INTERNATIONAL BURCH UNIVERSITY

FACULTY OF ENGINEERING, NATURAL AND MEDICAL SCIENCES

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

CYBERSECURITY IN DISTRIBUTION SYSTEMS

SEMINAR PAPER

VEDAD MUŠOVIĆ

Sarajevo

June 2024

TABLE OF CONTENTS

ABSTRACT i

LIST OF FIGURES ii

LIST OF EQUATIONS iv

LIST OF ABBREVATIONS v

1. INTRODUCTION 1

2. DISTRIBUTION SYSTEM VULNERABILITIES 2

2.1. Communication Infrastructure in Distribution Systems 3

2.2. Smart Grid Network Structure under Cyberattacks 4

3. ATTACK VECTORS 6

3.1. CYBERATTACK TYPES 7

3.1.1. False Data Injection Attacks (FDIA) 7

3.1.2. Denial of Service (DOS) Attacks 9

3.1.3. Man – in – the - Middle (MiTM) Attacks 9

3.1.4. Malware Attacks 10

3.1.5. Measurement – Based Attacks 11

3.1.6. Other Attack Types 12

4. CYBERSECURITY DEFENSIVE STRATEGIES 13

4.1. Defensive Algorithm 13

4.2. CYBERATTACK DETECTION METHODS 14

4.2.1. Association Rule Mining (ARM) 15

4.2.2. Clustering 17

4.3. PARTICULAR DEFENSIVE APPROACHES...19

4.3.1. Firewalls..19

4.3.2. Network Segmentation 20

4.3.3. PLCC and LAN 22

4.3.4. Security Training and Constant Assessment 22

4.3.5. Additional Measures...23

5. FUTURE CHALLENGES AND CONSIDERATIONS 24

6. CONCLUSION..25

REFERENCES 26

ABSTRACT

This seminar explores cybersecurity inside of distribution systems, which addresses the increasing threat of cyberattacks. These attacks can cause severe damage to the equipment, power outages, financial losses, data compromise and overall system instability. Inside Industrial Control Systems (ICS), distribution systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), alongside various sensors and actuators.

In operational technology (OT), low voltage distribution systems are open to data flows and remote access, which makes them vulnerable to cyberattacks. That is why, protective measures from the Information Technology (IT) sector need to be understood if the OT sector is to be protected properly as well. Means of attack are referred to as ‘attack vectors’. They are grouped into several categories, alongside common attack types.

SCADA systems are responsible for controlling data and monitoring the industrial process and are thus the most common target for cyberattacks. Systematic defensive approaches were developed in order to protect the system against cyberattacks. Importance of continuous assessment and security training for those who maintain the network is highlighted. Additionally, many methods center on firewalls, network segmentation and managing different events. The defensive algorithm is agreed protocol for determining an anomaly and attaching it to its proper defensive measure.

Keywords: cybersecurity, ICS, attack vectors, smart grid, SCADA systems, FDIA, firewalls, defensive algorithm, network segmentation, HMI

LIST OF FIGURES

FIGURE 1. A Graphical Representation of a TSO/DSO Network.

[Reference:] Krause T, Ernst R, Klaer B, Hacker I, Henze M (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors (Basel). 21(18):6225. Doi: 10.3390/s21186225. PMID: 34577432; PMCID: PMC8473297.

FIGURE 2. Hierarchal Cyberattack Control Blocks in a Microgrid.

[Reference:] Pinto, S.J.; Siano, P.; Parente, M (2023). Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. Energies 2023, 16, 1651.

FIGURE 3. Different Paths an Attack Vector can take to the Control Network.

[Reference:] Wandera, M., Jonasson, B., Benoit, J., Formea, J., Thompson, T., Tang, Z., Grinberg, D., Sowada, A., Andreou, D., Ruchti, T., Elwell, P., & Groat, J (2016). "Cybersecurity considerations for electrical distribution systems". Eaton

FIGURE 4. Graphical Representation of MiTM attack

[Reference:] Recommended Practice (2009): Improving Industrial Control Systems Cybersecurity with Defense-In-DepthStrategies, https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf. Accessed: June 7, 2024

FIGURE 5. Measurement – Based Attack Example

[Reference:] Liu, C. C (2023). "Cyber Security of SCADA, Substations, and Distribution Systems". Virginia Tech, delivered by Chen-Ching Liu, American Electric Power Professor and Director, Power and Energy Center

FIGURE 6. Flow Chart for ARM Cyberattack Detection inside Distribution Systems

[Reference:] Pinto, S.J.; Siano, P.; Parente, M (2023). Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. Energies 2023, 16, 1651.

FIGURE 7. Detecting Cyberattacks in Distribution Systems using Clustering

[Reference:] Pinto, S.J.; Siano, P.; Parente, M (2023). Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. Energies 2023, 16, 1651.

FIGURE 8. Control Network Three – Tier Architecture

[Reference:] Wandera, M., Jonasson, B., Benoit, J., Formea, J., Thompson, T., Tang, Z., Grinberg, D., Sowada, A., Andreou, D., Ruchti, T., Elwell, P., & Groat, J (2016). “Cybersecurity considerations for electrical distribution systems”. Eaton.

LIST OF EQUATIONS

EQUATION 1. Scenario Vulnerability Calculation Model

EQUATION 2. FDIA Attack Mathematical Model

EQUATION 3. Firewall First Mathematical Model

EQUATION 4. Firewall Second Mathematical Model

LIST OF ABBREVATIONS

SCADA	Supervisory Control and Data Acquisition
IT	Information Technology
ICS	Industrial Control System
FDIA	False Data Injection Attack
DM	Data Mining
OT	Operational Technology
PMU	Phasor Measurement Unit
DER	Distribution Energy Resource
RTU	Remote Terminal Unit
MTU	Master Terminal Unit
DCS	Distributed Control Systems
IoT	Internet of Things
HMI	Human – Machine Interface
AI	Artificial Intelligence
ARM	Association Rule Mining
PLC	Programmable Logic Controller
DoS	Denial of Service
TSO	Transmission System Operator
DSO	Distribution System Operator

PCN	Process Control Network
FSI	False Setting Injection
FCI	False Command Injection
MiTM	Man – in – the - Middle
IDS	Intrusion Detection System
SE	State Estimation
SM	System Monitoring
ARM	Association Rule Mining
AMI	Advanced Metering Infrastructure
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
PLCC	Power Line Carrier Communication
LAN	Local Area Network
DMZ	Demilitarized Zone
VPN	Virtual Private Network

1. INTRODUCTION

Modern distribution systems face a growing threat from cyberattacks, which can cause severe damage to equipment, power outages, financial losses, and data compromise. Within Industrial Control Systems (ICS), distribution systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), sensors, and actuators.

Understanding protective measures from Information Technology (IT) sector is crucial for proper protection inside low-voltage Operational Technology (OT) sector. Attack vectors, categorized into various types, target crucial components like SCADA systems, which control data and monitor industrial processes, making them primary targets for cyberattacks. Strong cybersecurity measures are needed to protect from potential threats, especially False Data Injection Cyber Attacks (FDIA).

Having real-time data about energy use and power flow improves how we manage energy, enhance security, and optimize sources in Smart Grid operations. The Smart Grid, which combines modern technology with power systems, has transformed how we control electricity distribution. However, ensuring proper cybersecurity is crucial, especially in protecting the communication networks that carry vital control information.

To counter these threats, systematic defensive approaches have been developed, emphasizing continuous assessment and security training for network maintainers. Strategies such as firewalls, network segmentation, and event management play a key role in defense. Additionally, a universal defense algorithm helps identify anomalies and apply appropriate defense measures.

2. DISTRIBUTION SYSTEM VULNERABILITIES

We define a system as the wide area interconnected, computer communication networks linking the control center and substations level networks. The vulnerability of a distribution system is the maximum vulnerability level, defined over a set of scenarios. [1]

Every possibly vulnerable point is called access point. It is essentially a port where an intruder can establish a connection to access and damage SCADA system. In assessing potential damage of a vulnerability scenario, these access points are used. It is possible that many potential damages arise from a vulnerability scenario. In that case, these damages are summed over a certain set. This can be expressed in a mathematical expression, shown in Equation 1.

$$V(i) = \sum_{j \in S} \pi_J \ x \ \gamma_j$$

EQUATION 1. Scenario Vulnerability Calculation Model

In Equation 1, π_j is the steady-state probability of SCADA system attack, through access point j. On the other side, γ_j is the damage level that a distribution system has experienced.

Cyberattacks are a threat to the distribution system due to their reliance on open data flows and remote access. Unlike transmission systems, distribution, including distributed generation and customer devices, are being more and more interconnected, introducing new layers of risk to the broader electricity ecosystem over time. Many kinds of cyber-attacks can be harmful for the data and security for communication of smart grids, including False Data Injection Attacks (FDIAs), Distributed Denial of Service (DDoS) attacks, topological attacks, and overloading attacks. [2]

These vulnerabilities are getting more apparent by the growth of network-connected devices, systems, and services in the industrial Internet of Things (IoT). While these advancements offer significant benefits, the security standards of IoT devices, have not kept pace with the rapid innovation and deployment in the field. As a result, the threats from cyberattacks continue to evolve, posing significant challenges to the security of distribution systems.

To address these vulnerabilities effectively, it is essential to understand protective measures from the Information Technology (IT) sector. While operational technology (OT), particularly low voltage distribution systems, have unique security requirements, IT security strategies can provide valuable insights and approaches for protecting the OT sector. By collaborations between public and private stakeholders, including energy grid operators, technological developers, and customers, critical protection infrastructure can be properly developed. System operators have to ensure that the transferred data remains available when needed, has high integrity (meaning it is not altered in an unauthorized manner), and is kept confidential to ensure that potential attacks will not exploit obtained information for any future attacks. [3]

2.1. Communication Infrastructure in Distribution Systems

In distribution systems, communication plays a crucial role as power grids become more digitalized. These systems consist of an office network and a process control network (PCN). This is depicted in Figure 1. The office network handles standard corporate tasks like email traffic and data processing, while the PCN connects the control room with substations and field devices.

Control messages are interpreted by programmable logic controllers (PLCs) and transmitted to the process layer. The control room contains essential components like a human-machine interface (HMI) and a database (DB) server. Ideally, data exchange between the office network and PCN should occur through a dedicated server to ensure security.

However, in reality, these networks are often interconnected, increasing vulnerability. This interconnectivity, sometimes facilitated by virtual private networks (VPNs), poses significant security risks. Incidents like the Ukraine attacks have demonstrated the dangers of such connections. The transmission of power is supervised by transmission system operators (TSO), while the distribution of power is carried out by distribution system operators (DSO). [4]

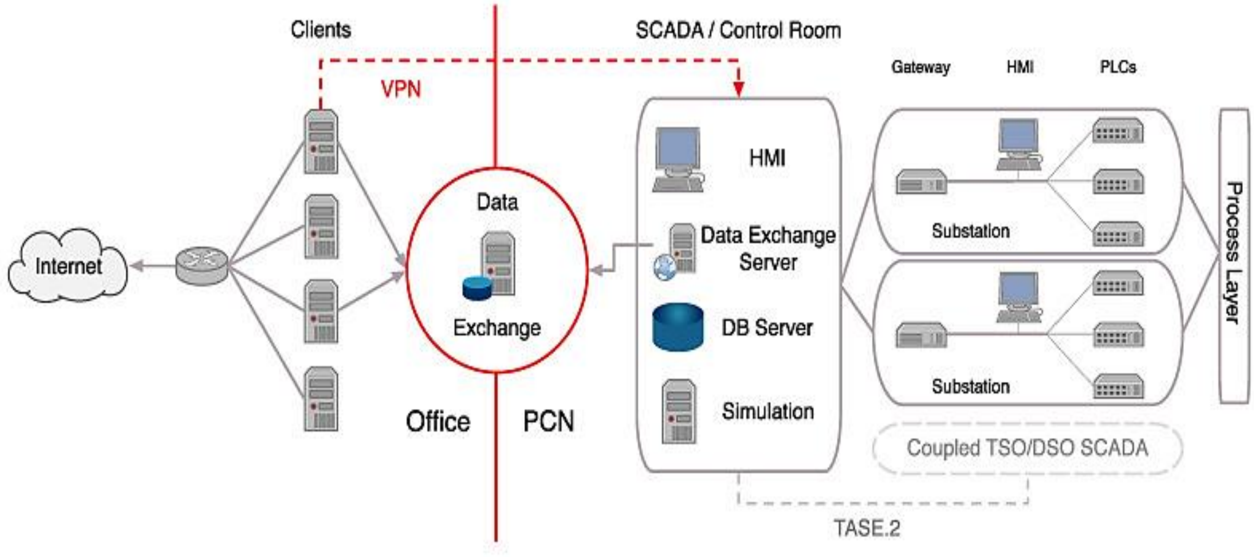

FIGURE 1. A Graphical Representation of a TSO/DSO Network

2.2. Smart Grid Network Structure under Cyberattacks

Various components like dispatcher sources, power electronic converters, communication cables, and loads comprise the physical layer of the grid. System protection measures are employed to counter physical layer threats. The cyber layer, on the other hand, consists of communication channels bridged among sources for data transfer. Networked converters are separated by large distances in cyber-connections to reduce costs, but this can pose security risks.

Centralized control strategies require large computations and communication over a wide area, making them impractical. On the other hand, fully decentralized solutions face challenges in maintaining tight coupling between unit operations. A hybrid cyber-layered microgrid with secondary, primary, and tertiary controllers offers a solution, enhancing coordination and efficiency. [2] The distributed control topology, with its lower communication needs and better scalability, presents advantages over centralized approaches.

Cooperative secondary controllers and a distributed communication layer enable enhanced performance and information exchange among units. Tertiary control handles power management and system optimization.

Smart grid's reliance on SCADA systems, IoT devices, and different communication protocols makes it susceptible to cyber threats. Wireless communication technologies like Zigbee and WiMAX, alongside well-known wired options like PLC, play a vital role in securing data transmission within the grid itself. [5]

In Industrial Control Systems (ICS), three main security objectives include: availability, integrity and confidentiality. [6] Maintaining security and privacy in information exchanges between customers and control centers is crucial, given the potential impact of malicious attacks. The hierarchical architecture of the smart grid network, represented in Figure 2, ensures connectivity while allowing for localized control and management. Ongoing research focuses on vulnerabilities in key protocols and infrastructure components to develop security measures for the smart grid.

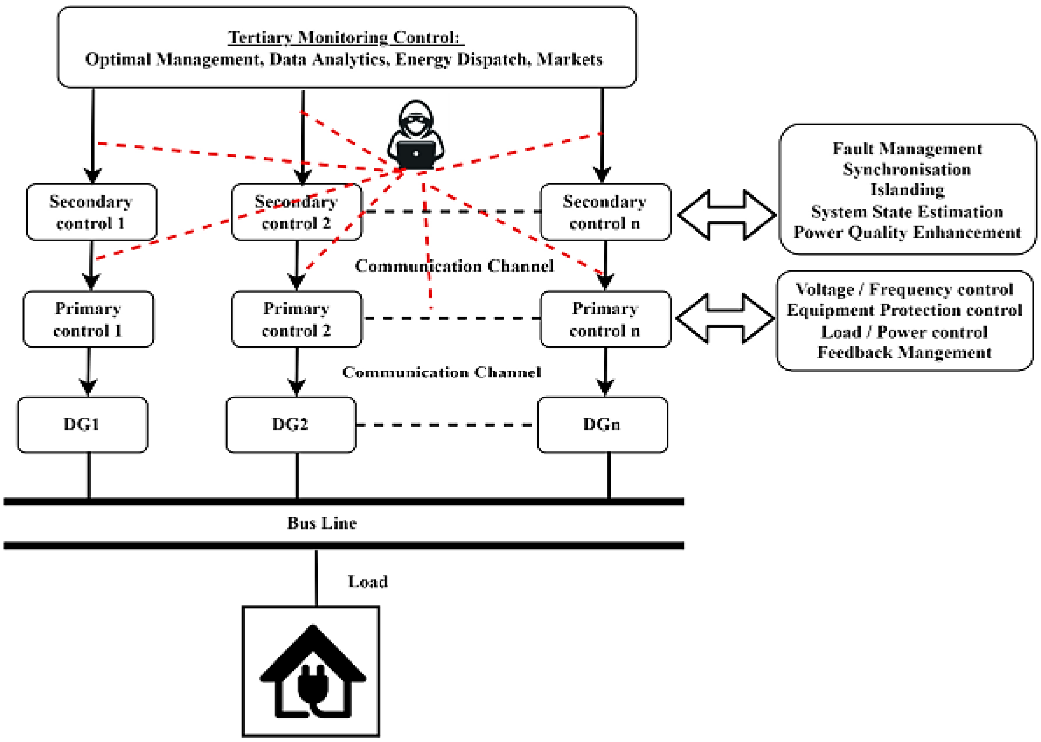

FIGURE 2. Hierarchal Cyberattack Control Blocks in a Microgrid

3. ATTACK VECTORS

A variety of attack vectors that target multiple resources in control systems can give lead to an increase in asynchronous attacks over an extended period of time and could target multiple weaknesses within a control system environment. [7] These vectors represent a path or a tool which an entity can use to gain access to a device or control network. This can be used to deliver a malicious attack. [8] A few examples of attack vectors affect a network are shown in Figure 3.

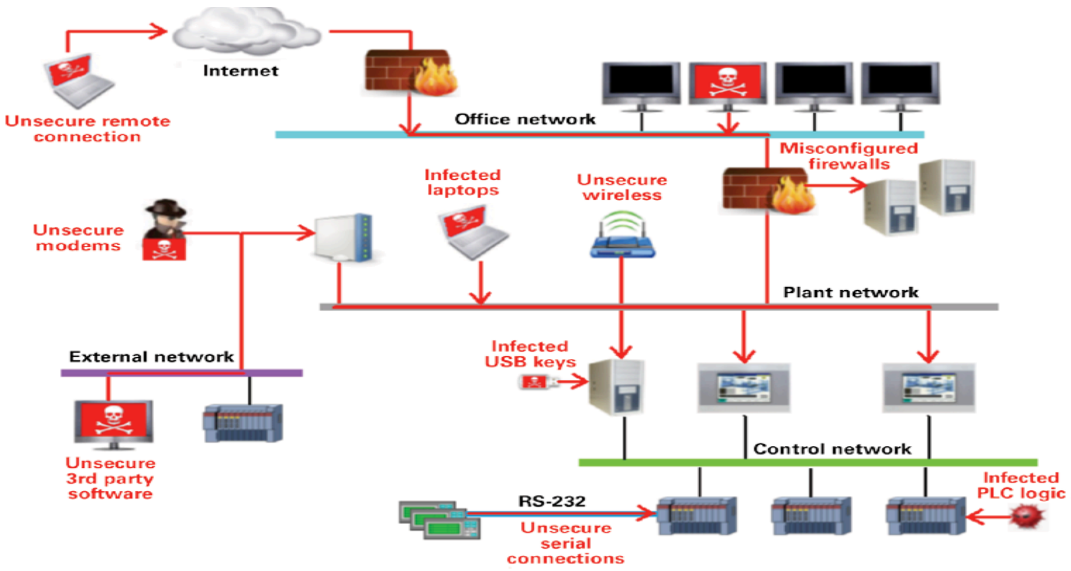

FIGURE 3. Different Paths an Attack Vector can take to the Control Network

Figure 3 represents following paths:

- Access from external users through internet
- Badly secured wireless routers or wired modems
- Improperly configured firewalls
- Infected laptops, USB keys or PLCS's outside of the network
- Insecure serial links

Each attack vector poses a significant threat to ICS security, increasing the need for quality defense measures, including intrusion detection systems, secure network configurations, employee training on cybersecurity, and regular security checkups and updates to mitigate the risks.

3.1. CYBERATTACK TYPES

After inspecting attack vectors, the aspect of many different cyberattack types can be grasped. Inside of ICS infrastructure, particularly distributed generation, False Data Injection Attacks (FDIA) are extremely common. Denial of service (DoS), replay, jamming, topological, overloading, resonance, Man in the middle, and other stealthy attacks are present as well. In addition, an effective defensive strategy requires an understanding of attack type on an ICS. [9]

Malicious attacks include malware - viruses in general, spread through the device using a malicious program. Trojan horse is the most severe one. Additionally, worms are spreading through the device without user interaction, while spywares change configuration of device.

Additionally, at a substation, measurement-based attacks are a common attack type. Other attack types include BlackEnergy, Unauthorized Access Attacks, Database and SQL Data Injection Attacks, as well as Social Engineering Attacks and are also linked to ICS structure.

3.1.1. False Data Injection Attacks (FDIA)

False Data Injection Attacks (FDIA) represent a significant threat to the security of smart grid systems. These attacks target the integrity of data transmitted within the grid’ infrastructure, manipulating sensor readings to deceive control systems and operators.

By injecting false data into the network, attackers can compromise critical functions such as voltage regulation, current control, and power distribution. This means that FDIAs can also target the operation of the distribution management system. [10]

In smart grid systems, ICS play a crucial role, integrating physical industrial processes with SCADA systems, smart sensors, and the Internet of Things (IoT). The use of sensors and networked devices in these systems makes them vulnerable to FDIA attacks, which can lead to disruptions in grid operations and compromise system stability. FDIA can be modelled mathematically in the following form, shown in Equation 2:

$$FD = D_{i,j} + F_{i,j}$$

EQUATION 2. FDIA Attack Mathematical Model

In this equation, $D_{i,j}$ is the original dataset, while $F_{i,j}$ is the injected data. [2] The injected data combines with the original data and the false data is generated. $F_{i,\ j}$ can be:

- Deleted data from the original dataset

- Changed data from the original dataset

- Fake data added to the original dataset

FDIA attacks can manifest in various forms, including false setting injection (FSI) and false command injection (FCI). These attacks can disrupt system behavior, compromise control processes, and sabotage device configurations, leading to safety hazards and inefficiencies.

Detecting FDIA attacks poses a significant challenge for smart grid security. Attackers can exploit vulnerabilities in the system architecture and exploit knowledge of the network topology to evade detection and launch stealthy attacks.

Effective defense against FDIA attacks requires robust security measures, including advanced anomaly detection algorithms, real-time monitoring systems, state estimation and secure communication protocols. Additionally, ongoing research is needed to develop resilient cybersecurity strategies capable of reducing the threats posed by FDIA attacks in smart grids.

3.1.2. Denial of Service (DOS) Attacks

In distribution systems, DoS attacks pose a significant threat by flooding the system with a large amount of traffic. This traffic is designed to exhaust system resources, making it unable to respond to legitimate user requests. When a DoS attack occurs, essential functions within the distribution system can become inaccessible, leading to disruptions in operations and potential service outages. For example, an attacker can conduct a distributed denial-of-service (DDoS) attack by making millions of smaller packets to bombard a target. [11]

Critical processes like voltage regulation and load balancing may be compromised, impacting the stability and reliability of the distribution network. DoS attacks can target various distribution system components, including SCADA systems, communication networks, and smart grid devices.

These attacks can be launched remotely in order to disrupt normal system operations or cause financial losses to utility providers. Detecting and mitigating DoS attacks in distribution systems requires robust cybersecurity measures, including intrusion detection systems, firewalls, and network traffic analysis tools. Additionally, proactive measures such as regular security assessments and employee training can help organizations better defend against DoS attacks.

3.1.3. Man – in – the - Middle (MiTM) Attacks

Man-in-the-Middle (MitM) attacks are a serious threat, especially in ICS networks, where they can have terrible consequences. In these attacks, the threat actor intercepts communication between devices, positioning themselves as a middleman without the knowledge of the communicating parties. By exploiting weaknesses in network protocols, attackers can manipulate routing tables to route all network traffic through their own compromised device.

This allows them to observe, capture, and modify sensitive data exchanged between legitimate devices. Once in control, attackers can manipulate control data, inject false information into critical databases, and even prevent alarms from being triggered, all while maintaining the appearance of normal network communication. MitM attacks are particularly dangerous in ICS environments due to common vulnerabilities like weak authentication protocols and poor firmware integrity checking, which attackers can exploit. In these types of attacks, an attacker is able to intercept, relay packets, or even inject new ones. [12] Figure 4 gives a graphical overview of MiTM attack.

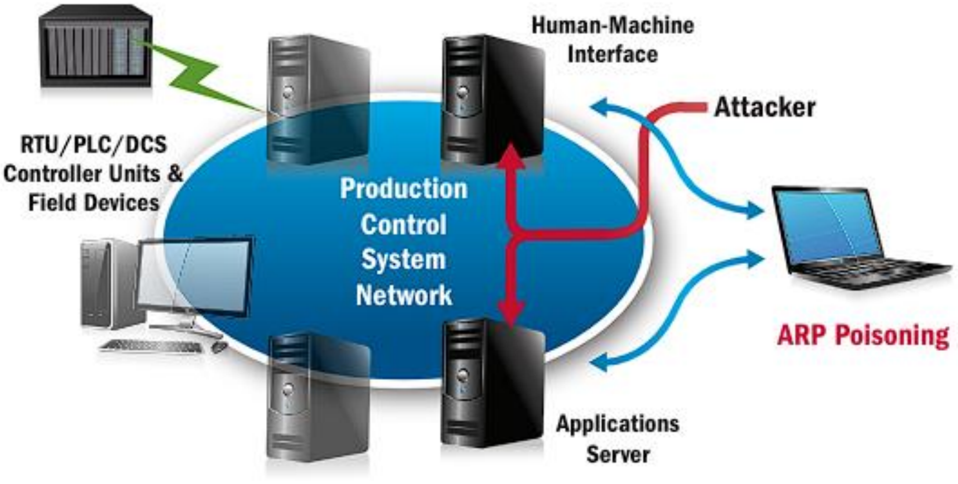
Human-Machine Interface
Attacker
RTU/PLC/DCS Controller Units & Field Devices
Production Control System Network
ARP Poisoning
Applications Server

FIGURE 4. Graphical Representation of MiTM attack

3.1.4. Malware Attacks

Malware attacks compromise distribution system integrity and security. Common types of malware include viruses, Trojan horses, worms, and spyware, each with the potential to disrupt operations and steal sensitive data. These malicious software programs can infiltrate distribution systems through various vectors, including email attachments, infected websites, and external devices like USB drives. Once inside the network, malware can spread rapidly, affecting multiple devices and compromising system stability and performance. [8]

To mitigate the risk of malware attacks, it's essential to implement robust security measures such as antivirus software and firewalls across all systems connected to the distribution network. Regular updates to antivirus definitions and security patches help safeguard against emerging malware threats. Additionally, user education and awareness training can help prevent inadvertent installation of malware through phishing scams or deceptive websites.

3.1.5. Measurement – Based Attacks

Measurement-based attacks lead to misinformation and compromised system operations. Attackers inject falsified measurements into the substation's data stream, deceiving system operators and causing incorrect decisions. Traditional intrusion detection systems (IDS) deployed at control centers may struggle to detect these attacks before they compromise state estimation processes. This is because IDS often cannot identify falsified measurements hidden within packets.

The attack lifecycle typically involves multiple stages, starting from the injection of malicious code into firmware or updates at the network, leading to the installation of backdoors at substation devices. Backdoor are represented by red boxes [13] , shown in Figure 5.

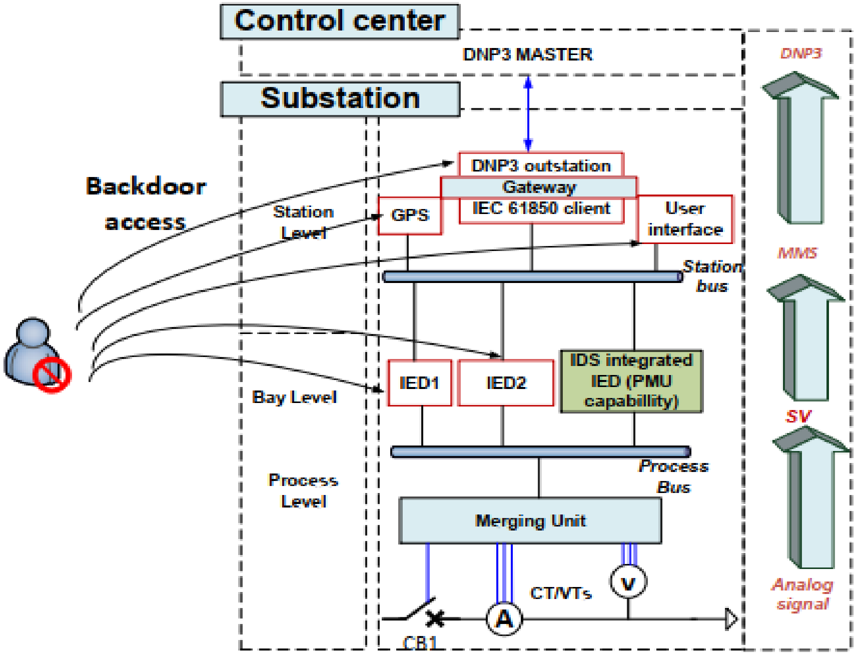

FIGURE 5. Measurement – Based Attack Example

Attackers may also attempt to steal signing keys or certifications to gain unauthorized access to different intelligent electronic devices. Once in control, attackers can steal sensitive information, falsify devices configurations, and inject malicious measurements into the substation data flow, disrupting system operations and compromising grid reliability.

3.1.6. Other Attack Types

Other attack types include BlackEnergy, Unauthorized Access Attacks, Database and SQL Data Injection Attacks, as well as Social Engineering Attacks and are also linked to ICS structure.

- **BlackEnergy** is a significant threat to organizations with Human-Machine Interface (HMI) systems directly connected to the internet. Its deployment often begins with social engineering tactics, tricking users into opening malicious attachments or emails, leading to installation of Trojan horses or infected files. Additionally, it is known that BlackEnergy backdoor is carefully constructed for the specific event. [14] Once inside system, BlackEnergy modular nature allows for execution of various attacks and communication with command and control servers.

- **Unauthorized Access Attacks** exploit vulnerabilities in control system architectures, particularly those with remote connections through publicly accessible networks or modems. These attacks, facilitated by low security measures and weak authentication protocols, can provide intruders with remote access to critical systems, allowing them to compromise devices.

- **Social Engineering Attacks** leverage human psychology and trust to deceive individuals into giving away sensitive information or performing actions that compromise security. Through emails or impersonation tactics, malicious actors target control system managers and operators, aiming to introduce malware into ICS environments. It has thus become increasingly more important to segregate connections between business functions as an email and ICS operations. [7]

- **Database and SQL Data Injection Attacks** target the interconnected nature of Industrial Control Systems (ICSs) and their reliance on databases for data storage and retrieval. These attacks exploit vulnerabilities in web-enabled applications and SQL databases, allowing attackers to inject malicious code and manipulate sensitive data. The consequences of such attacks extend beyond data corruption, potentially disrupting essential operational processes. These attacks are classified into First and Second Order Injection Attacks. [15] In first order attacks, the attacker receives the result immediately, while in the second order injection attacks, the code is still inserted by the attacker, but not activated immediately.

4. CYBERSECURITY DEFENSIVE STRATEGIES

Just like in traditional IT systems, defending ICS relies on a layered approach known as "defense in depth," which combines technology, people, and operational strategies to create multiple barriers against cyber threats. These defenses include firewalls, intrusion detection systems, and antivirus software, alongside physical security measures and proper training to reduce and identify cyberattacks. Smart Grid cybersecurity focuses on protecting communication networks to prevent unauthorized access and exposure of sensitive data like control commands and equipment settings.

While Smart Grid connectivity enables real-time data exchange, it also introduces vulnerabilities that can be exploited, emphasizing the need for robust cybersecurity measures. Prioritizing data protection helps with adjusting security measures to safeguard critical assets and sensitive information within the Smart Grid, ensuring resilience against cyber threats.

4.1. Defensive Algorithm

The defensive algorithm is an agreed protocol for determining potential cyberattacks. Its goal is to help with reaching recovery mode as fast as possible and is made of three main components: [13]

1. Anomaly detection,

2. Attack similarity, and

3. Detection system on Human-Machine Interface (HMI).

Anomaly detection involves identifying deviations from expected behavior within the system, alerting operators to potential threats. Attack similarity assesses incoming data for similarities to known attack patterns, mitigating of malicious activities. The detection system on HMI provides real-time monitoring and reporting directly to operators, allowing fast decision-making. By combining these components, the defensive algorithm enhances the system resilience against cyber threats, enabling proactive defense and efficient recovery in the event of an attack.

4.2. CYBERATTACK DETECTION METHODS

Cyberattack detection methods in smart grids focus on the utilization of Internet of Things (IoT) technologies and Artificial Intelligence (AI) algorithms. Smart grids employ IoT technologies to monitor environmental changes and physical conditions, with System Monitoring (SM) being a crucial application. However, FDIAs are still a significant threat to smart grids due to their nature. AI category includes various Machine Learning methods, including Supervised, Unsupervised, Semi-Supervised, and Reinforcement algorithms, to detect FDIAs. [2]

Supervised learning involves labeled training data, while unsupervised learning methods collect data points without labels. Semi-supervised models utilize both labeled and unlabeled data, and reinforcement learning employs reward-based error estimation. These models are classified into Semi-supervised classification and clustering which has much better accuracy than traditional supervised and unsupervised learning techniques. [16] Unsupervised algorithms, recommended for identifying cyberattacks in smart grids, analyze unlabeled data to detect anomalies.

Supervised techniques, although more effective, come with high computing costs and rely on labeled data, which is mostly limited in real-world. Large amounts of unlabeled data in smart grids are a challenge, leading to data loss and algorithm failure. However, unsupervised techniques offer a promising approach for detecting cyberattacks which cannot be observed, providing fast detection capabilities. It is known that corrupting voltage measurements has a much greater impact on state estimation than corrupting active and reactive power measurements.

The main goal of unsupervised learning techniques, is to recognize patterns of structures or relevant information in unlabeled data. [17] Among unsupervised algorithms, Association Rule Mining (ARM) identifies relationships between data attributes, collecting groups of data points with similar characteristics.

4.2.1. Association Rule Mining (ARM)

Association Rule Mining (ARM) is an unsupervised learning technique used to identify relationships between data items in smart grids. ARM is advantageous for its ability to extract rules that help detect faults and FDIAs in smart grids. Generally speaking, ARM finds correlation between frequent datasets and generates association rules from the most frequent ones. [18]

The process involves preprocessing and combining multiple datasets, including outage records, load data, and weather information. These datasets are labeled and processed to extract useful features for analysis. ARM algorithms are then applied to generate rules, which indicate the relationships between variables. These rules are evaluated to filter out important patterns that could indicate cyberattacks affecting the smart grid, as depicted in Figure 6. [2]

Figure 6 outlines the approach for detecting cyber-attacks in smart grids using ARM. It begins with the collection of data from various devices, including smart meters and telemetry units, which sense the current and voltage generated by Distributed Generation (DG) units. After preprocessing, heterogeneous datasets are integrated into a single source to identify recurring attacks on DG units.

Data related to cyber-attacks, such as FDIAs, are then selected for further analysis. Through data transformation, the selected data is formatted to achieve pattern extraction using various ARM algorithms. The extracted patterns are evaluated on metrics like support and confidence.

Various ARM algorithms, such as:

- Apriori – lattice approach, scanning for dependencies at each level (subset) of lattice [19]

- FP-Growth – finding lately frequent patterns, and using them for mining long and short patterns

- Prefixspan – project sequence recursively into a set of smaller databases

- Spade - decomposing the original problem into smaller sub-problems [20]

, are used to mine frequent patterns and association rules from the data. Each algorithm has its advantages and limitations in terms of processing speed, space utilization, and computational cost.

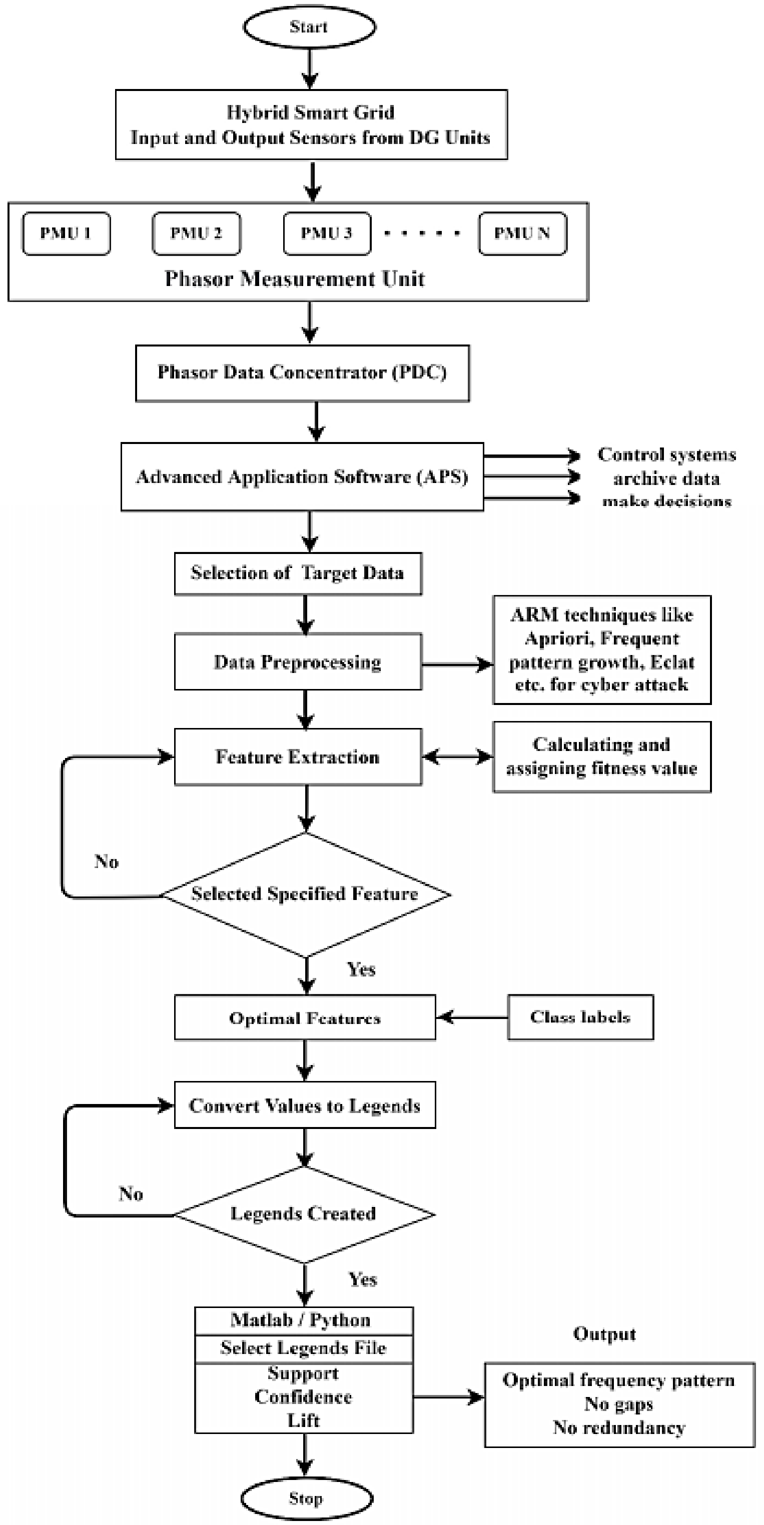

FIGURE 6. Flow Chart for ARM Cyberattack Detection inside Distribution Systems

4.2.2. Clustering

Clustering is a method used to categorize non-similar data into multiple clusters based on similarities, finding unusual patterns of activity in a network. It is useful in identifying data integrity attacks in Advanced Metering Infrastructure (AMI), an important component of smart grids. These attacks can lead to various problems, including energy loss and infrastructure damage. Detection systems for these attacks rely on mentioned methods like association and supervised algorithms. However, these methods struggle with fluctuating datasets, resulting in low detection accuracy and the potential for malicious data to go past the security measures. [2]

Clustering offers a solution by achieving high detection accuracy without predefined thresholds or external information, making it suitable for real-world applications.

Using cluster analysis, clusters of related data can be identified, enabling the detection of attacks that might otherwise be overlooked. Various clustering techniques, such as:

- **K-means** – the most used algorithm, clustering with random initialization cluster centroids [22]

- **K-Medoids** - more robust to noise by using real points as cluster centers, and

- **DBSCAN** - categorizing measurement data in power systems, requires only one input [23]

, can be employed to achieve correct identification, which leads to successful attack detection.

In the context of cyber threat detection in smart grids, Figure 7 presents a flowchart illustrating the process of clustering-based detection. [2]

In SCADA systems, this method follows a similar approach to ARM detection technique. [23] It involves data selection, preprocessing, transformation, interpretation, and evaluation. Attacked and normal data lead to the formation of different clusters.

By training personnel, it becomes possible to distinguish between attacked and normal data, and thereby detecting the cyber threats. However, as the dimensions of measurements increase with the size of the power system, clustering can become challenging in cases of computations.

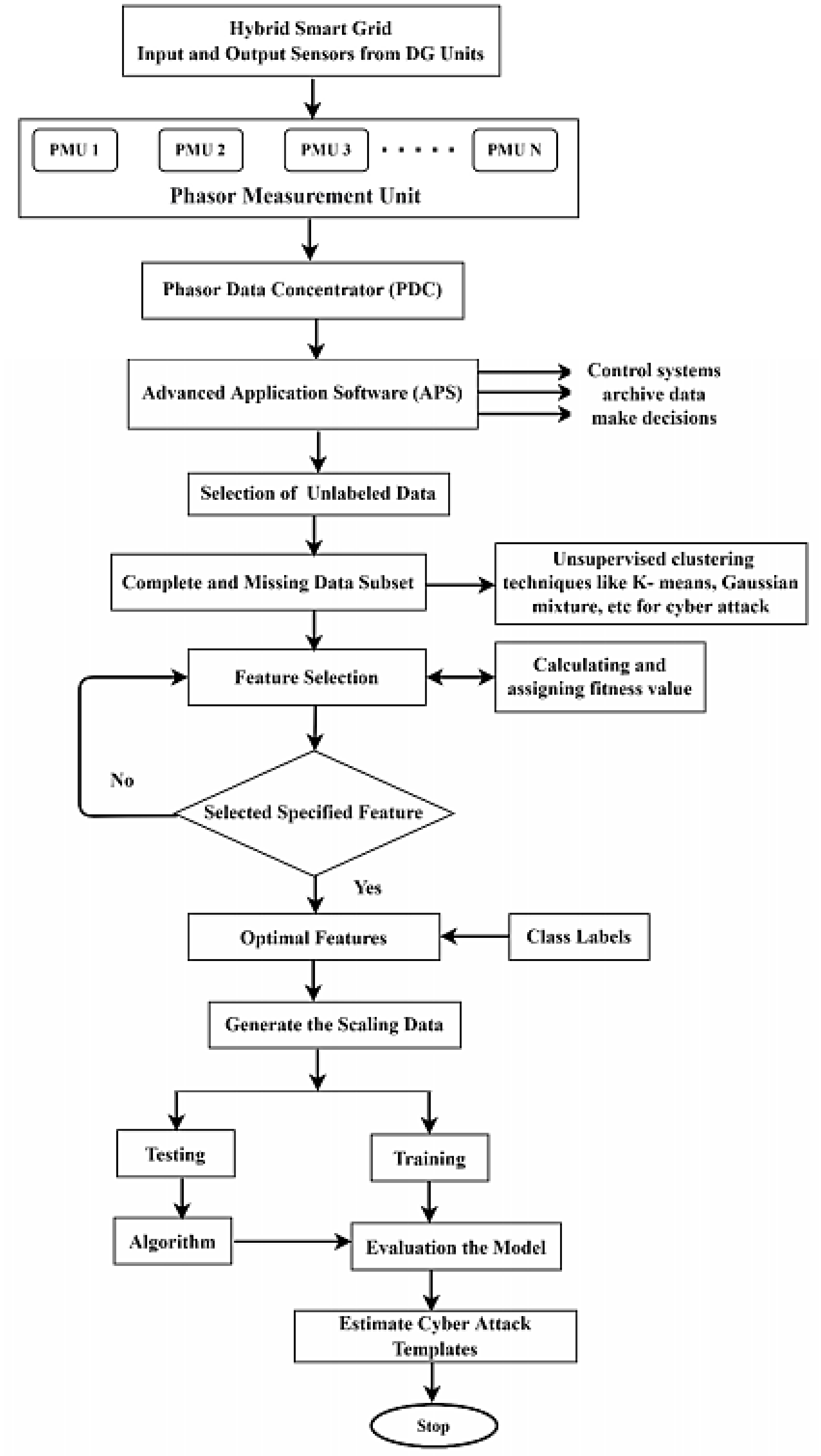
Hybrid Smart Grid
Input and Output Sensors from DG Units
PMU 1
PMU 2
PMU 3
PMU N
Phasor Measurement Unit
Phasor Data Concentrator (PDC)
Advanced Application Software (APS)
Control systems
archive data
make decisions
Selection of Unlabeled Data
Complete and Missing Data Subset
Unsupervised clustering techniques like K- means, Gaussian mixture, etc for cyber attack
Feature Selection
Calculating and assigning fitness value
No
Selected Specified Feature
Yes
Optimal Features
Class Labels
Generate the Scaling Data
Testing
Training
Algorithm
Evaluation the Model
Estimate Cyber Attack Templates
Stop

FIGURE 7. Detecting Cyberattacks in Distribution Systems using Clustering

4.3. PARTICULAR DEFENSIVE APPROACHES

A comprehensive cybersystem recovery strategy needs to be studied, so that it can recover the cyber system of substations, control center, and SCADA communication after attack occurs. [13]

Defensive measures in securing communication networks and control systems involve strategies like firewalls, network segmentation, and access control. Firewalls, including packet filter or boundary firewalls, host firewalls, and application-level proxy firewalls, control data flow and block unauthorized access. Network segmentation isolates critical components from the wide network, protecting from potential threats. Access control, both physical and logical, plays a crucial role in restricting interactions between network zones, minimizing vulnerabilities.

Independent communication networks offer improved security by eliminating external links and dependencies, although at higher costs. Combining Power Line Carrier Communication (PLCC) and Local Area Network (LAN) technologies provides flexibility and security to smart grid networks, reducing capital costs. Customer care or call center architectures enable secure information exchange between users and service providers. Strong passwords, regular data backups, and the installation of firewalls and antivirus protection are essential components of cybersecurity, helping prevent unauthorized access and data breaches.

4.3.1. Firewalls

Firewalls ensure safe communication channels within ICS networks by implementing strict rules. The firewall model involves denial or access of each rule and monitoring malicious packets traveling through each firewall. [13] They selectively block or allow data flow between different network segments. Understanding the devices and services within a network is essential for configuring firewalls effectively. Different types of firewalls offer different levels of protection.

The main security mechanisms have been implemented at the network boundaries where there is a security gateway. This gateway includes a firewall, an IDS and an anti-virus mechanism. [24]

Packet filter or boundary firewalls operate at the network layer, analyzing packets based on port numbers and protocols. Host firewalls protect individual devices by controlling incoming and outgoing traffic, typically found on mobile devices and computers connected to an ICS. Application-level proxy firewalls offer high security by hiding devices at the application layer. Stateful inspection firewalls operate at multiple layers, ensuring secure packet transmission by authenticating users and analyzing packet content. [8] SCADA hardware firewalls by detect abnormal behavior within the control network, triggering alarms to prevent potential risks.

Firewalls can be expressed in two ways, depicted in Equation 3 and Equation 4, both shown below:

$$p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}$$

EQUATION 3. Firewall First Mathematical Model

In Equation 3, $p_{i,\,j}^{fp}$ represents probability of malicious packets travelling through a firewall rule; $f_{i,\,j}^{fp}$ is the frequency of packet travel, while $N_{i,\,j}^{fp}$ is the total record of firewall rule j.

$$p_i^{fr} = \frac{f_i^{fr}}{N_i^{fr}}$$

EQUATION 4. Firewall Second Mathematical Model

In Equation 4, p_i^{fr} represents probability of malicious packets being rejected; $f_{i,}^{\ fr}$ is the number of rejected packets, while N_i^{fr} is the total number of packets in the firewall logs.

4.3.2. Network Segmentation

Network segmentation involves dividing the smart grid network into separate zones or segments to minimize the impact of security breaches and prevent attackers from moving further inside the network. [25] This segmentation is achieved by using firewalls to create DMZs (Demilitarized Zones) that isolate critical components from the traditional business IT network.

The segmentation, shown in Figure 8, follows a three-tier architecture, with DMZ situated between the core network and the isolated control system network. Each segment is designed to control access, resist DOS attacks, shield other network systems, and protect network traffic integrity. [8]

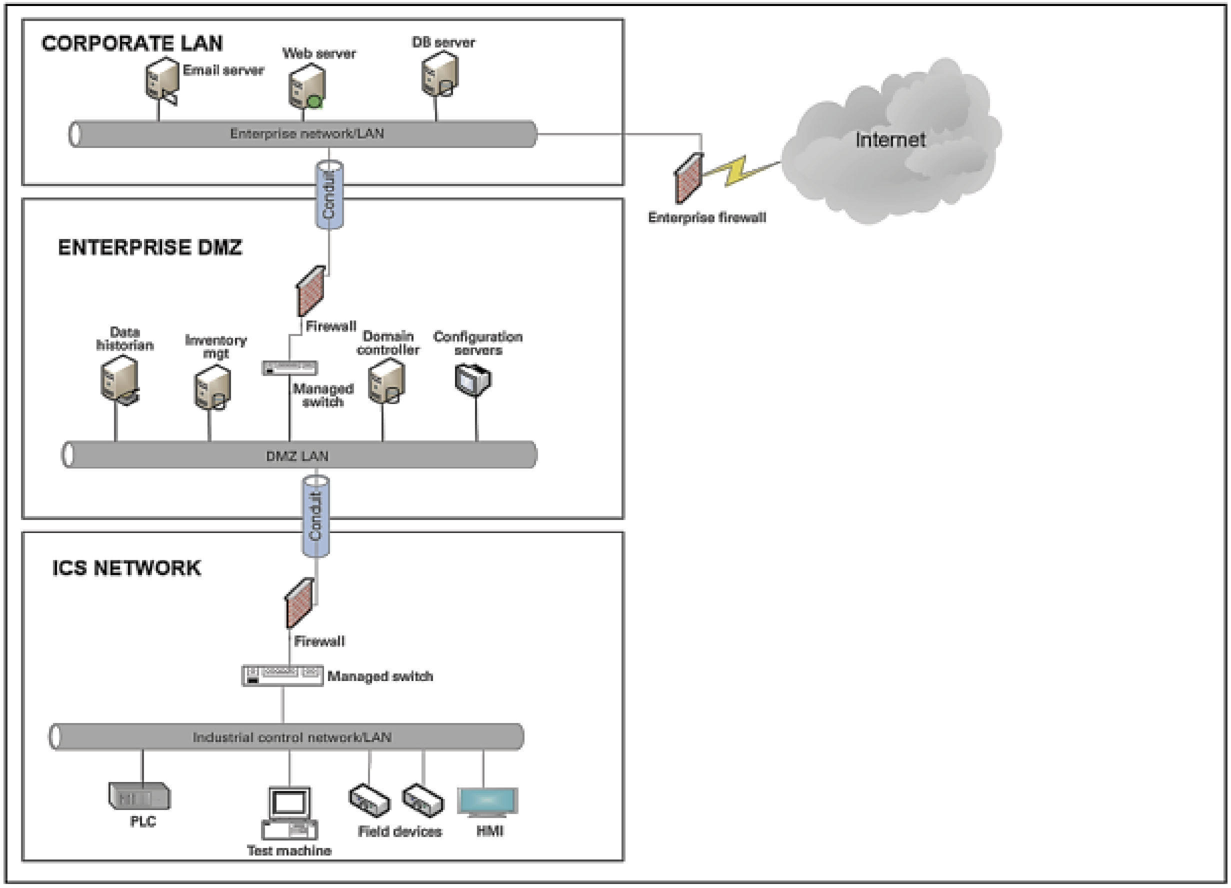

FIGURE 8. Control Network Three – Tier Architecture

Access control, both physical and logical, is crucial and should be implemented to prioritize interactions between the zones. Proper network segmentation minimizes the impact of cyberattacks on control system reliability and functionality.

4.3.3. PLCC and LAN

PLCC and LANs work together to enhance protection against cyberattacks in distribution systems. PLCC involves transmitting data over electric power lines, allowing for simultaneous transmission of AC electric power and data. This technology offers a cost-effective solution for transmitting high-speed data over existing power lines. However, this comes with technical challenges, such as radio interference and frequency limitations. LANs obtain localized data by using a combination of cables, switches, routers, and access points. [26] They allow devices to connect to internal servers, share data, and access shared resources.

By leveraging PLCC and LAN technologies, distribution systems can establish secure communication channels, minimizing the risk of cyberattacks. Additionally, LANs facilitate the network segmentation, done using logical grouping of devices and the control of their access.

4.3.4. Security Training and Constant Assessment

It is crucial to properly train ICS network administrators, as well as users to ensure the secure system and safety of those who depend on it. Vulnerability assessments are crucial for identifying issues and evaluating effectiveness of network defenses. These assessments cover various aspects, including monitoring capabilities, device configurations, connectivity and many more. A structured programs are established for conducting assessments, involving both in-house resources and qualified third-party organizations. Assessments should follow a clearly defined methodology that addresses physical security, network security, host security, and application security.

Mathematical models can be used to represent risk assessment. A variety of models can be used, based on Bayesian network, fault trees, and event trees. [27]

Patch management planning and procedures are crucial components as well, requiring timely awareness of issues and appropriate action. A regular patch deployment schedule should be established, considering the historical frequency of issues for each component. The analysis of the distribution network under normal operating condition or in the fault recovery process is carried out, and the reliability assessment of the distribution network for cyberattacks is constructed. [28]

Vulnerability information from various sources, such as advisories and public databases should be regularly reviewed. Additionally, the process should include preparation, scheduling, testing, and procedures for patch deployment, ensuring minimal disruption to the control system. If a patch cannot be deployed safely, compensating controls should be explored to mitigate the risks.

4.3.5. Additional Measures

Besides already discussed measures, countless other measures can be taken in order to reduce the chance and severity of cyberattack in a distribution system.

- **Customer Care Architecture:** This architecture ensures secure online communication between customers and service providers by a call center, minimizing intrusion risks. [29]

- **Strong Passwords**: Creating complex passwords and regularly changing them enhances online security by making it harder for unauthorized users to breach them.

- **Secure Computers/Mobiles:** Protecting computers and mobile devices with data encryption, password protection, and security measures prevents unauthorized access and data theft.

- **Regular Data Backup:** Scheduling automatic data backups to external storage devices minimizes the risk of data loss due to system failures or cyberattacks. The staff is in position to access backed-up data from anywhere with an internet connection.

- **Access Limit to Critical Data:** Restricting access to critical data to authorized personnel based on their authority levels minimizes the risk of data breaches and strengthens the overall security.

5. FUTURE CHALLENGES AND CONSIDERATIONS

There are many concerns regarding cybersecurity in distribution systems, which keep arising over the years. One major concern is the susceptibility of traditional and smart grids to human error, mostly due to overworked employees. The importance of maintaining service availability while enhancing security, such as using virtual private networks (VPNs) [2], during attacks is especially important. Future researches must address the unpredictable system parameters and dynamic properties, requiring standardized architectures and technology standards for the smart grid.

Outdated security protocols pose a significant risk, emphasizing the need for new or improved protocols. The emergence of hybrid AC/DC smart grids and microgrids presents additional security challenges due to increased potential points of vulnerability. [3] AI-based detection systems and unsupervised machine learning applications are proposed as strategies to identify and prevent cyberattacks, requiring significant training and education.

The effects of the cyber scenarios presented on utility-scale distribution systems are considered [30]. The exponential growth of network-connected devices in the industrial IoT raises concerns about security standards and the rapid evolution of cyber threats. Collaboration among public and private stakeholders is essential to ensure national security and critical infrastructure protection. Distribution system owners are urged to assess cybersecurity risks and implement supplemental strategies to respond to and recover from cyberattacks effectively.

Furthermore, information technology advancements facilitate the modernization of the conventional energy grid into an integrated platform. [31] Information sharing among industry stakeholders and government agencies is crucial for identifying and mitigating cybersecurity risks in network, hardware, software, and third-party services. Despite the challenges posed by smart technologies, the electric power industry remains committed to stepping up security measures and partnerships to protect the critical infrastructure and ensure grid’s security and reliability.

6. CONCLUSION

Cybersecurity in distribution systems has a goal of addressing an increasing threat of cyberattacks, emphasizing their potential to cause significant damage to equipment, finances, and overall system stability. ICS and OT highlight vulnerabilities of low-voltage distribution systems to various attack vectors, including those targeting SCADA systems. Defensive strategies, including firewalls and network segmentation, are crucial for mitigating the threats and maintaining system integrity.

Additionally, continuous assessment cannot be pointed to enough, as well as security training, and collaboration among companies to effectively tackle cyber threats.

Furthermore, the need for robust cybersecurity measures in the rapidly evolving landscape of smart grids is growing by day. In here, real-time data exchange introduces both opportunities and vulnerabilities. The use of both IoT technologies and AI algorithms offers promising approaches for detecting and preventing cyberattacks.

However, it is essential to remain careful and adaptable as cyber threats evolve over time, demanding for enhancing cybersecurity defensive algorithm, and thereby, the individual defensive measures as well. Integrating cybersecurity defensive measures into network architecture and promoting cyber awareness is crucial for protecting distribution systems against cyberattacks.

As the field of cybersecurity keeps evolving, collaboration, innovation, and proactive defensive approaches will be key to ensuring the security and reliability of distribution systems in the future.

REFERENCES

[1] C. W. Ten, C. C. Liu, M. Govindarasu (2008), “Vulnerability Assessment of Cybersecurity for SCADA Systems,” IEEE Trans. Power Systems, pp. 1836-1846

[2] Pinto, S.J.; Siano, P.; Parente, M (2023). Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. Energies

[3] “Electric Distribution System Cybersecurity Is Critical in Today’s Interconnected Society” (2018). Edison Electric Institute. Washington, D.C.

[4] Krause T, Ernst R, Klaer B, Hacker I, Henze M (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors (Basel). 21 (18):6225.

[5] Burg, A.; Chattopadhyay, A.; Lam, K.-Y. Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-things. 2017. Proc. IEEE 2018, 106, 38–60.

[6] Common Cybersecurity Vulnerabilities in Industrial Control Systems (2011). https://www.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf. Accessed: June 7, 2024

[7] Recommended Practice (2009): Improving Industrial Control Systems Cybersecurity with Defense-In-DepthStrategies,https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf . Accessed: June 7, 2024

[8] Wandera, M., Jonasson, B., Benoit, J., Formea, J., Thompson, T., Tang, Z., Grinberg, D., Sowada, A., Andreou, D., Ruchti, T., Elwell, P., & Groat, J (2016). “Cybersecurity considerations for electrical distribution systems”. Eaton.

[9] NIST.SP.800-82 (2011). Guide to Industrial Control Systems (ICS) Security. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf . Accessed: June 7, 2024

[10] Ahmed S. Musleh, Guo Chen, Zhao Yang Dong, Chen Wang, Shiping Chen (2023), Spatio-temporal data-driven detection of false data injection attacks in power distribution systems, International Journal of Electrical Power & Energy Systems, Volume 145, 108612, ISSN 0142-0615

[11] Bejtlich, R (2013). “The Practice of Network Security Monitoring: Understanding Incident Detection and Response”. San Francisco, CA: No Starch Press, Inc.

[12] Wang, Le; Wyglinski, Alexander M (2014). "Detection of man-in-the-middle attacks using physical layer wireless security techniques: Man-in-the-middle attacks using physical layer security". Wireless Communications and Mobile Computing.

[13] Liu, C. C (2023). “Cyber Security of SCADA, Substations, and Distribution Systems”. Virginia Tech, delivered by Chen-Ching Liu, American Electric Power Professor and Director, Power and Energy Center

[14] iTrust (2016). Analysis Report iTrust-Analysis-001: BlackEnergy - Malware for Cyber-Physical Attacks. Singapore University of Technology and Design, Center for Research in Cyber Security.

[15] Khaleel Ahmad et. Al (2010) / VSRD Technical & Non-Technical Journal Vol. I (4)

[16] Y. C. Padmanabha, Viswanath Pulabaigari, and Eswara B. (2018). "Semi-supervised learning: a brief review." *International Journal of Engineering & Technology*, 7, 81

[17] Ahsan M, Nygard KE, Gomes R, Chowdhury MM, Rifat N, Connolly JF (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy; 2(3):527-555. https://doi.org/10.3390/jcp2030027. Accessed: June 7, 2024

[18] Han, J., Kamber, M., & Pei, J (2012). Data Mining: Concepts and Techniques (Third Edition). Morgan Kaufmann, Elsevier.

[19] Agrawal R. & Srikant R (1994). Fast Algorithms for Mining Association Rules. In Proc. 20th Int. Conf. Very Large Data Bases (VLDB)

[20] Mohammed J. Zaki (2001). SPADE: An efficient algorithm for mining frequent sequences, Machine Learning

[21] Wei Wang, Gregorio Cova, Enrico Zio (2022), A clustering-based framework for searching vulnerabilities in the operation dynamics of Cyber-Physical Energy Systems, Reliability Engineering & System Safety, Volume 222,

[22] M. Emre Celebi, Hassan A. Kingravi, Patricio A. Vela (2013), A comparative study of efficient initialization methods for k-means clustering algorithm, Expert Systems with Applications, Volume 40

[23] Tomlin, Leary Jr.; Farnam, Marsella R.; and Pan, Shengyi (2016), "A Clustering Approach to Industrial Network Intrusion Detection". Information Security Research and Education (INSuRE) Conference. 5. https://louis.uah.edu/insure-conference/INSuRECon-16/Papers/5. Accessed: June 7, 2024

[24] Slay, Jill and Miller, Michael, "A Security Architecture for SCADA Networks" (2006). ACIS 2006 Proceedings. 12. http://aisel.aisnet.org/acis2006/12. Accessed: June 7, 2024

[25] Bouramdane, A.-A (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. J. Cybersecur. Priv, 3, 662-705.

[26] Saini, S., Beniwal, R. K., Kumar, R., Paul, R., & Saini, S. (2018). Modelling for Improved Cyber Security in Smart Distribution System. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(2), 56–59.

[27] Zhou B, Sun B, Zang T, Cai Y, Wu J, Luo H. (2023). Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. Entropy. 25(1):47. https://doi.org/10.3390/e25010047. Accessed: June 7, 2024

[28] B. Chen, Z. Lu and H. Zhou (2018), "Reliability Assessment of Distribution Network Considering Cyber Attacks," 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, pp. 1-6, doi: 10.1109/EI2.2018.8582610.

[29] Olaoye, Godwin & Luz, Ayuns. (2024). Data backup and disaster recovery in the cloud.

[30] Saraswat, Govind, Rui Yang, Yajing Liu, Yingchen Zhang (2020). Analyzing the Effects of Cyberattacks on Distribution System State Estimation: Preprint. Golden, CO: National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy21osti/77941.pdf. Accessed: June 7, 2024

[31] Naveen, Tatipatri & Arun, S. (2024). A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3361039.