SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I9P106

Volume 12 Issue 9, 49-65, September 2025
© 2025 Seventh Sense Research Group®

*Original Article*

# Cybersecurity Threat Modelling for Electric Power System SCADA Control Centers and Substation Automation Systems

Shivakumar V[1, 3], Veena M B[2, 3]

[1]*Smart Grid Research Laboratory, Central Power Research Institute, Bengaluru, India.*
[2]*Department of Electronics & Communication Engineering, BMS College of Engineering, Bengaluru, India.*
[3]*Visvesvaraya Technological University, Belagavi, India.*

[1]*Corresponding Author : shiva@cpri.in*

Received: 04 July 2025 Revised: 06 August 2025 Accepted: 05 September 2025 Published: 30 September 2025

***Abstract*** - *The increasing automation and reliance on Information and Communication Technologies (ICT) in electric power systems, from generation to utilization, introduce significant cyber threats to critical infrastructure. Malfunctions caused by cyberattacks can lead to cascaded effects across multiple sectors, including defence, aviation, and health, potentially resulting in severe consequences. It is essential to address these cybersecurity threats to ensure grid resilience, and a robust threat model is crucial for designing secure control centers and substation automation system architectures. This paper presents a detailed threat model study for typical Supervisory Control and Data Acquisition (SCADA) control center and substation automation system architectures. Utilizing the STRIDE methodology and the CIA triad principles, the authors identified threats and correlated them with ISO/IEC 27001, ISO/IEC 27002, and IEC 62351 series of standards for mitigation plans. The developed framework was applied to a laboratory SCADA Test bed, and the results are discussed. Several reported cyber incidents were reviewed, applicable ISO/IEC 27002 controls were identified, and it was demonstrated how implementing these controls could have prevented them. The study offers inferences and recommendations for mitigating threats with optimal cost, highlighting the critical role of human factors in minimizing cyber incidents within critical infrastructure.*

***Keywords*** - *Control system, Critical infrastructure, Cybersecurity, Risk management, Threat model.*

## 1. Introduction

The increasing integration of Information and Communication Technology (ICT) into electric power system operations aims to enhance efficiency and address the challenges posed by renewable energy sources and Electric Vehicle (EV) charging infrastructure. However, this integration introduces significant cyber threats to critical infrastructure. Unaddressed cyberattacks can lead to power interruptions, loss of sensitive information, environmental degradation, loss of life, economic disruption, and severe impacts on national security. Despite these risks, automation is inevitable for managing growing power demand and the large-scale integration of renewable energy sources. Therefore, effective and cost-efficient mitigation of cyber threats is paramount. In recent years, there has been a surge in cyberattacks targeting critical infrastructures, including the power sector. This trend has spurred increased efforts in developing national and international cybersecurity standards, guidelines, policies, and regulations specific to power systems. Critical infrastructure increasingly relies on Operational Technology (OT), which is rapidly converging with traditional Information Technology (IT) networks, often diminishing or eliminating "air gaps." OT systems comprise bidirectionally communicating field devices that control processes based on real-time parameter monitoring. In the power sector, common OT devices include Remote Terminal Units (RTUs), Feeder/Field Remote Terminal Units (FRTUs), Numerical Protection Relays/Intelligent Electronic Devices (IEDs), and Bay Protection and Control Units (BPCUs) used in substation automation systems. These devices utilize standardized communication protocols, such as IEC 60870-5-104 and IEC 61850, for control operations within the substations and communication with remote control centers, commonly known as Supervisory Control and Data Acquisition (SCADA) Control Centers for Energy Management Systems (EMS) or Distribution Management Systems (DMS). These systems involve extensive use of both OT and IT technologies, with interconnections to third-party communication service providers for information exchange and control via Internet Protocol (IP) with various transport protocols like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). While power sector applications, like those in finance, are vulnerable to IP-based cyber threats, critical infrastructure differs significantly. Unlike non-critical sectors primarily dealing with data exchange, the power sector involves direct control over physical processes. Consequently, due to unique operational demands, conventional IT cybersecurity measures often prove inadequate for critical infrastructure. Key challenges for OT security include the impracticality of frequent patch management and unscheduled downtime. Furthermore, power systems often integrate legacy systems with modern technologies, and asset lifecycles in OT can span 20 to 25 years or more, significantly longer than the typical 3 to 5 years for IT assets. These factors complicate the adoption of standard IT security practices.

Given these complexities, alongside cost, communication latency, and availability requirements, designing resilient SCADA architectures necessitates thorough threat modelling and cost-benefit analysis. Such an approach minimizes cybersecurity risks by focusing on the most critical vulnerabilities. As noted by expert opinions in critical infrastructure security, a strategic approach is essential: rather than attempting to protect "everything" uniformly, resources should be concentrated on the most critical and valuable assets to achieve an optimal defensive posture [1].

Furthermore, leveraging existing cybersecurity standards and best practice guidelines for OT environments is crucial for supporting risk management and establishing robust security programs, avoiding the need to "re-invent" solutions [2]. Effective cybersecurity solutions involve a "Defence-in-Depth" architecture, encompassing multiple layers from product design and testing to network systems, personnel, and process management. For utility operators, initiating with robust Information Security Management Systems (ISMS) and personnel/process management is foundational before implementing other security layers [3].

Building upon these principles, this paper emphasizes that effective threat modelling and risk assessment, grounded in ISMS and specific system architectures, enable the deployment of cost-effective countermeasures. This strategic approach prioritizes the most significant threats, leveraging established best practices and standards, rather than attempting an unfeasible "protect everything" strategy. Many published works on threat modelling are based on an IT system approach, and OT system requires a customized approach as priority in OT is in the order of AIC compared to Confidentiality, Integrity and Availability (CIA) in the IT system, and the life of OT assets is much higher than that of IT assets. In addition, many of the published works describe threat models for discrete components like power transformers and not for the entire system. In many of the OT systems, legacy devices continue to coexist, and this will increase the attack surface due to the vulnerabilities in the legacy devices/systems.

A comprehensive study of threat modelling of the complete power system SCADA control centre and substation automation system as a whole is required. This helps in understanding cyber threats as a whole and in mitigating them through risk management. What sets this effort apart is the creation of an extensive threat model that integrates the STRIDE methodology, CIA triad principles, and specific controls from ISO/IEC 27001, ISO/IEC 27002, and the IEC 62351 series of standards, applied to realistic SCADA control center and substation automation system architectures. This integrated approach offers a more holistic and actionable framework for identifying and mitigating threats in critical power infrastructure. Table 1 lists the Indian and International standards/guidelines referred to in this study. There are numerous published standards and recommendations for cybersecurity applications; some are sector-specific, while others are general and applicable to a variety of industries.

**Table 1. Selected international standards/guidelines on cyber security**

| Sl. No. | Standard No. | Standard Title |
|---|---|---|
| 1 | ISO / IEC 27001: 2022 | Information security, cybersecurity and privacy protection - Information security management systems - Requirements (third edition) |
| 2 | ISO / IEC 27002: 2022 | Information security, Cybersecurity and privacy protection - Information security controls (third edition) |
| 3 | ISO / IEC 27019: 2024 | Information security, Cybersecurity and privacy protection - Information security controls for the energy utility industry (second edition) |
| 4 | IS 16335: 2015 | Power control systems - Security requirements |
| 5 | IEC 62443-3-3: 2013 | Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels |
| 6 | IEC 62351-1:2007 | Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues |
| 7 | IEC 62351-2: 2008 | Part 2: Glossary of terms |
| 8 | IEC 62351-3: 2014 | Part 3: Communication network and system security - Profiles including TCP/IP |
| 9 | IEC 62351-5: 2013 | Part 5: Security for IEC 60870-5 and derivatives |
| 10 | IEC 60870-5-7: 2013 | Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351) |

| | | |
|---|---|---|
| 11 | IEC 62351-4: 2018 | Part 4: Profiles including MMS and derivatives |
| 12 | IEC 62351-6: 2020 | Part 6: Security for IEC 61850 |
| 13 | IEC 62351-8: 2020 | Part 8: Role-based access control for power system management |
| 14 | IEC 62351-100-1: 2018 | Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 |
| 15 | IEC 62351-100-3: 2020 | Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP |
| 16 | IEC 62351-100-4: 2023 | Part 100-4: Cybersecurity conformance testing for IEC 62351-4 |
| 17 | IEC 62351-100-6: 2022 | Part 100-6: Cybersecurity conformance testing for IEC 61850-8-1 and IEC 61850-9-2 |
| 18 | IEC 62443-4-2: 2019 | Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components |
| 19 | NIST SP 800-82r3, 2023 | Guide to Operational Technology (OT) Security |
| 20 | The NIST Cybersecurity Framework (CSF) 2.0, 2024 | The NIST Cybersecurity Framework (CSF) 2.0 |

The remainder of this paper is organized as follows: Section 2 provides an analysis of past and current research in this domain. Section 3 details the SCADA control center and substation automation system architectures under investigation. Section 4 describes the proposed threat modelling methodology.

Section 5 presents the threat modelling results. Section 6 discusses these results in the context of real-world cyber incidents and proposes mitigation strategies. Finally, Section 7 concludes the paper with a summary of the study's key findings and recommendations.

## 2. Related Work

Threat modelling has gained significant importance in Industrial Control Systems (ICS) for identifying and mitigating potential vulnerabilities, as extensively reviewed in recent literature. Shaymaa Mamdouh Khalil et al. [4] provide a systematic literature review on threat modelling methodologies for ICS, comparing various definitions and distinctions among threat modelling, attack modelling, and risk assessment.

Additionally, the authors outline several potential problems that could arise while creating threat models in ICS, as the threat landscape may vary, new threats may arise, and threat models need continuous improvement. Threat models are applicable to both software (coding and firmware) and hardware architectures.

For the present study, the definition of threat model as presented in [4] is adopted: "Threat modelling is a process that can be used to analyze potential attacks or threats, and can also be supported by threat libraries or attack taxonomies." Researchers have explored threat modelling across various domains within critical infrastructure. Soumya K. T. et al. [5] thoroughly investigated cybersecurity issues and frameworks for Smart Microgrids, detailing vulnerabilities, threat models, and the necessity for data-driven security solutions. While their focus is on Smart Microgrids, some aspects of their work are relevant to broader transmission and distribution automation systems.

Holik F. et al. [6] investigated threat modelling for digital secondary substations in smart grids, specifically using the STRIDE model to identify and evaluate threats through simulation. Their study also highlighted challenges, particularly the subjective nature of threat evaluation, which depends on criteria agreed upon by threat model participants. In a more device-specific application, the work focused on threat modelling for power transformer monitoring systems, also employing the STRIDE methodology and simulating the proposed model to address device-level security [7].

Expanding beyond individual components, I. Zografopoulos et al. [8] presented threat modelling and risk assessment for Cyber-Physical Systems (CPS) using integrated power system and communication modelling and simulation tools. Their study explored four simulated attack scenarios with a primary focus on electrical system operation, offering a unique perspective on control system threat modelling compared to conventional IT-centric approaches. Christoph Schmittner et al [9] described a Threat Modelling approach for identifying threats to the safety of the critical railway domain based on the STRIDE method integrated with the IEC 62443 standard.

Furthermore, Matta et al. [10] applied threat modelling and risk evaluation for standard compliance in rail systems, demonstrating how identified threats can be mapped to the established standards like IEC 62443-3-3 and how effective mitigation strategies can be implemented. The authors used the STRIDE model for threat classification. Reference [11] offers a hybrid framework that combines threat modelling methodologies that are system-centric, attacker-centric, and risk-centric, specifically STRIDE, attack tree, and PASTA (Process for Attack Simulation and Threat Analysis) for the oil and gas sector SCADA system, showing how a hybrid model would identify more threats. The authors also applied a quantitative security assessment, which helps with risk mitigation plans. B. Achaal, M. Adda, M. Berger, H. Ibrahim, and A. Awde thoroughly explain the communication networks, smart grid architecture, and the different cyber attacks that can target the system [12]. The authors make use of the NIST Cybersecurity Framework for classification and listing countermeasures.

Despite these advancements, a gap persists in comprehensive threat models that effectively integrate diverse threat modelling methodologies within the power sector. Developing a detailed threat model is essential for determining weak points, ranking risks, enhancing security protocols, and supporting risk-based investments [13]. This paper addresses this gap by developing a comprehensive threat model for the power sector, considering the SCADA control centre and substation automation system as a whole and integrating various security threat models and methods. This integrated approach aims to significantly enhance the security of the power sector against potential threats and enable the cost-effective implementation of countermeasures through strategic threat prioritization.

## 3. Utility SCADA Architecture

The electric power sector, encompassing generation, transmission, distribution, operations, service providers, consumers/customers, and the market, involves complex energy flow and extensive information exchange among these domains [14]. Operational criticality primarily involves the communication networks connecting generation, transmission, operations, and distribution domains. The operational layer includes SCADA systems, Energy Management Systems (EMS) and Distribution Management Systems (DMS), which are interconnected with generation, transmission, and distribution substations.

Extensive information sharing through the usage of OT and IT platforms and control across these domains, often leveraging public communication infrastructure, renders these networks and components vulnerable to cyber threats. Therefore, threat modelling is essential for designing secure architectures and deploying cost-effective countermeasures. This study specifically considers interconnected substation automation systems and SCADA control center architectures. The SCADA control center maintains connectivity with various substations (generation, transmission, and distribution based on the utility) and other control centers, such as regional load dispatch centers and backup control centers.

### *3.1. Scope of Threat Modelling*

Before initiating threat modelling, it is crucial to address fundamental questions: (1) what system or architecture are we analysing? (2) What potential issues or attacks could occur? and (3) what actions can be taken to mitigate these risks? Following the analysis, assessing the completeness is crucial for the implemented measures. For effective threat modelling, insights into potential adversaries, their motivations and goals, and their potential knowledge of the system were considered [13].

This study uses threat modelling for the power system SCADA control center and substation automation systems. The primary analytical objective is to identify how breaches in the fundamental security requirements of the CIA triad can manifest as security threats and to determine corresponding mitigation strategies. Furthermore, the availability of organizational security policies, detailed system architectures (indicating communication flow), and cybersecurity-related information (e.g., device configurations, known vulnerabilities for legacy equipment) significantly aids the threat model analysis of existing systems.

### *3.2. Substation Automation System (SAS) Architecture*

Electrical substations typically employ automation systems based on the IEC 61850 communication protocol. While their physical scale varies based on voltage levels, number of feeders, and transformer capacities, the underlying automation philosophy for transmission, distribution, and generation substations is largely consistent, relying on IEC 61850-compliant numerical relays for protection and control.

In addition to Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs) / Bay Protection and Control Units (BPCUs) that control circuit breakers, common ICT components within substation automation systems include servers, workstations, network switches, routers, firewalls, Global Positioning System (GPS) clocks, gateways (e.g., for converting IEC 61850 to IEC 60870-5-104 protocols), and communication interfaces/modems for connectivity to the utility's SCADA control center.

In most automated substations, the utility's enterprise (IT) network is either absent or maintained on a physically separate network. Many modern substations operate as unmanned facilities. Distribution substations serve as critical links for delivering electrical energy to various consumers via last-mile distribution transformers.

Many utilities implement feeder automation systems, which connect to the distribution control center via FRTUs. Figure 1 illustrates a typical substation automation system for a distribution substation. In non-SAS-based substations, RTUs are often used for control and measurements, typically employing IEC 60870-5-104 or IEC 60870-5-101 communication protocols.

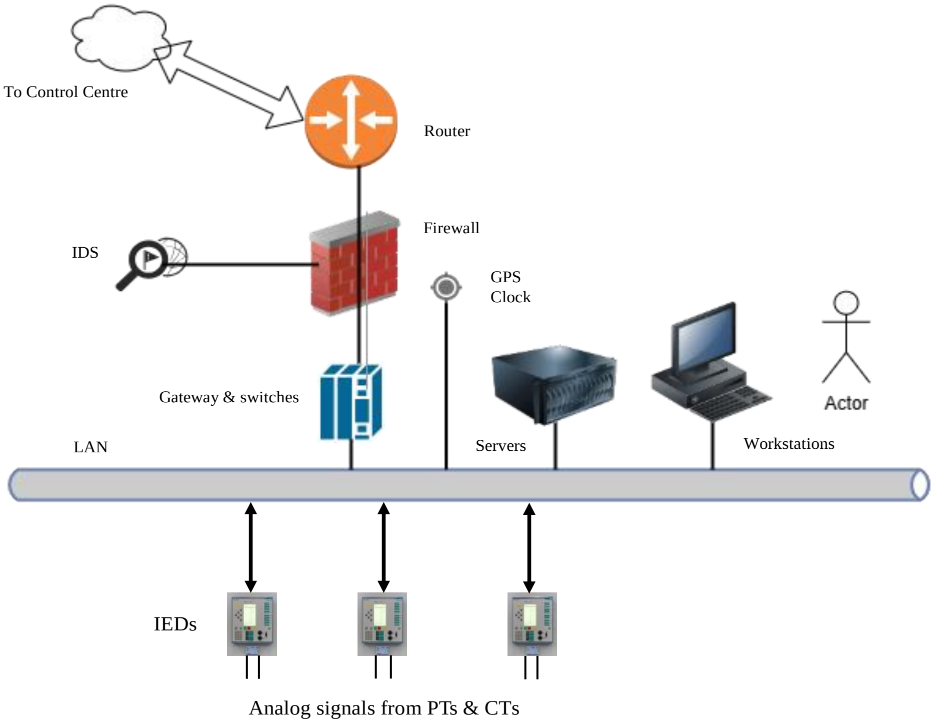

**Fig. 1 Simplified substation automation architecture**

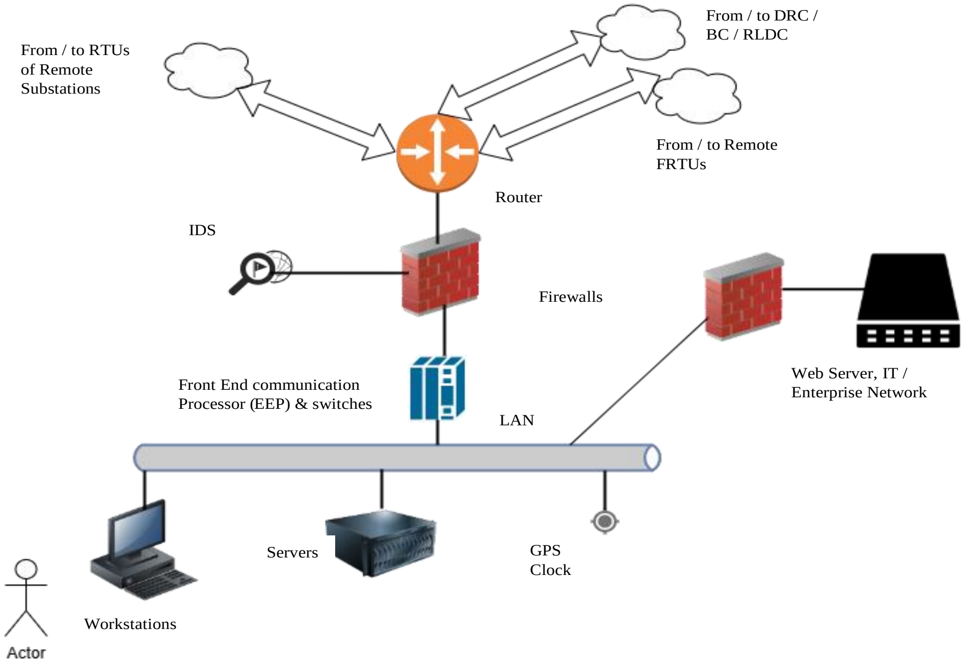

**Fig. 2 Simplified control centre architecture**

### *3.3. SCADA Control Center*

SCADA Control Centers can be specialized for either transmission or distribution systems. Transmission system SCADA control centers typically do not manage feeder level automation due to higher voltage levels and long distance lines, and serve primarily as a feeding substations to distribution substations.  A distribution automation control center is considered for this study. Figure 2 depicts a typical Distribution Automation SCADA control center. This control center maintains connectivity with numerous geographically dispersed substations and feeder automation FRTUs. Additionally, the control center interconnects with a Backup

Control Center (BC) or Disaster Recovery Center (DRC), a Regional Load Dispatch Center (RLDC) (for operational coordination), any sub-control centers, and the utility's enterprise or IT network.

### *3.4. Key IT and OT Assets*

A brief description of the IT and OT assets (equipment) used in the substations and control centers is provided below to facilitate the identification of potential cyber risks associated with these assets for the threat model analysis.

#### *3.4.1. Remote Terminal Units (RTUs) and Feeder Remote Terminal Units (FRTUs)*

RTUs are deployed in substations to collect measurement values (e.g., feeder voltages, transformer voltages, power) and control circuit breakers. Typically, a single RTU supports the necessary digital inputs/outputs, communication ports (Ethernet, USB, Serial), and analog inputs/outputs for various measurement and control functions within the substation. FRTUs are generally used for distribution of low voltage (e.g., 11 kV) feeder management functions, such as Fault Location, Isolation, and Service Restoration (FLISR) with sectionalizers, auto-reclosers, Ring Main Units (RMUs), and Fault Passage Indicators (FPI). These RTUs/FRTUs typically operate on IEC 60870-5-101/104 communication protocols, although DNP3-based units are common in North America. The RTU connects to the substation automation system via network switches, routers, and firewalls, and then to the wide area communication network using fiber, radio, or copper through utility-owned infrastructure or a communication service provider. Local communication ports (e.g., USB, Ethernet) allow for direct configuration of devices, and alternatively, remote configuration through the SCADA control center is also possible.

#### *3.4.2. Intelligent Electronic Devices (IEDs) and Numerical Protection Relays*

IEDs and numerical protection relays are used for substations' protection, control, and measurement. These IEDs are based on the IEC 61850 communication protocol and are networked to the substation automation system through network switches. They also possess local communication ports (e.g., USB, Ethernet) for configuration, which can also be performed remotely from the SCADA control center. Other variants of IEDs, such as transformer tap changers and BPCUs, also conform to IEC 61850 and offer similar local and remote configuration capabilities.

#### *3.4.3. Merging Units, Phasor Measurement Units (PMUs), and Phasor Data Concentrators (PDCs)*

Merging units digitally process analog signals (voltage and current) from field transformers, outputting sampled values that serve as inputs to IEDs on the process bus, compatible with IEC 61850. PMUs provide time-synchronized voltage, current, and other parameters crucial for grid state estimation and condition monitoring, while PDCs collect data from multiple PMUs and transmit it to the control center. PMUs and PDCs are predominantly used in transmission substations, with limited but anticipated future use in distribution substations. For the scope of this study, Merging Units, PMUs, and PDCs are not considered in the threat model analysis.

#### *3.4.4. Other Essential IT/OT Assets*

Beyond the above, substation automation systems and control centers incorporate various other IT assets, including communication interfaces/modems, routers, firewalls, network switches, servers, workstations, display systems, and printers. Control centers typically utilize multiple instances of these IT assets depending on their size and operational requirements.

## 4. Proposed Work and Methodology

This study employs an asset-centric threat modelling approach, as highlighted by Livinus Obiora Nweke and Stephen D. Wolthusen [15], where STRIDE is frequently combined with other methodologies. The CIA Triad and relevant ISO/IEC 27002 controls are integrated with STRIDE as this study's primary threat modelling technique. Various security threats, attacks, and countermeasures as defined in the IEC 62351-1 standard [16] are incorporated in this study. To facilitate threat analysis, Data Flow Diagrams (DFDs) for both a basic substation architecture (Figure 3) and a SCADA control center (Figure 4) are used, using the community version of IriusRisk to facilitate the threat analysis. A DFD is provided to IriusRisk as an input, which then provides an initial identification of threats based on its built-in threat library. Subsequently, manual analysis was performed to refine these results, leveraging expert knowledge of power system operations and specific device characteristics not fully captured by the automated tool. The STRIDE methodology, an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, guided the threat identification process.

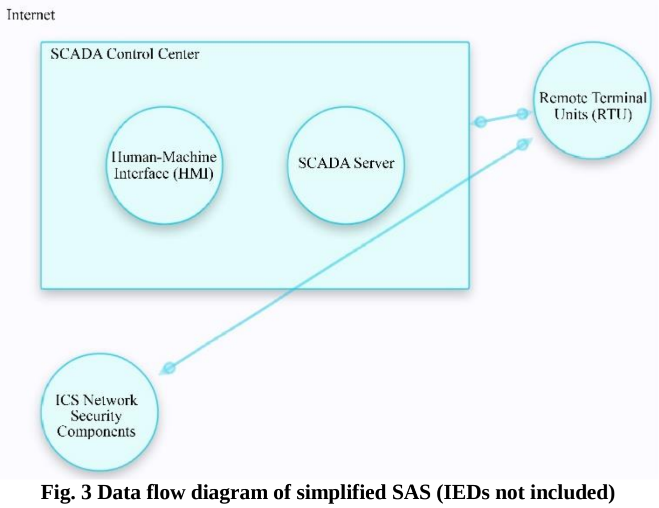
Internet
SCADA Control Center
Human-Machine Interface (HMI)
SCADA Server
Remote Terminal Units (RTU)
ICS Network Security Components

**Fig. 3 Data flow diagram of simplified SAS (IEDs not included)**

The analysis objective is focused on how deviations from the fundamental security requirements of the CIA triad manifest as threats, and how to mitigate them. For optimal threat model results, insights into potential adversaries, their motivations and goals, and their potential knowledge of the system were considered. The availability of organizational security policies, detailed system architectures (indicating communication flow), and cybersecurity-related information (e.g., device configurations, known vulnerabilities for legacy equipment) significantly aided the threat model analysis of existing systems.

### *4.1. Classification of Security Threats*

The possible threats and attacks are categorized based on their impact on fundamental security principles:

#### *4.1.1. Unauthorized Access to Information (Confidentiality)*

This threat violates the 'Confidentiality' requirement of the CIA triad, posing a risk of sensitive information disclosure. Potential attacks include listening, eavesdropping, media scavenging, wireless transmission interception, traffic capture, bypassing controls, Man-In-The-Middle (MITM) attacks, data theft, service spoofing, and Trojan horse attacks.

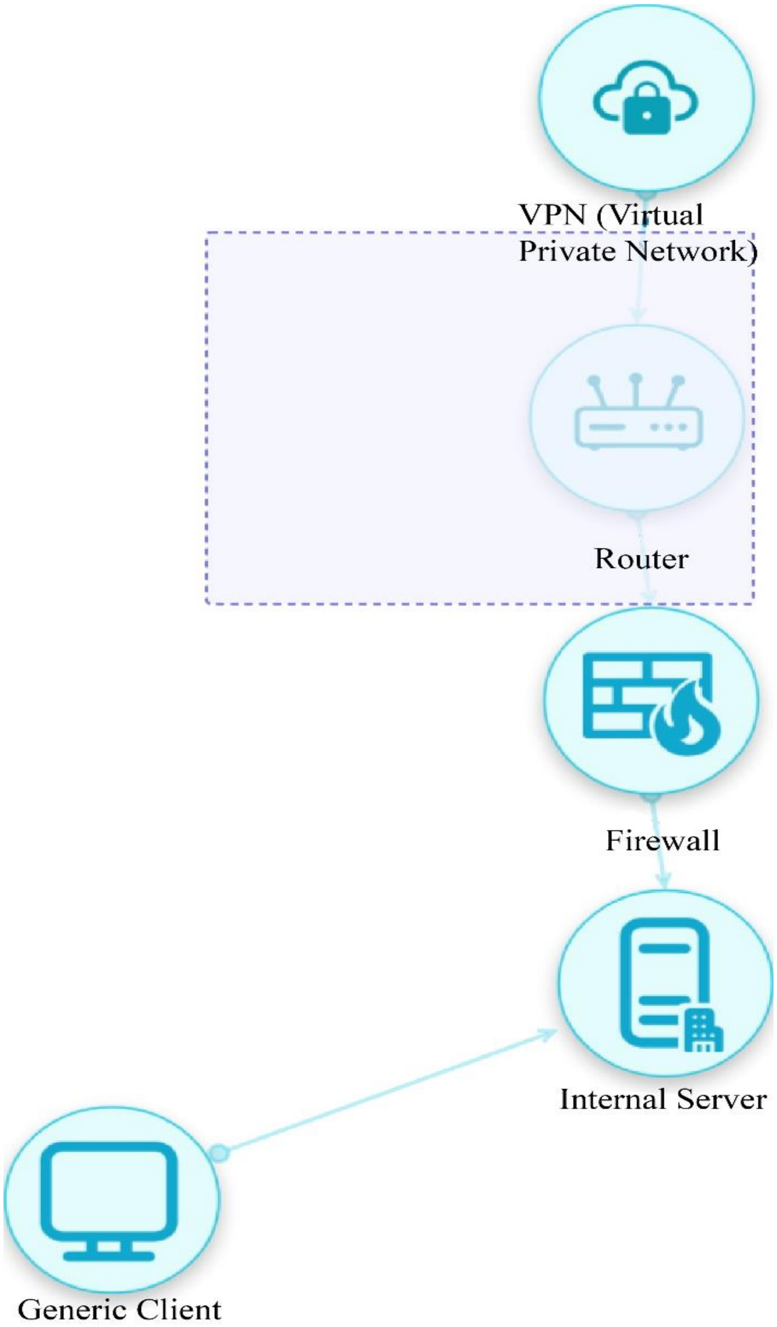

**Fig. 4 Data flow diagram of simplified control centre**

#### *4.1.2. Unauthorized Modification or Theft of Information (Integrity)*

This threat violates the 'Integrity' requirement of the CIA triad. Attacks may involve data modification, interception/alteration of data, bypassing controls, MITM attacks, data theft, service spoofing, and Trojan horse attacks.

#### *4.1.3. Denial of Service (DoS) or Avoidance of Permitted Access (Availability)*

This threat violates the 'Availability' requirement of the CIA triad. Unlike in general IT, 'Availability' holds the highest priority in critical infrastructure, such as power sector SCADA systems.

Possible attacks include DoS, resource exhaustion, bypassing controls, MITM attacks, data theft, service spoofing, and Trojan horse attacks.

#### *4.1.4. Accountability; Denial of Action or Claim of False Action (Non-Repudiation)*

While not typically part of the core CIA triad, 'Non-Repudiation' is a critical cybersecurity requirement, ensuring that parties involved in a transaction or communication cannot falsely deny their actions or message origination. Attacks include denial of action, false claim of action, stolen/altered credentials, bypassing controls, MITM attacks, data theft, service spoofing, and Trojan horse attacks. Figure 5 illustrates the possible interrelationships between attacks, threats, and security requirements.

### *4.2. Application of STRIDE Methodology*

There are two ways to perform STRIDE-based threat modelling, namely STRIDE per element and STRIDE per interaction [17]. STRIDE per element analyses the behaviour and operations of every component in the system.

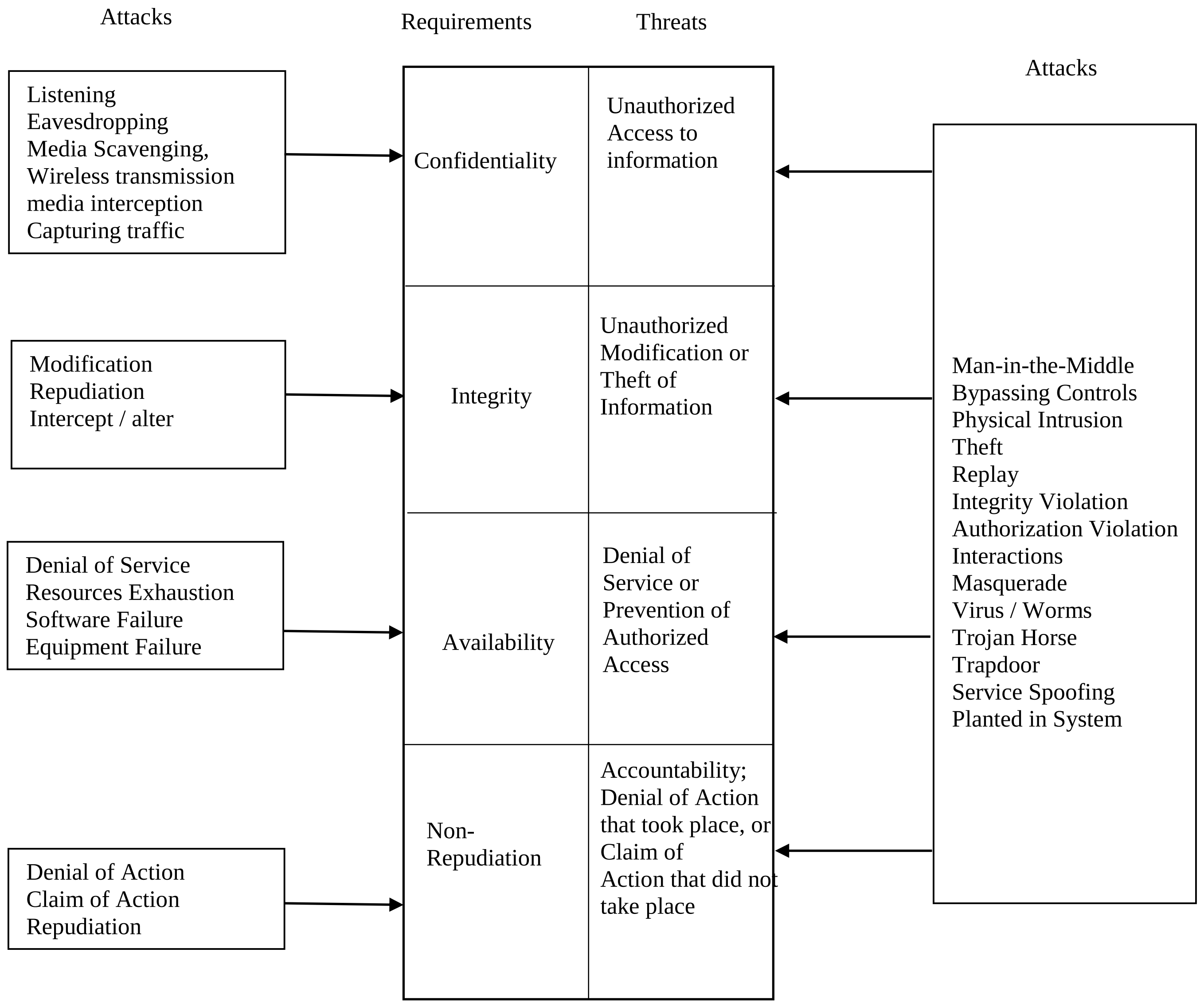

**Fig. 5 Cyber threats, attacks and requirements**

However, in most cases, threats can be more effectively identified in the interactions between system components, making this approach simpler and often more comprehensive for complex interconnected systems. Then, I applied the "STRIDE per interaction" approach for threat modelling.

For each data flow and interaction point identified in the DFDs, a systematic evaluation of potential threats corresponding to Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege, the categories of STRIDE (the acronym formed by the first letter of each word) is carried out. The high-level architectures of the control center and substations were first decomposed into simpler, manageable components:

SCADA Control Center Components:

- Servers and Workstations
- Front-End Communication Processors, GPS clock, and associated routers, firewalls, and switches
- Interface to IT / Enterprise Network
- Interface to other control centers (e.g., backup control center, regional/area load dispatch centers)

Substation Automation System (SAS) Components:

- Field OT devices (e.g., IEDs, transformer tap changers)
- Workstations and associated network switches, GPS clock
- Gateway with associated firewall, routers, and communication interface for connecting to the control center.

RTU-based Substation Components:

- Field OT devices (e.g., RTU and analog measurement devices like Modbus-based panel meters)
- Workstations and associated IT network switches
- Communication Interface with associated firewall, router for connecting to the control center.

The entire procedure of threat modelling is shown in the Flow chart in Figure 6. The process begins with identifying assets and defining security objectives. Identifying assets is very crucial, and the standards and best practices are to be applied at this stage. Asset identification in the context of cybersecurity for the power industry refers to the procedure of recognizing, categorizing, and recording all hardware, software, data, and other resources (assets) of the SCADA Control centre and substation automation system. The next process is how all these assets are interconnected in the system, forming the system architecture. Further, in the threat modelling, the architecture is decomposed into smaller elements for ease of identifying threats from the larger threat landscape. This process involves creating data flow diagrams.

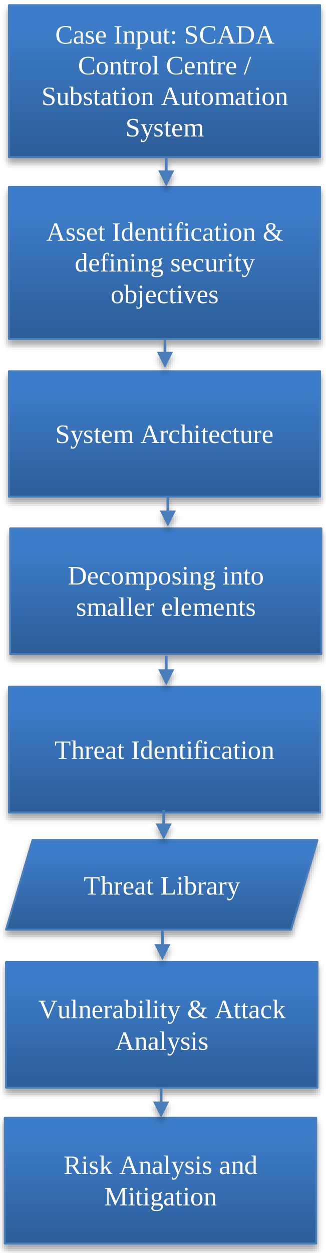
Case Input: SCADA Control Centre / Substation Automation System
Asset Identification & defining security objectives
System Architecture
Decomposing into smaller elements
Threat Identification
Threat Library
Vulnerability & Attack Analysis
Risk Analysis and Mitigation

**Fig. 6 Threat model process flow chart**

The data flow diagram involves communication data flow path, data storage, devices and the process. In this stage, the standards, regulations, organizational security policy, physical architecture and logical interconnection diagrams provide the input for moving to the next stage in the threat model.

Based on the assets of the system and its functionalities and interconnections, the type of threats that are likely to affect it will be identified at the threat identification stage. If the case under study is an existing SCADA control centre or substation automation system, the historical data, like past incidents, system logs and global cyber attack database, will be provided as an input for creating an attack model for the next step of vulnerability analysis. For the threat model analysis of the new system, the global cyber attack database and the threat library, which includes a repository of threat intelligence comprising known threats, vulnerabilities and attack methods, will be used. In this stage, the likelihood of threat and attack scenarios is created. In the vulnerability analysis stage, the key reasons for the security flaw are determined, and threats are classified as high risk and moderate to low risk based on the previous stage results of threats and attack scenarios. The attack analysis involves probable scenarios of attacks and mapping to the threat library. Based on all the previous steps, the mitigation plan for security has been developed, considering the risk factors associated with the threats. Based on priorities assigned considering the risks associated with the threats, cost-effective countermeasures are arrived at. The security standards, the organizational security policy and regulations considered in the threat modelling process, along with the outcome of the threat model, are used for devising effective threat countermeasures.

## 5. Threat Modelling Results

Following the application of the STRIDE methodology to the Data Flow Diagrams of substation automation systems (Figure 3) and the SCADA control center (Figure 4), the analysis identified several key cybersecurity vulnerabilities and potential threats. The assessment focused on how information and control of Confidentiality, Integrity, and Availability (CIA Triad) might be compromised. A primary finding for both SCADA control center and substation automation architectures relates to the communication protocols and their inherent lack of security features. The information exchange between substation OT components and the control center, often using IEC 61850 and IEC 60870-5-101/104 communication protocols, does not typically incorporate built-in authentication or encryption mechanisms. This characteristic of open protocols, especially when communication occurs over third-party communication networks, introduces significant vulnerabilities as given below:

- Tampering (Integrity): The absence of integrity checks makes these communications susceptible to Man-In-The-Middle (MITM) attacks, where malicious actors can intercept and alter data flows, potentially leading to incorrect measurements or unauthorized control commands.
- Denial of Service (Availability): These protocols' lack of robust security increases susceptibility to Denial of Service (DoS) threats, as network intrusions or message floods could disrupt critical real-time operational data and control commands.

Another significant area of concern arises from the interconnectivity between the OT and IT networks. Even when a Virtual Private Network (VPN) is used for communication channels, the control center's connectivity with the broader IT network of the organization’s enterprise system, typically facilitated by a Demilitarized Zone (DMZ) and firewalls, introduces specific vulnerabilities as given below:

- Information Disclosure and Spoofing (Confidentiality & Spoofing): As the IT network often connects to untrusted external services (for instance, internet DNS servers, email servers, and web servers), security is significantly weakened without stringent firewall policies, continuous network monitoring, and a robust organizational security policy. This creates vectors for phishing attacks via email or compromised web services, potentially leading to credential theft and subsequent unauthorized access or spoofing.
- Elevation of Privilege: Successful intrusion into the IT network can provide a pathway to elevate privileges within the control center environment, especially if security segmentation or access controls between IT and OT are insufficient.

Furthermore, the threat model identified vulnerabilities directly related to the OT equipment itself, particularly for substation automation systems:

- Spoofing (Authentication): Many legacy and even some modern OT equipment in substation automation systems lack strong Authentication and cryptographic protocols like Transport Layer Security (TLS). This makes them vulnerable to spoofing, where an attacker could impersonate a legitimate device or user to send false commands or data.
- Repudiation: Without strong Authentication and logging mechanisms, actions taken by OT devices or through their interfaces may lack non-repudiation, making it difficult to definitively prove the source of a command or data modification.

The analysis underscores that while robust communication channels (e.g., VPNs) are beneficial, the overarching security posture is heavily influenced by the weakest link, which often resides at the intersection of IT/OT networks and the inherent vulnerabilities of widely used industrial communication protocols and devices. These identified threats necessitate targeted mitigation strategies to enhance the resilience of electric power systems.

### *5.1. Case Study of Laboratory SCADA Testbed*

A multipurpose SCADA Test Bed is developed from the commercially available products for testing, training and research study purposes in a laboratory. This test bed is used to create a threat model based on the above studies. The SCADA test bed consists of the SCADA control centre rack and RTU rack. The SCADA control centre consists of workstations, servers, switches, routers, a firewall, a printer and a communication modem. Also, the SCADA application software and other associated software, including operating systems, are part of the control centre. The RTU rack emulates substations and consists of four small RTUs, which can be configured as four distribution substations or feeders. Management emulation application. The Large RTU emulates a one larger substation. All these RTUs are connected to the Gateway through switches and routers. Multifunction Transducers (MFT) / panel meters are connected to RTUs through serial communication (RS-485) using Modbus protocol. The RTUs communicate with the SCADA control centre using IEC 60870-5-104 protocol. Figure 7 shows the connection diagram of the RTU panel and control centre panels.

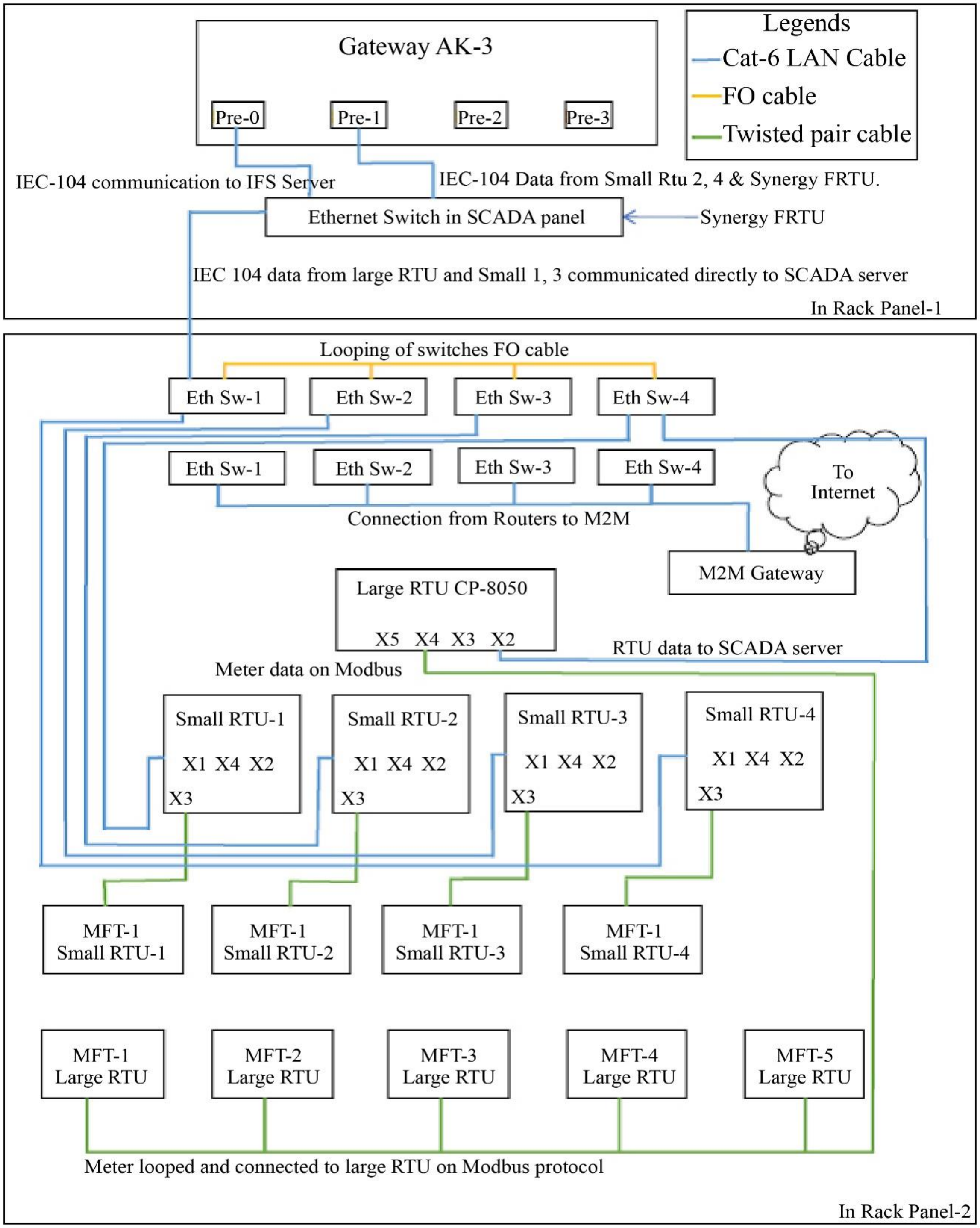

**Fig. 7 Connection diagram arrangement of laboratory SCADAD test bed**

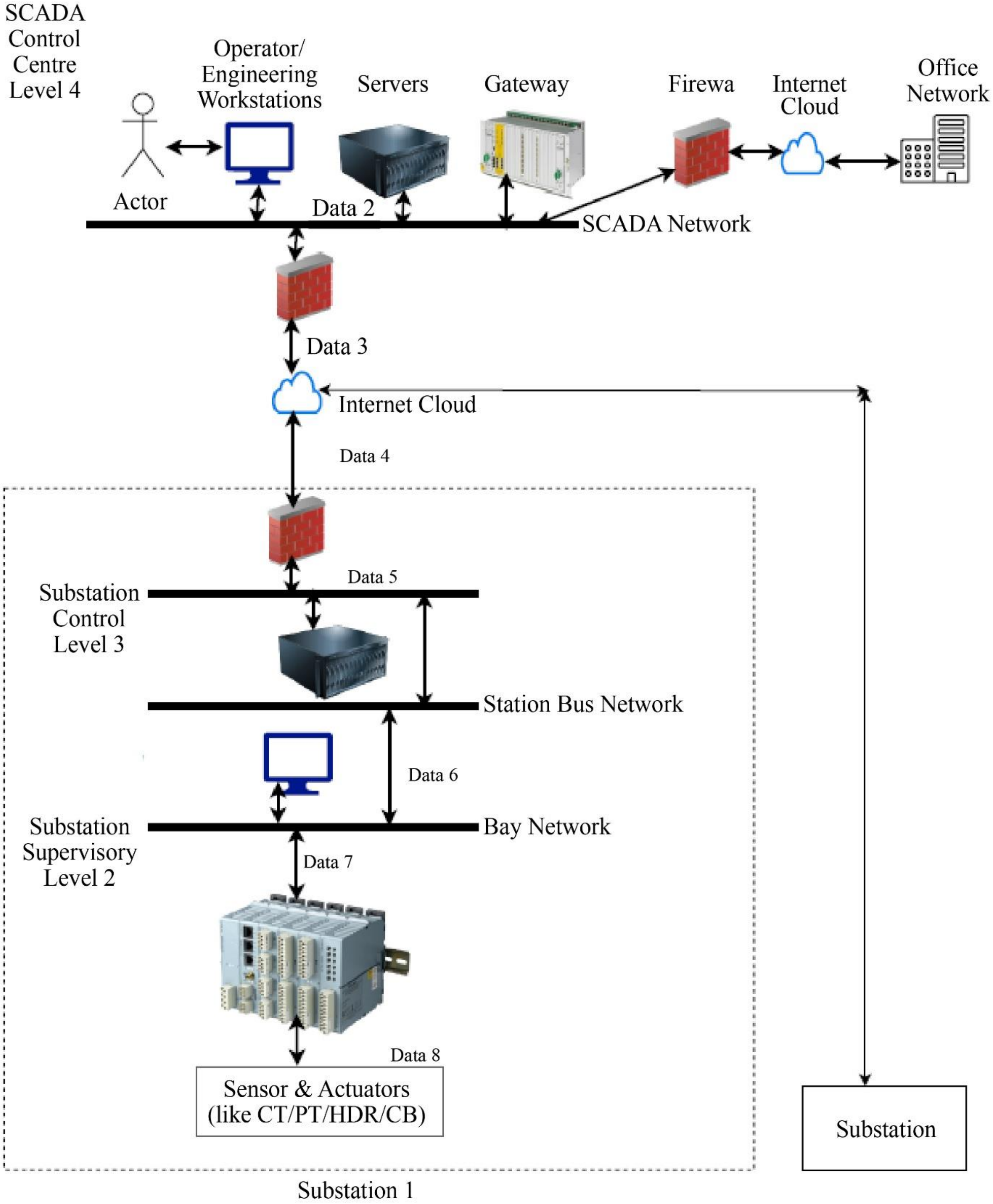

**Fig. 8 Data flow diagram of SCADA test bed**

Figure 8 shows a data flow diagram. For simplicity, the GPS clock is not shown in this diagram. The overall system includes five levels, namely Level 0, the field components like sensors (like CT/PT etc.), actuators (like Heavy Duty Relay (HDR), Circuit Breakers (CB) etc.), which receive control information and also send the status and values (measurement data like voltage, current etc.). The level 1 includes controlling devices like RTUs (in substation automation system-based stations, which also include IEDs). Then there is the Level 2, which comprises workstations for operators and engineering. The Level 3 includes the servers, firewall and other associated devices like switches, routers and software which control complete substations and facilities for connecting to the remote SCADA Control Centre. The Level 4 is the SCADA control Centre which connects to multiple remote substations and the enterprises/office network of the utility.

Applying the hybrid threat model discussed in the previous section to this laboratory SCAD testbed, Table 2 lists the process and the data flow with reference to each threat classification based on STRIDE. Correlating with the standards ISO / IEC 27002 and IEC 62351 series, the mitigation of threats plans are shown in Table 2. It can be seen that, as no authentication and encryption are used with the IEC 60870-5-104 protocol, the traffic can be decoded using software like Wireshark, and in attacks like man-in-the-middle, there is always a possibility to tamper with the data.

## 6. Discussion and Mitigation Strategies

This section interprets the threat modelling results presented in Section 5, correlating the identified vulnerabilities and threats with real-world cyber incidents in critical infrastructure. Then, potential mitigation strategies are discussed, emphasizing the role of established cybersecurity controls. Table 3 summarizes selected incidents, their root causes, and relevant ISO/IEC 27002:2022 clause numbers [18] that, if applied, could have prevented or significantly mitigated the attacks.

The spoofing, tampering, and denial of service threats identified in this SCADA and substation architectures, particularly concerning the use of unauthenticated and unencrypted IEC 61850 and IEC 60870-5-101/104 protocols, are consistent with several past incidents where attackers exploited weaknesses in the security of the communication protocols. For instance, the 2016 and 2015 Ukrainian power grid attacks [23-27] highlighted how adversaries could gain control of RTUs and IEDs, partly due to the lack of fundamental security mechanisms in these power system communication protocols.

While specific details of protocol exploitation were not always public, the general vulnerability identified in this model aligns with the outcome of these attacks. Implementing security specifications as per the IEC 62351 series of standards [28] is crucial here, as these standards specifically address data and communication security for power systems, including Authentication and encryption for these very protocols.

**Table 2. STRIDE threat classification and correlation with the standard**

| Sl. No | Threats | Data and Process Elements | Standard Clauses for Mitigation Plans |
|---|---|---|---|
| 1 | Spoofing | Operator at SCADA control Centre, Substation level 3, and office network | Access Control, Identity Management (ISO / IEC 27002), Authentication (IEC 62351 series) |
| 2 | Tampering Data | Bidirectional – Data 1,2,3,4,5, 6,7 and 8 | Authentication, policies for information security (ISO / IEC 27001), encryption (IEC 62351 series) |
| 3 | Repudiation | Operator at SCADA control Centre, Substation level 3, and office network | Access Control, Identity Management, policies for information security (ISO / IEC 27002) |
| 4 | Information Disclosure | Operator at SCADA control Centre, Substation level 3, and office network<br>Data 1,2,3,4,5, 6,7 and 8 | Authentication, policies for information security (ISO / IEC 27001) and encryption (IEC 62351 series) |
| 5 | Denial of Service | Workstations and servers at Substations and SCADA control Centres<br>Data 1, 2, 6 and 8 | Access Control, Identity Management, policies for information security (ISO / IEC 27002) |
| 6 | Elevation of Privileges | Workstations and servers at the SCADA control Centre, substations, and field devices (RTU) | Access Control, Identity Management, policies for information security (ISO / IEC 27002) |

**Table 3. Selected cyber incidents on critical infrastructure**

| Sl. No. | Year of Incidence | Location | Narration of Incident | Reference | Root cause and Reference to ISO / IEC 27002: 2022 Clause Nos. | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Human | Network System / Architecture | Product | Network System / Architecture / Product Design |
| 1 | 2023 | Denmark | Vulnerability in Zyxel | [19] | ✓<br>8.8, 8.16 | | ✓<br>8.25 | ✓<br>8.25, 8.29 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | firewalls of Danish utilities | | | | | |
| 2 | 2021 | USA | Colonial Pipeline | [20] | ✓<br>5.16, 5.15, 5.18, 5.17, 8.5 | ✓<br>8.16, 8.20, 8.21 | | |
| 3 | 2021 | USA | Florida Water Treatment Plant | [21] | ✓<br>6.7, 5.18, 8.9 | | | |
| 4 | 2018 | USA | New York Power Transformer explosion | [22] | | | ✓<br>8.8, 8.16 | ✓<br>8.25, 8.29 |
| 5 | 2017 | Middle East | Power plant shutdown | [23] | ✓<br>8.9, 8.8 | ✓<br>8.9, 8.16 | | |
| 6 | 2016 | Ukraine | Power supply interruptions | [23-25] | ✓<br>5.1, 6.3, 8.16 | ✓<br>8.9 | ✓<br>8.5 | ✓<br>8.25, 8.29 |
| 7 | 2015 | Ukraine | Power supply blackout for a longer duration | [2-27] | ✓<br>5.1, 6.3, 8.13 | ✓<br>8.9 | ✓<br>8.5 | ✓<br>8.25, 8.29 |
| 8 | 2010 | Iran | Stuxnet damaged a Nuclear power plant | [29, 30] | ✓<br>5.1, 6.3, 8.16 | | ✓<br>8.5 | ✓<br>8.25, 8.29 |
| 9 | 2007 | USA | Idaho Aurora experiment | [31, 32] | | ✓<br>8.9 | ✓<br>8.5 | ✓<br>8.25, 8.29 |

The vulnerabilities related to the IT/OT network interface and human factors, identified as potential pathways for information disclosure, spoofing, and elevation of privilege, are overwhelmingly supported by historical incident data. The analysis of these incidents in Table 3 reveals that human factors-such as susceptibility to spear phishing, unauthorized use of portable storage devices, and inadequate adherence to organisational cybersecurity policies and controls-are frequently the primary root causes of cyber incidents in critical infrastructure. This underscores the importance of continuous and systematic training and awareness programs for all personnel handling critical assets and operations, including temporary staff, outsourced personnel, and vendor staff. The STRIDE threat modelling of the SCADA control center and substation automation system shows that the human factor is a major threat, and training and security awareness programs are essential for minimizing security incidents. Also, using secure devices based on IEC 62351 standards, secured application software, and adherence to organizational cybersecurity policy and controls based on International Standards like ISO/IEC 27001 with a defence-in-depth security architecture will help make the electric grid resilient to cyberattacks. Appendix 1 lists the control clauses and descriptions of ISO/IEC 27002 for cyber incidents, as listed in Table 1, to mitigate cyberattacks. Specific mitigation strategies emerging from this threat model findings and validated by historical incidents include:

Enhanced Protocol Security: For IEC 61850 and IEC 60870-5-104 communications, implementing security extensions (e.g., as specified in IEC 62351 series of standards) for Authentication, integrity, and encryption is crucial. This can be applied at protocol gateways, field devices, and control center front-end processors. Robust Network Segmentation: Strict segmentation between IT and OT networks, using properly configured firewalls with explicit allow/deny rules, is paramount. This limits the lateral movement of threats from the IT domain into the critical OT environment. Multi-Factor Authentication (MFA): Implementing MFA for all remote access points and critical HMI/SCADA systems significantly reduces the risk of credential theft and spoofing.

Comprehensive Vulnerability Management: Regular patching of operating systems and applications (where feasible in OT environments, perhaps via scheduled downtime or specialized patching tools for critical systems), coupled with proactive vulnerability scanning and penetration testing, addresses product-level weaknesses. Strict Access Control and Identity Management: Implementing ISO/IEC 27002 controls such as 5.15 (Access control), 5.16 (Identity management), 5.17 (Authentication information), and 5.18 (Access rights) is vital. This includes least privilege principles and regular review of access rights.

Incessant Monitoring and Anomaly Revealing: Deploying Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems to monitor network traffic (clause no. 8.16 of ISO / IEC 27002) and system logs can help detect anomalous behaviour indicative of attacks like DoS tampering, or unauthorized access. Personnel Training and Awareness: Consistent and mandatory security awareness training (clause no. 6.3 of ISO / IEC 27002) for all personnel, including contractors and third-party vendors, is essential to mitigate human factors like phishing and the misuse of removable media. Establishing clear policies for remote working (clause no. 6.7 of ISO / IEC 27002) and removable media use (related to clause no. 5.1 of ISO / IEC 27002 is also critical. Secure Development Lifecycle (SDL): For new products and system upgrades, including security across the entire development process (clause no. 8.25 and 8.29 of ISO / IEC 27002), ensures that security is built-in, not bolted on.

These specific measures, derived from a comprehensive threat model and aligned with established standards, offer a prioritized and cost-effective approach to enhancing the cybersecurity posture of electric power system SCADA and substation automation systems. The proposed framework provides a comprehensive threat modelling for a whole SCADA control centre and substation automation system. It combines the STRIDE and PASTA methods and applies the cybersecurity standards for identifying and analysing cyber threats and attacks and their mitigation. Compared to threat modelling, which focuses on particular elements in the power system, such as power transformers [7, 22], this study gives a holistic view of complete power system automation, cybersecurity threats, and attack scenarios. Thus, utilities can assign priority to the cyber threats and apply countermeasures for the high-risk threats on priority, considering risk factors associated with the analysed threats.

## 7. Conclusion

The Security threat modelling provides a profound understanding of the security risks associated with complex systems, particularly in critical sectors like electric power. Conducting threat modelling early in the system design phase is invaluable for identifying and prioritizing potential security threats, enabling the implementation of cost-effective countermeasures from the outset. For existing systems, threat modelling aids security analysis and informs decision-making for mitigating and minimizing security risks.

Applying the IEC 62351 series of standards and the ISO/IEC 27001 standard requirements in conjunction with the STRIDE approach in threat modelling analysis offers critical insights for prioritizing threats and deploying cost-effective countermeasures. The study emphasizes that strict adherence to organizational security policies and controls and comprehensive and continuous training for human resources responsible for critical infrastructure are paramount for building grid resilience against cyber threats and attacks.

It is acknowledged that threat model analyses may sometimes yield subjective results, as inputs often depend on the analyst's understanding and interpretation of the system and available information. Further sample studies of existing systems are necessary to establish more universally applicable guidelines for the OT sector threat model analysis, especially since many current threat modelling techniques originate from software and IT system contexts.

The future work plans include conducting threat model analyses on multiple real-world SCADA control centers and substation automation systems using international standards-based approaches. This comparative study aims to derive comprehensive guidelines specifically tailored for the OT sector threat model analysis. It is also planned to integrate the IEC 62443 series of standards requirements along with ISO/IEC 27001 and ISO/IEC 27002 standards for an even more holistic threat modelling approach, further enhancing vulnerability mitigation in power control networks and SCADA architectures.

## Acknowledgments

The authors express sincere gratitude to the management of the Central Power Research Institute for supporting this research in Cybersecurity for power sector applications. The authors also thank the management of BMS College of Engineering for their encouragement and guidance in pursuing this work of contemporary interest.

## References

[1] Adriana Hemzacek, Today’s Toughest Questions Answered: Cybersecurity in Transit, Icomera, 2023. [Online]. Available: https://www.icomera.com/todays-toughest-questions-answered-cybersecurity-in-transit/

[2] “*Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment*,” Technology Report, International Electrotechncal Commission (IEC), 2019. [Online]. Available: https://www.iec.ch/basecamp/cyber-security-and-resilience-guidelines-smart-energy-operational-environment

[3] Keith Stouffer et al., “NIST SP 800-82r3: Guide to Operational Technology (OT) Security,” *NIST Special Publication*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shaymaa Mamdouh Khalil, Hayretdin Bahsi, and Tarmo Korõtko, "Threat Modeling of Industrial Control Systems: A Systematic Literature Review," *Computers & Security*, vol. 136, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] K.T. Soumya et al., "A Systematic Study on the Intelligent Cyber Security for Smart Microgrid," *Proceedings of the IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Mangalore, India, pp. 237-242, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Filip Holik et al., "Threat Modeling of a Smart Grid Secondary Substation," *Electronics*, vol. 11, no. 6, no. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] BoHyun Ahn et al., "Security Threat Modeling for Power Transformers in Cyber-Physical Environments," *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, pp. 1-5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ioannis Zografopoulos et al., "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *IEEE Access*, vol. 9, pp. 29775-29818, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Christoph Schmittner et al., "Threat Modeling in the Railway Domain," *International Conference on Reliability, Safety, and Security of Railway Systems*, Lille, France, pp. 261-271, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] George Matta et al., "Risk Management and Standard Compliance for Cyber-Physical Systems of Systems," *Infocommunications Journal*, vol. 13, no. 2, pp. 32-39, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mohamed Badawy, Nada H. Sherief, and Ayman A. Abdel-Hamid, "Legacy ICS Cybersecurity Assessment Using Hybrid Threat Modeling-An Oil and Gas Sector Case Study," *Applied Sciences*, vol. 14, no. 18, pp. 1-38, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Batoul Achaal et al., "Study of Smart Grid Cyber-Security, Examining Architectures, Communication Networks, Cyber-Attacks, Countermeasure Techniques, and Challenges," *Cybersecurity*, vol. 7, no. 1, pp. 1-30, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Suvda Myagmar, Adam J. Lee, and William Yurcik, "Threat Modeling as a Basis for Security Requirements," *Symposium on Requirements Engineeringfor Information Security (SREIS)*, pp. 1-8, 2005. [Google Scholar]

[14] Avi Gopstein et al., "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0," *National Institute of Standards and Technology*, pp. 1-212, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Livinus Obiora Nweke, and Stephen D. Wolthusen, "A Review of Asset-Centric Threat Modelling Approaches," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 11, no. 2, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] IEC Technical Specification 62351-1:2007, "*Power Systems Management and Associated Information Exchange - Data and Communications Security - Part 1: Communication Network and System Security - Introduction to Security Issues*," Report, International Electrotechncal Commission (IEC), pp. 1-7, 2007. [Google Scholar] [Publisher Link]

[17] Rafiullah Khan et al., "STRIDE-Based Threat Modeling for Cyber-Physical Systems," *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Turin, Italy, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] ISO/IEC 27001:2022, "*Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements*," Report, International Electrotechncal Commission (IEC), 2022. [Google Scholar] [Publisher Link]

[19] Traffic Light Protocol (TLP): Clear, "*The Attack against Danish Critical Infrastructure*," Report, SektorCERT, 2023. [Online]. Available: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

[20] Jack Beerman et al., "A Review of Colonial Pipeline Ransomware Attack," *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, Bangalore, India, , pp. 8-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Blaine Jeffries et al., "*Cyber Risk to Mission Case Study: Oldsmar*," Report, Defense Technical Information Center, 2022. [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1183009.pdf

[22] Hossein Rahimpour et al., "A Review of Cybersecurity Challenges in Smart Power Transformers," *IEEE Access*, vol. 12, pp. 193972-193996, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Georgios Michail Makrakis et al., "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," *IEEE Access*, vol. 9, pp. 165295-165325, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Vetrivel Subramaniam Rajkumar et al., "Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures," *IEEE Access*, vol. 11, pp. 103154-103176, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] David E. Whitehead et al., "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies," *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, pp. 1-8, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] Jean-Pierre Hauetet al., In Tech: Ukrainian Power Grids Cyberattack, International Society of Automation, 2017. [Online]. Available: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack

[27] Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC), 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

[28] IEC 62351:2025 SER, "*Power Systems Management and Associated Information Exchange - Data and Communications Security - All Parts*," Report, International Electrotechncal Commission (IEC), 2025. [Google Scholar] [Publisher Link]

[29] Nicolas Falliere, Liam O. Murchu, and Eric Chien, W32.Stuxnet Dossier, Symantec Security Response, 2011. [Online]. Available: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

[30] David Kushner, The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program, IEEE Spectrum, 2013. [Online]. Available: https://spectrum.ieee.org/the-real-story-of-stuxnet

[31] Aurora Generator Test, Wikipedia, The Free Encyclopedia, 2014. [Online]. Available: https://en.wikipedia.org/wiki/Aurora_Generator_Test

[32] Doug Salmon et al., "Mitigating the Aurora Vulnerability With Existing Technology," *36th Annual Western Protection Relay Conference*, Washington, pp. 1-7, 2009. [Google Scholar] [Publisher Link]

## Appendix 1

**ISO / IEC 27002 Control Clauses Description for the Incidents Mentioned in Table 3**

| Sl. No. | Clause No. | Description | Control |
|---|---|---|---|
| 1 | 5.1 | Policies for information security | Information security policy and topic-specific policies shall be defined and approved by management and shall be implemented in practice. |
| 2 | 5.15 | Access control | Rules to control physical and logical access to information and other associated assets shall be established and implemented. |
| 3 | 5.16 | Identity management | The full life cycle of identities shall be managed. |
| 4 | 5.17 | Authentication information | Allocation and management of authentication information shall be controlled by a management process. |
| 5 | 5.18 | Access rights | Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed. |
| 6 | 6.3 | Information security awareness, education and training | Security awareness, education and training for the personnel. |
| 7 | 6.7 | Remote working | Security measures shall be implemented when personnel are working remotely. |
| 8 | 8.5 | Secure Authentication | Secure authentication technologies and procedures shall be implemented. |
| 9 | 8.8 | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems. |
| 10 | 8.9 | Configuration management | Configurations, including security configurations, of hardware, software, services and networks shall be established. |
| 11 | 8.13 | Information backup | Backup copies of information, software and systems shall be maintained and regularly tested. |
| 12 | 8.16 | Monitoring activities | Networks, systems and applications shall be monitored for anomalous behavior. |
| 13 | 8.20 | Networks security | Networks and network devices shall be secured, managed and controlled. |
| 14 | 8.21 | Security of network services | Security mechanisms, service levels, and network service requirements shall be identified, implemented, and monitored. |
| 15 | 8.25 | Secure development life cycle | Rules for the secure development of software and systems shall be established and applied. |
| 16 | 8.29 | Security testing in development and acceptance | Security testing processes shall be defined and implemented in the development life cycle. |