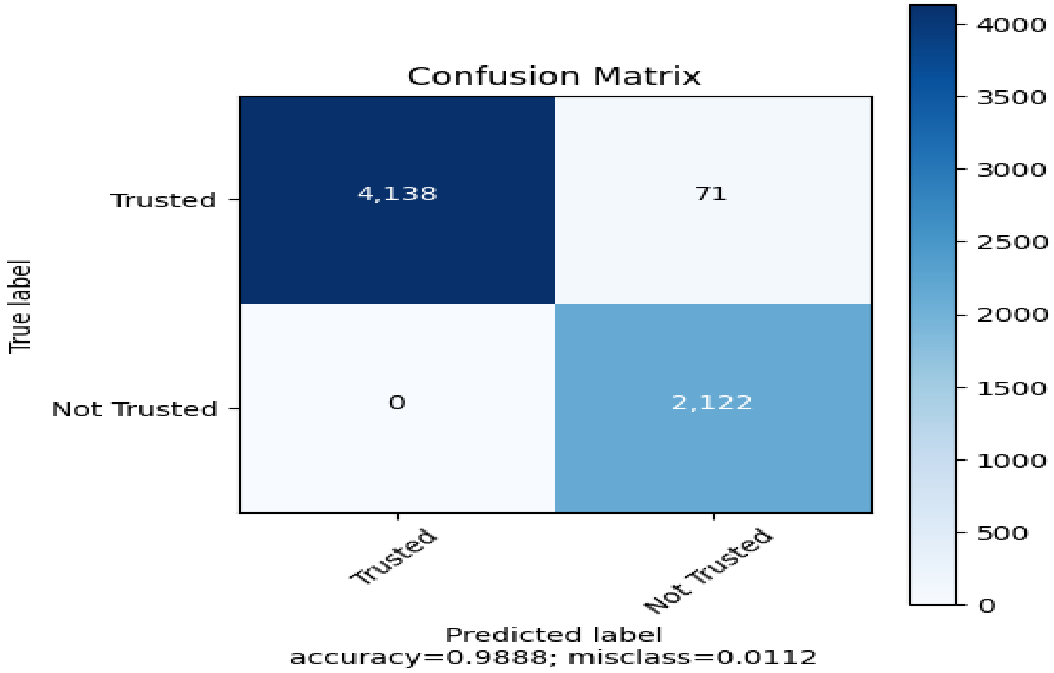


Figure 5-20. Confusion matrix showing accuracy and misclassification rate.

Table 5-3 summarizes the LSTM model performance for the training dataset with and without the FDIA attack. Class 0 and 1 are used to represent the false positive and false negative rates, respectively. The ROC (Receiver Operating Characteristic) curve is used for the graphical representation of the performance of a binary classification algorithm. It plots the True Positive Rate (TPR) against the False Positive Rate (FPR), where TPR is on the y-axis and FPR is on the x-axis, as the classification threshold is varied. The ROC curve provides a visual representation of the trade-off between the sensitivity and specificity of the classifier. Figure 5-21 shows the curve with and without the FDIA attack. Without the FDIA attack, the model has ROC near 1 which means it has a good measure of separability between true positive and false positive which is an ideal situation. While the FDIA attack shows that the TPR and FPR distribution overlap and there is a lower chance that the model will be able to distinguish between the positive class and the negative class.

The precision-recall curve plots the precision (the fraction of true positive predictions among all positive predictions) against recall (the fraction of true positive predictions among all positive instances in the data). It summarizes the trade-off between the true positive rate and the positive predictive value for our predictive model using different probability thresholds. Figure 5-22 shows the variation between the TPR and the positive predictive values for a constant threshold of 0.5.

Table 5-3. The LSTM model performance without the FDIA attack

Class	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
0	98.87	100	98	99
1	98.87	97	100	98

Table 5-4. LSTM model performance for training dataset with FDIA attack

Class	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
0	73.49	100	14	25
1	73.49	37	100	54

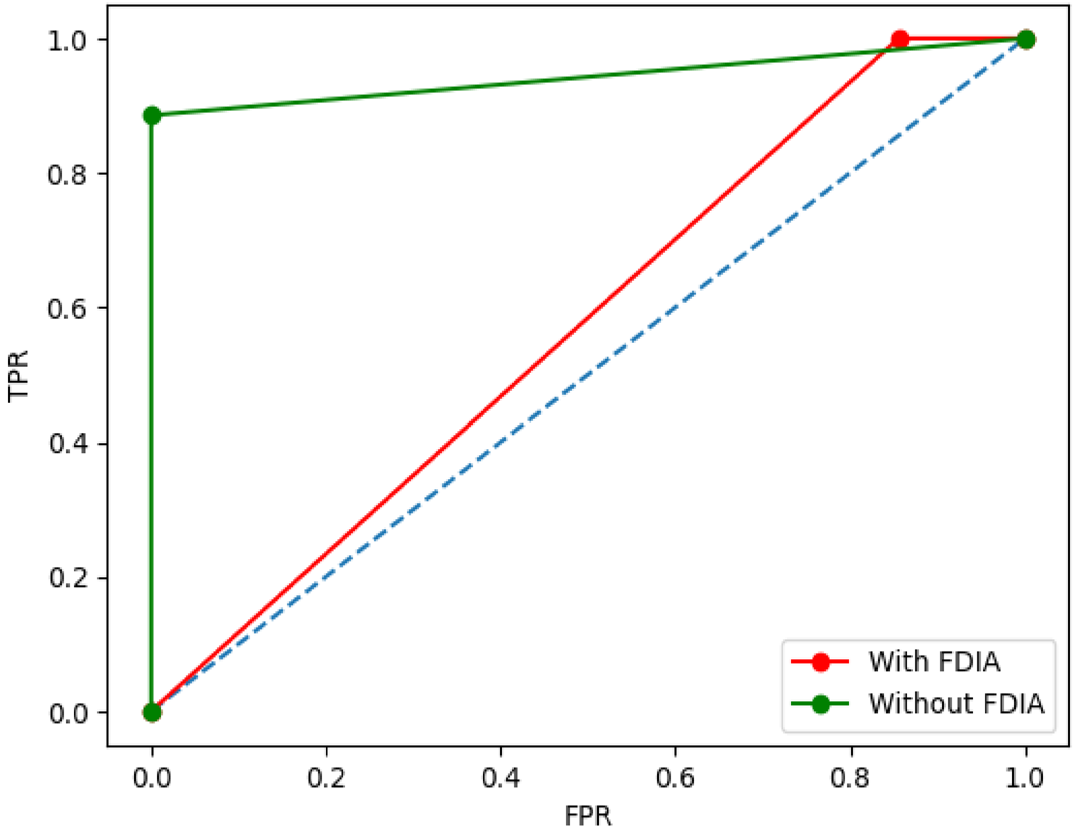


Figure 5-21. The ROC curve with and without FDIA attack as the threshold is varied from 0 to 1

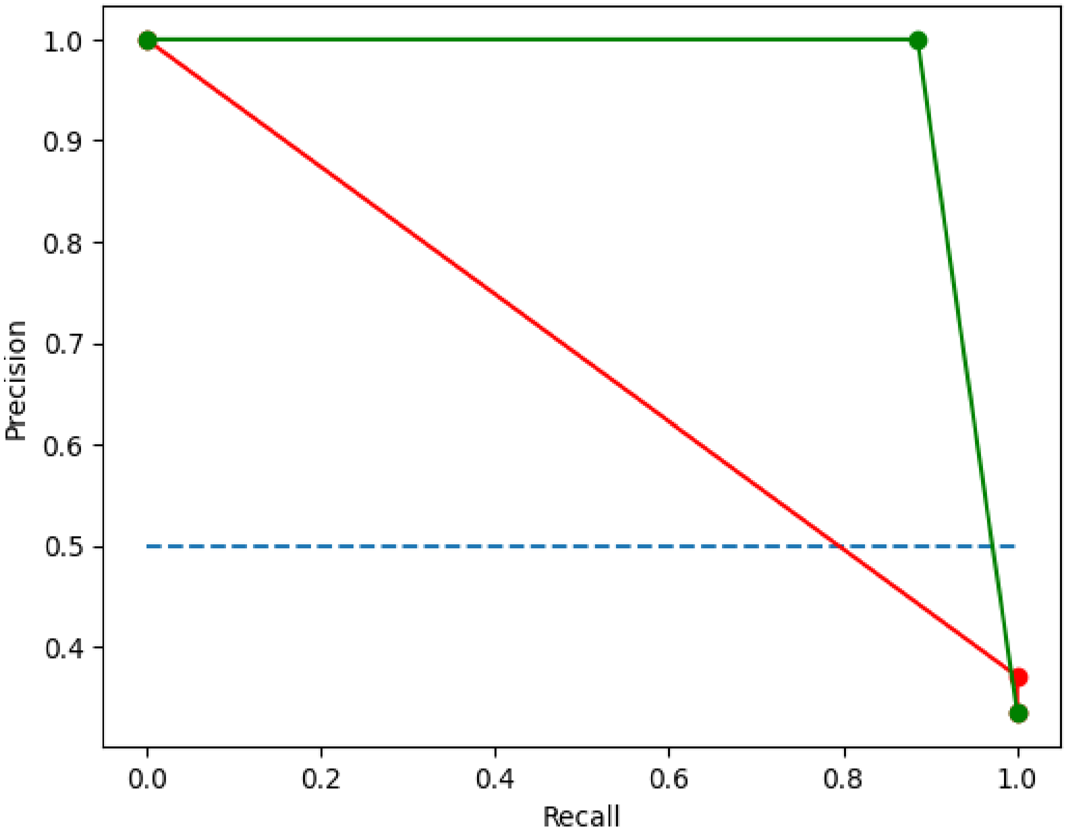


Figure 5-22. Precision-recall curve with and without FDIA attack for constant threshold.

Using the result from the LSTM training, the accuracy of the predicted datasets with and without the FDIA attack are compared. In the evaluation process, classification accuracy and other error metrics were used to show the effectiveness of our model, tested with a training dataset. Figure 5-23 summarizes the difference in the accuracy and the loss of the LSTM model trained with and without the attack on load measurements from the IEEE-118 bus. As the number of training datasets increases, the deviation between the normal and FDIA datasets appears to be more significant. Figure 5-24 also implies the inverse relationship between the accuracy and the loss of the model using the LSTM approach.

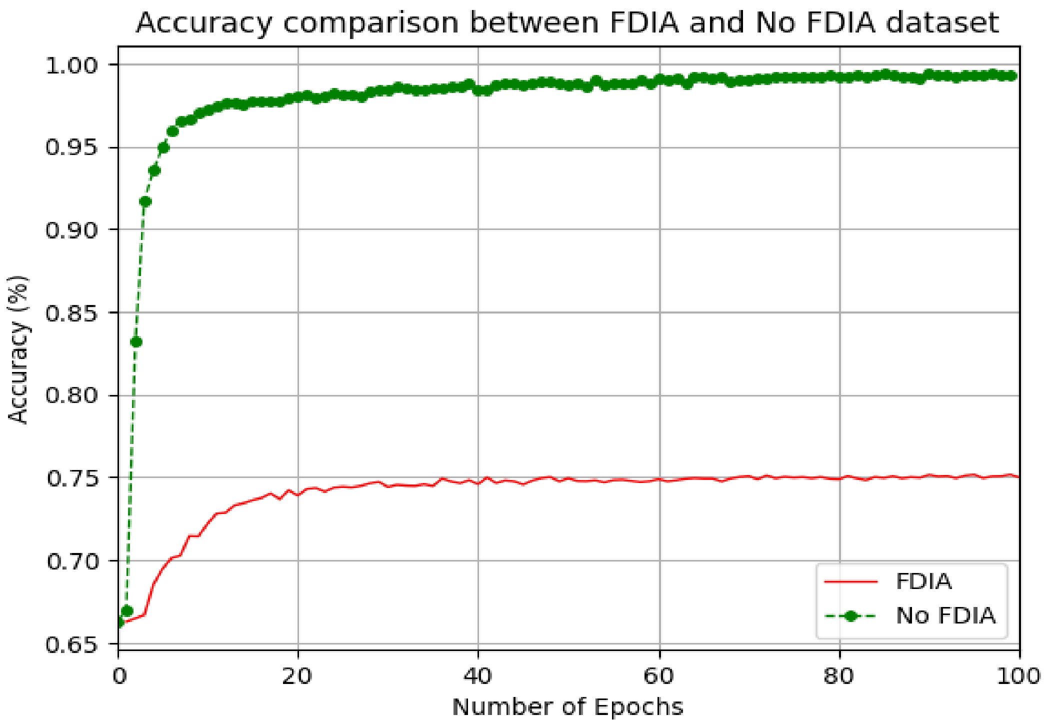


Figure 5-23. Accuracy and loss comparison between normal LSTM and FDIA LSTM model

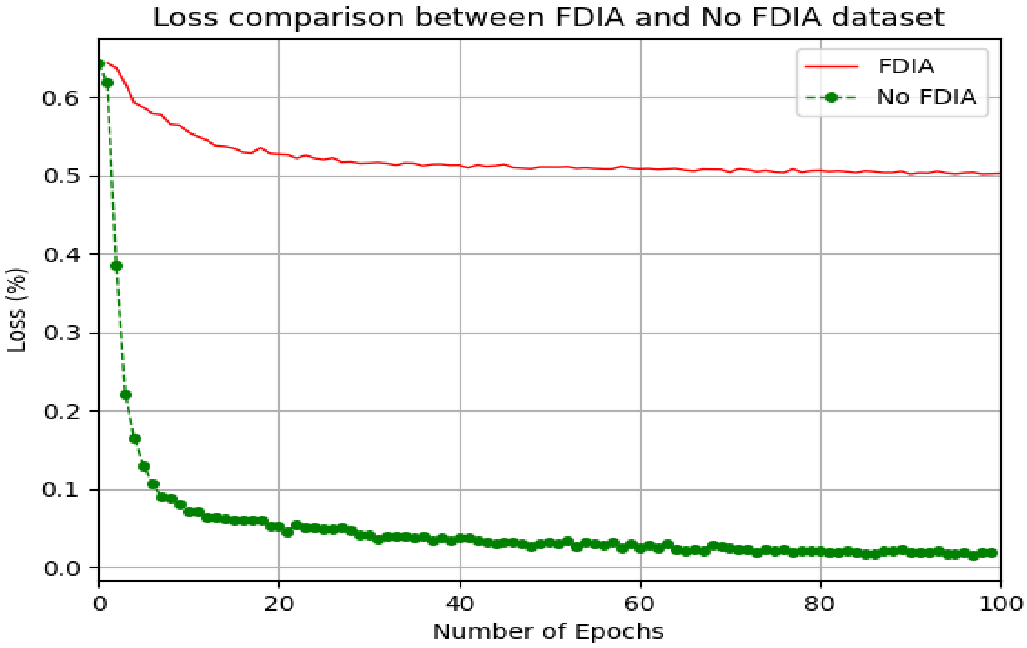


Figure 5-24. Loss comparison between normal LSTM and FDIA LSTM model

CHAPTER 6: CONCLUSIONS, RECOMMENDATIONS, AND FUTURE WORK

This chapter draws important conclusions from the results of the research study.

The purpose of the research was to develop a holistic cybersecurity framework for the digitalized power grid to enable proactive cybersecurity. The framework is aimed at enhancing the ICS cybersecurity maturity level and delivering threat intelligence to effectively predict, prevent, detect, and respond to cyber threats. To achieve the overall objective, the thesis included several research activities and case studies. The following insights are based on the results of the data analysis.

Firstly, it can be concluded that digitalization in power grid operation and maintenance provides such benefits as sustainability, availability, reliability, maintainability, capacity, safety, and security including cybersecurity. Yet Zambian stakeholders are facing challenges in the digitalization of the ICS.

Secondly, the concept of information assurance, a concept that also deals with aspects of cybersecurity, is receiving significant attention in ICS digitalization. However, the cybersecurity maturity level varies for different organizations.

6.1 Conclusions Related to Evaluating the Security Posture and Stochastic Modeling (Research Objectives 1 and 2)

In this work, we focused on the performance analysis of the SCADA firewalls and passwords as well as the applied intrusion detection and prevention methods in the case scenario. First, we provided three system defense scenarios and performance evaluation models based on stochastic Petri nets. The proposed three SPN models were then formally investigated. After that, we performed in-depth simulations on the PIPE[199] platform, and the outcomes demonstrate how well the SCADA Simulation (SCADASim) performs when using the recommended SPN models to enhance security.

This research presents a novel method for evaluating the effectiveness of the Smartgrid SCADA systems and Zambia's vital infrastructure as a whole. In some information fields with higher confidentiality requirements, such as the army combat command system, government office network, large enterprise servers, etc., the system's operator can choose whether to use a honeypot to strengthen the defense and protection of the system depending on the actual needs and can then estimate the system safety probability, defense success probability, etc. The study can improve the system's overall defensive performance and act as a roadmap for future cybersecurity efforts.

Thirdly, the SCADA and ICS systems (infrastructure and power grid) are intricate technological systems made up of numerous components with protracted lifecycles. It should be examined in the context of a complicated technical system with many different stakeholders, so cybersecurity must be taken into account. Therefore, it can be inferred that addressing cybersecurity necessitates a comprehensive strategy that takes into account the entire lifecycle of the power grid system as well as any changes in its configuration.

6.2 Conclusions Related to the Stochastic Impact Modeling (Research Objective 3)

In this study, the IEEE 4 and 24 Bus systems were modeled while taking into account four states: normal, vulnerable, failed, and restored. The innovative methodology can assign and analyze the likelihood that buses will be in a given condition. In addition, cascaded vulnerabilities are established to calculate the overall impact of escalation routes. Another unique feature of this approach was that we modeled the cyber risk in monetary form and combined it with the corresponding Locational Marginal Pricing (LMP) tabular results. In this instance, a transmission line and bus data integrity assault was modeled.

As a design guideline for the real-time system for the contingency analysis process in big power systems, the findings of this study can be used to perform reliability evaluation in terms of actual monetary aspects. This research has illustrated a novel approach to quantifying the effects of cyberattacks on the infrastructure of power systems and the economic effects they have. Actuarial scientists can also use the findings to determine the actual risk that cyber failures in power networks pose. Large-scale IEEE bus systems will use this novel approach to simulate the effects of cyber-based risks.

6.3 Conclusions Related to the Testbed Results (Research Objective 4)

This chapter examines the cyber risk landscape of wind farms and provides a simulated study of cyber events to achieve reasonable levels of security. The consequences of cyberattacks are identified, along with various approaches to protecting wind farms from cyber breaches. Also, the study has highlighted the need for research and development of cyber-resilient wind plant designs, the development of virtual testbeds, academic involvement regarding situational awareness and threat detection, responsive intrusion, and recovery mechanisms, as well as post-incident investigations.

6.4 Conclusions Related to the Mitigation of FDIA on the AGC (Research Objectives 4 and 5)

In large power networks with multiple areas sharing power, automatic generation control is a crucial controller. Cyber-physical attacks on AGC pose serious risks to the integrity of the entire power system since they give the attacker the ability to attack frequency and tie-line power signals in the communication system, leading to unneeded load shedding, power outages, and/or blackouts through the AGC. We model AGC nonlinearities and examine the potential vulnerabilities that could arise from neglecting them, in contrast to earlier efforts on AGC cyber-physical security. First, we demonstrated that if the nonlinearities are taken into account, the AGC's behavior and, subsequently, the control decision, differ. We showed that the linear AGC models that disregard nonlinearities do not provide appropriate defense against cyber-physical attacks that operate in the nonlinear region of the system. Second, we suggested and put into practice a two-stage strategy based on LSTM to identify and reduce the compromised signals to handle these threats. Its better performance in attack detection with good statistical metrics is confirmed by the examination of the detection model. The mitigation model can also improve the system's behavior and dramatically lower the RMSE of the attacked signals

We proposed an efficient algorithm for detecting, identifying, and mitigating cyber-physical attacks on the IEEE benchmark power grid. The model detected the presence of false measurements, which remain undetected with a standard bad data detection algorithm. The model does not depend on the underlying grid architecture and can be easily integrated on top of the existing detection algorithm. The validation of the algorithm is done using real measurements from the IEEE 118-bus system, and the presence of bad data has been verified using falsely injected measurements. Different performance metrics have been utilized to evaluate the validity and accuracy of the proposed detection techniques. In addition to this, the results can be further extended to develop the FDIA defense mechanism under different scenarios. The paper has explored the feasibility of the regression-based attack analysis model to develop the real-time FDIA defense algorithm for impact analysis and attack prevention.

6.5 Recommendations

This section provides cybersecurity policy recommendations for electric distribution systems in Zambia, with an emphasis on regulated electric distribution systems. Although there are many forms of critical infrastructure, including financial services, communications, healthcare, and water systems, these all rely on the electric grid for operation. Therefore, damage, disruption, or unauthorized access to the electric grid can disrupt the reliable operation of other critical infrastructure assets. The recommendations provided in this paper are tailored to the electricity sector but may be useful to other sectors of critical infrastructure as well.

The electric grid is currently undergoing a dramatic transformation which has massive cybersecurity implications. New technology is being connected to the grid, combining legacy systems and smart grid components, but technical standards for interconnection and cybersecurity are still in development. Legislation and regulations are emerging to address smart grid development. However, cybersecurity advancements are not often integrated with these efforts.

The policy recommendations made here are based on research and interviews with electric grid cybersecurity stakeholders. Legislative and regulatory actions, academic and technical reports, published standards and best practices, and news media reporting provided a foundation. Interviews were conducted with members of various state agencies, including the ZESCO, CEC, and the mines. Subject matter experts from non-government entities such as the Engineering Institute of Zambia (EIZ) and ICTAZ.

Some of the recommendations in this paper may be implemented by utilities currently. The cybersecurity posture and practices of utilities are not made public. Detailed information about regulator preparations for cybersecurity reporting also was not accessible. A complete picture of the current state of cybersecurity for the electric grid was not available to the author. The recommendations made are based on best practices and standards but do not necessarily address an existing shortcoming of current practices.

Recommendation 1. “Service quality and reliability standards” to include “cyber resiliency” in the list of topics to be addressed by the standards.

Recommendation 2. Define “resilience” to include “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks” so that cybersecurity will be an essential factor in determining system resilience.

Recommendation 3. Require utility providers to adopt security best practices such as the NIST Cybersecurity Framework and advance toward zero-trust architecture both with on-premises services *and* cloud services. Report to regulators on steps already completed. Identify the steps that will have the most immediate security impact, and a schedule to implement them.

Recommendation 4. Require utility providers to incrementally implement zero trust principles, process changes, and technology solutions that protect data assets and business functions by use case. Develop and maintain dynamic risk-based policies for resource access. Authenticate all connections and encrypt data. Design cybersecurity of newly interconnected resources around zero-trust principles.

Recommendation 5. Consult with grid owners and operators, and state and local government agencies to establish a process to identify, assess, and prioritize risks to the electric grid, considering current and foreseeable future cyber and physical threats, vulnerabilities, and consequences. Apply the process to periodically report to regulators on the risks. Use the report to establish a risk-based grant program focused on systematically increasing the resilience of the electric grid against the prioritized cybersecurity risks where market forces do not provide sufficient private-sector incentives to mitigate the risk without Government investment.

Recommendation 6. Engage state employees in cybersecurity standards development efforts to share knowledge and insights, and influence future directions.

Recommendation 7. Include a formal requirement for all state-funded grant recipients working on electric grid resilience or modernization to address cybersecurity risk both in the design and reporting phases of their work.

Recommendation 8. Include a formal requirement for all working groups to develop policy and plan for the grid to address cybersecurity risk in the reporting phase of their work.

Recommendation 9. Require electric grid resilience or modernization pilot programs to establish formal requirements for a cybersecurity plan. Cybersecurity vulnerabilities arise from weaknesses in policy and procedure; architecture and design; configuration and maintenance; supply chain; hardware; physical access controls; software development; and communications and networks. An effective cybersecurity plan must address all of these areas.

Recommendation 10. The maturity level of a cybersecurity program should be a factor in establishing an appropriate reporting period for each utility. Each utility should provide sufficient evidence to establish the maturity level of the company's cybersecurity program. The system operators should then tailor the reporting period accordingly. For utilities that can provide persuasive evidence of a high level of maturity in their cybersecurity program. For less mature programs, more frequent reporting to evidence growth in maturity level is recommended. An example of a maturity model available is The Cybersecurity Capability Maturity Model (C2M2) Version 2.0 (V2.0) which was released in July 2021.

Recommendation 11. Information technology (IT) and operational technology (OT) systems of utilities were likely developed separately and with separate groups of people. However, without strict network segregation, vulnerabilities in IT enable attacks on OT. Regulators must understand the extent to which utility IT and OT security experts work together to protect the grid and make recommendations to enhance communication within utility provider entities.

Recommendation 12. Utilities should work together and report together on risks and cybersecurity events. Bring GridEx participants together after the exercises are complete to assess and categorize the impacts of issues that were identified.

Recommendation 13. Each confidential cybersecurity brief required should be accompanied by a written report suitable for public release that summarizes the cybersecurity efforts of the company, especially concerning modernization efforts.

Recommendation 14. When smart meters were incorporated into the Zambian power grid, utilities shall be required to publicize security information about the change. This practice should be continued to include changes created by DER integration.

Recommendation 15. Although details of security processes and mechanisms should be protected as sensitive information, general information about utility security programs should be publicly available and easily accessible.

Recommendation 16. Require all utilities that rely on third-party IT or OT providers to include standard contract language with service providers to collect and preserve data for cybersecurity analysis and share such data, or report third-party security breaches to the utility or a government entity such as CISA.

Recommendation 17. Adopt the NIST definition of "critical software" and require utilities to maintain a list of the categories of software and software products in use or in an acquisition that meet the definition. Adopt NIST security guidance for critical software use, applying practices of least privilege, network segmentation, and proper configuration.

Recommendation 18. Require utilities to establish minimum security standards for IT and OT devices commensurate with the level of security risk applicable to such devices and specifically take into account any security risk associated with supply chains.

Recommendation 19. Allocate funds to provide Zambia Public Service Commission with staff dedicated to regulatory cybersecurity policy, strategy, auditing, and reporting.

Recommendation 20. Ensure employees involved in cybersecurity activities attend periodic training to keep skills and knowledge current regarding emerging trends in distributed energy resource cybersecurity issues.

Recommendation 21. Power grid engineers should take an active role in standards organizations upon which they rely to ensure that cybersecurity concerns are addressed during standards development.

Recommendation 22. Encourage utilities to establish a procedure where cybersecurity leadership of utilities may report directly to the company's Board of Directors or CEO.

The People's Counsel fills an important role in oversite and is included in the short list of representatives who may attend the utility cybersecurity reporting briefs. To fulfill its duty to protect the interests of residential and noncommercial users, the Office of People's Counsel should have access to cybersecurity expertise to participate in rate cases and other court appearances.

Recommendation 23. The utility should make available clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with the utility, utility-authorized third parties, and energy service providers that are not affiliated with a utility.

Recommendation 24. Incorporate existing privacy standards and frameworks to identify privacy risks, then apply privacy mitigation processes to match proportionate privacy controls for each relevant business activity that creates a risk to privacy. Privacy issues may also arise from state and utility entities sharing threat information.

Recommendation 25. Develop guidelines relating to privacy and civil liberties governing the receipt, retention, use, and dissemination of cyber threat indicators by the state, including safeguards such as sanctions for activities by officers, employees, or agents of state or local Government for misuse of information.

Recommendation 26. Modify the current Zambian statutory definition of "cybersecurity" to include the five goals of cybersecurity so that procurement will be guided by specific reference to availability, integrity, authentication, confidentiality, and nonrepudiation. In addition to defining cybersecurity, other key terms should be considered.

Recommendation 27. Adopt a statutory definition of "cyber resilience", "critical infrastructure", "supply chain risk", and "critical software".

6.6 Future Works

Future work includes expanding the risk analysis framework to include different types of coordinated attacks and comparing the impact expressed in different power system metrics. The mitigation techniques are based on Markov Decision Process (MDP) and Moving Target Defence (MTD). Finally, the attack resilient control framework should be enhanced to differentiate abnormal measurements due to cyber attacks from legitimate aberrations due to power system contingencies.

Future works include the intruders' decision to attack the AGC which is modeled over time using a Markov Decision Process (MDP). The research examines two tiers of the intruder's knowledge of potential power system situations. Taking into account the general scenario, where the intruder has less knowledge and uses a Markov Chain to describe the evolution of the system states, as well as the special case when the intruder can anticipate the future states for a brief time. In these two circumstances, the intruder's action process is defined as a finite-horizon MDP and an infinite-horizon MDP, respectively.

A mapping between power system states to the intruder's ideal actions (such as which buses to intrude on and what errors to inject) is the answer to the MDP. Based on the discovered attack strategy, the operator can additionally resolve the MPD and calculate the attack likelihood. When this happens, the operator can examine the susceptibility of specific parts and the effects of other variables (such as detection likelihood and system transition probabilities) on system vulnerability.

REFERENCES

[1] Hassan Bevrani. Robust power system frequency control. Springer, 2014.

[2] Jaime De La Ree, Virgilio Centeno, James S Thorp, and Arun G Phadke. Synchronized phasor measurement applications in power systems. IEEE Transactions on Smart Grid, 1(1):20{27, 2010.

[3] Hamid Gharavi and Bin Hu. Synchrophasor sensor networks for grid communication and protection. Proceedings of the IEEE, 2017.

[4] Aditya Ashok, Manimaran Govindarasu, and Jianhui Wang. Cyber-physical attacks resilient wide-area monitoring, protection, and control of the power grid. Proceedings of the IEEE, 2017.

[5] "The Cyber-Physical Security of the Power Grid." IEEE Smart Grid, https://smartgrid.ieee.org/bulletins/november-2019/the-cyber-physical-security-of-the-power-grid.

[6] Africa, https://www.hydropower.org/region-profiles/africa.

[7] Iea. "SDG7: Data and Projections – Analysis." IEA, https://www.iea.org/reports/sdg7-data-and-projections.

[8] "The National Energy Policy 2019." Ministry of Energy Integrated Resource Plan, 21 Oct. 2021, https://www.moe.gov.zm/irp/download/the-national-energy-policy-2019-2/.

[9] Final Report - Moe.gov.zm. https://www.moe.gov.zm/?wpfb_dl=45.

[10] "Home." Ministry of Energy Integrated Resource Plan, 1 Sept. 2021, https://www.moe.gov.zm/irp/.

[11] Energy Sector Report 2020 - Erb.org.zm. https://www.erb.org.zm/reports/esr2020.pdf.

[12] Awad, A.; Bazan, P.; German, R. SGsim: A simulation framework for smart grid applications. In Proceedings of the 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, Croatia, 13–16 May 2014; pp. 730–736.

[13] Al Ghazo, Alaa, "A framework for Cybersecurity of Supervisory Control and Data Acquisition (SCADA) Systems and Industrial Control Systems (ICS)" (2020). Graduate Theses and Dissertations. 17834.

[14] Davis, Katherine R., et al. "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures." *University of Illinois Urbana-Champaign*, Institute of Electrical and Electronics Engineers Inc., 1 Sept. 2015, https://experts.illinois.edu/en/publications/a-cyber-physical-modeling-and-assessment-framework-for-power-grid-3.

[15] Handa, A., Sharma, A., and Shukla, S. K. Machine learning in cybersecurity: a review. WIREs Data Mining Knowl Discov. 9, e1306.doi:10.1002/widm.1306

[16] Johnson, J., Onunkwo, I., Cordeiro, P., Wright, B.J., Ja-cobs, N. and Lai, C. Assessing DER network cybersecurity defenses in a power-communication co-simulation environment. IET Cyber-Physical Systems: Theory & Applications, 5: 274-282. https://doi.org/10.1049/iet-cps.2019.0084

[17] Li, Beibei & Xiao, Gaoxi & Lu, Rongxing & Deng, Ruilong & Bao, Haiyong. (2019). On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices. IEEE Transactions on Industrial Informatics. PP. 10.1109/TII.2019.2922215

[18] Christopher J Baker. Cybersecurity for critical infrastructure. Technical report, Air Command, And Sta
College Maxwell Air Force Base the United States, 2015.

[19] Office of Electricity Delivery and Energy Reliability. Cybersecurity risk management process (RMP). 2011.

[20] North American Electricity Reliability Council (NERC). Critical infrastructure protection (CIP) reliability standards. 2009.

[21] National Institute of Standards and Technology (NIST). Nistir 7628: Guidelines for smart grid cyber security. 2010.

[22] Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013

[23] EU Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, 6 July 2016.

[24] “African Union Cybersecurity Expert Group Holds Its First Inaugural Meeting.” *African Union Cybersecurity Expert Group Holds Its First Inaugural Meeting | African Union*, 27 June 2022, https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting.

[25] *Southern African Development Community Cybersecurity Maturity Report 2021.* CAPE TOWN: Cybersecurity Capacity Centre for Southern Africa (C3SA), 2022. http://hdl.handle.net/11427/36211

[26] The Cyber Security and Cyber Crimes Act, 2021.

[27] “National Cyber Security Policy Approved.” MISA Zambia, 27 Jan. 2021, https://zambia.misa.org/2021/01/27/national-cyber-security-policy-approved/.

[28] Lundgren, Björn, and Niklas Möller. “Defining Information Security.” *Science and engineering ethics* vol. 25,2 (2019): 419-441. doi:10.1007/s11948-017-9992-1

[29] Constantinou, Constantinos P., et al. “A Framework for Modeling-Based Learning, Teaching, and Assessment.” Home, Springer International Publishing, 1 Jan. 1970, https://gnosis.library.ucy.ac.cy/handle/7/62270?locale-attribute=en.

[30] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 588-608. doi:10.2307/2094589

[31] Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280.doi:10.1080/01639625.2015.1012409

[32] Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. International Journal of Offender Therapy and Comparative Criminology, 60(10), 1119-1139. doi:10.1177/0306624x15572861

[33] McNeeley, S. (2015). Lifestyle-routine activities and crime events. Journal of Contemporary Criminal Justice, 31, 30-52. doi:10.1177/1043986214552607

[34] Kavak, Hamdi & Padilla, Jose & Vernon-Bido, Daniele & Gore, Ross & Diallo, Saikou. (2016). A Characterization of Cybersecurity Simulation Scenarios. 10.22360/SpringSim.2016.CNS.003.

[35] Fischer, E. A. (2016). Cybersecurity issues and challenges: In brief (Congressional Research Service Report 7-5700). Retrieved from https://pdfs.semanticscholar.org/65e3/4c9bb7330fcfec378394b5d308b6a323947d. pdf

[36] Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: analysis of attack-proneness of information systems applications. Management Information Systems Quarterly, 39(1), 91–112. doi:10.25300/misq/2015/39.1.05

[37] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53-66. doi: 10.1016/j.ijcip.2014.12.002

[38] Soomro, Zahoor Ahmed, et al. "Information security management needs more holistic approach: A literature review." *Int. J. Inf. Manag.* 36 (2016): 215-225.

[39] "Common Weakness Enumeration." CWE, https://cwe.mitre.org/.

[40] "Vulnerabilities." Vulnerabilities | OWASP Foundation, https://owasp.org/www community/vulnerabilities/.

[41] Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection, 15,* 47-59. doi:10.1016/j.ijcip.2016.10.001

[42] Piggin, R. (2018). Cyber resilience 2035. ITNOW, 60(1). doi:10.1093/itnow/bwy014

[43] Luo, X. (2016). Security protection to industrial control system based on defense-indepth strategy. WIT Transactions on Engineering Sciences, 113, 19-27. doi:10.2495/IWAMA150031

[44] Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23. doi:10.1016/j.mfglet.2014.12.001

[45] Cilluffo, F. (2016). Emerging cyber threats to the United States [Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies].Washington, DC: George Washington Center for Cyber and Homeland Security.Retrieved from

http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf

[46] Gergen, K. J. (2015). From mirroring to world-making: Research as future forming. Journal for the Theory of Social Behaviour, 45(3), 287-310.doi:10.1111/jtsb.12075

[47] Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. Qualitative Research, 15(2), 219-234.doi:10.1177/1468794112468475

[48] W. Wang, Y. Xu, and M. Khanna, \A survey on the communication architectures in smartgrid," Computer Networks, vol. 55, no. 15, pp. 3604{3629, 2011.

[49] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, \Communication network requirements for major smart grid applications in HAN, NAN, and WAN," Elsevier Editorial System for Computer Networks, August 2013.

[50] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, \Communication network requirements for major smart grid applications in HAN, NAN, and WAN," Elsevier Editorial System for Computer Networks, August 2013.

[51] Z. Fan, P. Kulkarni, C. E. S. Gormus, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, \Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 21 { 38, First Quarter 2013.

[52] C. Gentile, D. Grith, and M. Souryal, \Wireless Network Deployment in the Smart Grid: Design and Evaluation Issues," IEEE Network, pp. 48 { 53, November/December 2012.

[53] Y. Kim, J. Lee, G. Atkinson, H. Kim, and M. Thottan, \SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications," IEEE Journal on Selected Areas in Communications, vol. 30, no. 6, pp. 1119 { 1136, July 2012.

[54] Smart Grid Consumer Benets, IEEE Smart Grid, [Online]. Available: http://smartgrid.ieee.org/questions-and-answers/964-smart-grid-consumer-benets. [Accessed 4 September 2013]

[55] Smart Grid Economic and Environmental Benefits, A Review and Synthesis of Research on Smart Grid Benefits and Costs, [Online]. Available: http://smartgridcc.org/wp-content/uploads/2013/10/SGCC-Econ-and-Environ-Benets-Full-Report.pdf. [Accessed 8 October 2013]

[56] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, \Wireless AMI Application and Security for Controlled Home Area Networks," in Proc. IEEE Power and Energy Society General Meeting, USA, July 2011.

[57] U.S.-Canada Power System Outage Task Force. Final report on the August 14, 2003 blackout in the United States and Canada., [Online]. Available: https://reports.energy.gov/B-F-Web-Part1.pdf [Accessed 8 April 2013]

[58] G. Dan, and H. Sandberg,\Stealth Attacks and Protection Schemes for State Estimators in Power Systems," in Proc. IEEE SmartGridComm, USA, October 2010.

[59] Y. Zhang, and J. Chen,\Wide-area SCADA system with a distributed security framework, "Journal of Communications and Networks, vol. 14, no. 6, pp. 597 { 605, December 2012.

[60] D. Wei, Y. Lu, M. Jafari, P. Skareand, and K. Rohde,\Protecting Smart Grid Automation Systems Against Cyberattacks," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 782{ 795, December 2011.

[61] M. Kim, A Survey on Guaranteeing Availability in Smart Grid Communications," in Proc.ICACT, Korea, February 2012.

[62] James H. Graham. Security considerations in scada communication protocols. 2004.

[63] Gordon Clarke, Deon Reynders, and Edwin Wright. Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes, 2004.

[64] Petr Matoušek. Description and analysis of iec 104 protocol. Technical report, 2017. URL:http://www.fit.vutbr.cz/research/view_pub.php?id=11570.

[65] Peter Maynard, Kieran McLaughlin, and Berthold Haberler. Towards Understanding Man-in-the-middle Attacks on IEC 60870-5-104 SCADA Networks. In ICS-CSR, 2014.

[66] Guillermo A Francia III, Xavier P Francia, and Anthony M Pruitt. Towards an In-depth Understanding of Deep Packet Inspection Using a Suite of Industrial Control Systems Protocol Packets. Journal of Cybersecurity Education, Research and Practice, 2016(2):2, 2016.

[67] Gordon Clarke, Deon Reynders, and Edwin Wright. Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes, 2004.

[68] Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, and Stephen Hilt. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. McGraw-Hill Education Group, 1st edition, 2016.

[69] Jeyasingam Nivethan and Mauricio Papa. A Linux-based firewall for the DNP3 protocol. In Technologies for Homeland Security (HST), 2016 IEEE Symposium on, pages 1–5. IEEE,2016.

[70] SCHNEIDER AUTOMATION. Modbus messaging on tcp/ip implementation guide v1. 0b. MODBUS Organization, 30, 2015.

[71] Acromag. Introduction to modbus tcp/ip. Technical report, ACROMAG INCORPORATED, January 2005.

[72] L van der Zel, Guidelines for Implementing Substation Automation Using IEC61850, the International Power System Information Modeling Standard, Technical Report, 2004.

[73] Kirrmann, H. Introduction to the IEC 61850 electrical utility communication standard, ABBCH-RD, 2012.

[74] IEC 61850-8-1:2011. Communication networks and systems for power utility automation – Part 8-1: Mappings to Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

[75] IEC 61850-9-1:2003. Communication networks and systems in substations – Part 8-1: Specific communication service mapping (SCSM) - Sampled values over serial unidirectional multidrop point-to-point link

[76] IEC 61850-9-2:2011. Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3

[77] IEC 61850-10:2006. Communication networks and systems in substations – Part 10: Conformance testing

[78] IEC 61850-3:2014. Communication networks and systems for power utility automation – Part 3: General requirements

[79] IEC 61850-4:2011. Communication networks and systems for power utility automation – Part 4: System and project management

[80] IEC 61850-5:2013. Communication networks and systems in substations – Part 5: Communication requirements for functions and device models

[81] IEC 61850-6:2010. Communication networks and systems for power utility automation – Part 6: Configuration language for communication in electrical substations related to IEDs

[82] IEC 61850-7-1:2011. Communication networks and systems for power utility automation – Part 7-1: Basic communication structure – Principles and models

[83] IEC 61850-7-2:2010. Communication networks and systems for power utility automation – Part 7-2: Basic communication structure – Abstract communication service interface (ACSI)

[84] IEC 61850-7-3:2011. Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common Data Classes - Ed.2

[85] IEC 61850-7-4:2010. Communication networks and systems for power utility automation – Part 7-4: Basic communication structure -Compatible logical node classes and data classes

[86] IEC 61850-7-410:2012. Communication networks and systems for power utility automation - Part 7-410: Basic communication structure -Hydroelectric power plants - Communication for monitoring and control

[87] IEC 61850-7-420:2009. Communication networks and systems for power utility automation – Part 7-420: Basic communication structure -Distributed energy resources logical nodes

[88] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized Phasor Measurement Applications in Power Systems," IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 20–27, 6 2010.

[89] A. Monticelli, State estimation in electric power systems: a generalized approach. Springer Science & Business Media, 2012.

[90] A. Monticelli, “Electric power system state estimation,” Proceedings of the IEEE,vol. 88, no. 2, pp. 262–282, 2000.

[91] G. N. Korres and N. M. Manousakis, “State estimation and bad data processing for systems including PMU and SCADA measurements,” Electric Power Systems Research, vol. 81, no. 7, pp. 1514–1524, 7 2011.

[92] Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies 2021, 14, 5894. https://doi.org/10.3390/en14185894

[93] Gauci, A.; Michelin, S.; Salles, M. Addressing the challenge of cyber security maintenance through patch management. CIREDOpen Access Proc. J. 2017, 2017, 2599–2601.

[94] Khalid, A.; Sundararajan, A.; Hernandez, A.; Sarwat, A. FACTS Approach to Address Cybersecurity Issues in Electric Vehicle Battery Systems. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEM-SCON), Atlanta, GA, USA, 12–14 June 2019.

[95] Zeng, R., Jiang, Y., Lin, C., & Shen, X. (2012). Dependability Analysis of Control Center Networks in Smart Grid Using Stochastic Petri Nets. IEEE Transactions on Parallel and Distributed Systems, 23, 1721-1730.

[96] Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 1–4.

[97] Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the

[98] 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.

[99] Huseinovi´c, A.; Mrdovi´c, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. IEEE Access 2020, 8, 177447–177470.

[100] Cameron, C.; Patsios, C.; Taylor, P.C.; Pourmirza, Z. Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes. IEEE Trans. Smart Grid 2019, 10, 3010–3019.

[101] Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. IEEE Trans. Inf. Forensics Secur. 2019, 14, 498–513.

[102] Chatfield, B.; Haddad, R.J.; Chen, L. Low-Computational Complexity Intrusion Detection System for Jamming Attacks in Smart Grids. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 367–371.

[103] Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. IEEE Trans. Smart Grid 2017, 8, 2431–2439.

[104] Ying, H.; Zhang, Y.; Han, L.; Cheng, Y.; Li, J.; Ji, X.; Xu, W. Detecting Buffer-Overflow Vulnerabilities in Smart Grid Devices via Automatic Static Analysis. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 813–817.

[105] He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. IEEE Trans. Smart Grid 2017, 8, 2505–2516.

[106] Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. J. Netw. Comput. Appl. 2020, 170, 102808.

[107] Deng, R.; Liang, H. False Data Injection Attacks With Limited Susceptance Information and New Countermeasures in Smart Grid. IEEE Trans. Ind. Inform. 2019, 15, 1619–1628.

[108] Riggs, H.; Tufail, S.; Khan, M.; Parvez, I.; Sarwat, A.I. Detection of False Data Injection of PV Production. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; pp. 7–12,

[109] Singh, V.K.; Ebrahem, H.; Govindarasu, M. Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6,

[110] Green, B.; Prince, D.; Busby, J.; Hutchison, D. The Impact of Social Engineering on Industrial Control System Security. In Proceedings of the First ACMWorkshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC '15, Denver, CO, USA, 16 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 23–29.

[111] Mrabet, Z.E.; Kaabouch, N.; Ghazi, H.E.; Ghazi, H.E. Cyber-security in smart grid: Survey and challenges. Comput. Electr. Eng. 2018, 67, 469–482.

[112] Pour, M.M.; Anzalchi, A.; Sarwat, A. A review on cyber security issues and mitigation methods in smart grid systems. In Proceedings of the SoutheastCon 2017, Concord, NC, USA, 30 March–2 April 2017; pp. 1–4.

[113] Rajendran, G.; Sathyabalu, H.V.; Sachi, M.; Devarajan, V. Cyber Security in Smart Grid: Challenges and Solutions. In Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 21–23 August 2019; pp. 546–551.

[114] Shitharth, S.; Winston, D.P. A novel IDS technique to detect DDoS and sniffers in smart grid. In Proceedings of the 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016; pp. 1–6.

[115] Pandey, R.K.; Misra, M. Cyber security threats—Smart grid infrastructure. In Proceedings of the 2016 National Power Systems Conference (NPSC), Bhubaneswar, India, 19–21 December 2016; pp. 1–6.

[116] Irita, T.; Namerikawa, T. Detection of replay attack on smart grid with code signal and bargaining game. In Proceedings of the 2017 American Control Conference (ACC), Seattle, WA, USA, 24–26 May 2017; pp. 2112–2117.

[117] Alohali, B.; Kifayat, K.; Shi, Q.; Hurst, W. Replay Attack Impact on Advanced Metering Infrastructure (AMI). In Smart Grid Inspired Future Technologies; Hu, J., Leung, V.C.M., Yang, K., Zhang, Y., Gao, J., Yang, S., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 52–59.

[118] ISA, ”ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models,” in Part 1-1: Terminology, Concepts, and Models, ed,2007

[119] International Electrotechnical Commission (IEC). IEC 62443-3-3:2013 Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels. Available online: https://webstore.iec.ch/publication/7033 (accessed on 2 August 2021).

[120] ISO/IEC. ISO/IEC 27001:2013: Information Technology Security Techniques Information Security Management Systems Requirements;ISO: Geneva, Switzerland, 2013.

[121] ISO/IEC. ISO/IEC 27002:2013: Information Technology—Security Techniques—Code of Practice for Information Security Controls; ISO:Geneva, Switzerland, 2013.

[122] National Institute of Standards and Technology (NIST). NIST SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations. Available online: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed on 3 August 2021).

[123] North American Electric Reliability Corporation (NERC). CIP Standards. Available online: https://www.nerc.com/pa/Stand/ Pages/CIPStandards.aspx (accessed on 3 August 2021).

[124] https://github.com/sarahtattersall/PIPE

[125] https://www.txone-networks.com/blog/content/txone-networks-2021-cybersecurity-report

[126] CISO MAG, “Are We Really Out of the Maze? The Ransomware Gang Announces Retirement”, Nov. 3, 2020

[127] Colonial Pipeline: The Darkside Strikes - Congress. https://crsreports.congress.gov/product/pdf/IN/IN11667.

[128] Associated Press, “Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after the attack”, The Guardian, May 20, 2021

[129] Shaun Nichols, “Kaseya ransomware attacks: What we know so far”, TechTarget, July 6, 2021

[130] Lance Whitney, “Kaseya supply chain attack impacts more than 1,000 companies”, TechRepublic, July 6, 2021

[131] Pedro Tavares, “A full analysis of the BlackMatter ransomware”, Infosec, Nov. 10, 2021

[132] Trend Micro Research, “Toward a New Momentum: Trend Micro Security Predictions for 2022”, Trend Micro, Dec. 7, 2021

[133] FireEye, "Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure”," 14 December 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html.

[134] T. W. S. Journal, "New Type of Cyberattack Targets Factory Safety Systems," 19 January 2018. [Online]. Available: https://www.wsj.com/articles/hack-at-saudi-petrochemical-plant-compromised-a-safety-shut-off-system-1516301692.

[135] Alessandro Di Pinto, Younes Dragoni, Andrea Carcano, TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, It's Communications, and Its OT Payload

[136] OFFIS e.V. “Home.” OFFIS E.V., https://www.offis.de/en/offis/publication/study-on-the-evaluation-of-risks-of-cyber-incidents-and-on-costs-of-preventing-cyber-incidents-in-the-energy-sector.html.

[137] N. Perlroth, In cyberattack on Saudi rm, U.S. sees Iran firing back,The New York Times, (www:nytimes:com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us:html),October 23, 2012.

[138] Symantec, The Shamoon attacks, Symantec, (www:symantec:com/connect/blogs/shamoon-attacks), August 16, 2011.

[139] “Mitre ATT&amp;CK®.” MITRE ATT&amp;CK®, https://attack.mitre.org/.

[140] Lockheed Martin, Gaining the advantage: Applying Cyber Kill Chain® Methodology to Network Defense, 2015 [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.ENISA,

[141] European Union Agency for Network and Information Security – Threat Landscape Report 2018, European Union Agency for Network and Information Security (ENISA), 2019.

[142] Lockheed Martin, Gaining the advantage: Applying Cyber Kill Chain® Methodology to Network Defense, 2015 [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

[143] R. Trifonov, Artificial intelligence methods for cyber threats intelligence, Int. J.Comput. 2 (2017) 129–135.

[144] Microsoft Corporation, Microsoft Advanced Threat Analytics, Jan 2018 [Online]. Available: https://www.microsoft.com/en-us/cloud-platform/advanced-threatanalytics.

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

[146] E. M. Hutchins, M. J. Cloppert and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Leading Issues in Information Warfare & Security Research, vol. 1.1, no. 80, 2011.

[147] Yadav, Tarun, and Arvind Mallari Rao. “[PDF] Technical Aspects of Cyber Kill Chain: Semantic Scholar.” Undefined, 1 Jan. 1970, https://www.semanticscholar.org/paper/Technical-Aspects-of-Cyber-Kill-Chain-Yadav-Rao/7efa9c701f01cd482c92edde5aa79cedf1e2d189.

[148] Velazquez, C. (2015). Detecting and preventing attacks earlier in the kill chain. SANS Institute Infosec Reading Room, 1-21.

[149] Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., & Zhang, W. (2018). Kill chain for industrial control system. In MATEC Web of Conferences (Vol. 173, p. 01013). EDP Sciences.

[150] L. Obregon, “Secure architecture for industrial control systems,” SANS Institute InfoSec Reading Room, 2015

[151] A. Hassanzadeh, S. Modi, and S. Mulchandani,“Towards effective security control assignment in the industrial internet of things,” in IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015, pp. 795–800.

[152] A. Cook, H. Janicke, R. Smith, and L. Maglaras, “The industrial control system cyber defence triage process,” Computers & Security, vol. 70, pp. 467–481, 2017.

[153] C. Peng, H. Sun, M. Yang and Y. -L. Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, pp. 1554-1569, Aug. 2019, doi: 10.1109/TSMC.2018.2884952.

[154] Yan, Ye & Qian, Yi & Sharif, Hamid & Tipper, David. (2012). A Survey on Cyber Security for Smart Grid Communications. Communications Surveys & Tutorials, IEEE. 14. 998-1010. 10.1109/SURV.2012.010912.00035.

[155] Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, Hamid El Ghazi, Cyber-security in smart grid: Survey and challenges, Computers & Electrical Engineering, Volume 67,2018, Pages 469-482, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2018.01.015.

[156] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27.

[157] Knowles, W., Prince, D., Hutchison, D., Pagna Disso, J.F., Jones, K., 2015. A survey of cyber security management in industrial control systems. Int. J. Crit. Infrastruct. Protect. 9, 52–80.

[158] Kriaaa, S. , Pietre-Cambacedes, L. , Bouissou, M. , Halgand, Y. , 2015. A survey of approaches combining safety and security for industrial control systems. Reliab.Eng. Syst. Saf. 139, 156–178

[159] Sajid, A. , Abbas, H. , Saleem, K. , 2016. Cloud-assisted IOT-based SCADA systems security: a review of the state of the art and future challenges. IEEE Access 4,1375–1384

[160] D. Ding, Q. L. Han, Z. Wang, and X. Ge, “A Survey on Model-based Distributed Control and Filtering for Industrial Cyber-Physical Systems,” IEEE Transactions on Industrial Informatics, vol. 15, no. 5, pp. 2483-2499, May 2019.

[161] E. Molina, E. Jacob, “Software-Defined Networking in Cyber-Physical Systems: A Survey,” Computers & Electrical Engineering, vol. 66, pp. 407-419, February 2018.

[162] P. Zeng and P Zhou, “Intrusion Detection in SCADA System: A Survey,” Springer Singapore, pp. 342-351, 2018.

[163] “The State of Security in Control Systems Today: A sans Survey.” Press Release | SANS Institute, https://www.sans.org/press/announcements/the-state-of-security-in-control-systems-today-a-sans-survey/.

[164] Häckel, Björn & Niesel, Oliver & Bogenreuther, Maximil-ian & Berger, Stephan. (2019). Modeling Availability Risks of IT Threats in Smart Factory Networks - A Modular Petri Net Approach.

[165] Razzaq M, Ahmad J (2015) Petri Net and Probabilistic Model Checking Based Approach for the Modelling, Simulation, and Verification of Internet Worm Propagation. PLoS ONE 10(12): e0145690. https://doi.org/10.1371/journal.pone.0145690

[166] T. M. Chen, J. C. Sanchez-Aarnoutse and J. Buford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," in IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 741-749, Dec. 2011, doi: 10.1109/TSG.2011.2160000.

[167] K. Labadi, A.-M. Darcherif, I. El Abbassi and S. Hamaci (2020) Petri Net-Based Approach for “Cyber” Risks Modelling and Analysis for Industrial Systems E3S Web Conf., 170 02001 DOI: https://doi.org/10.1051/e3sconf/202017002001

[168] Beibei Li, Rongxing Lu, Kim-Kwang Raymond Choo, WeiWang, and Sheng Luo (2018) On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach

[169] Mahmoudi-Nasr, Payam. (2018). Petri Net Model of Insider Attacks in SCADA System.

[170] Markiewicz, Michał & Gniewek, Lesław. (2017). A Pro-gram Model of Fuzzy Interpreted Petri Net to Control Discrete Event Systems. Applied Sciences (Switzerland). 7. 10.3390/app7040422.

[171] Radoglou Grammatikis, Panagiotis & Sarigiannidis, Panagiotis & Giannoulakis, Ioannis & Kafetzakis, Emmanouil & Panaousis, Emmanouil. (2019). Attacking IEC-60870-5-104 SCADA Systems. 10.1109/SERVICES.2019.00022.

[172] Jasiul, B.; Szpyrka, M.; Śliwa, J. Detection and Modeling of Cyber Attacks with Petri Nets. Entropy 2014, 16, 6602-6623. https://doi.org/10.3390/e16126602

[173] K. Yamashita, C.-W. Ten, Y. Rho, L. Wang, W. Wei, and A. F. Ginter, (2020) Measuring systemic risk of switching at-tacks based on cybersecurity technologies in substations,” IEEE Trans. Power Syst., vol. 35, no. 6, pp. 4206–4219, Nov. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9078877.

[174] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, Cyber-physical security and dependability analysis of digital control systems in nuclear power plants," IEEE Trans. Syst., Man, Cybern., vol. 46, no. 3, pp. 356–369, 2016. [Online].Available: https://ieeexplore.ieee.org/document/7192645

[175] Henry, M.H., Layer, R.M., Snow, K.Z., & Zaret, D.R. (2009). Evaluating the risk of cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations. 2009 IEEE Conference on Technologies for Homeland Security, 607-614.

[176] Zeng, R., Jiang, Y., Lin, C., & Shen, X. (2012). Dependability Analysis of Control Center Networks in Smart Grid Using Stochastic Petri Nets. IEEE Transactions on Parallel and Distributed Systems, 23, 1721-1730.

[177] Kundur, Deepa & Feng, Xianyong & Liu, Shan & Zourn-tos, Takis & Butler-Purry, K.L.. (2010). Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. 244 - 249. 10.1109/SMARTGRID.2010.5622049.

[178] Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & But-ler-Purry, K.L. (2012). A smart grid vulnerability analysis framework for coordinated variable structure switching attacks. 2012 IEEE Power and Energy Society General Meeting, 1-6.,

[179] The Essential Role of Cyber Security in the Smart Grid. Available online: https://electricenergyonline.com/energy/magazine/312/article/The-Essential-Role-of-Cyber-Security-in-the-Smart-Grid-.htm (accessed on 30 July 2021).

[180] Guide to Industrial Control Systems (ICS) Security - NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[181] Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. J. Inf. Secur. Appl. 2020, 50, 102419.

[182] Taylor, Carol & Alves-Foss, Jim. (2001). NATE: Network Analysis of Anomalous Traffic Event, A Low-Cost Approach. Proc. New Security Paradigms Workshop.

[183] Y. Gu and L. Xie, "Stochastic Look-Ahead Economic Dispatch With Variable Generation Resources," IEEE Trans. Power Syst., vol. 32, no. 1, pp. 17-29, Jan. 2017

[184] [35] Y. Zhou, Y. Li, W. Liu, D. Yu, Z. Li, and J. Liu, "The Stochastic Response Surface Method for Small-Signal Stability Study of Power System With Probabilistic Uncertainties in Correlated Photovoltaic and Loads," IEEE Trans. Power Syst., vol. 32, no. 6, pp. 4551-4559, Nov. 2017.

[185] [36] Basumallik, Sagnik, "Impact Assessment, Detection, And Mitigation Of False Data Attacks In Electrical Power Systems" (2021). Dissertations - ALL. 1301. https://surface.syr.edu/etd/1301

[186] [37] H. Wu, I. Krad, E. Ela, A. Florita, E. Ibanez, J. Zhang and B. Hodge, "Stochastic Multi-Timescale Power System Operations with Variable Wind Generation", IEEE Trans. Power Syst., vol. 32, no. 5, pp. 3325-3337, Sept. 2017.

[187] [38] M. Khodayar, M. Shahidehpour and L. Wu, "Enhancing the Dispatchability of Variable Wind Generation by Coordination With Pumped-Storage Hydro Units in Stochastic Power Systems", IEEE Trans. Power Syst., vol. 28, no. 3, pp. 2808-2818, Aug. 2013.

[188] [39] F. Milano and R. Zarate-Minano, "A Systematic Method to Model Power Systems as Stochastic Differential Algebraic Equations", IEEE Trans. Power Syst., vol. 28, no. 4, pp. 4537-4544, Nov. 2013.

[189] [40] Li, H.; Ju, P.; Gan, C.; Wu, F.; Zhou, Y.; Dong, Z. Stochastic Stability Analysis of the Power System with Losses. Energies 2018, 11, 678. https://doi.org/10.3390/en11030678

[190] [41] Xu Y, Wen F, Zhao H, Chen M, Yang Z, Shang H. Stochastic Small Signal Stability of a Power System with Uncertainties. Energies. 2018; 11(11):2980. https://doi.org/10.3390/en11112980

[191] [42] Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic load altering attacks against power system stability: Attack models and protection schemes. IEEE Trans. Smart Grid 2018, 9, 2862–2872.

[192] [43] Adeen, Muhammad, and Federico Milano. “Modeling of Correlated Stochastic Processes for the Transient Stability Analysis of Power Systems.” NASA/ADS, https://ui.adsabs.harvard.edu/abs/2021ITPSy..36.4445A/abstract.

[193] [44] Y. Zhang, L. Wang, and W. Sun, “Investigating the impact of cyber attacks on power system reliability,” IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, 2013, pp. 462-467.

[194] [45] K. Huang, C. Zhou, Y.-C. Tian, S.-H. Yang, and Y. Qin, “Assessing the physical impact of cyberattacks on industrial cyber-physical systems,” IEEE Transactions on Industrial Electronics, vol. 65, no. 10, pp. 8153-8162, Oct. 2018.

[195] [46] T. Meraj, S. Sharmin, and A. Mahmud, “Studying the impacts of cyber-attack on smart grid,” 2nd International Conference on Electrical Information and Communication Technologies (EICT), 2015, pp. 461-466.

[196] [47] Y. Xiang, L. Wang, and Y. Zhang, “Power system adequacy assessment with probabilistic cyber attacks against breakers,” IEEE PES General Meeting | Conference & Exposition, 2014, pp. 1-5.

[197] [48] Boyaci, Osman, et al. “Spatio-Temporal Failure Propagation in Cyber-Physical Power Systems.” 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE) (2022): 1-6.

[198] Vellaithurai, C.B., Biswas, S.S., Srivastava, A.K.: Development and Application of a Real-Time Test Bed for Cyber-Physical System. IEEE Systems Journal. 11 (4), 2192–2203 (2017)

[199] Min, K.-S., Chai, S.-W., Han, M.: An International Comparative Study on Cyber Security Strategy.International journal of security and its applications. (2015)

[200] Aghamolki, H.G., Miao, Z., Fan, L.: A hardware-in-the-loop SCADA testbed. In: 2015 North American Power Symposium (NAPS). pp. 1–6. (2015)

[201] S. Muyeen and S. Rahman, Communication, control and security challenges for the smart grid. The Institution of Engineering and Technology, 2017.

[202] "Idaho National Lab Grid Resilience Program." [Online]. Available:https://inl.gov/research-programs/grid-resilience/

[203] "Idaho National Lab Resilience Optimization Center." [Online]. Available: https://factsheets.inl.gov/FactSheets/INLResilienceOptimizationCenter.pdf

[204] Idaho National Lab Infrastructure and Capabilities." [Online]. Available:https://factsheets.inl.gov/SitePages/AboutINLFactSheets-Internal.aspx

[205] "Idaho National Lab Nuclear Programs." [Online]. Available:https://factsheets.inl.gov/FactSheets/NuclearPrograms.pdf

[206] "Idaho National Lab Nuclear Laboratory." [Online]. Available: https://factsheets.inl.gov/FactSheets/NationalNuclearLaboratory Overview.pdf

[207] C. Konstantinou, "Cyber-physical systems security education through hands-on lab exercises," IEEE Design Test, vol. 37, no. 6, pp. 47–55,2020.

[208] M. O. Faruque and V. Dinavahi, "Hardware-in-the-loop simulation of power electronic systems using adaptive discretization," IEEE transactions on industrial electronics, vol. 57, no. 4, pp. 1146–1158, 2009.

[209] "National Renewable Energy Laboratory (NREL)." [Online]. Available:https://www.nrel.gov/index.html

[210] "National Renewable Energy Laboratory Flatirons Campus." [Online].Available: https://www.nrel.gov/flatirons-campus/

[211] "Increasing Power Expands Research Capabilities at NREL's Flatirons Campus." [Online]. Available: https://www.nrel.gov/news/program/2020/increasing-power-at-flatirons-campus.html

[212] HELICS. (2020) Hierarchical engine for large-scale infrastructure co-simulation (HELICS). [Online]. Available: https://gmlc-tdc.github.io/helics.org/

[213] (2020) Tools with HELICS Support. [Online]. Available: https://docs.helics.org/en/latest/Tools using HELICS.html

[214] Le, T.D.; Mengmeng, G.; Phan, T.D.; Hien, D.H.; Adnan, A.; Beuran, R.; Seng, W.L.; Yasuo, T. CVSS Based Attack Analysis using a Graphical Security Model: Review and Smart Grid Case Study. In Proceedings of the International Conference on Smart Grid and Internet of Things, TaiChung, Taiwan, 5–6 December 2020; Springer: Cham, Switzerland, 2020.

[215] Islam, S.N.; Baig, Z.; Zeadally, S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. IEEE Trans. Ind. Inform. 2019, 15, 6522–6530.

[216] Beckers, K.; Heisel, M.; Krautsevich, L.; Martinelli, F.; Meis, R.; Yautsiukhin, A. Determining the probability of smart grid attacks by combining attack tree and attack graph analysis. In Proceedings of the International Workshop on Smart Grid Security,Munich, Germany, 26 February 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 30–47.

[217] Ge, M.; Hong, J.B.; SeongKim,W.G.D. A framework for automating security analysis of the internet of things. J. Netw. Comput. Appl. 2017, 83, 12–27.

[218] "(PDF) Cyberphysical Security Analysis of Digital Control Systems in Hydro Electric Power Grids." https://www.researchgate.net/publication/359508590_Cyberphysical_Security_Analysis_of_Digital_Control_Systems_in_Hydro_Electric_Power_Grids (accessed Nov. 21, 2022).

[219] L. Phiri and S. Tembo, "Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia," International Journal of Advances in Scientific Research and Engineering, vol. 08, no. 05, pp. 01–22, 2022, doi: 10.31695/IJASRE.2022.8.5.1.

[220] "Stochastic Quantification of Cyber Attacks Impact on Smart Grid Contingency Analysis | Phiri | Journal of Electrical Engineering, Electronics, Control and Computer Science." https://jeeeccs.net/index.php/journal/article/view/298 (accessed Nov. 21, 2022).

[221] "The five worst cyberattacks against the power industry since 2014 - Power Technology." https://www.power-technology.com/analysis/the-five-worst-cyberattacks-against-the-power-industry-since2014/ (accessed Nov. 21, 2022).

[222] S. Alhalali, C. Nielsen, and R. El-Shatshat, "Mitigation of Cyber-Physical Attacks in Multi-Area Automatic Generation Control," 2019, doi: 10.1016/j.ijepes.2019.05.014.

[223] Y. Liu, Z. Qu, H. Xin, and D. Gan, "Distributed Real-Time Optimal Power Flow Control in Smart Grid," IEEE Transactions on Power Systems, vol. 32, no. 5, pp. 3403–3414, Sep. 2017, doi: 10.1109/TPWRS.2016.2635683.

[224] M. H. Variani and K. Tomsovic, "Distributed automatic generation control using flatness-based approach for high penetration of wind generation," IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3002–3009, 2013, doi: 10.1109/TPWRS.2013.2257882.

[225] "Comprehensive Survey and Taxonomies of False Injection Attacks in Smart Grid: Attack Models, Targets, and Impacts | Papers With Code." https://cs.paperswithcode.com/paper/comprehensive-survey-and-taxonomies-of-false (accessed Nov. 21, 2022).

[226] Z. H. Pang, G. P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems," undefined, vol. 63, no. 5, pp. 3242–3251, May 2016, doi: 10.1109/TIE.2016.2535119.

[227] W. Ao, Y. Song, and C. Wen, “Adaptive cyber-physical system attack detection and reconstruction with application to power systems,” IET Control Theory & Applications, vol. 10, no. 12, pp. 1458–1468, Aug. 2016, doi: 10.1049/IET-CTA.2015.1147.

[228] H. M. Khalid and J. C. H. Peng, “Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction,” IEEE Trans Smart Grid, vol. 8, no. 2, pp. 697–707, Mar. 2017, doi: 10.1109/TSG.2015.2487280.

[229] R. Deng, G. Xiao, and R. Lu, “Defending Against False Data Injection Attacks on Power System State Estimation,” IEEE Trans Industr Inform, vol. 13, no. 1, pp. 198–207, Feb. 2017, doi: 10.1109/TII.2015.2470218.

[230] Z. H. Yu and W. L. Chin, “Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid,” IEEE Trans Smart Grid, vol. 6, no. 3, pp. 1219–1226, May 2015, doi: 10.1109/TSG.2014.2382714.

[231] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter,” IEEE Trans Control Netw Syst, vol. 1, no. 4, pp. 370–379, Dec. 2014, doi: 10.1109/TCNS.2014.2357531.

[232] P. Bangalore and L. B. Tjernberg, “An artificial neural network approach for early fault detection of gearbox bearings,” IEEE Trans Smart Grid, vol. 6, no. 2, pp. 980–987, Mar. 2015, doi: 10.1109/TSG.2014.2386305.

[233] A. Abdullah, “Ultrafast Transmission Line Fault Detection Using a DWT-Based ANN,” undefined, vol. 54, no. 2, pp. 1182–1193, Mar. 2018, doi: 10.1109/TIA.2017.2774202.

[234] S. Jana and A. De, “A Novel Zone Division Approach for Power System Fault Detection Using ANN-Based Pattern Recognition Technique,” Canadian Journal of Electrical and Computer Engineering, vol. 40, no. 4, pp. 275–283, Feb. 2022, doi: 10.1109/CJECE.2017.2751661.

[235] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. Vincent Poor, “Machine Learning Methods for Attack Detection in the Smart Grid,” 2015.

[236] J. Yan, X. Zhong, and Y. Tang, “Q-learning Based Vulnerability Analysis of Smart Grid against Sequential Topology Attacks,” 2016, doi: 10.1109/TIFS.2016.2607701.

[237] S. A. Foroutan and F. R. Salmasi, “Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method,” IET Cyber-Physical Systems: Theory & Applications, vol. 2, no. 4, pp. 161–171, Dec. 2017, doi: 10.1049/IET-CPS.2017.0013.

[238] Y. He, G. J. Mendis, and J. Wei, “Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism,” IEEE Trans Smart Grid, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.

[239] M. L. Puterman, “Markov decision processes: Discrete stochastic dynamic programming,” Markov Decision Processes: Discrete Stochastic Dynamic Programming, pp. 1–649, Jan. 2008, doi: 10.1002/9780470316887.

[240] Namukolo, Sebastian & Zulu, Ackim & Nswana, Changala & Sitwala, Nangalelwa. (2016). Turning to Smart Grid in Zambia.

[241] Copper Refinery Modernisation, Mopani Copper Mines Plc, Mufulira, Zambia. https://www.glencoretechnology.com/.rest/api/v1/documents/b2f07fc447fb27940a0e548c5b7c4c74/MCM%20Refinery%20Upgrade.pdf.

[242] “The Electronic Communications and Transactions Act, 2021.” The Electronic Communications and Transactions Act, 2021 | National Assembly of Zambia, https://www.parliament.gov.zm/node/8842.

[243] “The Data Protection Act, 2021.” The Data Protection Act, 2021 | National Assembly of Zambia, https://www.parliament.gov.zm/node/8853.

[244] “The Information and Communication Technologies (Amendment) Act 2010.” The Information and Communication Technologies (Amendment) Act 2010 | National Assembly of Zambia, 24 Mar. 2010, https://www.parliament.gov.zm/node/3259.

[245] Vaishnavi V, Kuechler W, and Petter S (Eds.) (2004/19) Design Science Research in Information Systems, (created in 2004 by Vaishnavi V and Kuechler W); last updated (by Vaishnavi, V, and Petter, S), June 30, 2019. URL: http://www.desrist.org/design-research-in-information-systems/

[246] Lindholm C (2015) Software risk management in the safety-critical medical device domain - involving a user perspective, Doctoral Dissertation 45, Department of Computer Science, Lund University, Sweden

[247] Hevner A. R (2007) A three cycle view of design science research, Scandinavian Journal of Information Systems, vol 19, no 2, pp 87-92

[248] Peffers K, Tuunanen T, Gengler C. E, Rossi M, Hui W, Virtanen V, and Bragge J (2006) The design science research process: a model for producing and presenting information systems research, the 1st Int. Conference on Design Science Research, Claremont, CA, pp 83-106

[249] Molleri J. S, Petersen K, and Mendes E (2016) Survey guidelines in software engineering: an annotated review, 10th ACM/IEEE Int. Symposium on Empirical Software Engineering and Measurement, ESEM’16, pp 58:1-58:6

[250] Dag I. K. Sjoberg, Tore Dyba, and Magne Jorgensen. 2007. The Future of Empirical Methods in Software Engineering Research. In 2007 Future of Software Engineering (FOSE '07). IEEE Computer Society, USA, 358–378. https://doi.org/10.1109/FOSE.2007.30

[251] Easterbook S, Singer J, Storey M. A, and Damian D (2008) Guide to advanced empirical software engineering. Chap: Selecting empirical methods for software engineering research, Springer-Verlag, pp. 285-311

[252] Wieringa R.J (2014) Empirical research methods for technology validation: Scaling up to practice, Journal of Systems and Software, vol 95, pp 19-31

[253] Runeson P, and Höst M (2009) Guidelines for conducting and reporting case study research in software engineering, Empirical Software Engineering, Springer, vol 14, no 131

[254] Yin R. K (2009) Case study research: Design and Methods, Fourth Edition, Applied Social Research Methods Series

[255] Fraenkel, J.R. & Wallen, N.E. (2002). How to design and evaluate research in education (5th Ed.). Boston: McGraw Hill.

[256] Hamed Taherdoost. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. International Journal of Academic Research in Management (IJARM), 2016, 5. hal-02546796

[257] Lethbridge T. C, Sim S. E, and Singer J (2005) Studying Software Engineers: Data Collection Techniques for Software Field Studies, Empirical Software Engineering, 10, pp 311-341

[258] Basili V. R (1992) Software modeling and measurement: the Goal/Question/Metric paradigm, University of Maryland, CS-TR-2956, UMIACS-TR-92-96

[259] Basili V, Caldiera G, and Rombach H. D (1994) Encyclopedia of Software Engineering, vol. 2, pp 528-532, John Wiley & Sons, Inc

[260] Runeson P, and Höst M (2009) Guidelines for conducting and reporting case study research in software engineering, Empirical Software Engineering, Springer, vol 14, no 131

[261] Robson C (2002) Real-world research (2nd ed.) Oxford UK: Blackwell Publishers

[262] Kontio J, Lettola L, and Bragge J (2004) Using the focus group method in software engineering: obtaining practitioner and user experience, IEEE Int. Symposium on Empirical Software Engineering, Doi: 10.1109/ISESE.2004.1334914

[263] F. Bause and P. S. Kritzinger, Stochastic Petri Nets: An Intro-duction to the Theory, 2nd ed. Braunschweig, Germany: Vieweg, 2002.

[264] Trivedi, Kishor S. “Probability and Statistics with Reliability, Queuing, and Computer Science Applications, 2nd Edition.” Wiley.com, 28 Nov. 2001, https://www.wiley.com/en-us/ProbabilityandStatisticswithReliabilityQueuing andComputerScienceApplication2ndEdition-p-9780471333418Trivedi

[265] K. Yamashita, C.-W. Ten, Y. Rho, L. Wang, W. Wei, and A. F. Ginter, (2020) Measuring systemic risk of switching attacks based on cybersecurity technologies in substations,” IEEE Trans. Power Syst., vol. 35, no. 6, pp. 4206–4219, Nov. 2020. [Online]. Available: https://ieeexplore.ieee.org/ document/9078877.

[266] P. J. B. Donald L. Evans Arden L. Bement, Jr., "Standards for Security Categorization of Federal Information and Information Systems, FIPS 199," Nist, no. February. 2004. [Online]. Available: %3Ccsrc.nist.gov/publications/fips/fips199/FIPS-PUB-199.pdf%3E

[267] Mohammadpourfard, M.; Sami, A.; Weng, Y. Identification of False Data Injection Attacks with Considering the Impact of Wind Generation and Topology Reconfigurations. IEEE Trans. Sustain. Energy 2017, 9, 1349–1364.

[268] C. Konstantinou, "Towards a secure and resilient all-renewable energy grid for smart cities," IEEE Consumer Electronics Magazine, 2021.

[269] S. Muyeen and S. Rahman, Communication, control and security challenges for the smart grid. The Institution of Engineering and Technology, 2017.

[270] J. Ospina, X. Liu, C. Konstantinou, and Y. Dvorkin, "On the feasibility of load-changing attacks in power systems during the covid-19 pandemic," IEEE Access, vol. 9, pp. 2545–2563, 2021.

[271] Abliz, Mehmud. "Internet Denial of Service Attacks and Defense Mechanisms." (2011).

[272] A Comparison of Phasor Communication Protocols - PNNL. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28499.pdf.

[273] Y. Yang et al., "Man-in-the-middle attack testbed investigating cyber-security vulnerabilities in Smart Grid SCADA systems," International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), 2012, pp. 1-8, doi: 10.1049/cp.2012.1831.

[274] Ouafi, Khaled & Overbeck, Raphael & Vaudenay, Serge. (2008). On the Security of HB # Against a Man-in-the-Middle Attack. 10.1007/978-3-540-89255-7_8.

[275] P. Kundur, N. J. Balu, and M. G. Lauby, Power system stability and control. McGraw-hill New York, 1994.

[276] MITRE foundation. “Assets in MITRE ICS”. In: MITRE ICS (2020).Accessed: 18.04.2020, https://collaborate.mitre.org/attackics/index.php/All_Assets.

[277] Infosec. “What is Enumeration?” In: (2020).Accessed: 10.08.2020, https://resources.infosecinstitute.com/what-is-enumeration.

[278] McAfee. “Introduction to McAfee ePolicy Orchestrator”. In: (2020).Accessed: 16.05.2020, https://www.mcafee.com/enterprise/en - us / downloads / trials / epolicy - orchestrator .html.

[279] McAfee. “Managing McAfee ePO users with Active Directory”. In:(2020). Accessed: 16.05.2020, https://docs.mcafee.com/bundle/epolicy-orchestrator-5.9.x-product-guide/page/GUID-17CC4F49-DDAA-4282-A778-5B4D71BE236B.html.

[280] Department of US homeland security. “CISA: Industry Control Systems”.In: (2016).Accessed: 18.04.2020, https://www.us-cert.gov/ics.

[281] Stefan Axelsson. Intrusion detection systems: A survey and taxonomy.Tech. rep. Technical report, 2000.

[282] Y. Guo, L. Wang, Z. Liu, and Y. Shen, “Reinforcement-learning-based dynamic defense strategy of multistage game against dynamic load altering attack,” International Journal of Electrical Power & Energy Systems, vol. 131, p. 107113, Oct. 2021, doi: 10.1016/J.IJEPES.2021.107113.

[283] C. Luo, H. G. Far, H. Banakar, P. K. Keung, and B. T. Ooi, “Estimation of wind penetration as limited by frequency deviation,” IEEE Transactions on Energy Conversion, vol. 22, no. 3, pp. 783–791, Sep. 2007, doi: 10.1109/TEC.2006.881082.

[284] F. Thuijsman, S. H. Tijs, and O. J. Vrieze, “Perfect equilibria in stochastic games,” Journal of Optimization Theory and Applications 1991 69:2, vol. 69, no. 2, pp. 311–324, May 1991, doi: 10.1007/BF00940646.

[285] Y. Chen et al., “Vector Auto-Regression-Based False Data Injection Attack Detection Method in Edge Computing Environment,” Sensors, vol. 22, no. 18, Sep. 2022, doi: 10.3390/s22186789.

[286] D. A. Haughton and G. T. Heydt, “A linear state estimation formulation for smart distribution systems,” IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 1187–1195, 2013, doi: 10.1109/TPWRS.2012.2212921.

[287] C. Pei, Y. Xiao, W. Liang, and X. Han, “A Deviation-Based Detection Method against False Data Injection Attacks in Smart Grid,” IEEE Access, vol. 9, pp. 15499–15509, 2021, doi: 10.1109/ACCESS.2021.3051155.

[288] Y. Chen et al., “Vector Auto-Regression-Based False Data Injection Attack Detection Method in Edge Computing Environment,” Sensors, vol. 22, no. 18, Sep. 2022, doi: 10.3390/s22186789.

[289] A. Sayghe et al., “A Survey of Machine Learning Methods for Detecting False Data Injection Attacks in Power Systems,” Aug. 2020, [Online]. Available: http://arxiv.org/abs/2008.06926

[290] Q. Wang, Y. Ma, K. Zhao, and Y. Tian, “A Comprehensive Survey of Loss Functions in Machine Learning,” Annals of Data Science, vol. 9, no. 2, pp. 187–212, Apr. 2022, doi: 10.1007/s40745-020-00253-5.

[291] Becejac T., C.R. Eppinger, A. Ashok, U. Agrawal, and J.G. O'Brien. 2020.PRIME: A real-time cyber-physical systems testbed: From Wide-Area Monitoring, Protection and Control prototyping to operator training and beyond.IET Cyber-Physical Systems: Theory & Applications 5, no. 2:186-195.PNNL-SA-145117.doi:10.1049/iet-cps.2019.0049EDMAND

[292] 2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Vienna, Austria, 2016, pp. 1-6.

[293] W. Ren, T. Yardley, K. Nahrstedt. To Appear in proceedings for the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids 29 Oct - 1 Nov 2018, Aalborg, Denmark.

[294] Helerea, Elena. “Interconnections between Reliability, Maintenance and Availability.” IFIP Advances in Information and Communication Technology, 19 Aug. 2016, https://www.academia.edu/27901809/Interconnections_between_Reliability_Maintenance_and_Availability.

[295] M. Kim, A Survey on Guaranteeing Availability in Smart Grid Communications," in Proc.ICACT, Korea, February 2012.

[296] SGTF EG2. Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity, Second Interim Report, Smart Grid Task Force Expert Group. 2018. Available online: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf (accessed on 29 January 2019).

[297] Software Simulation ┃ Real-Time Applications ┃ RT Labs." OPAL, 15 July 2021, https://www.opal-rt.com/software-rt-lab-2-2/.

[298] Keysight. "Exata Network Modeling – Critical Infrastructure." Keysight, 2 Jan. 2018, https://www.keysight.com/us/en/product/SN050ECPA/exata-network-modeling-critical-infrastructure.html.

[299] L. Zhang et al., "Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools." [Online]. Available: http://conference-americas.pacw.org/

[300] L. S. Shapley, “Stochastic Games*,” Proceedings of the National Academy of Sciences, vol. 39, no. 10, pp. 1095–1100, Oct. 1953, doi: 10.1073/PNAS.39.10.1095.

[301] A. J. Conejo, Miguel. Carrión, and J. M. Morales, “Decision making under uncertainty in electricity markets,” p. 539, 2010.

[302] GRIF-Workshop, Retrieved from 2021. Satodev, Total. http://grif-workshop.com.

APPENDICES

APPENDIX A (Transitions for the combined firewall and password models)

Table 0-1 .The transitions rates for the combined model

	λ_a	λ_b	λ_c	λ_d	λ_e	λ_f	λ_g	λ_h	λ_i	λ_j	λ_k	λ_l	λ_m	λ_n	λ_o	λ_p	λ_q	λ_r
	0.01	0.99	0.01	0.99	0.01	0.99	1E-5	1E-5	1E-5	1E-5	0.5E-7	-	-	-	-	-	-	
	0.01	0.99	1E-5	0.9987	0.0013	1E-6	0.5E-7	0.02	-	-	-	-	-	-	-	-	-	
	0.01	0.99	0.01	0.99	0.01	0.99	1E-6	1E-6	1E-6	1E-6	0.01	0.99	0.5E-7	1E-6	0.00130	0.9987	1E-5	0.01

Table 0-2.The steady-state probabilities of the combined model

Model	π_0	π_1	π_2	π_3	π_4	π_5	π_6	π_7	π_8	π_9	π_{10}	π_{11}	π_{12}
I	0	0	0.0049	0	0.0048	0.95109	0.0475	0.00048	-	-	-	-	-
II	0.00001	0.0097	0.95592	0.00001	0.02485	0.00955	-	-	-	-	-	-	-
III	0	0	0.0004	0	0.00043	0.00001	0.04176	0.00042	0.78902	0.1594	0.00001	0.00788	0.00103

APPENDIX B (Stochastic Impact scenarios and results)

Table 0-3.The modeling instances

	Number of histories	First random number	Maximum calculation time
Instance 1	10	12345681	10
Instance 2	100	12345681	10
Instance 3	1000	12345681	10
Instance 4	10,000	12345681	10

Table 0-4.The probabilities for the first scenario

State	Instance 1 Probability	Instance 2 Probability	Instance 3 Probability	Instance 4 Probability
Gen 1_Up	0.218912037	0.16771764	0.15347399	0.141604717
CyberAttack_Failure	0	0	0	0
Physical_failure	0	0	0	0
Bus1_Vulnerable	0.158933134	0.110965197	0.106574945	0.10042471
Bus1_down	0.149654942	0.117068243	0.106371085	0.10017746
Cascade_begin	0.036801102	0.048744505	0.047475634	0.046191394
Bus2_Up	0.144268051	0.159321881	0.148026631	0.138944834

Bus2_Vulnerable	0.050134476	0.109162418	0.104100555	0.099417391
Gen 2_down	0.112241987	0.109186027	0.104415866	0.098710829

Table 0-5.The probabilities for the second scenario

State	Instance 1 Probability	Instance 2 Probabilities	Instance 3 Probabilities	Instance 4 Probabilities
BUS1_UP	0.433850811	0.43452249	0.431120969	0.432954469
Cyber_Failure	0	0	0	0
Physical_Failure	0	0	0	0
Bus1_Vulnerable	0.085838129	0.057241576	0.051214666	0.048893878
Bus1_Down	0.05369558	0.083681461	0.091316239	0.085387221
Bus1-2_Cascadebegins	0.047193387	0.041509163	0.038681341	0.038476318
BUS2_UP	0.168198255	0.131439965	0.126147693	0.112466913
Bus2_Vulnerable	0.124942457	0.070541997	0.075268742	0.067284266
Bus2_Down	0.066882864	0.085536671	0.073917414	0.065913581
Bus3_UP	0.088703859	0.114639195	0.111429556	0.109050511

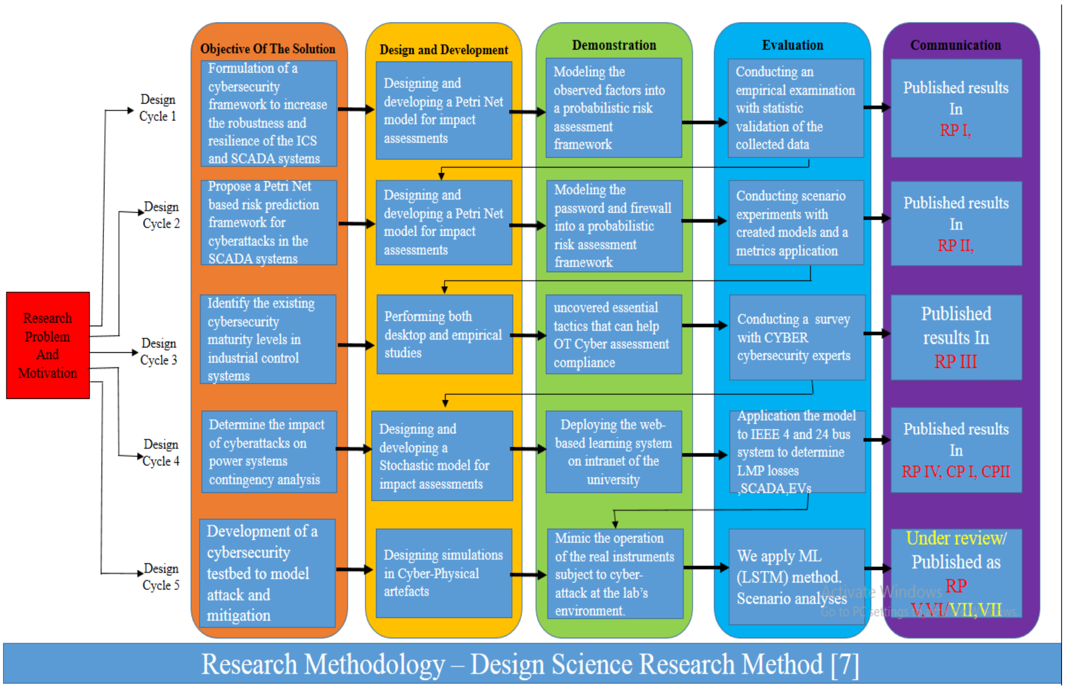
Bus3_Vulnerable	0.028640047	0.069577334	0.069194784	0.066200892
Bus3_Down	0.060073606	0.058586149	0.061599753	0.064143721
Bus1-4_Cascadebegins	0.045620111	0.050869293	0.04724814	0.046404441
Bus4_Up	0.139295519	0.151801784	0.146124909	0.138172721
Bus4_Vulnerable	0.117320166	0.11057571	0.105408834	0.099395137
Bus4_Down	0.060704225	0.099873658	0.099526062	0.097858459

Table 0-6. The Locational Margin Pricing (LMP)

BUS	LMP ($/hr)	BUS	LMP ($/hr)
1	56.3169	**13**	58.6915
2	56.5817	**14**	67.3583
3	52.6700	**15**	44.2975
4	57.2618	**16**	44.5828
5	59.8611	**17**	40.5909
6	60.5628	**18**	41.5488
7	46.1486	**19**	52.5032
8	58.4498	**20**	54.0081
9	57.8183	**21**	42.4102
10	59.0814	**22**	41.6976
11	61.6508	**23**	54.8289

12	57.8578	**24**	47.4390

APPENDIX C (Research design matrix)



Research Problem And Motivation

Objective Of The Solution | Design and Development | Demonstration | Evaluation | Communication

Design Cycle 1: Formulation of a cybersecurity framework to increase the robustness and resilience of the ICS and SCADA systems → Designing and developing a Petri Net model for impact assessments → Modeling the observed factors into a probabilistic risk assessment framework → Conducting an empirical examination with statistic validation of the collected data → Published results In RP I,

Design Cycle 2: Propose a Petri Net based risk prediction framework for cyberattacks in the SCADA systems → Designing and developing a Petri Net model for impact assessments → Modeling the password and firewall into a probabilistic risk assessment framework → Conducting scenario experiments with created models and a metrics application → Published results In RP II,

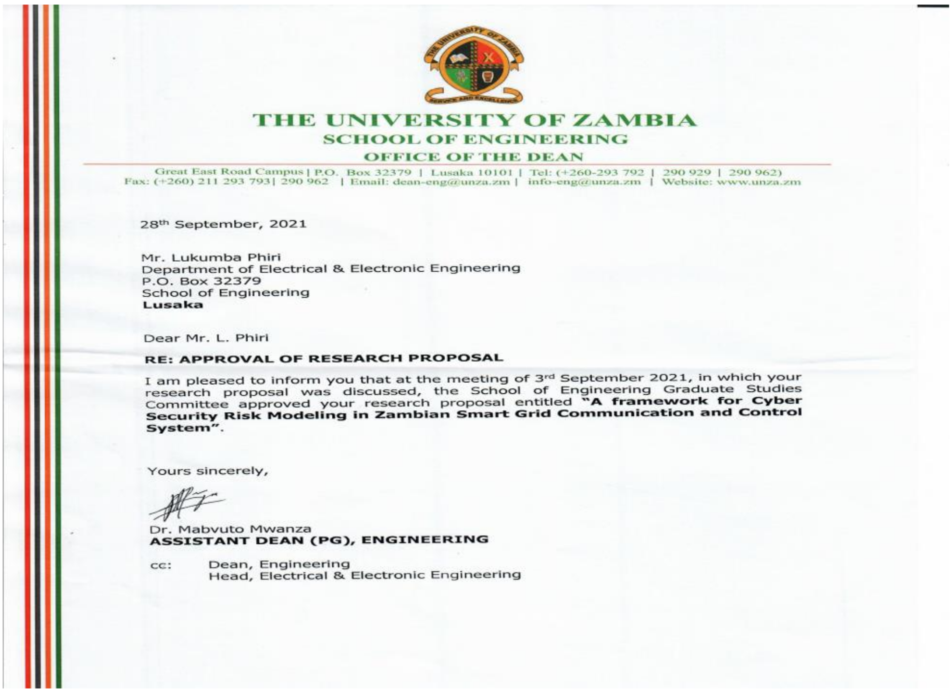
Design Cycle 3: Identify the existing cybersecurity maturity levels in industrial control systems → Performing both desktop and empirical studies → uncovered essential tactics that can help OT Cyber assessment compliance → Conducting a survey with CYBER cybersecurity experts → Published results In RP III

Design Cycle 4: Determine the impact of cyberattacks on power systems contingency analysis → Designing and developing a Stochastic model for impact assessments → Deploying the web-based learning system on intranet of the university → Application the model to IEEE 4 and 24 bus system to determine LMP losses ,SCADA,EVs → Published results In RP IV, CP I, CPII

Design Cycle 5: Development of a cybersecurity testbed to model attack and mitigation → Designing simulations in Cyber-Physical artefacts → Mimic the operation of the real instruments subject to cyber-attack at the lab's environment → We apply ML (LSTM) method. Scenario analyses → Under review/ Published as RP V,VI/VII,VII

Research Methodology – Design Science Research Method [7]

APPENDIX D (Research Approval and Ethical Clearance)



THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260-293 792 | 290 929 | 290 962)
Fax: (+260) 211 293 793| 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

28th September, 2021

Mr. Lukumba Phiri
Department of Electrical & Electronic Engineering
P.O. Box 32379
School of Engineering
Lusaka

Dear Mr. L. Phiri

RE: APPROVAL OF RESEARCH PROPOSAL

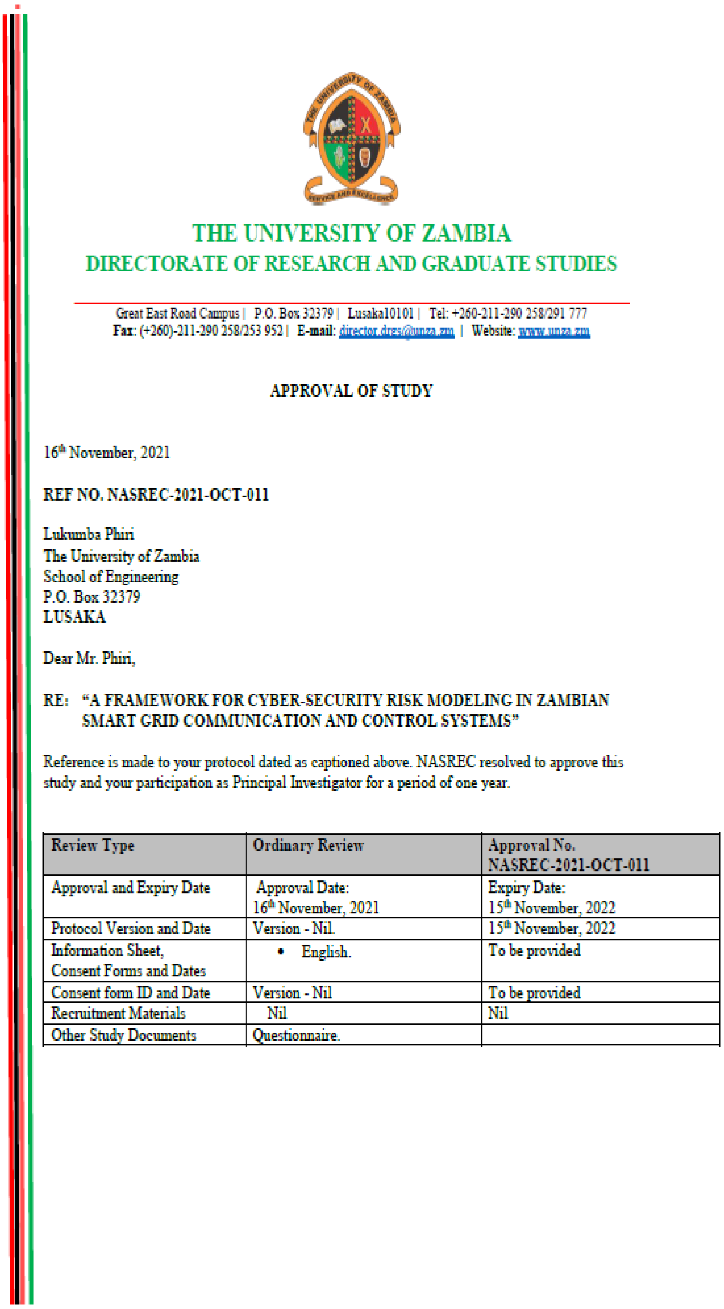
I am pleased to inform you that at the meeting of 3rd September 2021, in which your research proposal was discussed, the School of Engineering Graduate Studies Committee approved your research proposal entitled **"A framework for Cyber Security Risk Modeling in Zambian Smart Grid Communication and Control System".**

Yours sincerely,

Dr. Mabvuto Mwanza
ASSISTANT DEAN (PG), ENGINEERING

cc: Dean, Engineering
Head, Electrical & Electronic Engineering

Study Approval



THE UNIVERSITY OF ZAMBIA
DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Great East Road Campus | P.O. Box 32379 | Lusaka10101 | Tel: +260-211-290 258/291 777
Fax: (+260)-211-290 258/253 952 | **E-mail**: director.drgs@unza.zm | Website: www.unza.zm

APPROVAL OF STUDY

16th November, 2021

REF NO. NASREC-2021-OCT-011

Lukumba Phiri
The University of Zambia
School of Engineering
P.O. Box 32379
LUSAKA

Dear Mr. Phiri,

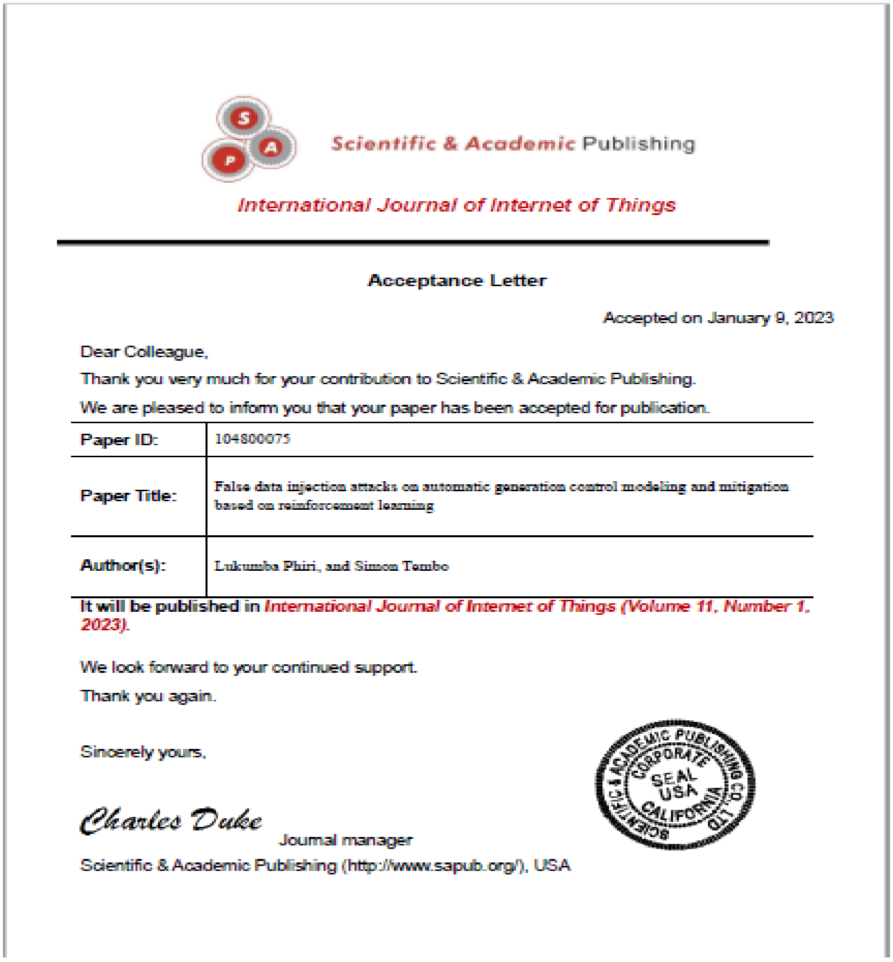
RE: "A FRAMEWORK FOR CYBER-SECURITY RISK MODELING IN ZAMBIAN SMART GRID COMMUNICATION AND CONTROL SYSTEMS"

Reference is made to your protocol dated as captioned above. NASREC resolved to approve this study and your participation as Principal Investigator for a period of one year.

Review Type	Ordinary Review	Approval No. NASREC-2021-OCT-011
Approval and Expiry Date	Approval Date: 16th November, 2021	Expiry Date: 15th November, 2022
Protocol Version and Date	Version - Nil.	15th November, 2022
Information Sheet, Consent Forms and Dates	• English.	To be provided
Consent form ID and Date	Version - Nil	To be provided
Recruitment Materials	Nil	Nil
Other Study Documents	Questionnaire.	

Ethical clearance

APPENDIX E (Research Publications)



Scientific & Academic Publishing

International Journal of Internet of Things

Acceptance Letter

Accepted on January 9, 2023

Dear Colleague,

Thank you very much for your contribution to Scientific & Academic Publishing.

We are pleased to inform you that your paper has been accepted for publication.

Paper ID:	104800075
Paper Title:	False data injection attacks on automatic generation control modeling and mitigation based on reinforcement learning
Author(s):	Lukumba Phiri, and Simon Tembo

It will be published in *International Journal of Internet of Things (Volume 11, Number 1, 2023).*

We look forward to your continued support.

Thank you again.

Sincerely yours,

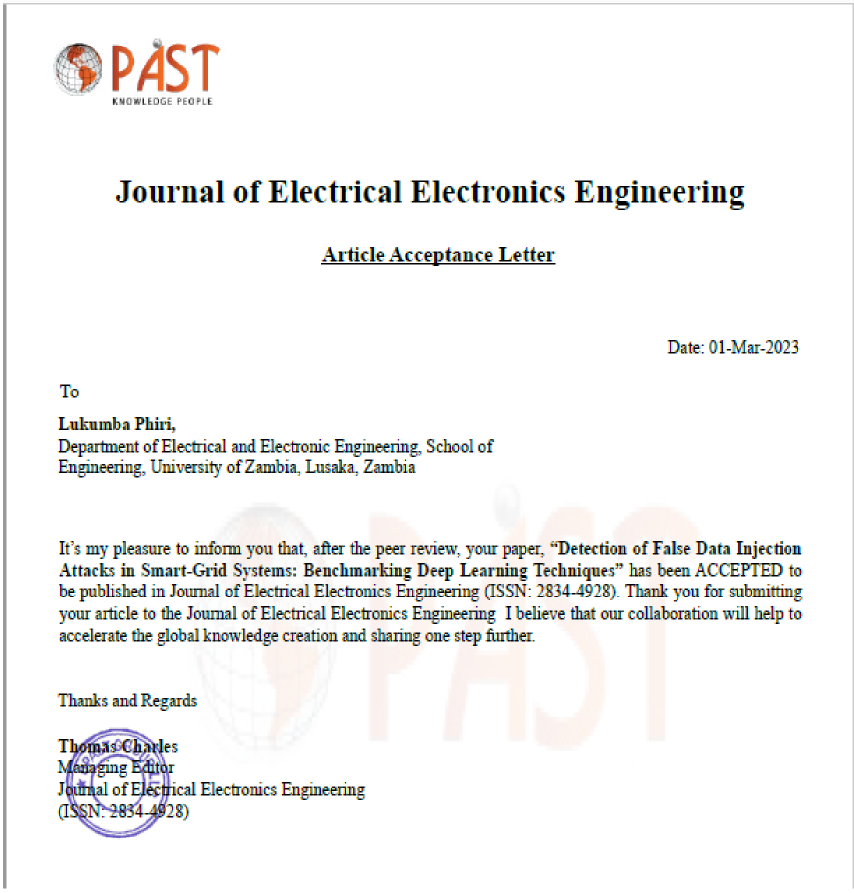
SCIENTIFIC & ACADEMIC PUBLISHING CO. LTD CORPORATE SEAL USA CALIFORNIA

Charles Duke

Journal manager

Scientific & Academic Publishing (http://www.sapub.org/), USA

FDIA Detection and Mitigation



PAST
KNOWLEDGE PEOPLE

Journal of Electrical Electronics Engineering

Article Acceptance Letter

Date: 01-Mar-2023

To

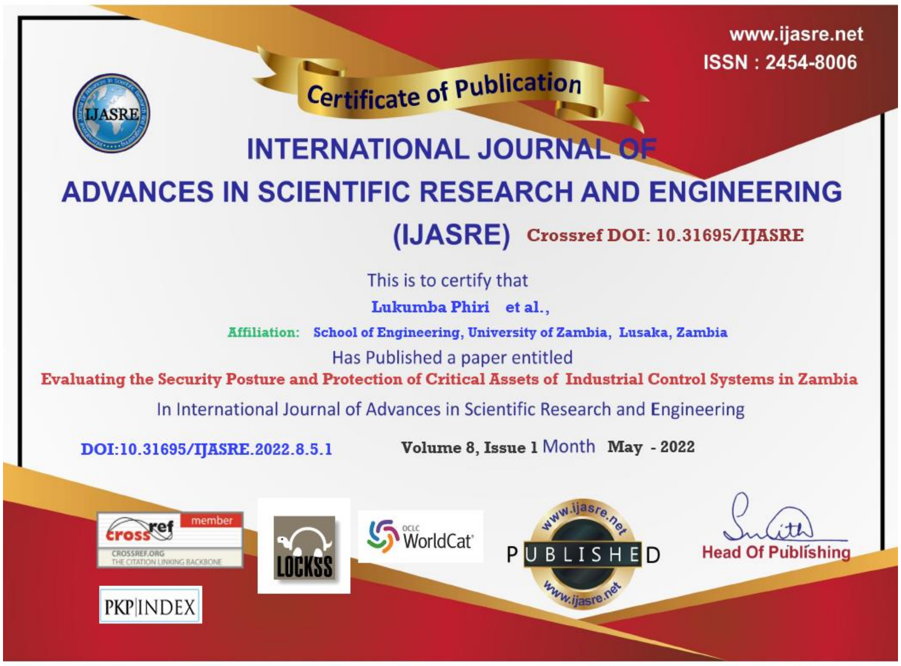
Lukumba Phiri,
Department of Electrical and Electronic Engineering, School of
Engineering, University of Zambia, Lusaka, Zambia

It's my pleasure to inform you that, after the peer review, your paper, **"Detection of False Data Injection Attacks in Smart-Grid Systems: Benchmarking Deep Learning Techniques"** has been ACCEPTED to be published in Journal of Electrical Electronics Engineering (ISSN: 2834-4928). Thank you for submitting your article to the Journal of Electrical Electronics Engineering. I believe that our collaboration will help to accelerate the global knowledge creation and sharing one step further.

Thanks and Regards

Thomas Charles
Managing Editor
Journal of Electrical Electronics Engineering
(ISSN: 2834-4928)

Benchmarking Deep Learning Techniques



www.ijasre.net
ISSN : 2454-8006

IJASRE

Certificate of Publication

INTERNATIONAL JOURNAL OF
ADVANCES IN SCIENTIFIC RESEARCH AND ENGINEERING
(IJASRE) Crossref DOI: 10.31695/IJASRE

This is to certify that

Lukumba Phiri et al.,

Affiliation: School of Engineering, University of Zambia, Lusaka, Zambia

Has Published a paper entitled

Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia

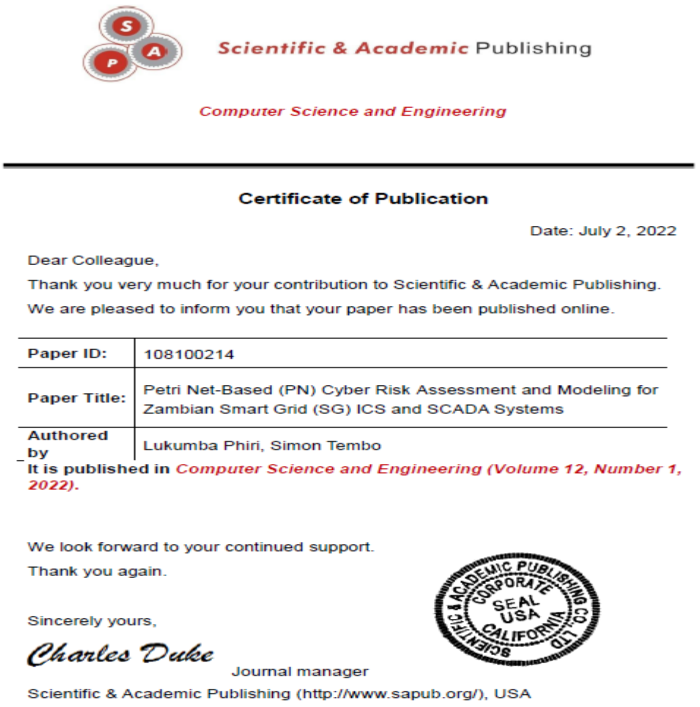
In International Journal of Advances in Scientific Research and Engineering

DOI:10.31695/IJASRE.2022.8.5.1 **Volume 8, Issue 1** Month **May - 2022**

Crossref member
CROSSREF.ORG THE CITATION LINKING BACKBONE
LOCKSS
OCLC WorldCat
PKP|INDEX
www.ijasre.net PUBLISHED www.ijasre.net

Head Of Publishing

Evaluating the Security Posture of ICS



Scientific & Academic Publishing

Computer Science and Engineering

Certificate of Publication

Date: July 2, 2022

Dear Colleague,

Thank you very much for your contribution to Scientific & Academic Publishing.

We are pleased to inform you that your paper has been published online.

Paper ID:	108100214
Paper Title:	Petri Net-Based (PN) Cyber Risk Assessment and Modeling for Zambian Smart Grid (SG) ICS and SCADA Systems
Authored by	Lukumba Phiri, Simon Tembo

It is published in *Computer Science and Engineering (Volume 12, Number 1, 2022).*

We look forward to your continued support.

Thank you again.

Sincerely yours,

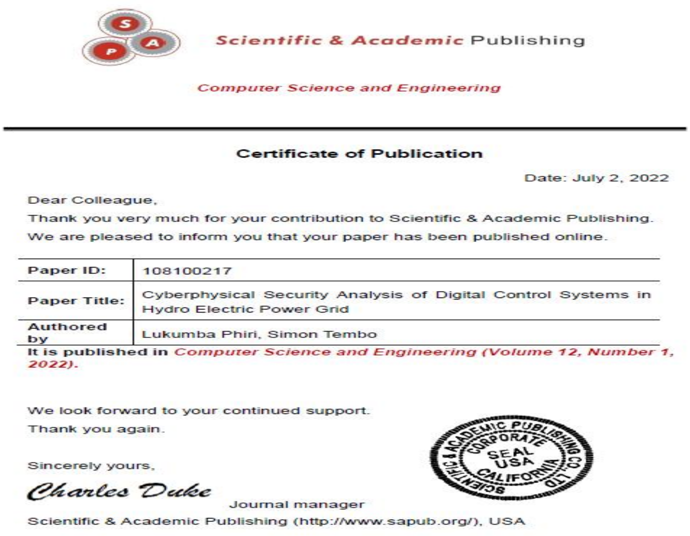
Charles Duke

Journal manager

SCIENTIFIC & ACADEMIC PUBLISHING CO. LTD CORPORATE SEAL USA CALIFORNIA

Scientific & Academic Publishing (http://www.sapub.org/), USA

Petri Net-Based Risk Assessment



Scientific & Academic Publishing

Computer Science and Engineering

Certificate of Publication

Date: July 2, 2022

Dear Colleague,

Thank you very much for your contribution to Scientific & Academic Publishing.

We are pleased to inform you that your paper has been published online.

Paper ID:	108100217
Paper Title:	Cyberphysical Security Analysis of Digital Control Systems in Hydro Electric Power Grid
Authored by	Lukumba Phiri, Simon Tembo

It is published in *Computer Science and Engineering (Volume 12, Number 1, 2022).*

We look forward to your continued support.

Thank you again.

Sincerely yours,

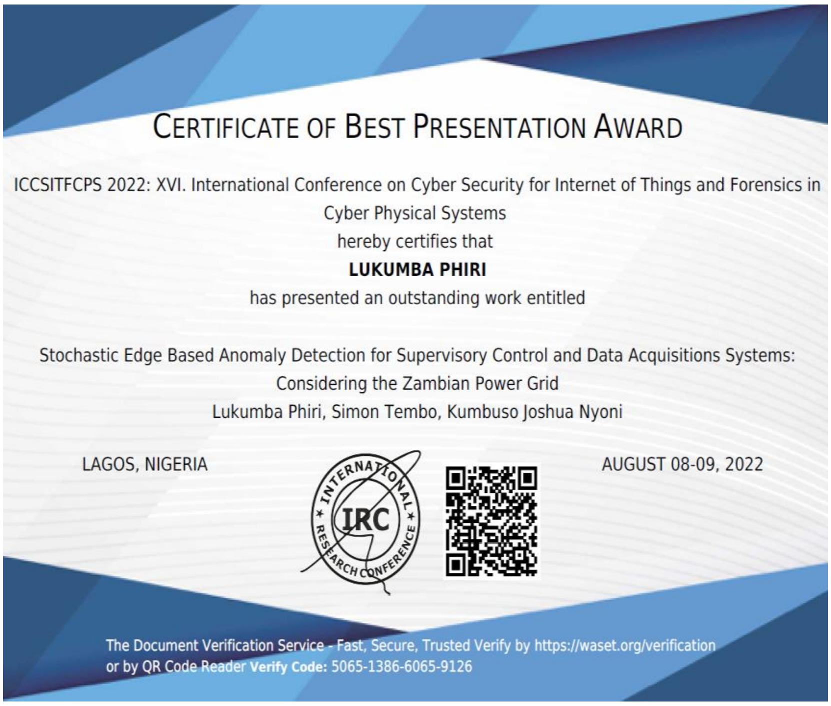
Charles Duke

Journal manager

SCIENTIFIC & ACADEMIC PUBLISHING CO. LTD CORPORATE SEAL USA CALIFORNIA

Scientific & Academic Publishing (http://www.sapub.org/), USA

Cyber-Physical Security Analysis



CERTIFICATE OF BEST PRESENTATION AWARD

ICCSITFCPS 2022: XVI. International Conference on Cyber Security for Internet of Things and Forensics in Cyber Physical Systems

hereby certifies that

LUKUMBA PHIRI

has presented an outstanding work entitled

Stochastic Edge Based Anomaly Detection for Supervisory Control and Data Acquisitions Systems: Considering the Zambian Power Grid

Lukumba Phiri, Simon Tembo, Kumbuso Joshua Nyoni

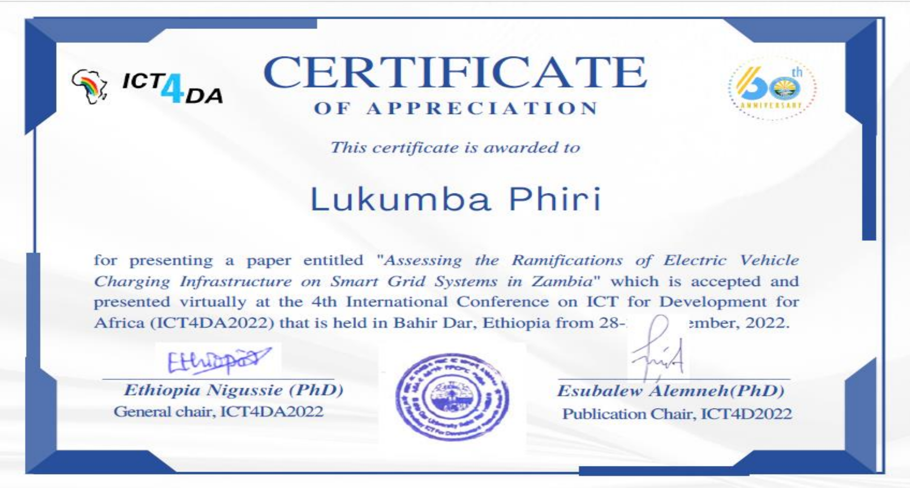
LAGOS, NIGERIA

AUGUST 08-09, 2022

INTERNATIONAL RESEARCH CONFERENCE IRC

The Document Verification Service - Fast, Secure, Trusted Verify by https://waset.org/verification
or by QR Code Reader **Verify Code:** 5065-1386-6065-9126

SEADS



ICT4DA

CERTIFICATE

OF APPRECIATION

This certificate is awarded to

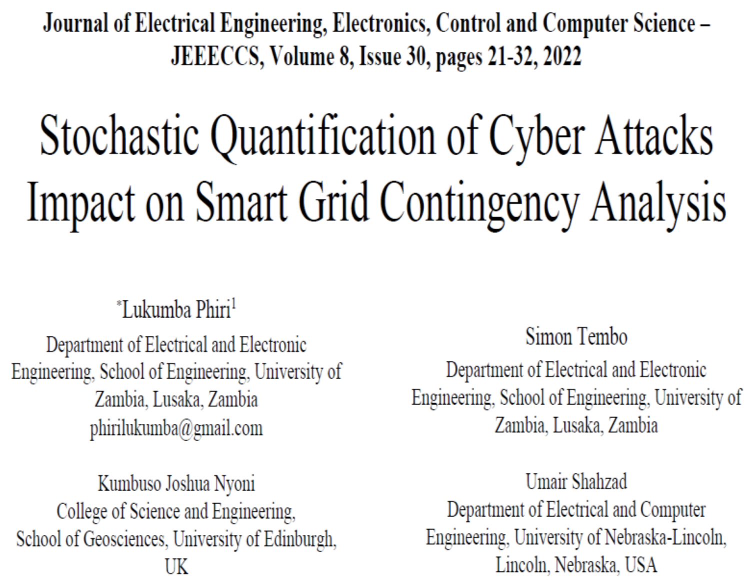
Lukumba Phiri

for presenting a paper entitled "*Assessing the Ramifications of Electric Vehicle Charging Infrastructure on Smart Grid Systems in Zambia*" which is accepted and presented virtually at the 4th International Conference on ICT for Development for Africa (ICT4DA2022) that is held in Bahir Dar, Ethiopia from 28-[illegible]ember, 2022.

Ethiopia Nigussie (PhD)
General chair, ICT4DA2022

Esubalew Alemneh(PhD)
Publication Chair, ICT4D2022

Impact of EVs



Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 8, Issue 30, pages 21-32, 2022

Stochastic Quantification of Cyber Attacks Impact on Smart Grid Contingency Analysis

*Lukumba Phiri[1]
Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia
phirilukumba@gmail.com

Simon Tembo
Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia

Kumbuso Joshua Nyoni
College of Science and Engineering, School of Geosciences, University of Edinburgh, UK

Umair Shahzad
Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, Nebraska, USA

Stochastic Quantification of cyber Attacks