AUTOMATIC POWER MANAGEMENT SYSTEM FOR CYBER SECURITY-ENABLED NAVAL SHIP

A Project Report

submitted by

KUSH NARAYAN NAGAR

in partial fulfillment of the requirements
for the award of the degree of

MASTER OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS

JUNE 2022

QUOTATIONS

Electric power is everywhere present in unlimited quantities and can drive the world's machinery without the need of coal, oil, gas or any other of the common fuels.

NIKOLA TESLA

DEDICATION

To my beloved Snigdha Nagar, R.S Nagar and Lina Nagar

CERTIFICATE

This is to certify that the project report titled AUTOMATIC POWER MANAGEMENT SYSTEM FOR CYBER SECURITY-ENABLED NAVAL SHIP, submitted by **KUSH NARAYAN NAGAR**, to the Indian Institute of Technology Madras, for theaward of the degree of **Master of Technology**, is a bonafide record of the research work done by him under my supervision. The contents of this project report, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Place: Chennai

Date: June 2022

Prof. K. S. Swarup
Project Guide Professor
Dept. of Electrical Engineering
IIT Madras, 600 036

ACKNOWLEDGEMENTS

First and foremost, I would like to thank God for his showers of blessings and for helping me overcome the stumbling obstacles.

The completion of my work would not have been possible without the excellent guidance, expertise, and motivating support of my guide, **Prof. K S Swarup,** and no amount of gratitude and thanks would be enough. I consider myself fortunate and privileged to work under his supervision and his overwhelming helping temperament has helped me complete my work in time. I would also like to thank **Prof. Krishna, Prof. Mahesh & Prof. Sarathy** for sharing their valuable knowledge and answering all my questions throughout the course of my studies.

I thank Lt Cdr Lav Shanker and Capt. R Subramanian for offering technical support to the extent possible by clarifying my doubts regarding the existing setup.

My appreciation also extends to my lab colleagues, Amulya and Pallav, for mentoring, motivating, and enlivening the lab with humor.

I also take this opportunity to thank my wife, Snigdha, for encouraging me during tough times. I wouldn't have achieved anything without her constant motivation and support.

Last, but not least, I would like to thank all the professors of the institute for helping me elevate my knowledge to what it is now. I consider myself lucky to have utilized their wisdom and knowledge.

ABSTRACT

KEYWORDS: Cyber-Enabled Ship; Cyber-Physical Systems; Secure Tropos; Automatic Power Management System; False Data Injection Attack; Single Spectral Analysis; Raspberry Pi 3B; SIMULINK.

The cyber-enabled ship (C-ES) is a self-contained or remotely controlled vessel that operates via interconnected cyber-physical systems. Cyber-attacks are not adequately secured on such systems. Given the importance of the functions provided by such systems, it is necessary to address their security concerns in order to ensure the ship's safe trip. We use the marine reference architecture to examine and explain the C-ES environment in this report. The Secure Tropos technique is then used to systematically elicit the security requirements of the most susceptible cyber-physical systems (CPSs) onboard a C-ES, specifically the Automatic Power Management System (APMS). As a result, a set of cyber-security standards for the C-ES ecosystem in general, and these systems in particular, has been developed. We created the same system on the MATLAB Simulink platform for the Experimental Validation after achieving the Sectro Model for Automatic Power Management System. This Simulink APMS Model was evaluated under a variety of settings, including no cyberattack and cyberattack, in order to determine the system's accurate behavior in real-world scenarios. To make the system more realistic, a cyberattack called False Data Injection was used. Single Spectral Analysis was used to construct a detection algorithm to detect this cyberattack. The Algorithm was proven to be quite effective and capable of detecting the FDIA Attack. A Hardware was constructed utilizing the Raspberry Pi 3B for easy use and practical implementation of this Algorithm. The algorithm was written in Python code and then implemented in hardware. One Raspberry Pi was coded to serve as a ship, and another was coded to operate as a shore control center, to match the practical scenario. It was discovered that the hardware was fully functional in detecting the cyberattack. As soon as a cyberattack is detected, a red alarm LED will illuminate, alerting the entire system. The system was tested in a variety of scenarios.

TABLE OF CONTENTS

Table of Contents (continued) **Page**

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

ABBREVIATIONS

CES	Cyber Enabled Ship
CPS	Cyber Physical System
APMS	Automatic Power management System
SECTRO	Secure Tropos
SSA	Single Spectral Analysis
HDBSCAN	Hierarchical Density Based Spatial clustering of Application with Noise
SVD	Singular Value Decomposition
FDIA	False Data Injection Attack
IMO	International Maritime Organization
IPMS	Integrated Platform Management System
DA	Diesel Alternator
GTG	Gas Turbine Generator
IEEE	Institute of Electrical and Electronics Engineers
SCC	Shore Control Centre

NOTATION

English Symbols

ΔV	Voltage Variations
ΔV_{PSS}	Voltage variations in Power system stabilizer
$\Delta\omega$	Rotor Speed
Δf	Frequency deviation
ΔPe	Active Power deviation
R_L	Euclidean Space
U_1	Eigen Vectors
C_{OV}	Covariance matrix
P	Projection Matrix
Ss	Signal Subspace
c	Centroid
Z_J	Lagged Vector
D_J	Distance
T	Threshold

CHAPTER 1

INTRODUCTION

The cyber-enabled ship (C-ES) is a self-contained or remotely controlled vessel that operates via interconnected cyber-physical systems. Cyber-attacks are not adequately secured on such systems. Given the importance of the functions provided by such systems, it is necessary to address their security concerns in order to ensure the ship's safe trip. We use the marine reference architecture to examine and explain the C-ES environment in this report. The Secure Tropos technique is then used to systematically elicit the security requirements of the most susceptible cyber-physical systems (CPSs) onboard a C-ES, specifically the Automatic Power Management System (APMS). As a result, a set of cyber-security standards for the C-ES ecosystem in general, and these systems in particular, has been developed.

We created the same system on the MATLAB Simulink platform for the Experimental Validation after achieving the Sectro Model for Automatic Power Management System. This Simulink APMS Model was evaluated under a variety of settings, including no cyberattack and cyberattack, in order to determine the system's accurate behavior in real-world scenarios. To make the system more realistic, a cyberattack called False Data Injection was used. Single Spectral Analysis was used to construct a detection algorithm to detect this cyberattack. The Algorithm was proven to be quite effective and capable of detecting the FDIA Attack. A Hardware was constructed utilizing the Raspberry Pi 3B for easy use and practical implementation of this Algorithm. The algorithm was written in Python code and then implemented in hardware. One Raspberry Pi was coded to serve as a ship, and another was coded to operate as a shore control center, to match the practical scenario. It was discovered that the hardware was fully functional in detecting the cyberattack. As soon as a cyberattack is detected, a red alarm LED will illuminate, alerting the entire system. The system was tested in a variety of scenarios.

Defense in Depth Mechanism: We first built a model for the security requirements of APMS in the Defense in Depth Mechanism. Even after establishing the model and determining the precise security needs, the system can still be attacked or hacked by hackers, posing a cyber-security risk. To address this, a detection method based on the single spectrum analysis approach was created and applied in the system to defend it against cyberattacks. The Defense in Depth Mechanism, which we have implemented in our work, provides this level of security.

1.1 LITERATURE REVIEW

In 2016, the phrase Shipping 4.0 was established to characterize new improvements in the digitalization of shipping in order to parallel comparable developments in the land-based economy, which is known as Industry 4.0[1].

Despite the fact that practically all ships are now automated in some fashion, the shipping industry is moving closer to Industry 4.0 with the introduction of crewless vessels[2]. The term "cyber-enabled ship" refers to both remotely piloted and autonomous ships (C-ES).

The C-ES is a cyber-physical ecosystem made up of the vessel, a shore control centre (SCC) that controls and manages the C-ES, communication links between the vessel and the SCC, and other ships in the area. The C-ES ecosystem includes both information technology (IT) and operational technology (OT) systems, both of which are critical to the vessel's secure and safeoperation.

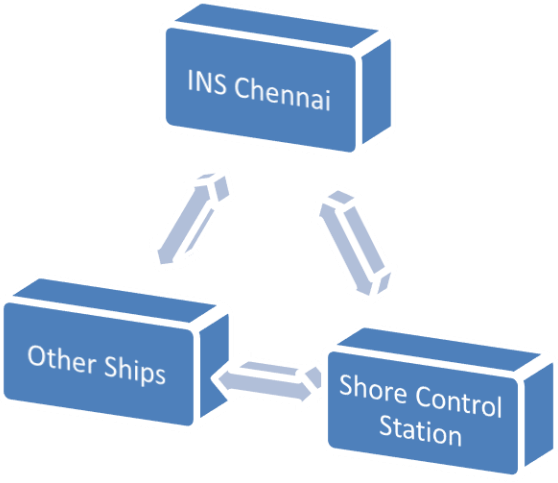

Fig 1.1 Basic Block Diagram of the Cyber-Enabled System

The integration of IT and OT, which is a critical part of the digital transformation process in every application domain, invariably leads to an expansion and diversification of the domain's

cyber hazards, with old risks becoming more severe and new risks emerging. This is due to the fact that, whilst conventional operations were not designed with cyber-security in mind, modern IT-enabled operations are permitted to be accessed and managed by information systems connected to the internet, using interfaces that are rarely fully secure.

The shipping business, in especially the C-ES, is no exception. Although the majority of the C-ES cyber-physical system (CPS) systems are found on today's traditional ships, their exposure to modern technologies aimed at being controlled and monitored remotely expands the attack surface and makes them more vulnerable to cyberattacks. Indeed, studies of the cyber-security concerns posed by autonomous and unmanned vessels [3], [4] have indicated a larger attack surface and more vulnerable systems. Ship-side cyber-security incidents, such as those documented in [5]– [7], have already been made conceivable by this expanded attack surface. The promotion of cyber-security and the safety of the C-ES ecosystem is very important [9] in view of these findings, the rising financial importance of the sector [8], and the multiplicity of possible attackers, particularly those with advanced skills.

It is vital to develop a security architecture in order to improve the ecosystem's cyber-security posture. Given the high complexity of the C-ES ecosystem, as well as the complex interconnections, dependencies, and interdependencies among its constituent CPSs, it follows that establishing cyber-security requirements for the ecosystem as a whole, as well as each CPS in the ecosystem, requires a systematic approach.

We initially suggest a security requirements elicitation process for the C-ES ecosystem in this work. To generate such requirements, an architectural framework must be linked with a mechanism for eliciting security requirements.

Important factors for implementing the procedure were identified as the Secure Tropos methodology [10] and the maritime architectural framework (MAF) reference architecture [11]. The Automatic Power Management System (APMS) was determined as the most vulnerable onboard system of the C-ES based on a threat analysis of onboard systems of the C-ES [3], a risk assessment of such systems [4], and the known vulnerabilities of such systems [12]. The technique is then applied to the C-ES ecosystem in general, and in particular to these systems. The result is a set of cyber-security standards for these systems that have been validated using the criteria outlined in [13].

1.2 MOTIVATION

After reading the full literature study and numerous research articles, I discovered that very little work had been done on the Cyber Security of an Automatic Power Management System installed onboard a Cyber-Enabled Ship. Working on this system in my previous job provided me with a tremendous amount of motivation to work on this topic. With the number of cyber-crimes increasing on a daily basis, it is critical to analyse this system for cyber dangers. These systems are extremely vulnerable to these threats since they have been in place since before the cyber cyber-Enabled-Era. I used this as an opportunity to thoroughly analyze and research this system in order to identify any loopholes that hackers could exploit. The APMS system is extremely important onboard ships because it is responsible for the entire power generation and control. If the Hackers succeed in breaking into this system, the entire ship will become non-operational. To avert such a dire situation, I used my M-tech project work to find solutions for this system that would protect it from cyber-attacks.

1.3 OBJECTIVES

The proposed project is expected to Analyze the Automatic Power Management System & find the shortfalls in cybersecurity. Following are the objectives of the proposed project,

(a) Development (Software) of an Automatic Power Management System (APMS) for shipboard power systems.

(b) Development (Hardware) of Cyber-physical system security (CPSS) for APMS and shore control center (SCC) for cyber-enabled Naval Ships.

1.4 ORGANIZATION OF THESIS

Chapter 2. provides a general overview of the Security Requirements Model's methodology. It also goes into how the Sec-Tro Tool works. It provides an overview of the APMS system's environment while taking into account various constraints. It provides an overview of the elicitation of security requirements.

Chapter 3. shows how the Sec-Tro Model of Automatic Power Management System works. The results of applying the technique to the C-ES example are shown, with a focus on the cyber security requirements for the most vulnerable Automatic Power Management system.

Chapter 4 deals with the experimental examination of the Shipboard Power System design in Mat-lab Simulink. It begins by discussing the APMS and describing the shipboard model. It also mentions the system's frequency and voltage control. It presents a quick overview of the frequency sensor and communication channel control system model. The False data injection attack is also discussed.

Chapter 5 APMS and Shore control station cyber-physical system security is discussed. It also discusses the Single Spectral Analysis, which is used to detect cyber-attacks. It demonstrates how an algorithm was created to identify a False data injection attack. It contains the Simulation and Detection Algorithm results.

Chapter 6 The Hardware Implementation of the Algorithm is discussed. It provides a fundamental overview of the Raspberry Pi. It demonstrates its benefits over its competitors. The algorithm is written in the Python programming language. Following the testing of the hardware, the results are presented.

Chapter 7 The results of the Simulink model and the hardware prototype are shown. It goes into great detail about the findings.

Chapter 8 summarizes the project work by listing the benefits of the proposed system as well as the project's future scope, followed by references.

CHAPTER 2

SHIPBOARD POWER SYSTEM

2.1 RELATED WORK

The autonomous vessels' security requirements have only been evaluated infrequently and in a non-systematic manner. [14] examined the technical and non-technical communication needs for an autonomous merchant ship. The security needs for such communications systems, on the other hand, were not taken into account. The data requirements for autonomous ship wireless communication were identified in [15]. Bureau Veritas [16] stated the functional needs of the autonomous ship's six primary systems, but did not go into detail into the security requirements.

[17] describes the security standards for the components of a vessel's control system. Only conventional boats are studied in Ref. [17], which gives a detailed study of the cyber-security requirements as they originate from applicable standards. The security requirements of marine navigation and radio communication equipment and systems onboard conventional ships are described in the IEC 61162-460 standard [18].

To our knowledge, no previous work has used a systematic approach to address the problem of determining the security requirements of the Cyber-physical CES's systems. There are many different ways for eliciting security needs, and various studies have compared methodologies, tools, and frameworks for eliciting security requirements [19]–[21]. The majority of studies examine the benefits and drawbacks of the methods under consideration before making a recommendation about their suitability. Several of these, for example, [22], [23], advocate the Secure Tropos technique [10] as having many of the desirable features. In various applications, including industrial IoTs [24], [25], the technique has been utilised to extract security and privacy requirements. In addition, [26] proposes a framework for extracting security, privacy, and safety needs for connected automobiles that integrates EBIOS, Secure Tropos, and PriS techniques.

Because no personally identifiable data is involved in the functioning of the CPS systems under consideration, Secure Tropos was chosen as the most suited methodology for the analysis of the complex C-ES ecosystem and the elicitation of its security requirements based on these findings. The MAF [11] is a domain-specific architectural technique created to address the challenge of coordinating the development of new systems in the maritime sector between technology challenges, governance issues, and users across current architectures. The MAF is based on the smart grid architecture model (SGAM) [27], a well-established architecture model in the energy area. The multidimensional cube, which integrates numerous viewpoints to produce a graphical representation of the under-lying maritime environment and the analyzed system architecture, is the MAF's most important component. The cube has three dimensions: interoperability, hierarchical structure, and topological structure.

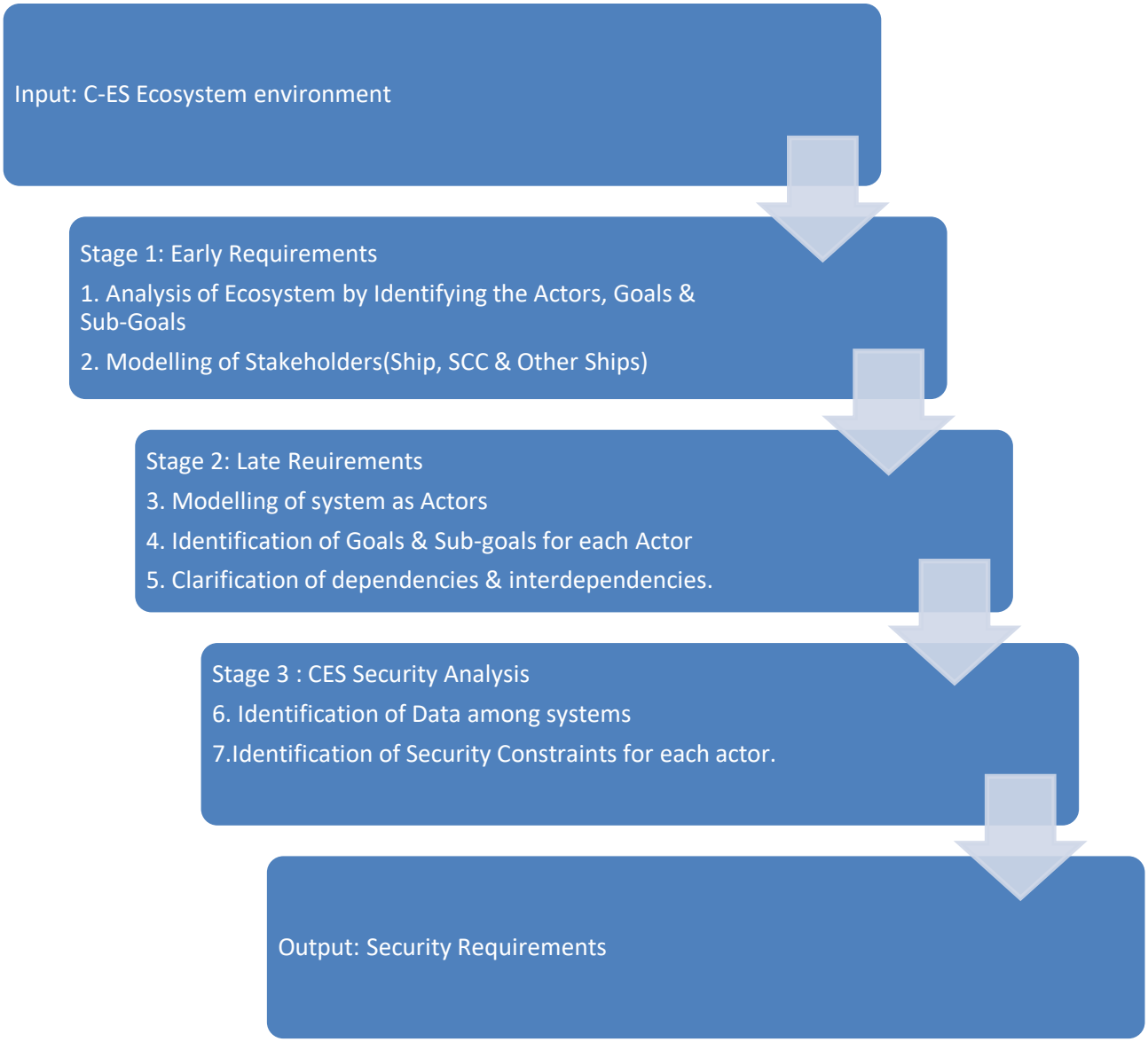

Fig. 2.1 Security requirements elicitation process.

2.2 SECURITY REQUIREMENTS ELICITATION PROCESS

Figure 2.1 depicts the proposed process for eliciting security needs for the C-ES. The C-ES ecosystem's participants, goals, assets, and resources are identified at the first stage, dubbed "Early needs." An actor diagram and multiple goal diagrams are the results of this phase. The actor diagram of the early needs is extended in the next stage, named "late requirements," with the introduction of the system as an actor with various dependencies on the other actors. The system's functional and non-functional requirements will be these dependencies. The global architecture of the C-ES, as well as security limitations, are created in the third stage, dubbed "security analysis," based on system requirements and data and control flows among actors. The security requirements are the result of the overall procedure.

This procedure is carried out using the Secure Tropos approach, which was created as a security-aware software development methodology that blends requirements engineering terms like "actor," "goal," and "plan" with security engineering concepts like "threat," and "security constraint." This method can visually express different ecosystem components, dependencies, interdependencies, links, and interconnections among systems, as well as security-related arguments including security limitations, threats, vulnerabilities, and countermeasures. The SecTro tool aids in the application of the technique.

The Sectro Tool performs three types of analysis for the Automatic Power Management system: environmental, organizational, and security requirements.

2.3 ANALYSIS

2.3.1 ENVIRONMENTAL ANALYSIS

The analysis of the system under investigation's surroundings is the initial phase in the procedure. We use the MAF to accomplish this. This paradigm allows for a structured representation of the marine domain in terms of ecosystem aspects like information assets, people, and technology. The MAF multidimensional cube is used to represent the environment, with three layers depicted: the C-ES, the SCC, and the communication link between them and the ecosystem's parts.

The CES environment is essentially made up of the players in a ship's ecosystem, goals, and interdependencies between actors and goals.

The most appropriate definition of security needs is requirements for the operational and environmental restrictions of the system under investigation. As a result, a detailed identification of such restrictions is an important part of the elicitation process for security needs. Environmental restrictions are inextricably tied to the operational constraints of the C-ES, as they limit the ship's numerous aims and plans, which might be exploited by attackers, posing security concerns.

Because the SCC is such an important aspect of the C-ES ecosystem, environmental restrictions for it should be addressed as well. Table I depicts and briefly describes the identified environmental restrictions for the C-ES, while Table II depicts and briefly describes those for the SCC.

TABLE I C-ES ENVIRONMENTAL CONSTRAINTS

Constraint	**Description**
Weather Conditions	Heavy weather conditions, such as strong winds and dense fog, obstruct visibility.
Communication	Support a Multitude of Communication Technologies
Cyber Attacks	Because the C-ES is made up of cyber-physical systems, it is vulnerable to physical and cyber-attacks.
Human Factors	Ensure people's safety and deal with unexpected events.
Harbors	Navigation is different harbors when they are controlled by other Authorities

Table 2.1 CES Environmental Constraints

TABLE II SCC ENVIRONMENTAL CONSTRAINTS

Constraint	Description
Weather Conditions	Harsh weather may create malfunctions in the SCC Building's external sensors or antennae, affecting the delay.
Communication	The C-ES may be disrupted if a communication link is lost or if the satellite provider fails.
Geographic	The SCC's location is critical for smooth communication with both the vessel and the Ships Company.
Cyber Attacks	Cyber and physical systems make up the SCC.
Multi-Role Environment	The SCC is a place where people of various professional backgrounds and roles coexist.

Table 2.2 SCC Environmental Constraints

2.3.2 ORGANIZATIONAL ANALYSIS

The organizational study of the ecosystem and its constituents is comprised of Stages 1 and 2 of the security needs elicitation process. As shown in Fig. 1, this is accomplished by following Steps 1.1 through 2.3. The analysis is conducted for both the ecosystem as a whole and one of the particular systems under consideration, the APMS.

(a) **APMS Ecosystem Analysis**: In this analysis the whole Ecosystem is considered and Analyzed. We Get a Full Ecosystem Diagram.

(b) **APMS System Analysis**: In this the whole APMS System is Analyzed & we get an APMS Sec-Tro Model with Security Constraints.

2.3.3 SECURITY REQUIREMENTS ANALYSIS

The C-ES system's general design is illustrated in Fig. 3.2 as an organisational view of the ecosystem. The data and control flows are identified based on the functionality and technical aspects of the system under investigation, as needed in Step 3.1 of the security needs elicitation process.

Step 3.2 necessitates the identification of each actor's security limitations. In our situation, these limitations are the Parkerian Hexad's elements, i.e.,

(a) Integrity – completeness, wholeness, and readability of information are defined as completeness, wholeness, and readability of information are unchanged from a prior state
(b) Availability – Usability of information for a specific purpose is defined as
(c) Possession – Having the ability to hold, control, and utilize information is described as having the ability to hold, control, and use information.
(d) Authenticity – Validity, conformity, and genuineness of information are all terms that can be used to describe the quality of information.

Fig. 2.2. APMS Perkian Hexad Model.

The security constraints in the systems diagram are the security requirements of the targeted system when employing the Secure Tropos technique. The system goals, as well as the processes and resources used to attain them, are identified as a result of the defined system functional and operational requirements. The Parkerian hexad is used to identify the security limitations that will secure the defined processes and goals. Here's an example of how to do it. Two security requirements have been identified: continuous connectivity between the system and external actors, as well as between onboard systems, and the transmission of Power Generation-related data to the SCC must be safeguarded against tampering or damage. Using the Secure Tropos technique, we first examine the target system's environment and define its operational and functional requirements, which include informing SCC about vessel power generation and sending power generation data to SCC, respectively. The system's operational and functional

requirements are then determined, together with the goals and sub-goals that must be met.

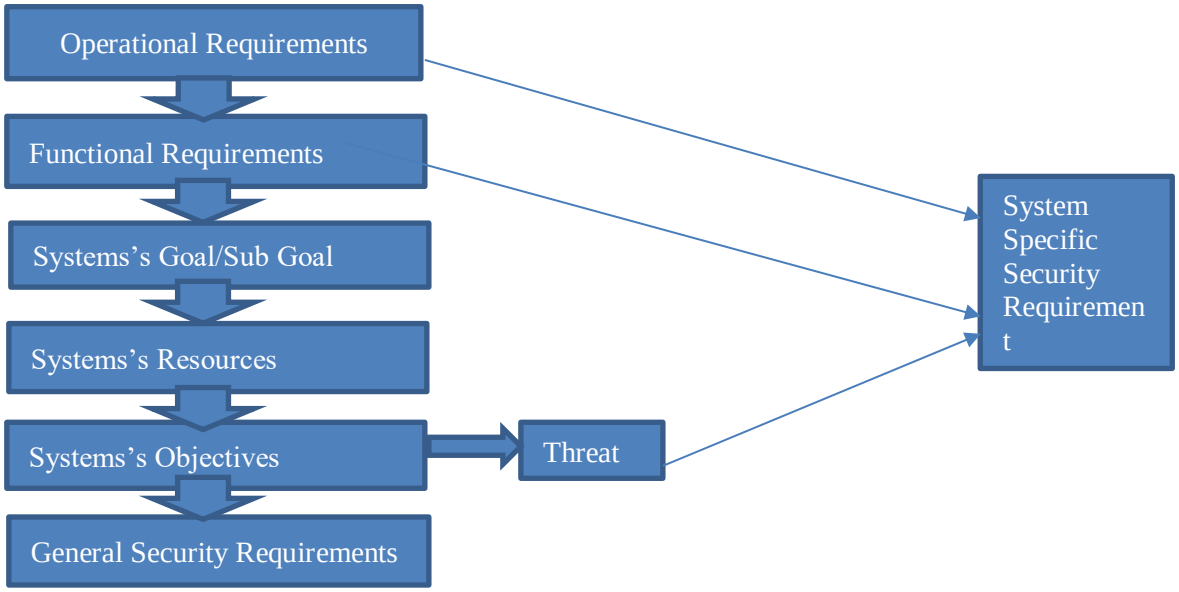

Fig. 2.3 Security requirements elicitation process.

2.4 COMMON SECURITY REQUIREMENTS

Human resource security: The system administrator must be well-versed in both functional and non-functional requirements of the system (e.g., APMS modes and communication capabilities).

Asset management: i) Data and signals must be identified and categorized according to their level of protection. ii) Third-party component documentation, versioning, and publicly disclosed system vulnerabilities must be maintained;

Access control: i) A strong password policy must be implemented, specifying the duration and lifetime of each credential combination (e.g., passwords to log in to the APMS should be regularly changed); ii) With suitable authentication procedures, nonrepudiation and traceability of operations conducted either from the SCC or physically to the onboard system must be ensured.; iii) When the system administrator requests it or after a set period of inactivity, the system must be able to implement lock mechanisms.; iv) The number of consecutive system login attempts must be given.; v) Multifactor authentication must be supported by the system.; and vi) Only authorized entities and authorized marine actors are allowed to submit data into the system.

Cryptography: i) During the voyage, the system must enable encryption techniques capable of ensuring data security and integrity, as well as meeting data transfer timing requirements.; ii) Data supplied to external and internal actors should be encrypted using appropriate cryptographic algorithms in each situation [for example, dynamic data passed from Generator to APMS must be encrypted]; iii) The strength of the encryption system should be determined by the type of data being held and the potential relevance of maritime legal or regulatory requirements.

Physical and environmental security: i) The physical integrity of the SCC sensors aboard must be safeguarded.; ii) To avoid physical damages such as floods or fire, the system must be implemented.; and iii) All of the system's physical and virtual connection points must be properly protected or prevented (e.g., USB ports or any other human interface device-HID).

Operations security: i) Both onboard and SCC systems must be able to function in high-stress network scenarios, such as a denial-of-service attack.; ii) To safeguard the system from malicious code, security methods must be developed.; iii) Backups of system data should be performed on a regular basis (e.g., Power generation data should be backed up regularly to the VDR); iv) The system must be able to tell whether an action was conducted by a system onboard or by a human user operating from a distance from the SCC.; v) The integrity of the data, both static and processed, must be safeguarded.; vi) The privacy of data in transit and storage must be safeguarded.; vii) It is necessary to verify that data is current.; vii) It is necessary to secure the validity of services, transmitted data, and software sources (for example, APMS upgrades should only be conducted by approved sources/vendors).; viii) The utility of dynamic and voyage data should be guaranteed, and efforts to protect data confidentiality and integrity should not reduce their utility.

Communication security: i) Depending on the players and the type of data in transit, appropriate procedures should be used to maintain the confidentiality and integrity of data transmitted between internal (onboard systems) and external (SCC or another vessel) actors.; ii) It is necessary to guarantee that the onboard components are separated into distinct trust levels.; iii) It's crucial to make sure that the onboard components are divided into different trust levels.; iv) Mutual authentication of onboard systems is required.; v) The system's traffic from and to must be monitored.; vi) Considering the actor and the type of data in transit, the systems should be able to manage the data sent.; vii) The source of data flows emanating from the onboard systems must be determined by all external actors in the C-ES ecosystem.; viii) The data exchange between

onboard systems should be set up in such a way that the legitimacy of the data can be checked.; ix) To protect data in transit, the systems must use transport-layer security.; x) Mechanisms to detect malicious data packets should be included in the system.; xi) The authentication of services between onboard systems and external actors (SCC/another vessel) is required.; xii) Communication channels between onboard systems should be redundant.; and xiii) The maximum permissible delay in system-to-system communication should be in accordance with relevant standards and the operating needs of the systems.

System acquisition, development, and maintenance: i) System development and deployment must adhere to relevant cyber-security guidelines.; ii) Time-of-check vs. time-of-use attacks must be avoided during the update process.; iii) Authentication of the software's source is required.; iv) Regular maintenance is required for both aboard and shore-based devices.; v) Both onboard and shore-based equipment require routine maintenance.; vi) Only authorized entities are allowed to make system updates and upgrades.; vii) To prevent malicious intrusions, the integrity of the maintenance process must be assured., viii) Only well-trained employees should do system maintenance.; ix) The system's configuration and installation must be done by authorised individuals.; x) The infrastructure of the ship must be well-designed, with the proper systems installed in accordance with the ship's kind., and xi) Downgrading to older system software versions must be prohibited by the system.

Supplier relationships: i) To validate hardware, software, and data from suppliers, proper techniques must be used.; and ii) A thorough examination of the system's vendor's security rules is required.

Information security incident management: i) The system must recognise and generate an alert when a user or an external actor makes an unusually large number of requests.; ii) During a security issue, such as APMS signal jamming, the system's functional and non-functional needs should be maintained; and iii) When a system abnormality is discovered, the SCC must be contacted.

Information security aspects of business continuity management: i) It is necessary to guarantee that system operations are not disrupted.; ii) The system, whether onboard or on land, must be able to run on alternate power sources.; iii) The system must be able to run 24 hours a day, seven days a week., and iv) The operational complexity of the C-ES and the system

operations should be taken into account while installing redundant systems.

Compliance: i) It is necessary to obtain formal certification of compliance with applicable legal and regulatory standards.

CHAPTER 3

AUTOMATIC POWER MANAGEMENT SYSTEM

3.1 ECOSYSTEM ORGANIZATIONAL ANALYSIS

The ship, the SCC, and other ships are depicted in Fig. 3.1, which illustrates the organizational picture of the C-ES ecosystem. These entities are represented as different organizations by rectangles, according to the Secure Tropos technique. The bridge and the Power Management system have been identified as actors within the ship, and are shown by circles; these interact with external actors like as the SCC's human-machine interface (HMI) and other ships in the area. The limits of actors are represented by dashed rounded rectangles, which contain the actors' goals and sub-goals (represented by rounded rectangles), as well as the resources they need to achieve those goals (represented by rectangles). As shown in Fig. 3.1, the actors are described by their interdependencies and dependencies. It should be emphasized that different types of data are included in the organizational perspective of the ecosystem, depending on the players from whom these data are derived. Bridge systems, for example, share data pertaining to navigation, trip, and safety, whereas Power Management systems interchange data related to Power Generation.

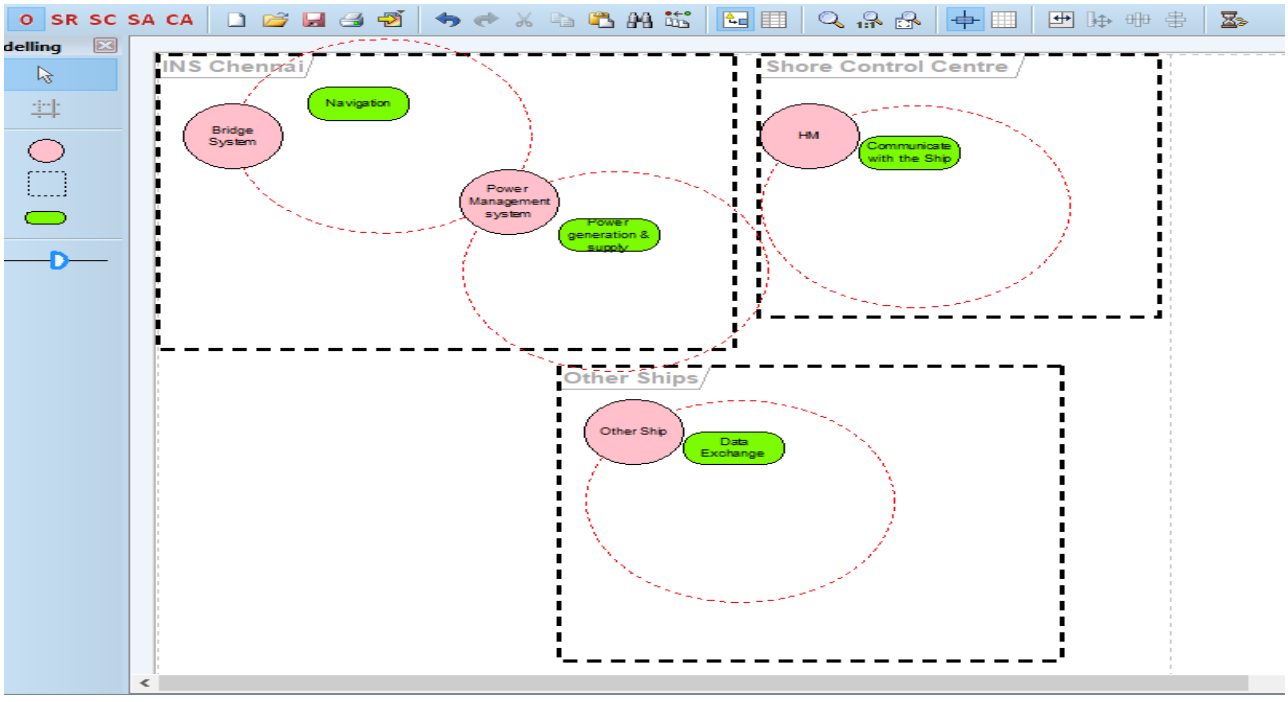

Fig. 3.1 General Ecosystem Organizational Analysis of Cyber-Enabled Ship

3.2 APMS ORGANIZATIONAL ANALYSIS

The APMS gives data on the ship's whole power generation and load, with the goal of ensuring a smooth ship's operation. The APMS communicates with the Bridge as well as two external actors: the SCC and other ships in the area. Depending on the system interconnections and interdependencies, the transmitted data can be static, dynamic, or safety-related, as seen in the APMS's entire organizational perspective.

Interfacing is done within APMS via Modbus communication. The APMS may operate the Alternator and Air Circuit Breakers as well as monitor the Switchboard. Onboard a ship, the APMS performs the following activities.

1. Auto Synchronizing
2. Auto load sharing
3. Governor Control
4. AVR Control
5. Alternator ACB Open/Close.
6. Feeders MCCB Open/Close
7. Voltage Check
8. System status feedback
9. Alarm status feedback

In the event of an emergency, the APMS guarantees that shore authorities are quickly notified. The types of signals and data that are conveyed have been used to describe the goals and sub-goals of each actor, indicating dependencies and interdependencies. The resources required for each player to achieve their objectives are transmitted signals and data. The onboard and onshore systems, the engine and navigation systems, and the SCC are all interconnected by the APMS.

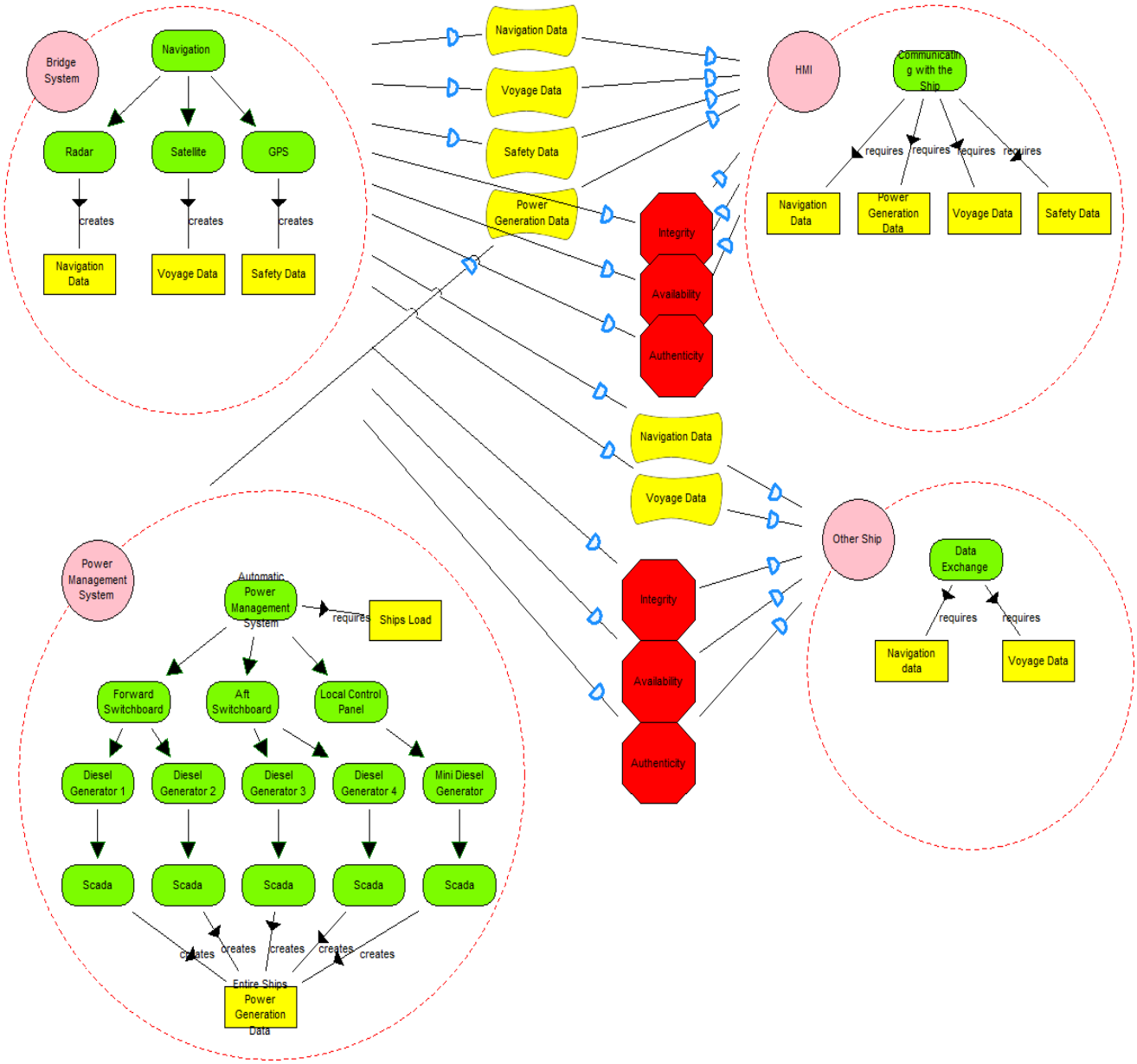

Fig. 3.2 APMS Organizational Analysis

3.3 SECURITY REQUIREMENT ANALYSIS

These tasks include receiving and evaluating data from generators, as well as delivering the evaluated data to SCC. The APMS data is a valuable resource for achieving these objectives. The security limitations are established in order to develop the system-to-be (in this example, a secure APMS system). The security constraints of the interconnections and interdependencies between the APMS and the SCC are identified in this scenario as availability, integrity, and authenticity. Because the security constraint in the systems goal diagram is a security requirement, the

resulting security requirements are as follows: the availability of the transmitted data between APMS and SCC must be ensured, the integrity of the processed and transmitted data must be protected, and the data must be authenticated [28].

A system-specific security requirement is that power generation data transmitted to the SCC be protected against tampering or damage, taking into account the operational and functional requirements of the targeted system and the potential threats to the APMS (denial of service, tampering) that could violate the identified constraints (availability, integrity, and Authenticity). The availability criterion is refined to "the connectivity between the system and external actors and between onboard systems must be continuous," because the protection of the sent data is a common requirement for the system. This need belongs to the first category of requirements (common security requirements). The security requirements are the result of Stage 3 of the security requirements elicitation process, which is directed and assisted by the SecTro tool.

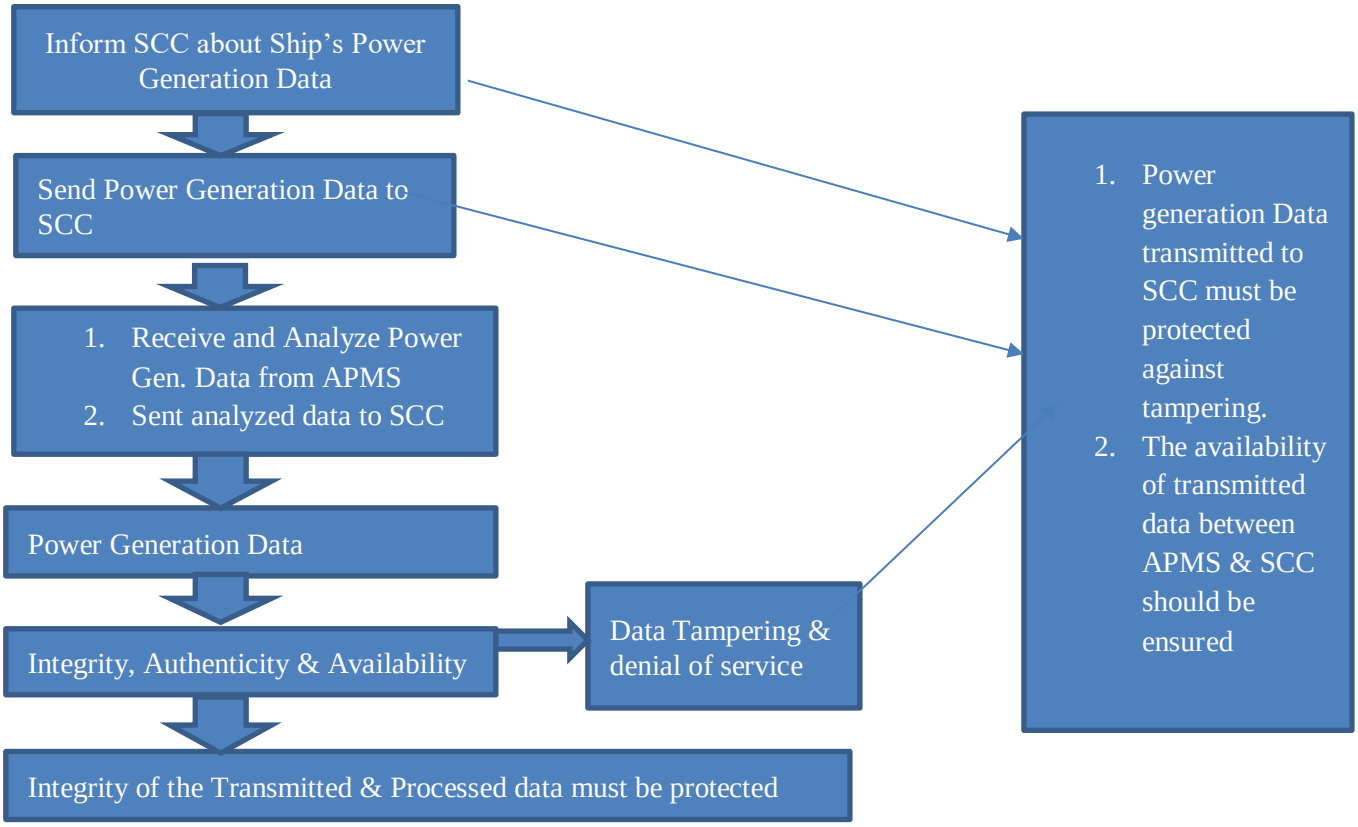

Fig. 3.3 APMS Security requirements elicitation process

The ISO 27 k family of standards, NEC's CIP family of standards, and the ISA IEC IEC-62443 series are among them. Software security requirements standards (such as ECSS-Q-ST-80 C, IEEE 830-1998, ISO/IEC 25010, ISO/IEC 27034-1, and ISO/IEC 27034-3) are also applicable.

Ref. [17] gives a classification of cyber-security requirements in the maritime environment. Because the ultimate purpose of this study is to provide cyber-security criteria for the entire C-ES ecosystem, we've chosen to describe the needs using the ISO 27001-27002 standards, which apply to companies rather than isolated systems, software or otherwise.

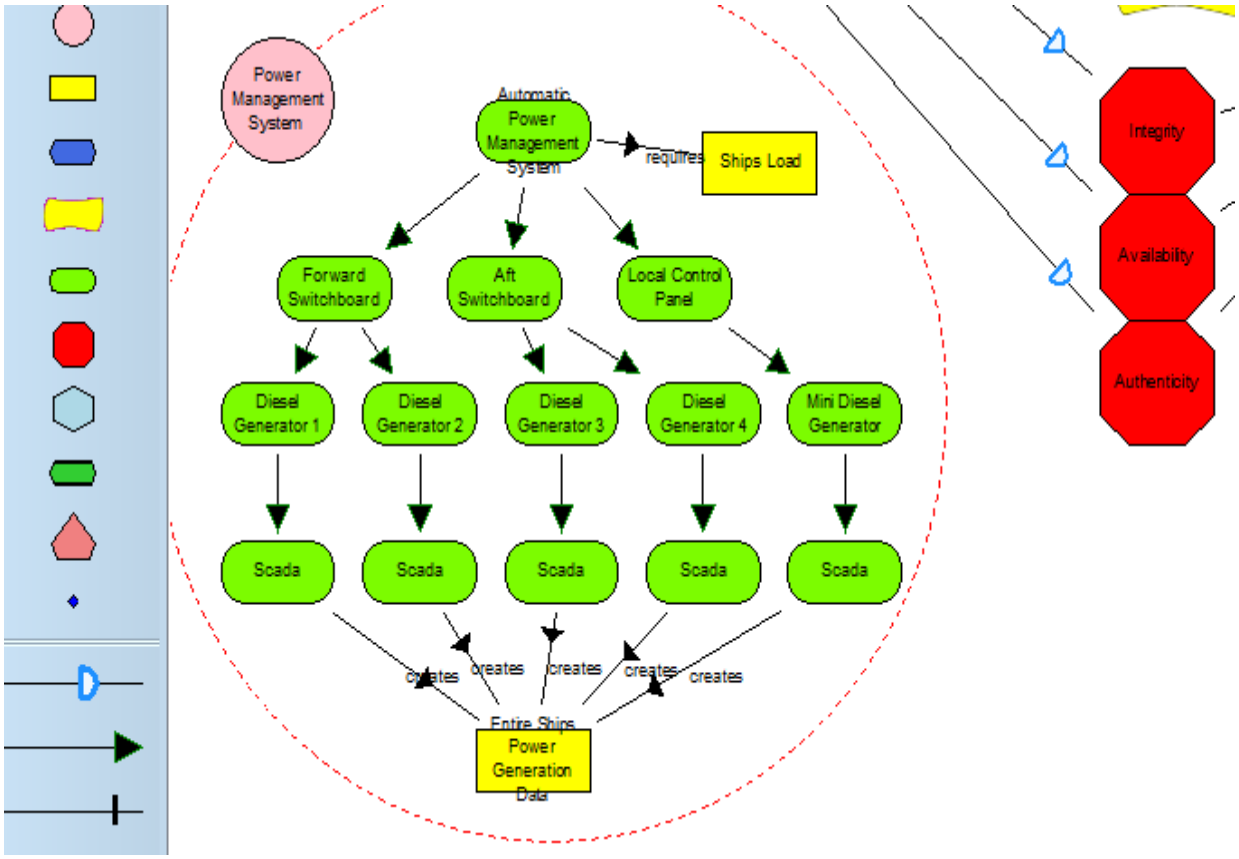

Fig. 3.4 APMS security requirements.

3.4 APMS-SPECIFIC SECURITY REQUIREMENTS: Figure 3.4 depicts a portion of the APMS's security requirements view.

(a) **Operations security:**

(i) To safeguard the system from losing control or custody of information, the APMS should integrate security services.

(ii) Data about power generation should be kept private to avoid any leaking to adversaries.

(b) **Communications security:**

(i) The APMS communication route should be redundant.

(ii) Data linked to power generation that is sent to the SCC must be secured from tampering or damage.

(c) **Access control:**

(i) To uniquely identify the actors accessing, changing, and transferring APMS data, as well as to authenticate the system and its services, effective authentication procedures must be in place.

(ii) The APMS must be able to implement lock mechanisms (e.g., lock the HMI screen) on the administrator's request or after a defined period of inactivity.

(d) **Cryptography:**

(i) Security measures such as digital signatures must be used to assure the legitimacy of APMS functions (e.g., request, read, process, and send).

3.5 SUMMARY

After evaluating the Automatic power management system installed onboard a cyber-enabled ship, we discovered that the three most significant security criteria for this system are Data Availability, Data Integrity, and Data Authenticity. To make the APMS System less exposed to cyber threats, it is critical to protect these security criteria. We will now simulate the ship's power system in MatLab Simulink to conduct the experimental investigation, keeping this concept in mind. The processes to construct the Simulink Model so that we can conduct the Experimental analysis will be covered in the future chapter.

CHAPTER 4

MODELLING APMS & SCC IN SPS

4.1 INTRODUCTION

We used SECTRO Tool to create a model of an Automatic Power Management system after studying the MAF Architecture and the Perkian Hexad. New APMS systems for remotely/autonomously controlled ships can be designed with higher sense of security for cyber security with the help of this Model. We examined how APMS communicates with multiple Power Systems installed onboard and controls them for proper Power Onboard generation in the Model. For the remote-controlled operation, we also saw how this system connects with the Shore Control Station and vice versa.

A shipboard power system consisting of four 1000KW diesel generators with AVR and governors was created and modelled using Matlab Simulink to demonstrate the efficacy of this concept. The Generator's Frequency Data set was deemed the Main Parameter for the detection of the attack throughout Model development.

4.2 SHIPBOARD POWER SYSTEM

A ship's power system network differs from a standard on-shore power network in that it includes dedicated generators and loads that are situated near to each other with short-length feeders. The generated energy is supplied locally to many high-power loads that require a consistent and high-quality supply. A master console or one of the multiple slave controls of an Automatic Power Management System can control the entire power network (APMS). An APMS performs a variety of activities, including automatic starting, paralleling, and loading of DAs, load sharing, and blackout start of DAs. The configuration of a maritime power system generation is depicted in Fig. 4.1.

A synchronous generator, which is operated by a diesel or gas prime mover and is frequently referred to as a Diesel Alternator, is the principal source of power supply onboard (DA). There

are a total of four diesel alternators onboard, each rated at 1000KW or 1MW. They are in charge of catering to all the Loads present onboard a ship. The Automatic Power Management System controls and monitors the whole operation of these generators.

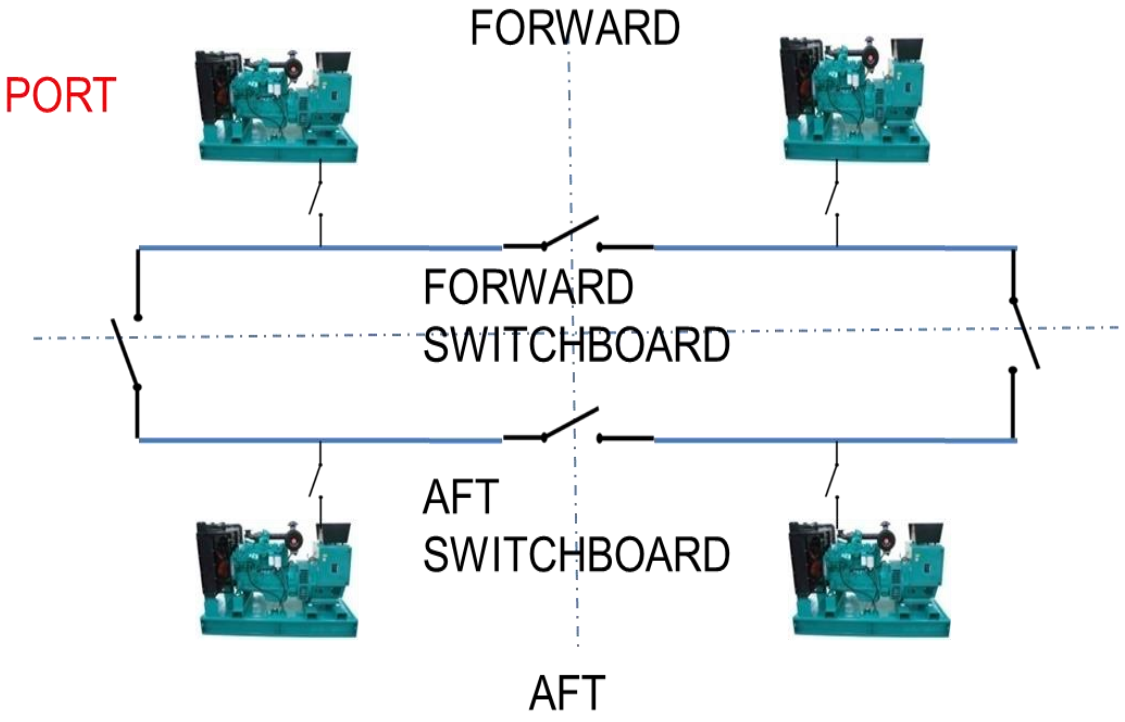

Fig. 4.1: Typical Power System Generation

Because power availability is so important for a marine vehicle, the cumulative MW rating of all the generators will be around double the maximum demand, providing redundancy and enhancing reliability. The generators are distributed throughout a combatant vessel to provide redundant power in the case of a missile or torpedo strike on one section of the ship.

A supply breaker connects each generator to a specific area of the main switchboard, with a bus-coupler breaker linking numerous parts of the same switchboard and inter-connecting breakers connecting separate switchboards. Two or more main switchboards, as well as an isolated emergency switchboard, will be powered by an emergency generator and connected to critical loads such as navigation, communication equipment, steering gear, and so on. There are numerous secondary supplies available in addition to the primary supply, which are generated from the primary supply using rectifiers and/or converters.

Various types of load available onboard the ship are as follows:

(a) Service Loads: AC, Firemain & Lighting etc.

(b) Weapon/Sensor Loads: Radars & Guns

(c) Propulsion Loads: Gas Turbine etc

4.3 VOLTAGE & FREQUENCY CONTROL

Three critical characteristics for power system operation and control are nodal voltage angles (rotor/power angles), nodal voltage magnitudes, and network frequency.

4.3.1 VOLTAGE CONTROL

Small- and large-disturbance stability are two types of angle and voltage stability. Angle and voltage stability refer to the dampening of power swings inside and across subsystems on an interconnected system, as well as voltage excursion beyond set threshold limits [29]. Using proper control devices placed into the power system to find a smooth shape for the system dynamic response can significantly reduce the danger of losing angle and voltage stability. PSS, AVR, and FACTS devices are important control devices for improving stability.

The AVR, which controls the excitation of the machine via the electric field exciter, is commonly used to keep the generators running at a consistent voltage. The exciter generates the appropriate flux in the rotor by supplying direct current to the synchronous machine's field winding. A Power System Stabilizer is a controller that, in addition to the turbine-governing system, conducts a supplemental control loop to a generating unit's AVR system. The extra control loop is required due to the rotor speed and voltage dynamics' conflicting behavior.

ΔV_{PSS} must be equal to zero in the steady-state to avoid distorting the voltage regulation mechanism. However, in the transient condition, the generator speed is not constant, the rotor swings, and V varies due to rotor angle changes [30]. The PSS compensates for this voltage variation by sending a damping signal ΔV_{PSS} in phase with the generator speed change ($\Delta\omega$).

The input signal is routed through a combination of low and high-pass filters in the PSS's general structure. The prepared signal is then transmitted via a lead-lag compensator to achieve the needed amount of phase shift. Finally, the PSS signal is amplified and restricted in order to produce a useful output signal (ΔV_{PSS}). The input signal to the PSS is often the rotor speed/frequency deviation ($\Delta\omega/\Delta f$), the generator active power deviation (ΔPe), or a combination of rotor speed/frequency and active power changes. Advanced measurement instruments and sophisticated

communications are already being installed in advanced power systems used in cyber-enabled ships. The parameters of the PSS and AVR can be modified using these capacities via an online monitoring-based tuning method [31].

Voltage control, like frequency control, is characterized by many control loops at various system levels. The AVR loop, which controls the voltage at generator terminals, is located at a lower system level and normally responds in a second or less. Secondary voltage control, on the other hand, is engaged at a higher system level and operates on a timescale of tens of seconds or minutes, determining the voltage reference values of distributed voltage compensators (e.g., AVR). Secondary voltage control is necessary to coordinate the set point adjustments of AVRs and other reactive power sources in a specific network in order to improve the voltage stability of the Shipboard Power system.

4.3.2 FREQUENCY CONTROL

Frequency deviation is a helpful index to detect generation and load imbalance since it is a direct outcome of an imbalance between the electrical load and the power supplied by the linked generators. By destroying equipment, reducing load performance, and triggering protection devices, a permanent off-normal frequency deviation can have an impact on power system operation, security, reliability, and efficiency.

Because the frequency generated in an electric network is related to the generator's rotation speed, the frequency control problem can be easily transformed into a turbine-generator unit speed control problem. This is originally addressed by the addition of a regulating mechanism (Governor) that detects machine speed and adjusts the input valve to vary the mechanical power output to track load changes and restore frequency to the nominal value of 50Hz. Different frequency control loops may be necessary to ensure power system frequency stability depending on the frequency deviation range [32]. A substantial frequency deviation can harm equipment, reduce load performance, and interfere with system protection measures, resulting in an unstable shipboard power system. Small frequency deviations can be dampened by the principal control in normal operation. The secondary control, known as LFC, is responsible for restoring system frequency for higher frequency deviations (off-normal operation) based on the available quantity of power reserve.

The two major principal objectives of a Shipboard Power System Load Frequency Control are to maintain frequency and power interchanges with other Generators at the scheduled values. These

goals are achieved by measuring a control error signal known as the area control error (ACE), which is a linear mixture of net interchange and frequency variations and represents the real power imbalance between generation and load. The ACE is used to perform an input control signal for a proportional-integral (PI) controller after filtering. Limiters, delays, and gain constants are used to condition the output control signal based on the characteristics of the control region. This control signal is subsequently divided across the LFC participant generator units based on their participation factors, resulting in suitable control commands for specified plant set points. To get optimal LFC performance, tuning the dynamic controller is critical [33].

Due to the growing size, changing structure, and complexity of linked Shipboard power systems, frequency regulation is becoming more important. Increased economic pressures on power system efficiency and reliability have necessitated keeping system frequency as close to scheduled values as practicable. As a result, LFC is critical in providing power exchanges and frequency control in a contemporary shipboard power system.

The primary frequency control loop adjusts the speed governors in seconds following a disturbance to offer local and automatic frequency management. The assigned spinning reserve is engaged in the time span of a few seconds to minutes following a disturbance, and the secondary frequency control loop initiates a centralized and automatic control task employing it.

4.4 SHIPBOARD CONTROL SYSTEM MODEL

We created a Mat-Lab Simulink Model of Shipboard Power System to realize the above ideas of Frequency and Voltage Control. We explored using four 1000KW diesel alternators with automatic voltage regulators and governors. The Generators are connected to the ship's forward and aft switchboards, which provide power to the entire ship's load.

We included a Variable Ships Load in the Model to represent a realistic scenario. After creating the Simulink model, we ran simulations for three different scenarios: no load-no cyberattack, load-no cyberattack, and load-with cyberattack.

For creating the Simulink model of the Power system, refer to the Values in **APPENDIX C**.

4.4.1 SHIPBOARD POWER SYSTEM WITHOUT CYBER-ATTACK

In the Matlab Simulink Model, the Shipboard Power System is illustrated. The Cyber Attack is not taken into account in this scenario. The simulation's results are as follows:

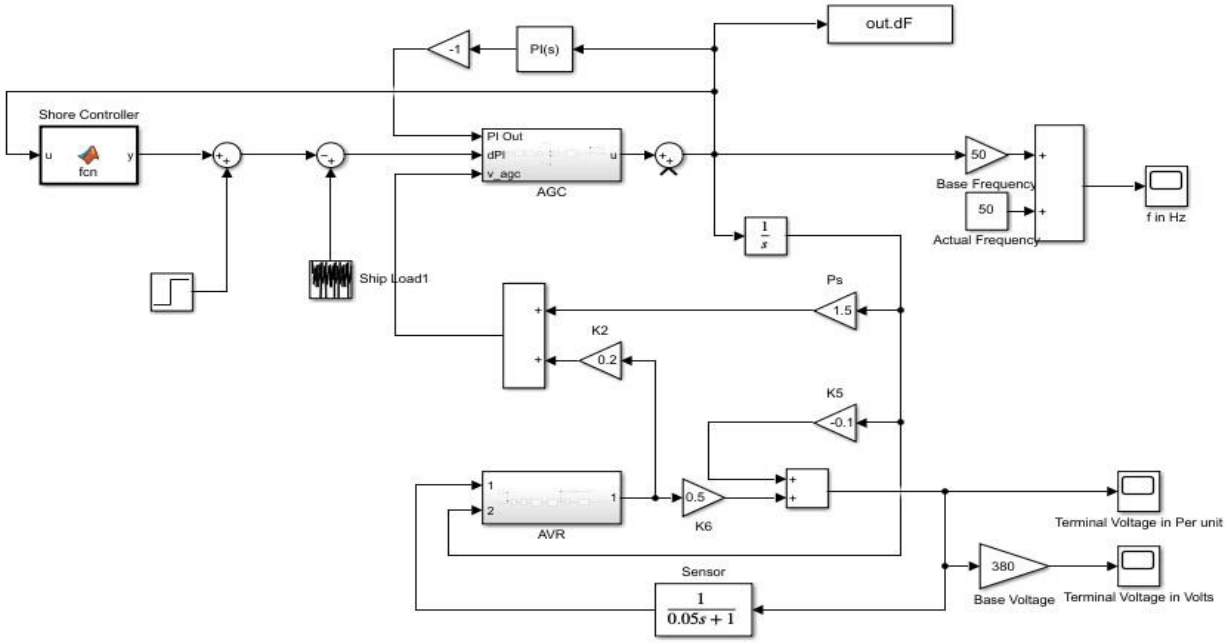

Fig 4.2 Shipboard Power System without Cyber Attack

(a) **Frequency output Without Load & Without Cyber Attack**: In this case, the power system is operating normally with no load. There is no cyber-attack at this time. We can see from the Frequency Waveform that the frequency is stable at 50Hz.

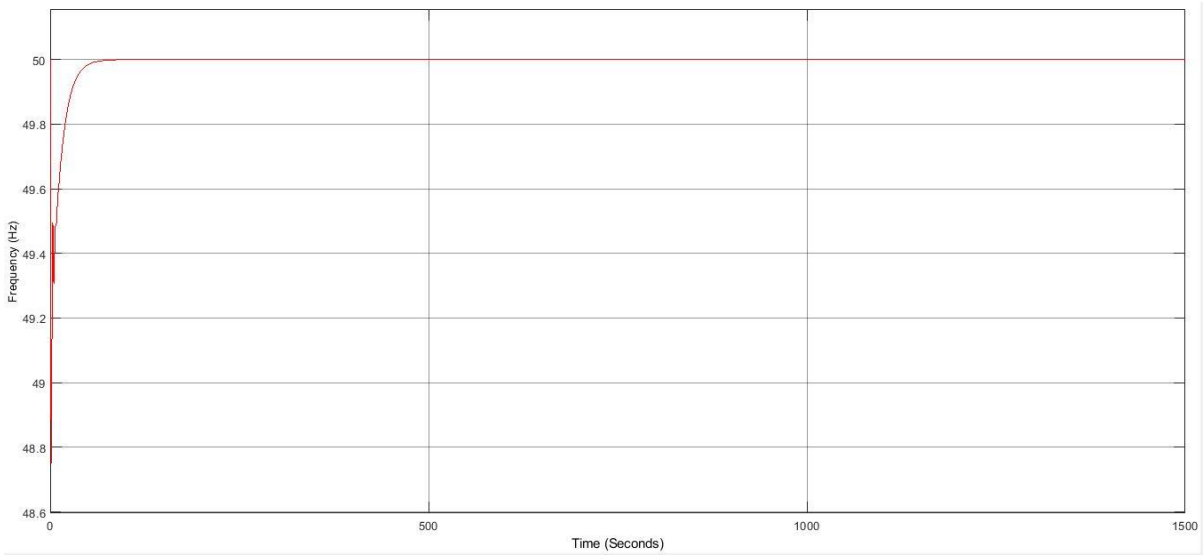

Fig 4.3 Frequency Waveform without Load

(b) **Voltage Output Without Load & Without Cyber Attack**: In this situation, the power system is operating in normal conditions with no load. There is no Cyber-Attack at this time. We can tell that the Voltage Waveform is stable at 380 volts after looking at it.

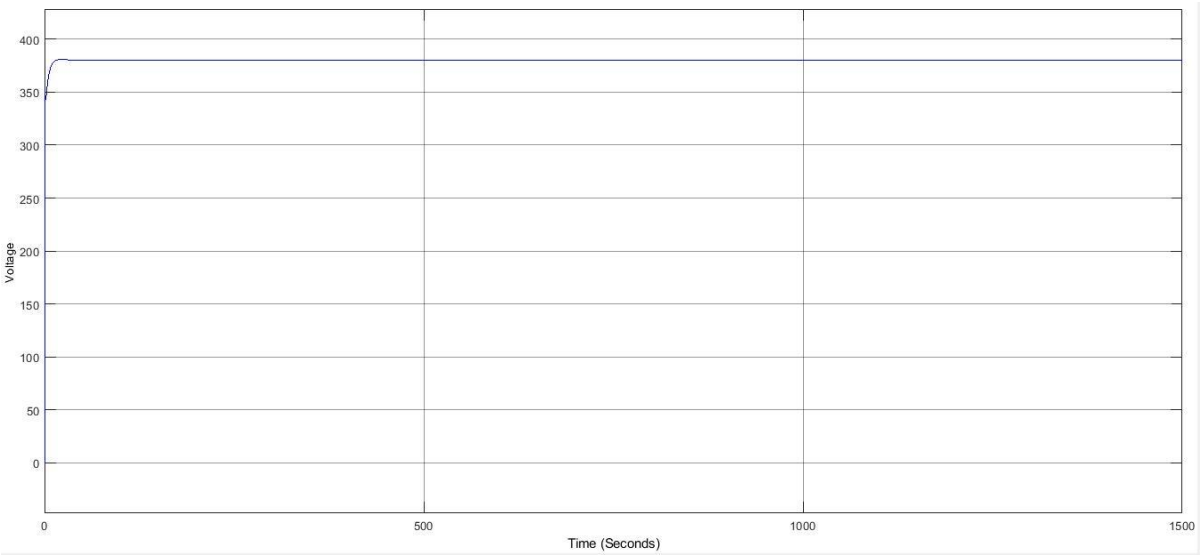

Fig 4.4 Voltage Waveform without Load

(c) **Frequency output with Ships Load & Without Cyber Attack**: In this case, the power system is operating normally with the ship's load. There is no cyber-attack at this time. We can see from the Frequency Waveform that the frequency varies towards 50Hz but stays inside the boundaries.

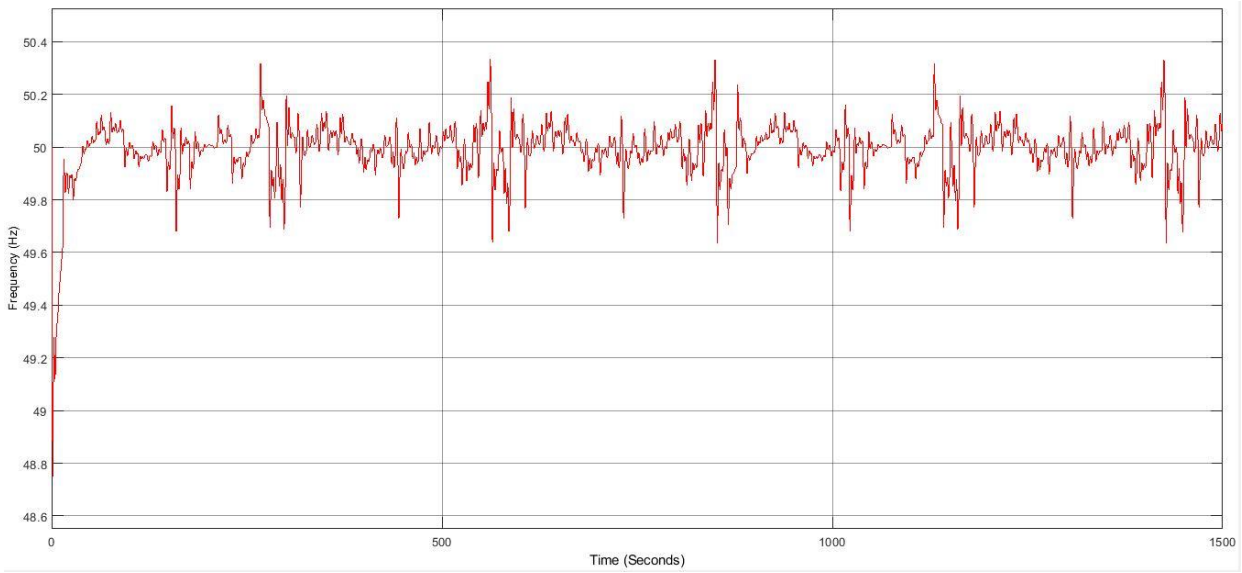

Fig 4.5 Frequency Waveform with Ships Load

(d) **Voltage Output with Ships Load & Without Cyber Attack**: In this situation, the Power System is operating normally at Ships Load. There is no Cyber-Attack at this time. We can see from the Voltage Waveform that it is changing near 380 volts, although it is within limits.

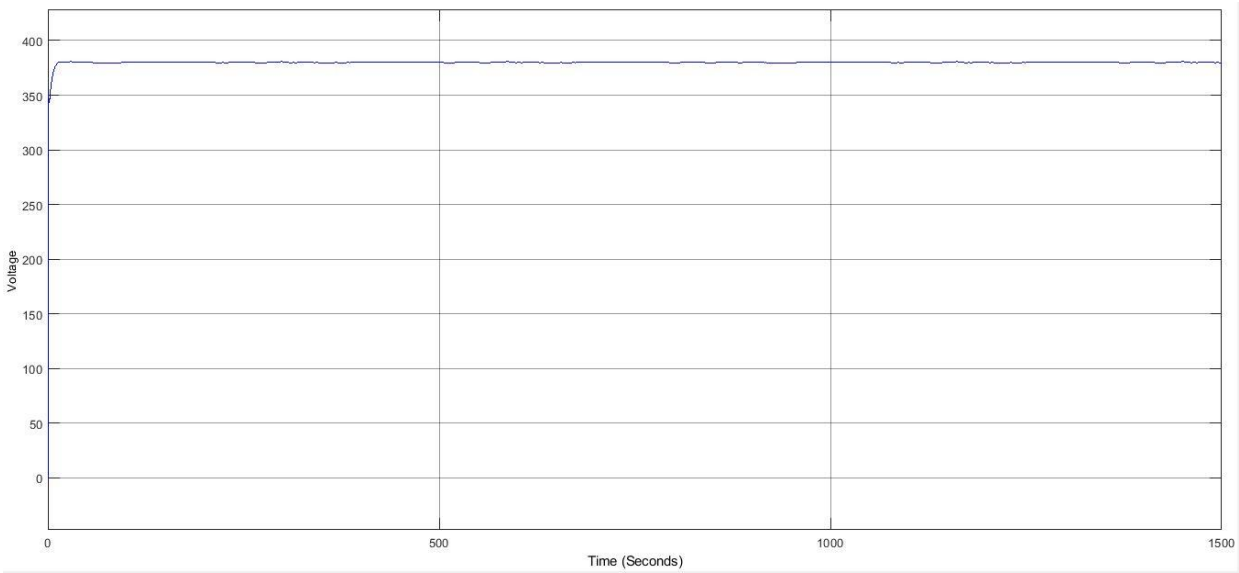

Fig 4.6 Voltage Waveform with Ships Load

4.4.2 FREQUENCY SENSOR & COMMUNICATION CHANNEL

As we all know, a cyber-attack on the Shipboard Power System might happen at two points: the Frequency Sensor and the Communication Channel.

(a) **Frequency Sensor**: The major instrument that measures the accurate Frequency of the System and provides this data to the Automatic Power Management System installed onboard as well as the Shore Control Centre is the Frequency sensor. The APMS uses this information to control the system's whole power generation in accordance with the load requirements. It determines whether to increase or reduce the frequency of the generator for the desired output based on the frequency and load. The entire system might be brought down if hackers launch a cyber-attack on the frequency sensor and manipulate the data. The power supply will be disrupted as a result of this entire ship, and the ship will be stranded.

(b) **Communication Channel**: The APMS senses the frequency sensor data in real time and sends it to the Shore Control Centre through Communication Channel. Every minute of

the ship is monitored in real time by the Shore Control Centre. It gets the information, analyses it, and saves it. If a hacker uses a cyber-attack to manipulate data in the communication channel, the Shore control centre and the ship will both receive incorrectly manipulated data, causing them to take the erroneous action/command. The operation of the ships will be completely disrupted as a result of this.

4.4.3 FALSE DATA INJECTION ATTACK

By inserting Step input, Ramp input, and Mixed Input, the hacker can modify the data. We considered the False data injection attack to make the Shipboard Power system realistic because this form of Cyber-attack is difficult to detect. The term "false data injection attack" (FDIA) was first used in the context of smart grids. While the word may appear generic, it refers to the situation in which an attacker manipulates sensor readings in such a way that undetected errors are introduced into state variable and value calculations.

Cyber attackers are interested in leveraging similar tactics in other application fields such as defense and governance, because to the rapid growth of the Internet and accompanying complex adaptive systems. FDIA has become one of the top-priority concerns to cope with in today's more dangerous cyber environment of sophisticated adaptive systems. Greater awareness and a stronger method to counter such attacks in cyberspace are now essential. As a result, this paper provides an overview of the attack, analyses FDIA's impact in crucial sectors, and discusses countermeasures.

4.4.4 SHIPBOARD POWER SYSTEM WITH CYBER-ATTACK

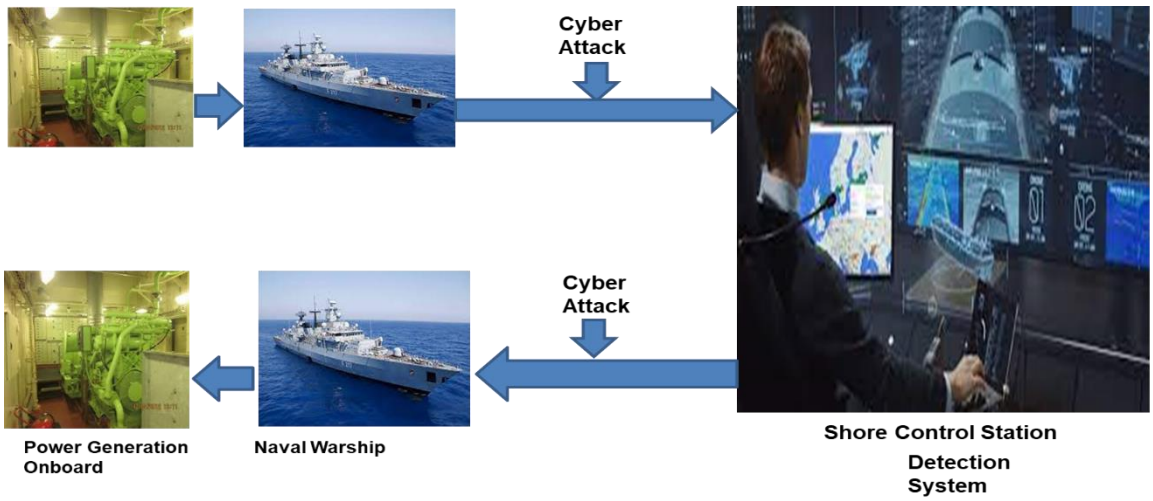

Fig 4.7 Shipboard Power system with cyber-attack

In the Matlab Simulink Model, the Shipboard Power System is illustrated. The Cyber Attack in this situation is classified as a False Data Injection Attack. The simulation's results are as follows:

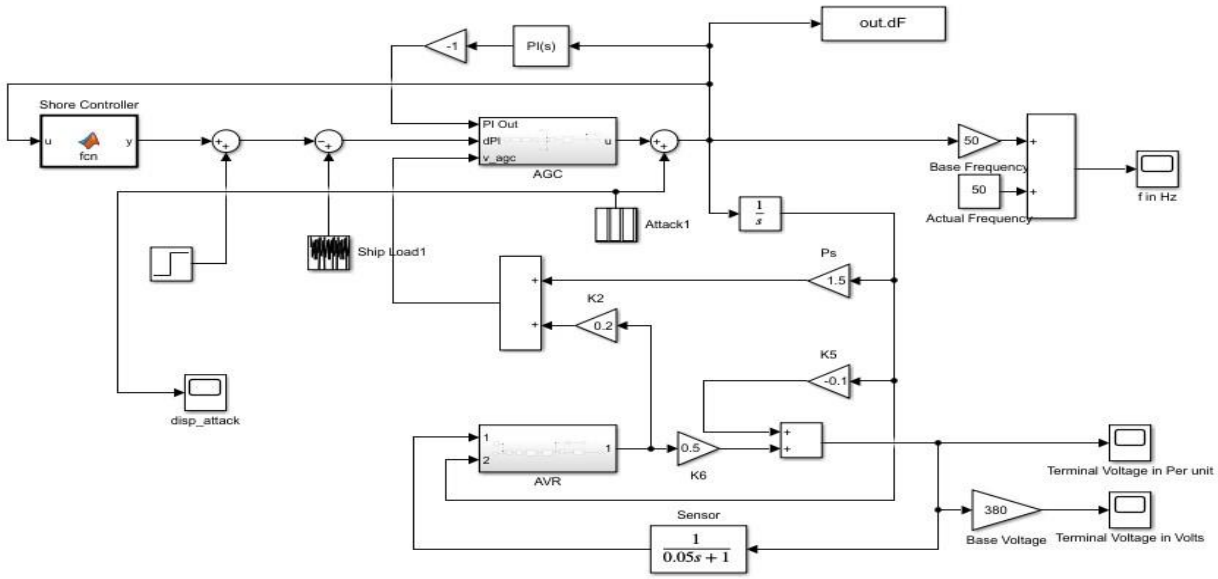

Fig 4.8 Shipboard Power System with False data injection Cyber-Attack

(a) **Frequency output with Ships Load & With Cyber Attack**: In this case, the power system is operating at full capacity. At this point, we've evaluated a cyber-attack on the system data via false data injection. We can see from the Frequency Waveform that the frequency was not stable at 50Hz at the time of the Cyber-attack. The Frequency has two large spikes that can destroy the ship's system and cargo. These Spikes have the potential to knock out the ship's entire power source.

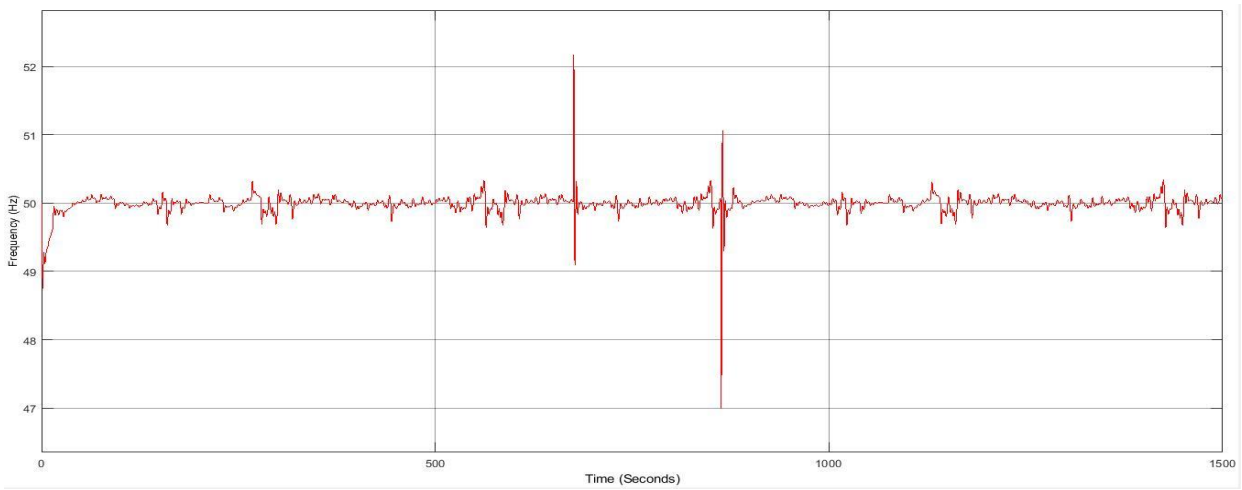

Fig 4.9 Frequency Waveform with Ships Load & cyber-attack

(b) **Voltage Output with Ships Load & With Cyber Attack**: The Power System is now operating at Ships Load. At this point, we've explored the Cyber-Attack of fake data injection. We can see from the Voltage Waveform that it is changing near 380 volts, although it is within limits.

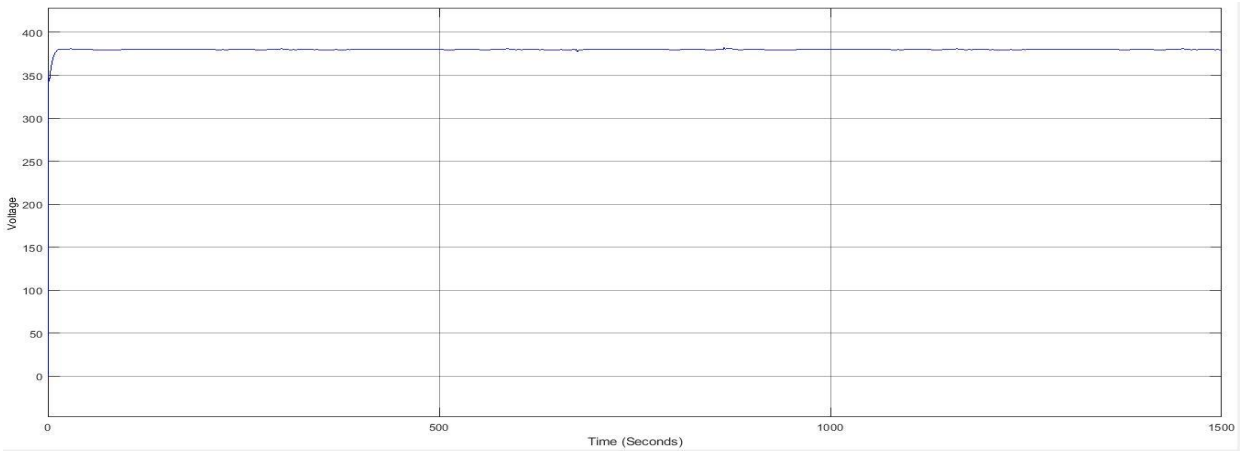

Fig 4.10 Voltage Waveform with Ships Load & cyber-attack

CHAPTER 5

ATTACK DETECTION FOR APMS & SCC

5.1 INTRODUCTION

In this chapter, we describe a detection strategy that uses the characteristics of the frequency data to determine whether there is an attack or not. Most of the literature uses specific system models to analyze the control system and design detection strategies. For example, a Kalman filter-based technique first estimates the values of the measurements at a future instant based on the system model and current values. If the error between the two is considerably high, an attack is said to be detected. However, the system models are not exact and most of the system models do not consider nonlinearities, uncertainties, noise, time delay, etc. Thus, the detection mechanism might fail under such situations.

This is where the data-based algorithms can help in the detection process. A large amount of data is available using various sensor measurements. These data are produced by an actual system rather than approximate system models and thus are a perfect representation of the system dynamics. Under normal conditions, the system dynamics follow a specific pattern and during an attack, there are dynamic changes that create variations in the signals. These variations may not be very evident if an attacker is smart enough to model the attack to surpass bad data detection techniques. However, advanced data analytics can be used to extract signal pattern information that can be effectively utilized to detect attacks.

In this chapter, we make use of a signal processing method to extract the system dynamics during normal and attack states to detect the attacks. It is an anomaly detection method, i.e, it detects a change in patterns from a normal state and thus can be used to detect different types of attacks [34].

5.2 SIGNAL PROCESSING BASED ATTACK DETECTION

The different steps for attack detection are as shown in Figure.5.1

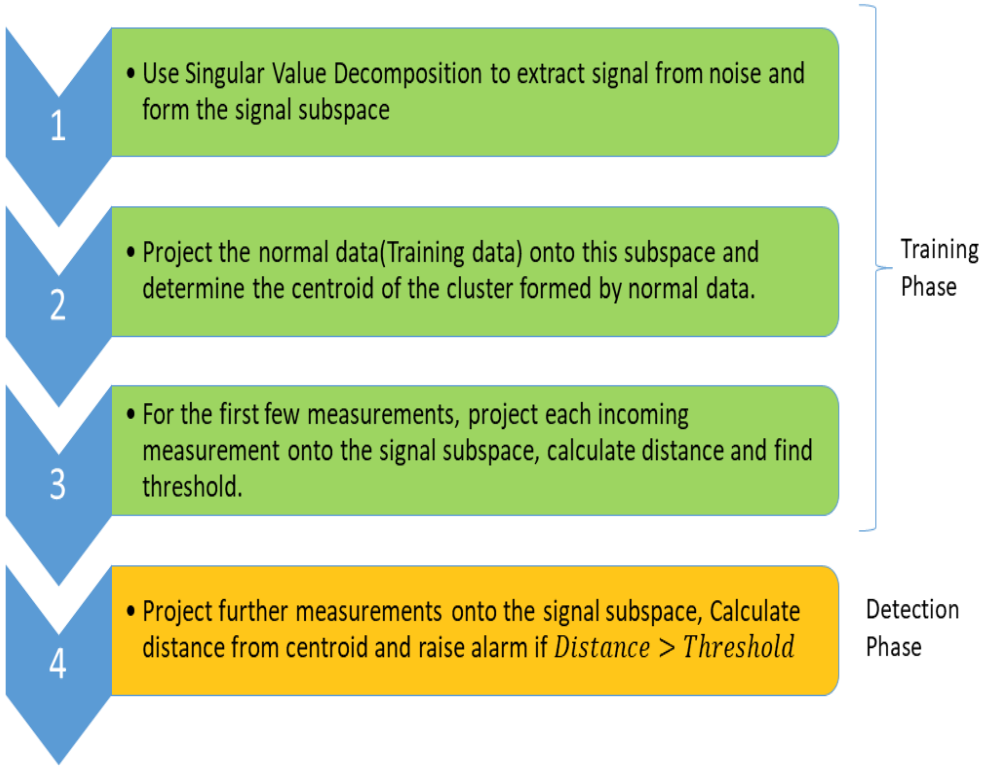

Fig 5.1 Various Steps for Attack detection

The algorithm can be broken down into the following steps:

(a) **Singular Spectrum Analysis** (SSA): Singular Value Decomposition is utilized to decompose the frequency measurement data into components that are representative of the normal behavior of the Power system. On the basis of these elements, a projection matrix is derived for the Power system.

(b) **Normal Data Cluster Analysis**: The projection matrix is used to project training data onto the signal subspace. In the signal subspace, these projected data form a cluster with a center.

(c) **Detection**: The distance from the cluster's core is established by projecting new measurements into the signal subspace. It's a sign of an attack if the data is far away from the cluster.

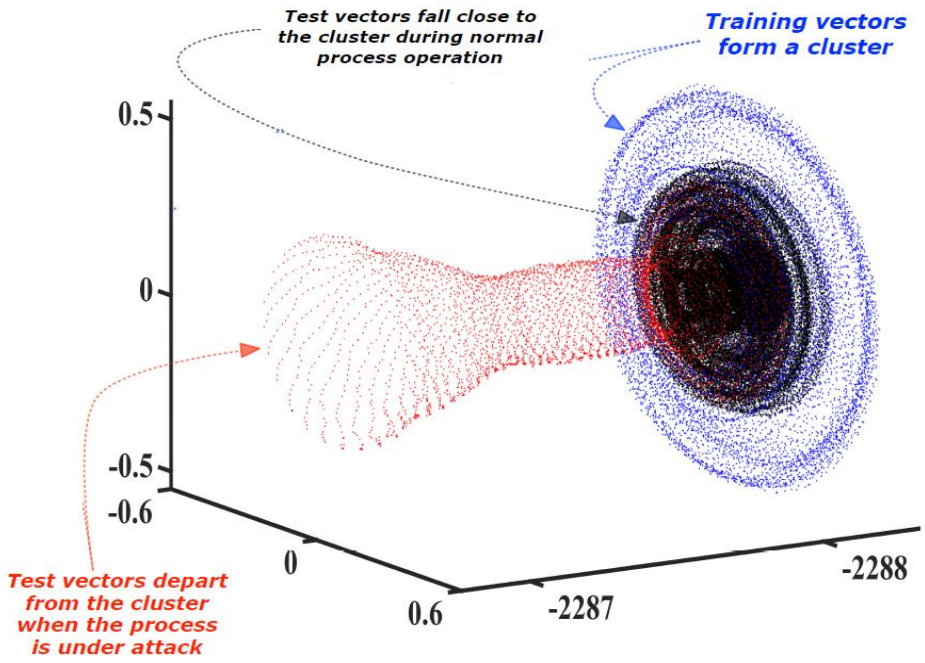

Fig 5.2 Signal Subspace Data Projection

The Fig 5.2 shows the data points that are projected onto the signal subspace. The blue data-points represent the training data. It can be seen that these data points form a cluster whose centroid can be determined. Each incoming measurement is added to the trajectory matrix and is projected to the signal subspace represented by the black and red data points. In case the measurements are normal, it will fall near to the blue cluster. In case there is an attack, the projected data points move farther away from the cluster as indicated by the red data points and thus attack can be detected.

5.3 DETAILED METHODOLOGY OF ATTACK DETECTION

The Detailed methodology used for detecting the False Data Injection Cyber-attack & developing the detection Algorithm is Mentioned below in the following steps:

(a) **Training Phase**:

(i) The forecasted load data is used to simulate & obtain the sensor data (Z_1, Z_2,…. Z_n).

(ii) This Training Dataset is embedded in a matrix, $T \in R_{L*k}$

$$\mathbf{T} = \begin{vmatrix} Z_1 & Z_2 & Z_k \\ Z_2 & Z_3 & Z_{k+1} \\ & & \\ Z_L & Z_{L+1} & Z_n \end{vmatrix}$$

(iii) Eigen vectors of TT'= U_1, U_2,…….U_L using singular value decomposition.

(iv) Separate out Eigen vectors into dominant (U_1, U_2,….U_r) & Non-dominant (Y_{k+1}, U_2,……U_L).

(b) **Projection on to Signal Subspace**:

(i) Find a p ∈ Sr which is nearest to z, i.e. ||p−z||, p = Pz

(ii) Since columns of U are orthonormal, U'U=I.

(iii) Find Centroid of cluster $c\tilde{} = Pc = P\ 1/K \sum z_i$

(c) **Detection**:

(i) $D_j = ||c\tilde{} - Pz_j|| = ||P(c - z_j||$

(ii) If D_j > Threshold = Attack detected.

(d) **Threshold determination**:

The first few normal measurements in the detection phase are used for the threshold determination. The distance is calculated for a set of measurements that are known to be normal and the maximum distance is used as the threshold.

5.4 SUMMARY

With the Single spectral analysis methodology, we developed the detection algorithm which can detect Cyber-attack. The algorithm was tested & simulated in MatLab, we found that the Algorithm was working satisfactorily. The MatLab Algorithm was able to detect the false data injection attack as soon as it received the frequency data from the ship. To Make the Hardware prototype for the detection Algorithm we choose Raspberry pi as the computer for processing the program. The raspberry pi supports the Python language which is very useful in implementing the codes.

CHAPTER 6

HARDWARE DEVELOPMENT & IMPLEMENTATION OF SCC-APMS

6.1 Introduction

We chose to create a Hardware Prototype for the Same. system in order to identify and simulate Cybersecurity for the APMS and Shore Control Centre. We bought two Raspberry Pi 3 computers to do this. The Raspian OS was installed on both Raspberry Pis. The Raspberry Pi was configured to communicate with the Ethernet and could access the internet after installing the OS.

After that, one raspberry pi was designated as the Ship, and the other raspberry was designated as the Shore Control Centre. The Frequency Dataset received from Matlab Simulink was supplied to the Raspberry Pi that was designated as the Ship. The same data set was transmitted from the Raspberry Pi using appropriate coding to imitate it as a ship. The other Raspberry Pi, which served as the shore control centre, was programmed to receive and record data in real time. The connection was formed, and both Raspberry Pis were interacting in real time with each other.

An attack detection programme was written in Matlab for the Shore Control Center and then ported to Python for use on the Raspberry Pi, so that if a cyberattack occurs, it will be detected and an alarm will be triggered, which will turn on a Red LED.

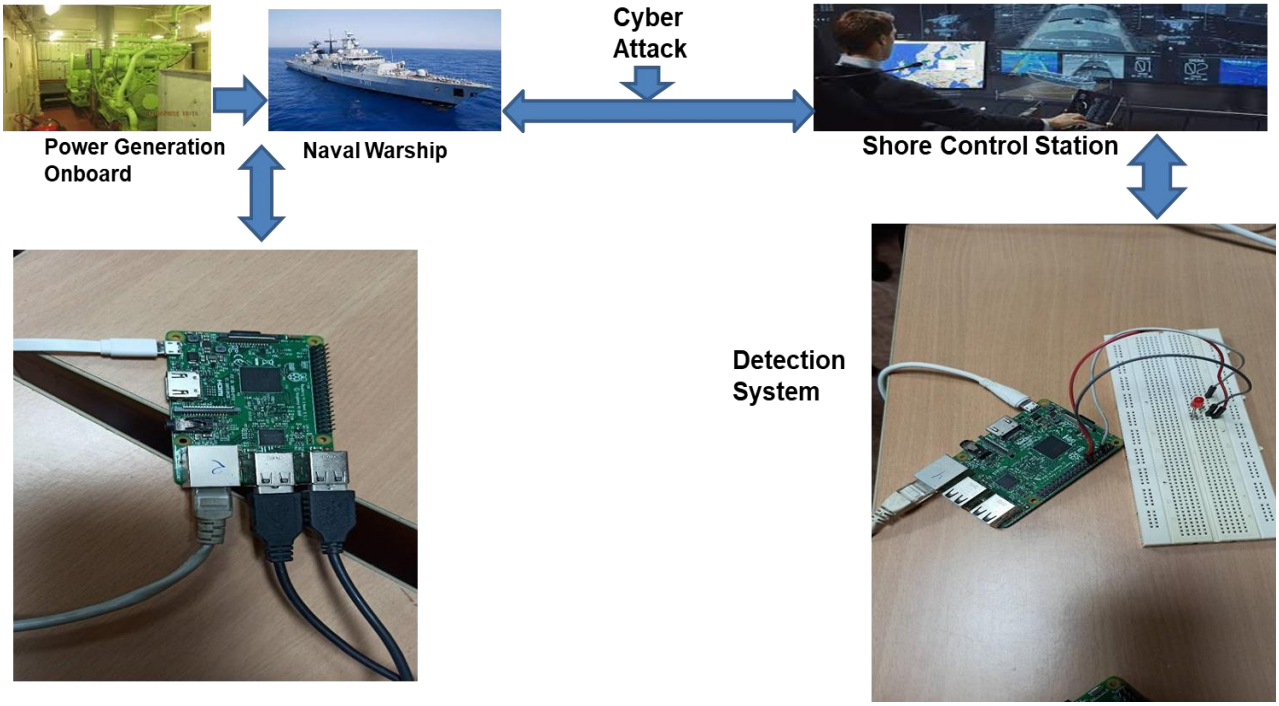

Fig 6.1 Block diagram for hardware implementation

6.2 Raspberry pi

The Raspberry Pi is a low-cost, little computer that connects to a computer monitor and operates with a conventional keyboard and mouse. The Raspberry Pi is a computer that can communicate with the outside world and can write in Scratch and Python. It uses less energy and requires only a few simple configurations to identify intruders in the network.

This paper's proposed detection algorithm is simple to implement on a Raspberry Pi. This detection system is entirely based on the Raspberry Pi and is designed as a client-server system.

Malicious activity are captured on client workstations and reported straight to the server for processing. Depending on the substance of the data received, the Server analyses it and decides whether or not to issue a security warning. Architecture of the Server The server is connected to numerous clients and is set to receive all incoming bound traffic, which is subsequently saved in the knowledge database, due to the centralization of data obtained. In this example, the proposed server architecture monitors and controls from a central place.

A few Advantages of Raspberry pi are as follows:

• Low cost

• High computing power in a small package

• Multiple interfaces (HDMI, multiple USB, Ethernet, on-board Wi-Fi and Bluetooth, many GPIOs, USB powered, etc.)

• Linux and Python are supported (making it easy to build applications)

• Examples that are readily available, as well as community assistance

6.3 WORKING OF THE HARDWARE

The Raspian Operating System was installed on the Raspberry Pi. We installed the essential applications to run the codes on the System after it was set up with the OS. We needed two Raspberry Pis, two monitors, two keyboards, two mice, two VGA to HDMI converters, two power cables, and two Ethernet cables to create the hardware. We assembled all of the hardware once it was ready to create a functioning operating system. On the Raspberry Pi, we started building the python code for detecting cyber-attacks. The following is a full step-by-step explanation of the complete process:

(a) **Raspberry pi model for Ship:**

The Raspberry Pi model was programmed to behave like a ship at sea. The system was fed frequency data from the ship's power system, which was communicated to the Shore Control Center by the Automatic Power Management System. The frequency data came from the Matlab Simulink Model of the Ship's Power System. With the help of the Ships Data Send Program fed into the Raspberry Pi, the data was saved in a file with time stamping and transferred to the Shore Control Centre. The Entire Setup for the Ship is placed in the Lab, as seen in Fig 6.2.

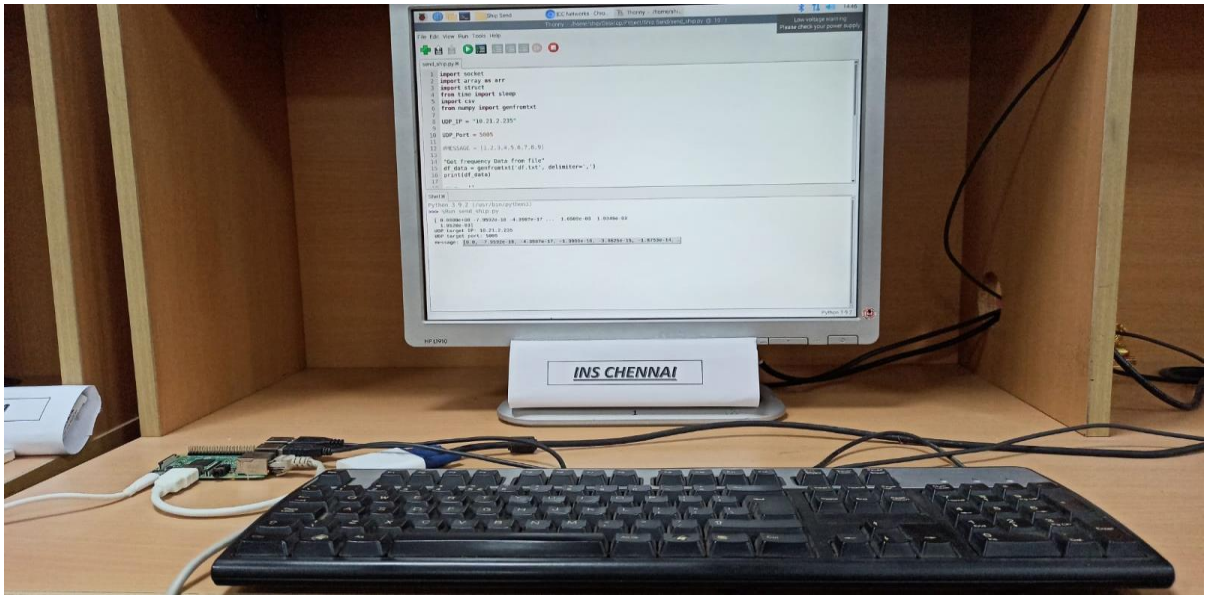

Fig 6.2 Raspberry pi Ships Model

(b) **Ship Sending Frequency Data to SCC**:

The system was supplied the frequency data from the Simulink simulation so that it could communicate it to the shore control centre via the communication channel, which in this case was Ethernet. The data is being transferred to the SCC, as shown in Fig 6.3. Please see **APPENDIX A** for more information.

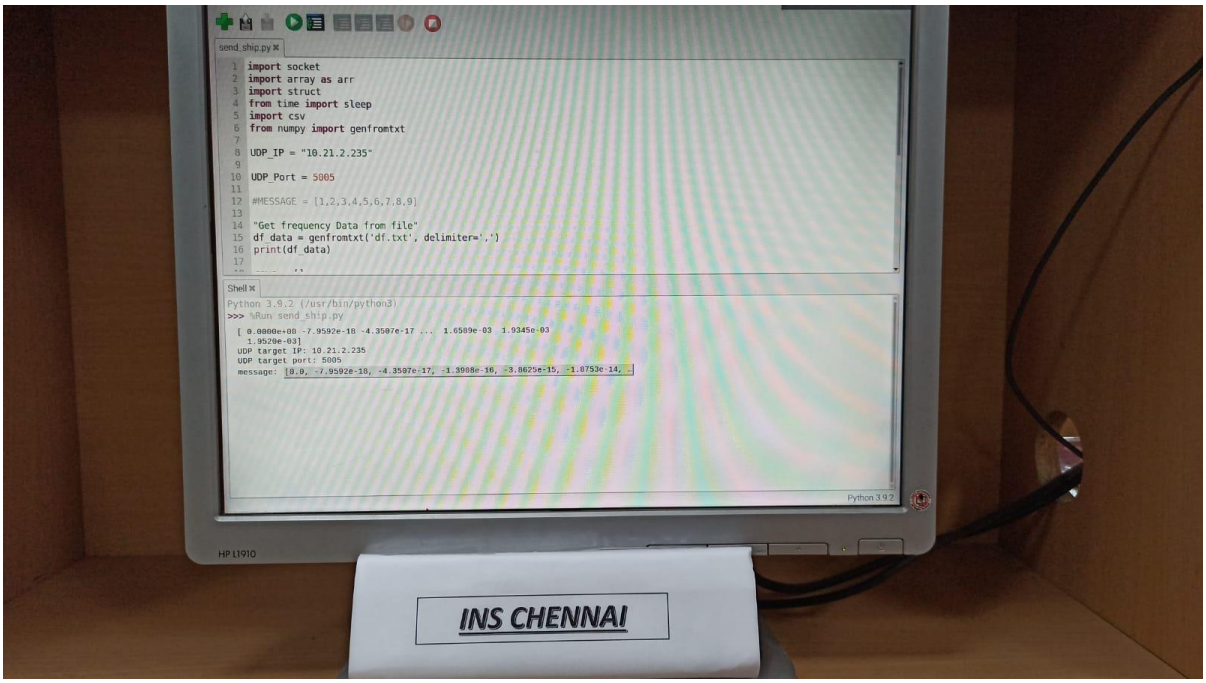

Fig 6.3 Ship sending frequency data to SCC

(c) **Raspberry pi Model for SCC**:

The Raspberry Pi was programmed for the Shore Control Centre in such a way that it can receive the ship's Frequency Data in real time and execute the detection algorithm in order to detect a cyber-attack. The whole setup of the Shore control centre can be shown in Fig. 6.4.

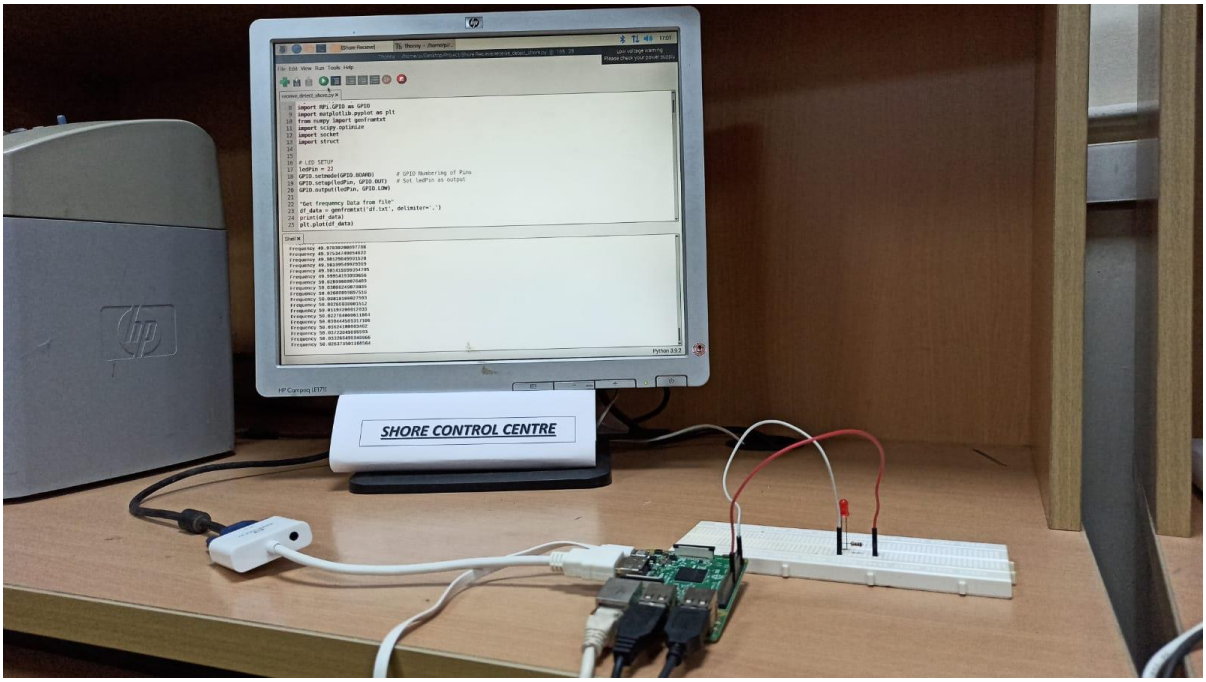

Fig 6.4 Raspberry pi Shore control centre model

(d) **SCC Receiving the Frequency Data from Ship:**

The Shore control centre receives the frequency data sent by the ship in real time. The SCC is responsible for regularly monitoring the data and identifying any anomalies. The code can be found in APPENDIX B.

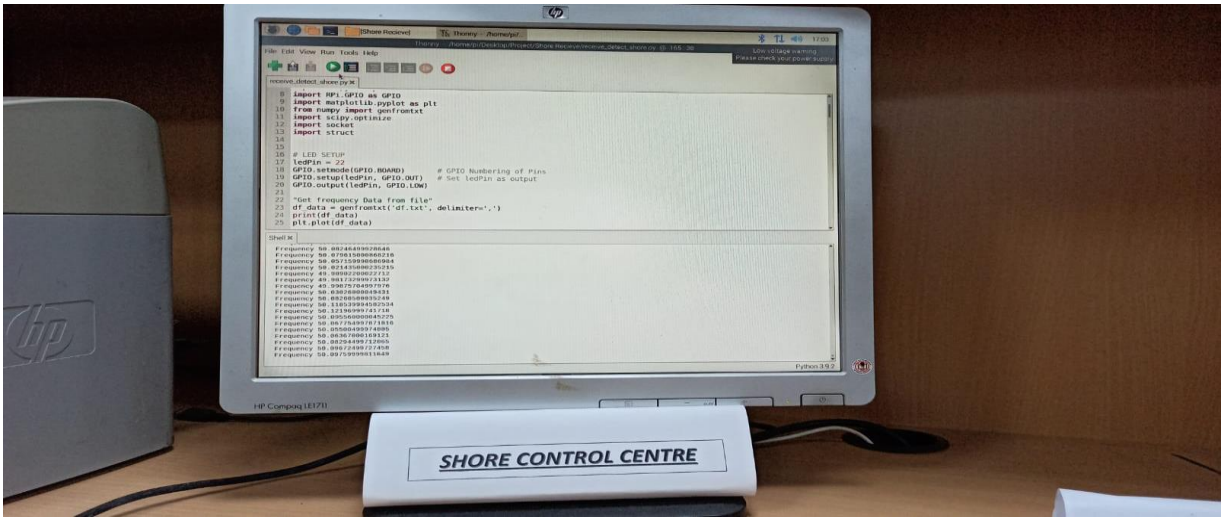

Fig 6.5 SCC receiving data from the Ship

(e) **Alarm System for Cyber-attack:**

The SCC will analyse the data and run the detection programme to detect the cyber-attack after it has been received. With the use of a breadboard, some wires, and a red LED light, we created an alert system that provided a clear indicator of the attack. The Raspberry Pi was used to code the alarm system. When a cyber-attack occurs, the detection algorithm detects it and sends a signal to the alarm system, which activates the Red Led light. The attack has been identified in the Frequency data, as indicated by the Red Led light on.

Fig 6.6 Alarm system for cyber-attack

6.4 SUMMARY

The full hardware system was assembled and put through its paces in a variety of circumstances. The Ship Hardware was successful in providing the frequency data to the SCC, as shown in the above stages. The Shore control center's hardware proved successful in receiving data from the ship. By running the detection algorithm, the SCC hardware was able to monitor and evaluate the data. The SCC system alerted the alarm system when the attack was detected. By turning on the Red Led light as an alarm, the Alarm system hardware was also successful in demonstrating the attack detection. The operation of the Raspberry Pi hardware prototype proved successful. The Algorithm's Results and Hardware are explained in the following chapter.

CHAPTER 7

RESULTS AND DISCUSSION

7.1 Introduction

Onboard a cyber-enabled ship, the automatic power management system was deemed the most susceptible power system. As a result, the entire system was examined in order to make it less vulnerable to the growing number of cyber-attacks. On the system, we deployed the Secure Tropos Methodology, and we created the APMS Environment Analysis, APMS Organizational Analysis, and APMS Security Analysis. The major security needs for the APMS system were discovered to be data availability, data integrity, and power system data authenticity. To test this hypothesis, we created the Simulink Model for the Power System installed onboard the ship. To generate accurate findings, the simulations were run in a variety of real-world circumstances. Because fake data injection attacks are difficult to detect, they were integrated in the Simulink system. Following the completion of the simulations, a cyber-attack detection system based on single spectral analysis was created. The frequency data from the Simulink power system model was supplied into the detection method. The programme was discovered to be capable of detecting cyber-attacks. To recreate the process in the real world, hardware was created using the Raspberry Pi. The following are the outcomes of the algorithm and hardware:

7.2 Results

The results achieved by the Simulink Model of the Power System fitted onboard are mentioned below in various steps:

Step 1: The simulation uses load forecast data as shown in the Fig 8.1 obtained from INS Chennai for the training phase. The actual load data is then used for the testing phase.

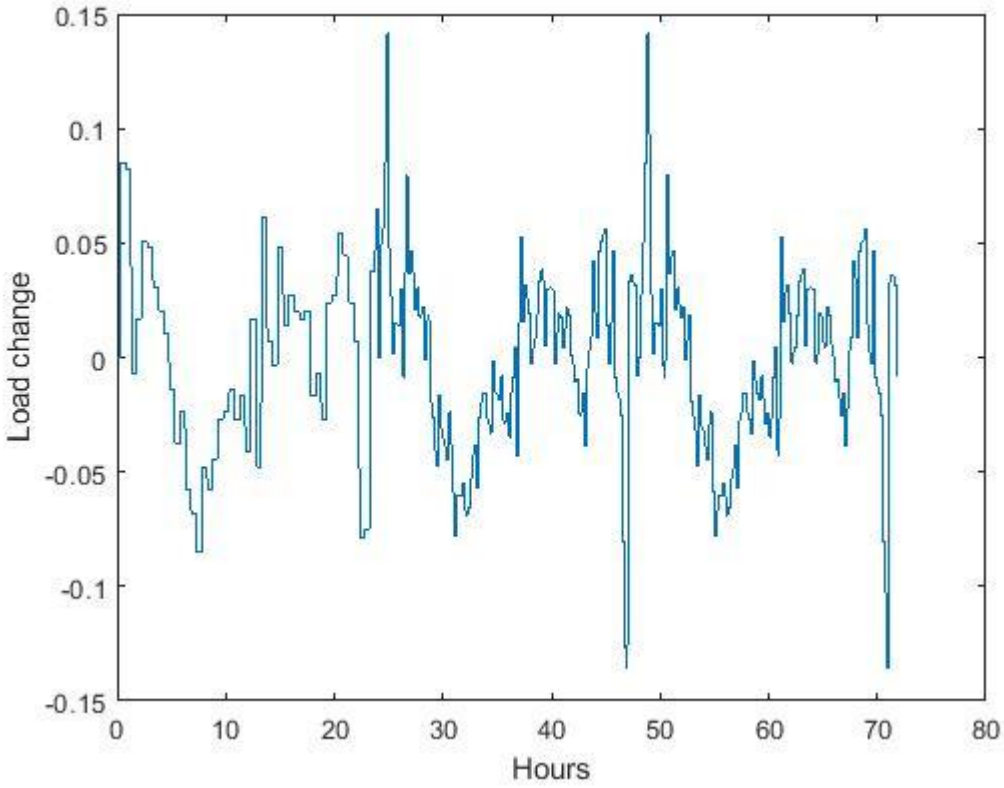

Fig 7.1 Waveform for Load Data

Step 2: Attack simulation is conducted by injecting the FDIA attacks mentioned in the previous sections at a time of τ. Attack values are selected such that frequency remains within the prescribed limits to maintain the stealthiness of the attack.

The simulation of Frequency control is performed by using the Ships load data mentioned in Step 1 by adding noise at different signal-to-noise ratios (SNR) and the attacks to obtain the study dataset.

Step 3: In the detection phase, we first determine the threshold using the data till a time T_{th} such that $0 < T_{th} < \tau$.

Step 4: The algorithm raises an alarm if the distance D_j goes beyond the threshold for any incoming measurement.

The Data or Waveform used in Algorithm is divided into mainly three parts:

(a) Data in Green Sector is used for training phase

(b) Data in White Sector is used for testing & detection

(c) Data in Red Sector is used for testing & detection.

It may be noted that in data received during the training phase we don't consider any Cyber-Attack. The Fig 7.2 shows the 03 Types of data used in the Algorithm.

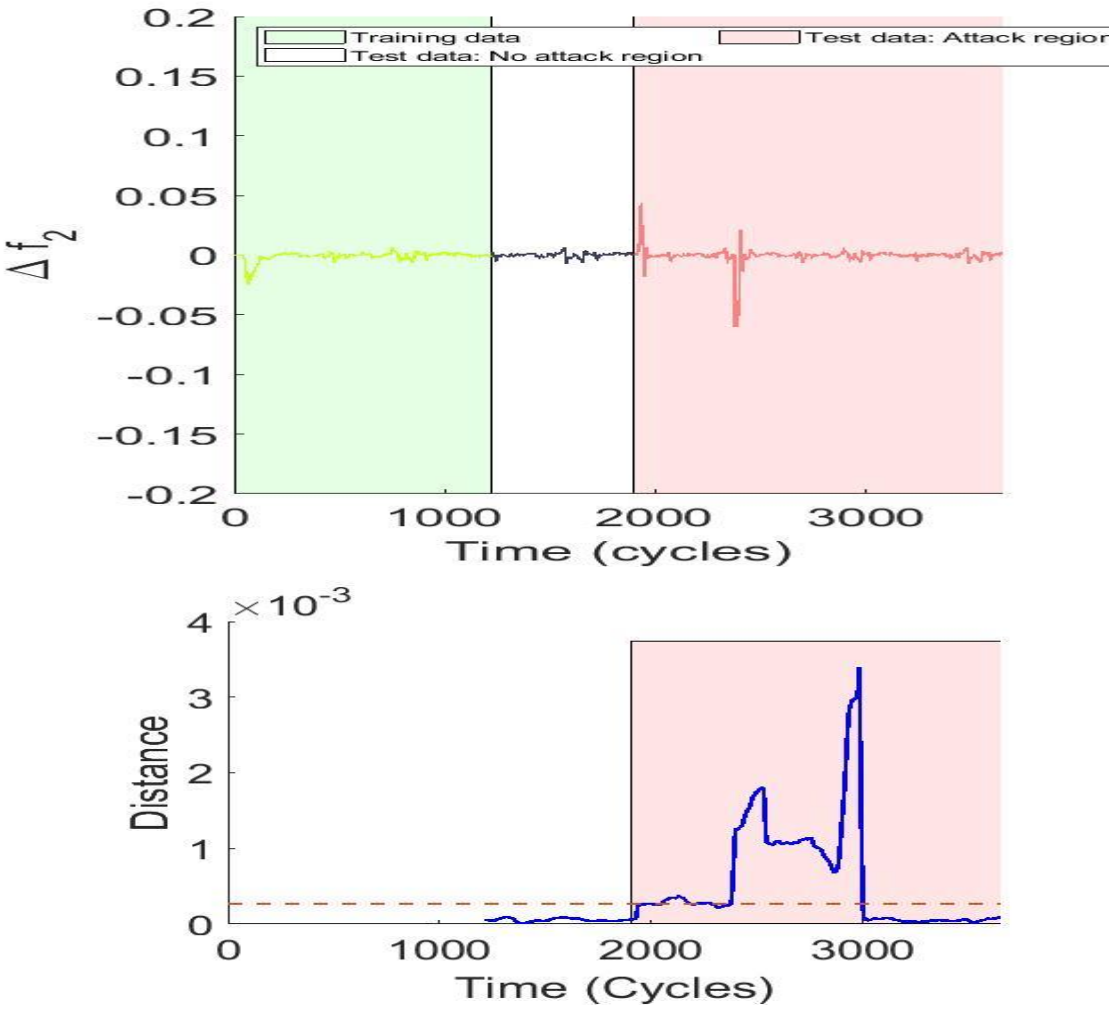

Fig 7.2 Attack Detection Waveform

As we can see in Fig 7.2 the Attack detection waveform, the Blue line indicates the distance calculated. This distance calculated is used for cyber-attack detection. The Redline in the waveform indicated the threshold value set after the training phase. Once the threshold value is set, the blue line should not cross the red line in the normal operating scenario. Whenever the Hacker Manipulates the frequency data, the Blue line will cross the red line which is the threshold value & will indicate the presence of the cyber-Attack.

Inference taken from the results is that the detection algorithm is able to run properly & detect the Normal Data & False injection data Attack very accurately.

7.3 RESULT OF THE HARDWARE MODEL

(a) **Attack detected by SCC**:

When the data is received by the Shore control centre, the detecting algorithm is started. Whenever a hacker injects False Data into the Frequency dataset, the programme recognises it with great accuracy. The message 'Attack Detected' is printed in the command window and remains there until the Cyberattack is halted. Any operator sitting at the console watching the data will be alerted to the cyber-attack instantly. The entire crew can be quickly notified of the situation, and the same information can be shared with the nearby ship. The Attack detected Message is printed, as seen in Figure 7.3.

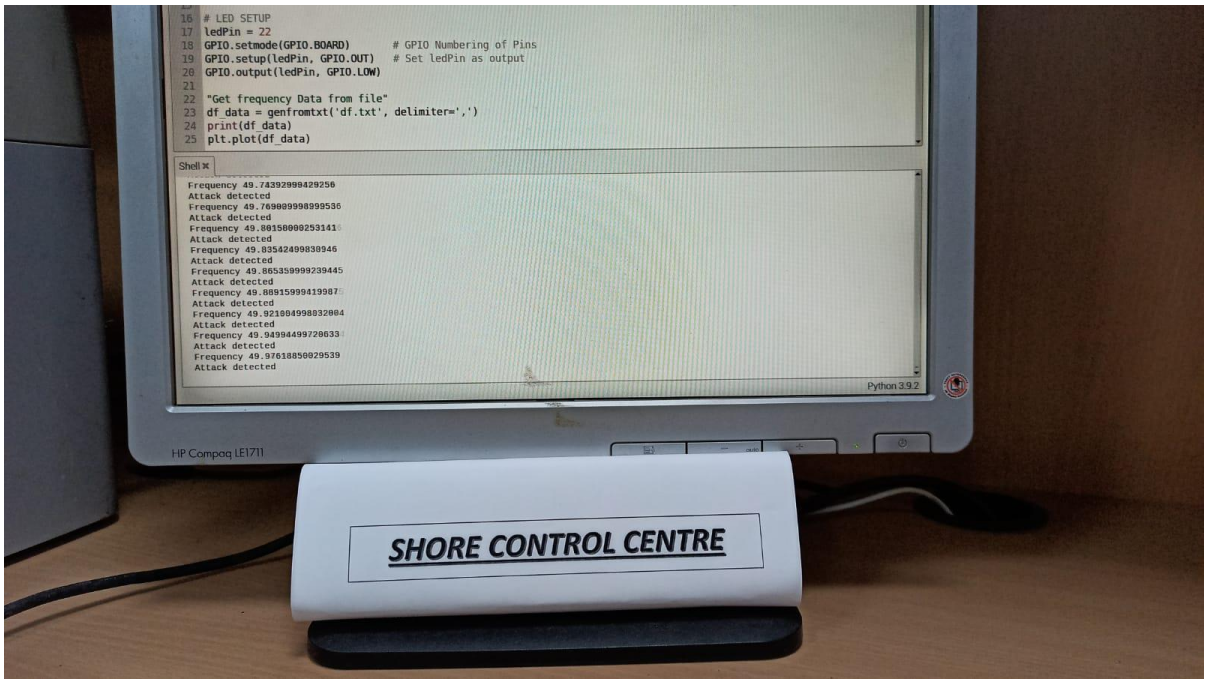

Fig 7.3 Attack detection by SCC

(b) **Alarm system indicating cyber-attack**:

When a False Data Injection Attack is identified by the Shore Control Center, a command is sent to the Alarm system connected to the SCC at the same time. When this command is received by the alarm system, a red LED light illuminates immediately. The Attack has been detected, as shown by the Red Led going on. The Red Led light was turned off to signal that the data set received was normal and that no cyber-attack had occurred. This Visual Alarm system ensures that the Operator is always informed of the attacks so that necessary counter-measures can be taken.

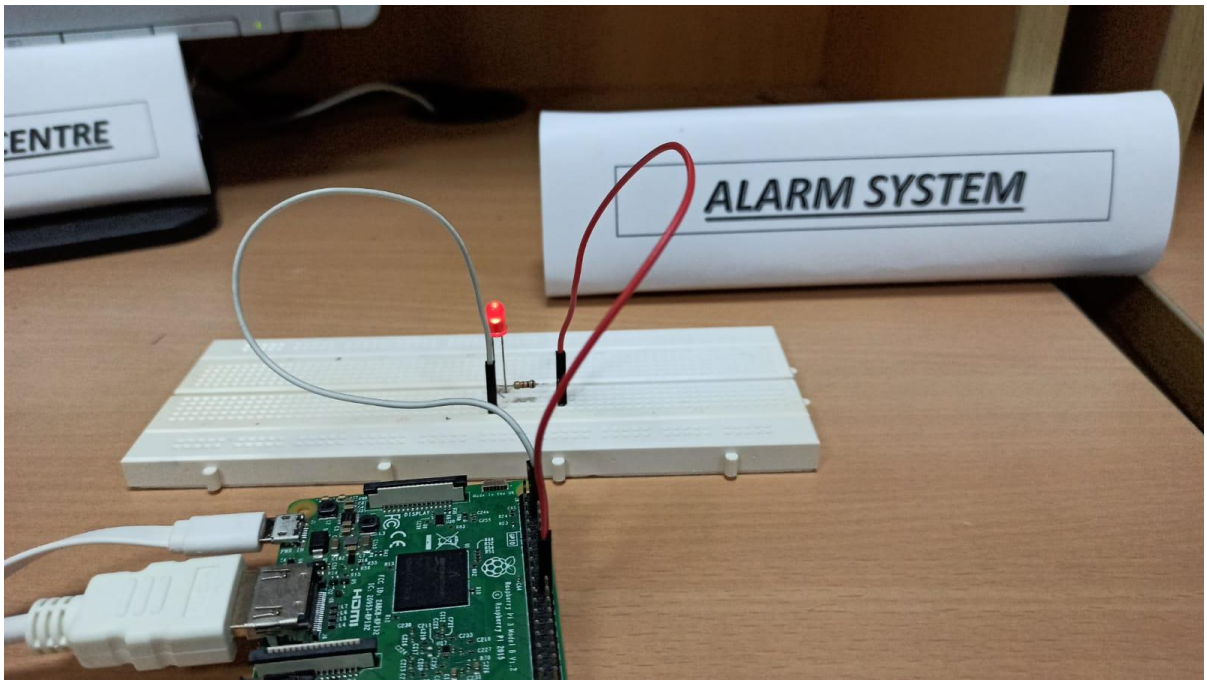

Fig 7.4 Alarm system indicating cyber-attack

7.4 SUMMARY

The Simulink Model, MatLab Algorithm, and Hardware Implementation all produced extremely accurate results. During the process, we discovered that the algorithm could easily distinguish between normal and attacked data without making any mistakes. With the Single spectral analysis method, there are no assumptions, and the Data cloud and threshold level are set according to the input data received, making it very accurate when compared to other methods. The approach shown that detection is quick, making it successful in preventing cyber-attacks.

CHAPTER 8

CONCLUSION

8.1 Project Summary

The implementation of the Sec-Tro model for automatic power management system, as well as the Detection Algorithm to detect the false data injection cyber-attack utilised onboard a Cyber-Enabled Ship, has been successfully verified through simulation and hardware prototype. It has been discovered that using a single spectral analysis technique to detect the False data injection cyberattack improves the overall security of the power management system. Various scenarios for effective realisation were determined to be perfect and yielded encouraging simulation results. Because the APMS System is so critical because it controls the ship's whole power generation, all precautions must be taken to secure it from hackers. Even though detecting a hack takes a few seconds, it is acceptable for a cyber-enabled maritime vessel. Once the detection is complete, the APMS system can compare the received data to the feedback values and adjust the values. As a result, the APMS system will not perform the inappropriate action on board and will be safeguarded from cyber-attack. Furthermore, vital loads linked during regular journeys, such as steering gear, navigation radars, and power generation equipment, will not be harmed and will continue to function normally.

As the security of the APMS and the shore control centre improves, the task of giving adequate power to the loads onboard becomes easier, resulting in a more reliable power supply. The ship's operation will become more reliable, secure, and continuous as a result of this detection algorithm. Furthermore, because little effort is put into its protection, this system is vulnerable to cyber assaults. With increased research and development in the field of cybersecurity, this system will grow more powerful and less prone to cyber-attacks in the future.

8.2 Future Scope

There is a lot of room for the project to grow, especially in terms of establishing mitigation measures so that cyber-attacks may be dealt with more easily, making the system more reliable and less vulnerable. The Security Model created for the APMS system can be used as a starting point for creating a new system. This will strengthen the system's defences against cyber-attacks. For the tried-and-true simulation concept, a complete hardware configuration can be created. On board a ship, space is restricted, hence the size of the system should be regulated by the available space. For improved product utilisation, additional forms of cyberattacks can be simulated and more types of detection methods can be incorporated.

REFERENCES

(1) SINTEF, "Shipping 4.0 presented at singapore maritime week," [Online]. Available: https://www.sintef.no/en/latest-news/shipping-4.0-presented- at-singapore-maritime-week/

(2) J. Cross and G. Meadow, "Autonomous ships 101," *J. Ocean Technol.*, vol. 12, pp. 23–27, 2017.

(3) K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," in *Proc. IEEE Int. Conf. Cyber Secur. Protection Digital Services*, 2018, pp. 1–8.

(4) G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *SECPRE 2018, CyberICPS 2018. Lecture Notes in Computer Science*. Springer, 2018, vol. 11387, pp. 20–36. USCG, "Cyber incident exposes potential vulnerabilities onboard com- mercial vessels," [Online]. Available: https://www.dco.uscg.mil/Portals/ 9/DCO%20Documents/5p/CG-5~PC/INV/Alerts/0619.pdf

(5) M. Jones, "Spoofing in the black sea: What really happened?" [On- line]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea- what-really-happened/

(6) MARAD, "2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Ara- bian Sea, Red Sea-Threats to Commercial Vessels by Iran and its Proxies," [Online]. Available: https://www.maritime.dot.gov/content/2019-012- persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea- threats- commercial-vessels

(7) G. Kessler, J. P. Craiger, and J. C. Haass, "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identifica- tion system," *TransNav: Int. J. Marine Navigation Safety Sea Transp.*, vol. 12, no. 3, p. 429, 2018.

(8) S. Katsikas, "Cyber security of the autonomous ship," in *Proc. 3rd ACM Workshop Cyber-Physical Syst. Secur.*, ACM, 2017, pp. 55–56.

(9) H. Mouratidis and P. Giorgini, "Secure tropos: A security-oriented exten- sion of the tropos methodology," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 17, no. 2, pp. 285–309, 2007.

(10) B. Weinert, A. Hahn, and O. Norkus, "A domain-specific architecture framework for the maritime domain," in *Informatik 2016*, H. C. Mayr and

(11) M. Pinzger, Eds, Bonn, Germany: Gesellschaft für Informatik e.V., 2016, pp. 773–784.

(12) L. Kretschmann, Ø. J. Rødseth, B. S. Fuller, H. Noble, J. Horahan, and

(13) H. McDowell, "MUNIN D9.3: Quantitative assessment," 2015, p. 150.

(14) Body of Knowledge and Curriculum to Advance Systems Engineering Editorial Board, "The guide to the systems engineering body of knowledge (SEBoK), v. 2.0," [Online]. Available: www.sebokwiki.org.

(15) Ø. J. Rødseth, B. Kvamstad, T. Porathe, and H. Burmeister, "Communi- cation architecture for an unmanned merchant ship," in *Proc. MTS/IEEE OCEANS – Bergen*, Norway, 2013, pp. 1–9.

(16) M. Höyhtyä, J. Huusko, M. Kiviranta, K. Solberg, and J. Rokka, "Con- nectivity for autonomous ships: Architecture, use cases, and research challenges," in *Proc. IEEE Int. Conf. Inf. Commun. Technol. Convergence*, 2017, pp. 345–350.

(17) Bureau Veritas, "Guidelines for autonomous shipping," Tech. Rep., 2017. [Online]. Available: https://www.bureauveritas.jp/news/pdf/641-

(18) NI_2017-12.pdf

(19) DNVGL, "Cyber security capabilities of control system components," Det Norske Veritas Germanischer Lloyd, Tech. Rep, 2018.

(20) International Electrotechnical Commission – IEC, "Maritime navigation and radiocommunication equipment and systems," NEK IEC 61162- 460:2018, 2018, p. 152.

(21) N. Mead, "How to compare the security quality requirements engineering (SQUARE) method with other methods," Tech. Rep., Aug. 2017, [Online].

(22) Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a471104.pdf

(23) A. Nhlabatsi, B. Nuseibeh, and Y. Yu, "Security requirements engineering for evolving software systems: A survey," *Int. J. Syst. Syst. Eng.*, vol. 1, pp. 54–73, 2010.

(24) A. Pattakou, C. Kalloniatis, and S. Gritzalis, "Security and privacy requirements engineering methods for traditional and cloud-based sys- tems: A review," *Cloud Comput.*, vol. 155, pp. 145–151, 2017.

(25) D. Mellado, C. Blanco, L. Sánchez, and E. Fernández-Medina, “A sys- tematic review of security requirements engineering,” *Comput. Standards Interfaces*, vol. 32, no. 4, pp. 153–165, 2010.

(26) D. Muñante, V. Chiprianov, L. Gallon, and P. Aniorté, “A review of security requirements engineering methods with respect to risk analysis and model-driven engineering,” in *Proc. Int. Conf. Availability Rel. Secur.*, 2014, pp. 79–93.

(27) V. Diamantopoulou and H. Mouratidis, “Applying the physics of notation to the evaluation of a security and privacy requirements engineering methodology,” *Inf. Comput. Secur.*, vol. 26, no. 4, pp. 382–400, 2018. doi:10.1108/ICS-12-2017-0087.

(28) Sep. 2018. Kavallieratos G, Diamantopoulou V, Katsikas S. Shipping 4.0: Security Requirements for the Cyber-Enabled Ship. IEEE Transactions on Industrial Informatics. 2020;16(10):6617-6625.

(29) H. Bevrani, T. Hiyama, Power system dynamic stability and voltage regulation enhancement using an optimal gain vector. Control Eng. Practise 2008.

(30) P. Kundur, Power System Stability and Control (McGraw-Hill, New York, 1994) & J. Machowski et al., Power System Dynamics: Stability and Control, 2nd edn. (Wiley, Chichester, 2008)

(31) H. Bevrani, M. Watanabe, Y. Mitani, Power System Monitoring and Control (Wiley-IEEE Press, New York, 2014)

(32) H. Bevrani, Automatic Generation Control, ed. by H. Wayne Beaty. In Standard Handbook for Electrical engineers, 16th edn, Section 16.8 (McGraw-Hill, New York, 2013), pp. 138–159.

(33) N.K. Stanton, J.C. Giri, A. Bose, Energy Management, Power System Stability and Control, Chapter 17 (CRC Press, Boca Raton, 2007.

(34) Amulya A, Shanti Swarup K, Ramu Ramanathan, Spectral Analysis based robust Multi-level intrusion detection in wide area frequency control

APPENDIX A

PROGRAM FOR SENDING DATA FROM SHIP TO SCC

```
import socket
import array as arr
import struct
from time import sleep
import csv
from numpy import genfromtxt

UDP_IP = "10.21.2.235"

UDP_Port = 5005

#MESSAGE = [1,2,3,4,5,6,7,8,9]

"Get frequency Data from file"
df_data = genfromtxt('df.txt', delimiter=',')
print(df_data)

rows = []
for row in df_data:
    rows.append(row)

MESSAGE = rows

print ("UDP target IP:", UDP_IP)

print ("UDP target port:", UDP_Port)

print ("message:", MESSAGE)

sock = socket.socket(socket.AF_INET, # Internet

socket.SOCK_DGRAM) # UDP

for i in range(0,len(MESSAGE)):
    a=float(MESSAGE[i])
    data = struct.pack('f',a)
    sock.sendto(data, (UDP_IP, UDP_Port))
    sleep(0.1)
```

APPENDIX B

PROGRAM FOR RECEIVING DATA & ATTACK DETECTION IN SCC

```
import numpy as np
import RPi.GPIO as GPIO
import matplotlib.pyplot as plt
from numpy import genfromtxt
import scipy.optimize
import socket
import struct


# LED SETUP
ledPin = 22
GPIO.setmode(GPIO.BOARD)       # GPIO Numbering of Pins
GPIO.setup(ledPin, GPIO.OUT)   # Set ledPin as output
GPIO.output(ledPin, GPIO.LOW)

"Get frequency Data from file"
df_data = genfromtxt('df.txt', delimiter=',')
print(df_data)
plt.plot(df_data)

"Input other required values for SSA"
at_time = 1901;
Ts= 1;
s = df_data;
plot_no =1;
N = round(len(s)/3);
L = round(N/2);
T = len(s);
K = N-L+1;

"Range of attack"
atck_rg = np.arange(at_time,T);

" Constructing the (Hankel) trajectory matrix and solving its (SVD)"
C = s[0:L];
X = scipy.linalg.hankel(s[0:L],s[L:N+1]);
"X_test = Hankel(s[0:L],s[L:N+1]);"

print('SVD decomposition started ...');
t, e, vh = np.linalg.svd(X);
ev = e;
print('SVD decomposition complete');

r= 120;
print('Training is complete');

" Constructing the matrix whose columns form an orthonormal basis for
the signal subspace."
r_rang = np.arange(0,r-1);
U = t[:,r_rang];
```

```
" Computing the centroid of the cluster"
c = X.mean(axis=1);
utc = np.dot(np.transpose(U),c);

"A vector containing the normalization weights for computing the
squared"
" weighted Euclidean distance in the detection phase."
nev = np.sqrt(ev[r_rang]/sum(ev[r_rang]));


" Reconstring the approximate signal using the diagonal averaging step
in SSA"
print('Reconstructing signal ...');
ss = np.dot(U,np.dot(np.transpose(U),X));

sig = np.zeros(N);

for k in range(0,L-1):
    for m in range(1,k+2):
        sig[k+1] = sig[k+1]+(1/(k+1))*ss[m-1,k-m+1];


for k in range(L-1,K):
    for m in range(1,L+1):
        sig[k+1] = sig[k+1]+(1/(L))*ss[m-1,k-m+1];

for k in range(K,N):
    for m in range(k-K+2,N-K+1):
        sig[k+1] = sig[k+1]+(1/(N-k))*ss[m-1,k-m+1];

print('Signal reconstruction complete');

"Detection Phase"
print('Testing started...');
d = np.zeros(T-N);

"Constructing the first test vector."
x = s[np.arange(N-L,N)];

Threshold = np.max(d[np.arange(1,round(N*2/3))]);
test_label = np.ones(T-N)
for i in range(N+1,T-1):
    " Constructing the current test vector by shifting the elements to"
    " the left and appending the current sensor value to the end."
    x = x[np.arange(1,len(x))];
    x = np.append(x,s[i]);


    " Computing the difference vector between the centroid of the"
    "% cluster and the projected version of the current test vector."
    y = utc - np.dot(np.transpose(U),x);
    ac = np.dot(np.transpose(U),s[i]);

    "% Computing the weighted norm of the difference vector."
    y = nev*y;
    d[i-N] = np.dot(np.transpose(y),y);
```

```
print('Testing complete.');
Threshold = np.max(d[np.arange(1,round(N*2/3))]);
Th = Threshold*np.ones(T);

"""for i in range(N+1,T-1):
    if d[i-N]>=Threshold:
        test_label[i-N] = -1;
        GPIO.output(ledPin, GPIO.HIGH)
        print('Attack detected')
    #else:
     #   GPIO.output(ledPin, GPIO.LOW) """

"Detection Phase from data"
print('Detection Started')

UDP_IP = ""             #Receive from any port

UDP_PORT = 5005

sock = socket.socket(socket.AF_INET, # Internet

                     socket.SOCK_DGRAM) # UDP

sock.bind((UDP_IP, UDP_PORT))

while True:

    data, addr = sock.recvfrom(1024) # buffer size is 1024 bytes

    data=struct.unpack('f',data)     # Extract value from data received
    freq = data[0]*50+50;            # Convert to actual frequency to
display
    print("Frequency", freq)


    " Constructing the current test vector"
    x = x[np.arange(1,len(x))];
    x = np.append(x,data[0]);

    " Computing the difference vector between the centroid of the"
    " cluster and the projected version of the current test vector."
    y = utc - np.dot(np.transpose(U),x);
    ac = np.dot(np.transpose(U),s[i]);

    "Computing the weighted norm of the difference vector."
    y = nev*y;
    d_det = np.dot(np.transpose(y),y);

    "DEtect attack if distance d_det is above threshold"
    if d_det>=Threshold:
        print('Attack detected')
        GPIO.output(ledPin, GPIO.HIGH)
    else:
        GPIO.output(ledPin, GPIO.LOW)
```

APPENDIX C

DATA USED FOR MATLAB SIMULINK SIMULATION

Parameter	Gain	Time Constant
Turbine	KT = 1	TT =0.5
Governor	Kg =1	Tg = 0.2
Amplifier	KA =10	TA =0.1
Exciter	KE = 1	TE = 0.4
Sensor	KR = 1	TR = 0.05
Inertia	H = 5	
Regulation	R = 0.05	
Generator	KG = 0.8	TG = 1.4

For every 1% variation in frequency, the load changes by 0.8 percent, or D = 0.8. Assume Ps = 1.5 synchronisation coefficient and K6 = 0.5 voltage coefficient. K2 = 0.2, K4 = 1.4, and K5 = -0.1 are the coupling constants.