Power Research - A Journal of CPRI, Vol 22(1), 2026 | pp. 77-91

Threat Modelling and Risk Assessment in Power System Control Center

Kamakshi Swain* and Krishnan Venkatraman

Synergy Systems and Solutions, Faridabad - 121003, Haryana, India; Kamakshi_swain@s3india.com

Keywords: Control Centre, Risk Assessment, SCADA, Secure Development Lifecycle, STRIDE Model, Threat Model

Article Received: 15-01-2026
Article Revised: 29-01-2026
Article Accepted: 11-02-2026

DOI: 10.33686/pwj.22.1.2026.77-91

*Author for Correspondence

Abstract

Power System Control Centres consist of many different complex assets and data flows. It also facilitates bidirectional flow of data through varied communication infrastructure, including control commands to remote assets. In this paper, an overview and relevance of threat modelling in cyber-physical power systems are presented. A case study is demonstrated by leveraging the threat model formulation for the control centre and simulating the data flow among various entities. The high-fidelity threat model is used to evaluate the systems' operation under adverse conditions. Risk assessment enables the system vulnerability prioritisation considering impact on the system. The objective of the paper is to demonstrate the step-by-step process of threat modelling to achieve a more reliable operation of the control centre. This study also increases awareness for the utilities, system integrators, vendors, or asset owners to make an educated investment in system security and develop appropriate countermeasures at the system development life cycle stage.

This is an open access article under the terms of the **CC BY:** Allows others to copy, distribute, and build upon the work for any purpose, provided they credit the original creator

© 2026 The Author(s). *Central Power Research Institute* published by Informatics Publishing Limited

1. INTRODUCTION

The control centre has traditionally been the decision centre for the electric generation, transmission, and distribution system. The control centre acts as the nerve centre of the power system by providing the functions necessary for monitoring and coordinating the minute-by-minute physical and economic operation of the power system. It is essential that the security of the power system control centre is maintained, especially with the integration of legacy systems into the communication infrastructure as part of digitalisation. Supervisory Control And Data Acquisition (SCADA) applications are tightly coupled to their data sources, other dependent applications and the platform on which the SCADA system is implemented. Modern control centres routinely include functions like steady-state contingency analysis and optimal power flow, with real-time measurements. In recent years, the integration of sensors and actuators with intensive use of TCP/IP-based communication (like IEEE C37.118 or IEC 61850) network along with monitoring and control operations, has opened vulnerable points in the control centre. The control centre allows to enhance the operational efficiency by having a complex control and communication architecture with the need to coordinate with different systems and devices, many of which are not owned by the utilities.

Over the past decade, threat actors have increasingly exhibited a strategic intent to compromise power systems[1,2]. This trend is most prominently exemplified by the series of cyberattacks on the Ukrainian power grid. The initial incident in 2015 resulted in a widespread blackout affecting approximately 225,000 consumers[3]. A subsequent attack in 2016 targeted a single substation; although its immediate impact was limited, forensic analysis later revealed an unsuccessful attempt to disable protective relay mechanisms embedded within the grid infrastructure. In 2022, researchers identified a novel variant of the malware associated with the 2016 incident, which had been deployed against high-voltage substations in Ukraine[4].

A recent report by the Operational Technology (OT) cybersecurity firm Dragos[5] underscores the persistence of this threat landscape, documenting 18 active adversarial groups that have either previously targeted or continue to target the electric power sector. One technique for ensuring the security of power systems is gaining insight into possible vulnerabilities and threats.

For IT systems, various frameworks and knowledge databases, like MITRE ATT&CK. Threat models exist. They use different qualitative and quantitative threat assessment techniques[6,7]. In power systems, various research studies[8-10] have proposed a range of attack scenarios, system architectures, or mitigations for these attack scenarios. However, most of these studies are focused on the conventional SCADA system or target vulnerabilities on specific power system assets.

In this study, threat analysis and risk assessment are performed for the control centre architecture, considering signal in-flow and out-flow to/from the control centre. The specific contributions of this paper are as follows:

- Perform a threat model for the power system control centre architecture with the goal of determining the vulnerabilities associated with it.
- Evaluate the risk identified via the threat model, prioritise the vulnerabilities, and suggest remediation procedures.

This paper is organised as follows: Section 2 gives background information on threat modelling, risk assessment, and a state-of-the-art review of threat models in power systems. Section 3 describes the process and design methodology of threat modelling, followed by Section 4, which demonstrates a case study of control centre architecture and how to identify the risk while assessing the threat model. Section 5 discusses mitigation techniques associated with identified threats, and Section 6 concludes the work.

2. BACKGROUND AND RELATED WORK

In this section, the state-of-the-art research in threat model, risk assessment, tools, and related work for securing cyber-physical systems is discussed.

2.1 Threat Model

Threat Modelling is a process to understand potential threat events to a system, determine risks from those threats, and establish appropriate mitigation procedures. With threat events, potential attack scenarios to the system are identified. Common terminology associated with threat models is as follows:

- *Threat Actor*: who performs the attack scenario
- *Risk*: Potential loss caused by a threat event.
- *Data Flow Diagram (DFD)*: DFDs are a graphical representation of a system, and here the user will specify each element, their interaction, and helpful context.
- *Mitigation*: These are the actions that may decrease the risk associated with a threat event.

The objective of threat model analysis is to understand the risk represented by a system and identify potential mitigations. The intent is to enable the identification of a number of mitigations which, if implemented, would reduce the overall residual risk to an acceptable level. There is an important interplay between requirements, threats, and mitigation. A threat model aids in finding any design issue before the system is implemented or developed. Threats can be categorised in multiple ways, and this paper follows the approach defined by Microsoft, called STRIDE. The initials define the six categories of attack, as shown in Table 1.

2.2 Risk Assessment

The first step in designing the security framework for a system is to create threat models to identify the assets which need security, various attack vectors targeting the assets, classifying the threats based on criticality and possible mitigation. The second step pertains to risk assessment of the defined threats. Risk assessment prioritises which threats to be dealt with immediately and what security requirements are needed to remediate the threats identified in the threat model.

There are several risk assessment ratings and processes to assess and rank the cyber risk. To address the risk assessment and pre- and post- compromise events, MITRE has developed the ATT&CK for Enterprise framework[11]. MITRE ATT&CK is an open-source knowledge base which includes common attack

Table 1. Categories of cyber attacks

Category	Desired property	Definition
Spoofing	Authentication	Impersonating someone or something else
Tampering	Integrity	Unwarranted modification of code or data
Repudiation	Non-repudiation	Ability to claim to not have performed some action against the solution
Information Disclosure	Confidentiality	Exposure of information to unauthorised users
Denial of service	Availability	The ability to deny or degrade the service to the legitimate users.

vectors and techniques, and it is continuously updated according to the most recent cyber-attack incidents. This framework presents tactics, techniques, and procedures that an adversary could follow to fabricate a stealthy attack and compromise the asset. Later in 2020, MITRE included attack vectors concerning the Industrial Control System (ICS) and launched the ATT&CK for ICS framework[12]. MITRE has developed the EMB3D™ model to improve the overall security of embedded devices' hardware and software. While MITRE ATT&CK framework focuses on traditional IT environments, EMB3D™ framework specifically targets embedded devices.

The ATT&CK for ICS framework is also a community-supported threat knowledge base that includes information regarding the tactics, techniques, and procedures for attacks concerning ICS assets and networks. Further, the EMB3D™ framework aims to provide a comprehensive understanding and single repository of information defining known threats to embedded devices. The MITRE EMB3D™ framework includes the following components:

- *Device properties*: describe a device's hardware and software components and its capabilities such as physical hardware, network services and protocols, software, and firmware.
- *EMB3D threats*: define how threat actors can achieve their objective or cause an effect on a system or device. Each description of a threat includes:
    - information about the targeted technical features
    - the actions that must be taken, including the impact of the threat if successful
    - vulnerabilities within that mechanism required for the threat to succeed
- Mitigation strategies and techniques for each threat.

In a power system control centre, the ICS includes operating systems, workstations, communication protocols co-existing with several field devices such as Remote Terminal Unit (RTU), Intelligent Electronic Devices (IEDs), Programmable Logic Control (PLC), and data flow among various internal as well as external entities. Embedded device-level vulnerabilities in RTU and PLC will come under the purview of EMB3D™.

MITRE ATT&CK framework is segregated into four components such that it is applicable to a wide range of cyber-physical components. The first category includes assets which consist of servers, field controllers, and Human-Machine Interface (HMI). The second core factor of the ATT&CK framework focuses on the functional levels of Purdue architecture. Primarily, there are five levels of Purdue architecture, and they are:

- Level 0: The physical process (equipment that produces products).
- Level 1: Intelligent devices (sensing and controlling physical processes)
- Level 2: Control systems (supervising, monitoring, and controlling physical processes, HMIs)
- Level 3: Manufacturing operations system
- Level 4: Business logistics systems (managing business-related activities)
- Level 5: Enterprise networks

The last two parts of the framework focus on the adversary, *i.e.*, the tactics and techniques. Tactics refer to the attacker's objective, such as disrupting an industrial process control routine. Techniques are the 'how' and methods utilised by the hacker to accomplish a malicious goal. This may include exploiting a vulnerability to actively infiltrate a system.

2.3 Tools for Threat Modelling

The following overview presents commonly used threat-modelling and risk-assessment tools in a more approachable tone. For teams just getting started, free and open-source options such as OWASP Threat Dragon and the Microsoft Threat Modelling Tool (TMT) offer straightforward STRIDE-based diagramming and are ideal for developers and small projects.

2.4 Related Work

Threat modelling has emerged as a viable practice for secure development, deployment, and maintenance, in which the respective stakeholder identifies, specifies, evaluates, and assigns potential countermeasures for potential attack scenarios. It can be conducted in various stages of the system lifecycle such as requirements analysis, design, implementation, and even the testing phase[13]. The literature presents a range of threat modelling approaches for Cyber-Physical Systems (CPS), each tailored to different research and practitioner needs. Selecting an appropriate method typically hinges on stakeholders' expertise, goals, available time, and tools. Although many techniques have been proposed, only a handful, such as STRIDE and LINDDUN, are widespread in practical adoption. The authors[14] present a STRIDE-based use case within the smart grid domain, proposing a five-step methodology for applying STRIDE to Cyber-Physical Systems (CPS). The steps include: (i) decomposing the system into components, (ii) constructing Data Flow Diagrams (DFDs) for those components, (iii) analysing threats within the DFDs, (iv) identifying vulnerabilities, and (v) planning mitigation strategies. Although the framework[14] offers a lightweight approach, it relies on the prior identification of threat consequences by domain experts during the threat analysis stage. This dependency poses challenges for teams lacking expertise in both electrical engineering and cybersecurity, as it requires defining threat consequences before the actual process of threat identification. STRIDE is applied to Advanced Metering Infrastructure (AMI)[15] to categorise the common attack vectors in AMI. The study[16] presents a STRIDE case study based on a proposed solution for controlling industrial processes. The research prioritises the threats based on a risk assessment model, where the risk is calculated by the multiplication of Likelihood and Impact, and a value on a scale of (0–10) is assigned for both Likelihood and Impact. The threat model[17] is applied to a power transformer diagnosis system and proposes a STRIDE threat model chart, and each threat is mapped to a Common Vulnerability Enumeration (CVE) and Common Vulnerability Scoring System (CVSS), and this mapping was used to prioritise the threat. Reference[18] leverages a threat modelling template in the Microsoft Threat Modelling tool to identify threats to a smart grid secondary substation and proceeds to analyse a subset of the threats through emulation. Works that use alternatives to STRIDE include those of Ling and Ekstedt[19,20], Hawrylak *et al.*[21], Suleiman *et al.*[22] and Omerovic *et al.*[23].

The work presented in the literature tends to apply to theoretical testbeds, or it focuses on a particular asset, the literature also shows that there is a lack of detailed threat modelling methodologies, which highlights the procedure related to trust boundaries and threat modelling assumptions in the context of power systems.

3. THREAT MODEL PROCESS IN POWER SYSTEM

In this section, the need for threat modelling in cyber-physical power systems, along with the design methodology and process to perform threat modelling, is described. In a power system control centre, attackers may intercept the power system asset data, power consumption reports, control commands, outage reports, and fault notifications. Attackers may compromise the control centre and its communication links by flooding them with unwanted or spoofed data traffic. This will impact the control centre's resources. Communication links could be congested and lead to communication latency due to limited bandwidth. Thus, the threat model helps in identifying and capturing the system vulnerabilities which could be potentially exploited by an adversary. Various steps to design a threat model are discussed in upcoming subsections.

3.1 Design Methodology

Asset identification is one of the initial stages of threat modelling. The information in the asset list is crucial, as they play a significant role in comprehension of threats and the information flow. This understanding of

assets is mature in IT -based system, however, in cyber-physical power systems, it is not as clear to perceive like in IT-based systems.

When identifying assets and threats, the central question is "What requires protection?" In a perfect scenario, every component that contributes value to the system would be protected. However, complexity and expenses restrict the choice to protect what is necessary. These features are referred to as assets, and each asset has one or more properties to protect, such as availability, integrity, confidentiality, non-repudiation, and authorisation. System attacks will address one or more security goals of the CIA triad, including confidentiality, integrity, and availability. Active cyber-attacks can directly or indirectly change or damage the system processes and components. In contrast, passive attacks are only used to obtain valuable information, like sensor configuration, asset information, credentials, *etc*.

The threat models are represented through the diagrams derived from Data Flow Diagrams (DFDs). As per IEC 62443, there are entities which describes various parts to be analysed. The main types are hosts, network devices, embedded devices, and zones. The main steps of threat modelling are the following: (i) identifying the assets of an application, (ii) determining the threats to an application, (iii) ranking the threats, and (iv) mitigating the threats.

3.2 Identification of Assets

Threat modelling begins with gathering various information from the component's specifications and compiling it into the DFD. The initial step is to specify which entity will be covered in threat modelling. Then the following details should be captured to develop a threat model:

- *Assets and components*: Inventory of physical devices (RTUs, IEDs, PLCs), communication links, control servers, HMIs, and cloud/IT systems.
- *Data flows and protocols*: Message paths, telemetry rates, and protocols (*e.g.*, IEC 61850, DNP3, Modbus).
- *Trust boundaries and zones*: Delineation between corporate IT, OT, field networks, and third-party connections.
- *Operational procedures*: Maintenance schedules, patching policies, remote access practices, and incident response playbooks.
- *Threat and vulnerability context*: Historical incidents, known CVEs

Collecting these categories is foundational to structured threat modelling frameworks.

3.3 Ranking threats

Threat types and events are assigned different severities to represent their importance, in accordance with Table 2.

Table 2. Threat severity ranking

Severity	Description
Critical	*Critical Severity*. Critical-level threats are related to the most important issues, both for the probability and potential impact.
High	*High Severity*. High-level threats are related to important issues both for their probability and potential impact. They have a significant probability of causing major damage to the solution and the involved counterparts.
Medium	*Medium Severity*. Medium-level threats are related to average issues, both for their probability and potential impact.
Low	*Low Severity*. Low-level threats are related to minor issues, both for their probability and potential impact.
Info	*Informational only*. It is related to mitigated issues that have a negligible probability of causing even minor damage to the solution and the involved counterparts.
Unknown	Unknown or unassigned severity.

4. CASE STUDY

The case study demonstrates the threat modelling of a typical control centre and how it can be used to assess the risk and security concerns of a control centre.

4.1 Control Centre Architecture

The SCADA function in a control centre starts with the RTUs/Gateways/PMUs collecting data from the field devices, and these data are telemetered via a dedicated communication channel. In Figure 1, Remote Terminal Units (RTUs) send the analogue and digital measurement values, like feeder voltage, line power flow, or breaker status, to the SCADA server.

RTUs typically communicate on the IEC 60870-5-101/104 protocol; however, DNP3-based communication is prevalent in North America. Computer communication on the Internet, as well as in LANs, uses standard protocols.

The threat model for the control centre architecture is shown in Figure 2, and the DFD is modelled using the tool Threats Manager Studio. The DFD presents a graphical schematic of various components, demonstrating all the inputs and outputs, routing data flow along with different trust boundaries in the control centre. DMZ to management/SCADA zone contains public-facing services like web, mail, and SMS gateway, and they expose an attack surface for remote exploits. The model is created by picking out the specific components, attack steps and defences relevant to the scenario or system that one would like to assess. The asset list for the demonstrated case study is as follows:

- *SCADA server*: These devices cover the functionality of data acquisition and processing in real-time from various sensors and IEDs. It serves as an interface between the field device and the operator.
- *Engineering Workstation*: These units are the peripheral devices used to edit and generate the control system databases, schematics, *etc.* and reside within the control centre environment. They include hardware components and software packages.
- *Data Historian*: They serve as the database to keep records, gather data from SCADA, and store process data. Historians are specialised tools that capture, log, and store time-series data and events, making historical records available for review and analysis.
- *Human-Machine Interface (HMI)*: A graphical user interface that enables users to monitor the system operations, diagnose anomalous system behaviour, and initiate control and remediation actions.
- *Communication server*: Data collected from the SCADA server is communicated using the comm server.

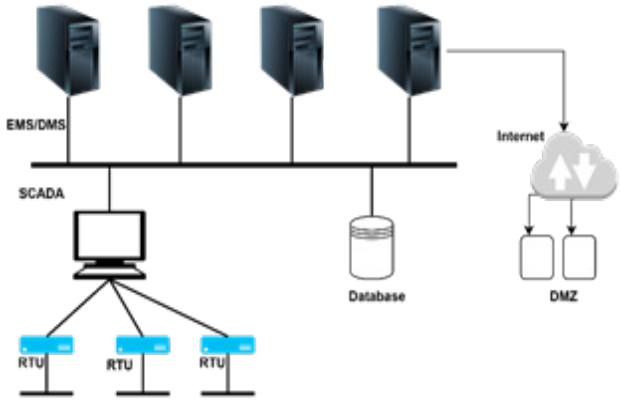


Figure 1. Generic control centre architecture.

In Figure 2, the DMZ LAN connects the Internet-facing services to the external firewall and routers, and this LAN isolates public traffic from internal systems. SCADA LAN connects the core OT network, and FEP LAN is the bridge between field communication and SCADA servers. The external DMZ boundary has the least trust as it contains the public-facing services, and to emphasise the same, the external DMZ has a red halo in the threat model. Possible threat actors and entry points for this case study are the web client, operator workstation, and RTU, respectively. The least-trusted boundary and threat points are highlighted in Figure 2.

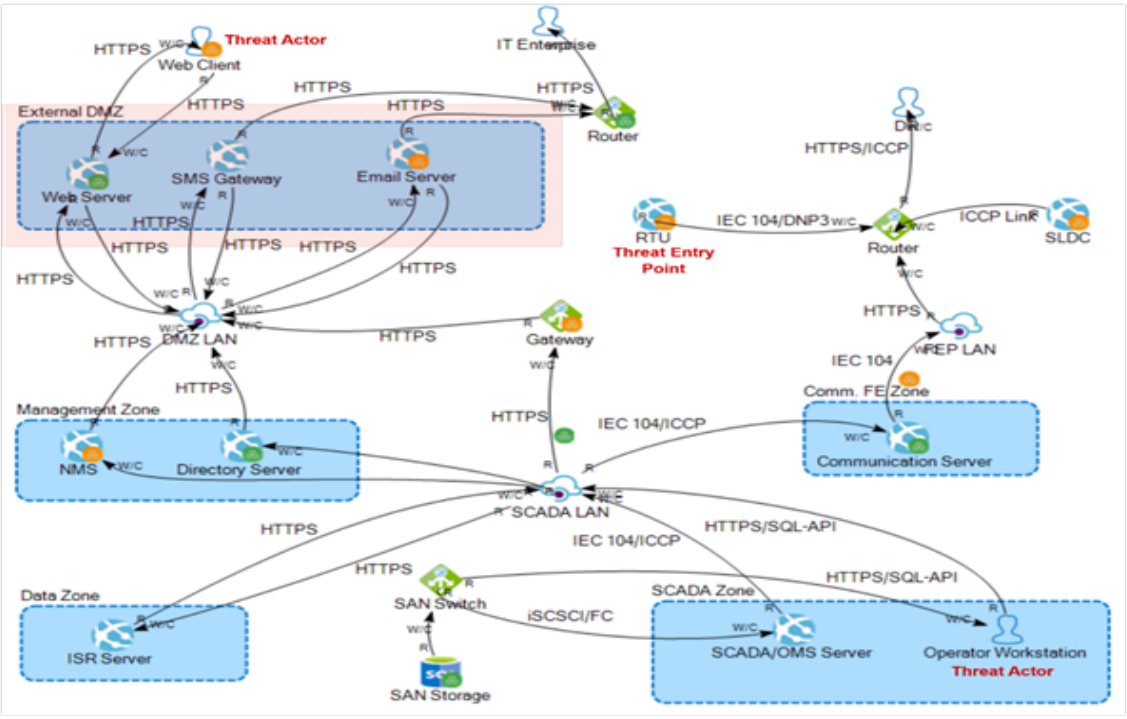


Figure 2. Threat model for the control centre.

An adversary may exploit vulnerabilities in these endpoints—through an external link from the IT/web environment or the RTU communication link to manipulate the information presented to control-centre personnel by intercepting or altering the communication protocols used for data exchange. Unauthorised access to workstations can enable attackers to assume control of development or operational processes executed on those hosts, while impersonation of an HMI can present a falsified interface that induces operators to execute inappropriate control actions on the SCADA system. The HMI displays data reported from RTUs and PLCs, including equipment status collected from actuators and sensors and archived in the historian server; compromise of these data flows therefore permits deception of situational awareness. This class of compromise is a network-based threat that commonly manifests as a man-in-the-middle attack. The threats anticipated from the data flow diagram, along with their severity, are listed in Table 3.

Table 3. Threats for the DFD of the control centre

Name	Associated To Type	Associated To	STRIDE Tag(s)	Severity
Weak or missing authentication allows unwarranted access to sensitive data	Process	Communication Server	S, I, E	High
High-privileged accounts can be exploited to perform malicious actions	Process	External Firewall	S, R, E	High
Secrets may be disclosed due to weak protection	Process	NMS	I	High
Malicious content may be sent to the solution	Process	RTU	S, T	High
Misconfigurations may allow compromise	Process	SMS Gateway	T, E	High

Attacks may go undetected due to lack of monitoring	Process	Web Server	R	High
Sensitive data may be disclosed in transit	Flow	HTTPS	I	High
An internal resource may be accessed by external actors	Process	Directory Server	S, I, E	Medium
A malicious actor may compromise the content of the storage	Process	Email Server	T, I	Medium
Communications towards an external service may be intercepted	Process	Email Server	T, D	Medium
Solution may be tampered due to weak protection	Process	Router	T, I	Medium
A malicious actor may compromise the content of the storage	Process	SLDC	I, T	Medium
Communications towards an external service may be intercepted	Process	SMS Gateway	I, T	Medium
Communications towards an external service may be intercepted	Process	Web Server	I, T	Medium
A malicious actor may compromise the content of the storage	Data Store	SAN Storage	I, T	Medium
Communications towards an external service may be intercepted	Flow	IEC 104	I, T	Medium
A malicious actor may cause a full-scale outage	Process	Web Server	D, T	Low

Note: S= Spoofing; T= Tampering; R= Repudiation; I= Information disclosure; D= Denial of service; E= Elevation of privilege

4.2 Evaluation of Security Risk

4.3 Risk Assessment

The Threat Types identified during the Threat Modelling exercise do not necessarily correspond to vulnerabilities which will necessarily be exploited by attackers. This means that the Threat Model do not describe a prescriptive set of activities that must necessarily be done, but rather guides to understand the risk represented by the analysed solution and a starting point to decide how to address it. Thus, the recommended approach is to discuss and define what measures to take for each threat type, which will lead to one of the following options:

- Simply accept the risk, track it and do not implement any action. This is often referred to as acceptable residual risk.
- Select one or more mitigations, picking from the proposed list or identifying additional options to mitigate the risk.
- Avoid the risk by completely removing the functionality that is causing it.
- Transfer the risk to someone else.

Potential risks for the control centre architecture considered in Section 4(A) are as follows:

Remote control over SCADA protocols: An adversary with sufficient know-how or in possession of malware that knows SCADA protocol operations can potentially masquerade as a SCADA control system, and thus capture the information flow between the RTU and the SCADA control system. The attacker may even issue control commands over the communication channel while masquerading as a SCADA control system.

Remote access via internet/public/unsecured networks: Connecting the RTU to Internet/Public/ Unsecured networks will increase the possibility of attacks on the RTU. In such a scenario, the attacker may cause the device to malfunction or take control of the device using publicly documented methods.

Exploiting unwanted/unused/default services: In many applications, not all features provided by an IED are required. Novice or careless engineers might leave these features enabled, which can allow access to the IED by a potential cybercriminal, either by directly using those services or by exploiting known weaknesses in such services.

5. MITIGATION PROCESS

Once threats are identified and prioritised according to their severity, the next step is to determine if the device sufficiently defends against those threats. This study utilises MITRE EMB3DTM for probable mitigation techniques. In EMB3DTM, each threat description includes a set of Foundational, Intermediate, and Leading mitigations. Foundational or tier 0 mitigations are the minimal capability deployed to devices as a remediation step from an associated threat. These mitigations have been deployed across embedded devices, showing their implementation and operational feasibility. Tier 0 mitigations do not require additional hardware or dependence on other commercial technology. Intermediate or tier 1 mitigations have been commercially adopted by systems, thus demonstrating their significant value. However, Tier 1 mitigations lack specific artefacts focused on implementation. Leading or tier 2 mitigations are the most robust mitigations for the identified threat and include state-of-the-art research. With limited deployment, technical guidance for implementation may not be available.

Mitigations will be associated with a threat type or event, and the objective is to reduce the risk for an asset. When a threat occurs, the associated mitigation will be considered a standard procedure or logical link to follow. It can be grouped accordingly with a control type, which describes when the mitigation is effective and how it operates. Control types could be the following categories as mentioned in Table 4.

Table 4. Categories of mitigation

Name	Description
Preventive	Reduces the probability or impact of the threat event
Detective	Detects an attack while it is in progress
Corrective	Responds to an attack, limiting the damage done
Recovery	Recovers from the damage that occurred from an attack
Other	Other types of security control

Table 5 provides a high-level view of mitigations, showing which mechanisms address a particular threat and leaving room for different implementation approaches depending on each device's limitations.

Table 5. Proposed mitigation for the identified threats

Threat event	Mitigation proposed	Mitigation tier	Control type	Associated to
Communications towards an external service may be intercepted	Apply strong channel encryption	Foundational	Preventive	Web Server
Sensitive data may be disclosed in transit	Configure the minimum required version of Transport Layer Security (TLS)	Foundational	Preventive	HTTPS

Threat event	Mitigation proposed	Mitigation tier	Control type	Associated to
Weak or missing authentication allows unwarranted access to sensitive data	Limit exposure to inbound network traffic	Foundational	Preventive	Communication Server
Sensitive data may be disclosed in transit	Limit Shared Access Signature (SAS) tokens to HTTPS connections only	Foundational	Preventive	HTTPS
A malicious actor may compromise the content of the storage	Lock resources to prevent unexpected changes	Foundational	Preventive	SAN Storage
Malicious content may be sent to the solution	*Decidable protocols and parsers*: Structured data and protocols should be designed using the lowest level of grammar possible so that parsers can be made using minimally and appropriately matched computational models	Intermediate	Preventive	RTU
Solution may be tampered with due to weak protection	*Security-relevant auditing and logging*: Devices should include audit logs of all user access, configuration changes, program updates, service starts and stops, and other events related to security. This allows device operators and security teams to investigate device actions and hunt for unusual behaviour that may be indicators of compromise.	Foundational	Detective	Router
Solution may be tampered with due to weak protection	*Require authentication for privileged functions*: Privileged functions that can severely affect the performance or critical functions of a device should only be accessible to authenticated privileged users. This includes functions such as configuration changes, user account changes, role and permission changes, operating state changes, *etc.*	Foundational	Preventive	Router

Threat event	Mitigation proposed	Mitigation tier	Control type	Associated to
Solution may be tampered with due to weak protection	*Physical presence validation*: Requirements such as a key being inserted, a button being pressed, a switch being flipped, *etc*. can provide a device with guarantees around the physical presence of an operator. Devices can then choose not to perform a critical operation until that physical step is taken, with a lack of action preventing all critical actions.	Foundational	Corrective	Router
A malicious actor may compromise the content of the storage	*Authenticate network messages*: Authenticating network traffic makes it more difficult for threat actors to leverage unauthenticated network data sent by or to the device. By authenticating network traffic, threat actors cannot send any data that will be accepted unless they also compromise the corresponding authentication credentials.	Foundational	Preventive	Email Server
Secrets may be disclosed due to weak protection				NMS
A malicious actor may compromise the content of the storage				SAN Storage
Communications towards an external service may be intercepted				IEC 104
An internal resource may be accessed by external actors	*Encrypt network traffic*: Encrypting network traffic typically involves taking network data and running it through an encryption algorithm such that the network data cannot be read in its encrypted form - this achieves data confidentiality. Therefore, encrypting network traffic allows devices to share critical or secret information without worrying about a third party reading the data.	Foundational	Preventive	Directory Server

Threat event	Mitigation proposed	Mitigation tier	Control type	Associated to
Weak or missing authentication allows unwarranted access to sensitive data	*Authenticate for administrative actions*: Administrative actions on a device usually involve a subset of device actions that, if undertaken, could have an impact on the integrity of the device or its operations. These may include accessing certain I/O interfaces, changing the roles of another user, changing user permissions or credentials, using debugging modes, or altering device operating states, to name a few.	Foundational	Preventive	Communication Server
The solution may be tampered with due to weak protection				Router
A malicious actor may compromise the content of the storage				SLDC
A malicious actor may compromise the content of the storage				SAN Storage
Cross-Site Scripting (XSS)	*Sanitised and escaped user data for web applications*: Web applications should encode all outputs of user data, put safety controls around all inputs, and store variables in safe attributes.	Foundational	Preventive	Web Client
An internal resource may be accessed by external actors	*Secure network tunnels*: When a protocol itself does not support authentication, encryption, and/or message integrity checking, secure network tunnels can be implemented to provide communications with those security features.	Intermediate	Preventive	Directory Server
A malicious actor may compromise the content of the storage				Email Server
High-privileged accounts can be exploited to perform malicious actions				External Firewall
The solution may be tampered with due to weak protection	*Network firewall/access control list*: If a device has routing capabilities, the device should have a firewall and Access Control List (ACL) present to prevent unintended network connections from being made and maintained	Foundational	Preventive	Router
Sensitive data may be disclosed in transit	Redirect HTTP to HTTPS	Foundational	Preventive	HTTPS
Sensitive data may be disclosed in transit	Reject requests not protected by TLS	Foundational	Preventive	HTTPS
Communications towards an external service may be intercepted	Use secure connections when accessing on-premises resources	Foundational	Preventive	Web Server

6. CONCLUSION

This paper demonstrates the threat modelling analysis for a typical power system control centre. The main security threats are discussed in detail along with the procedure to develop a data flow diagram. The case study presents the threat analysis together with the objective to provide the means to gain a better understanding of how an adversary may compromise the control centre security, provide foundational background to investigate more sophisticated attacks and vulnerabilities along with their impact on the system, and, most importantly, to envision critical security vulnerabilities existing in the underlying communication and network architecture as a precautionary measure. This study also increases awareness for the utilities and system integrators to make an educated investment in system security and develop appropriate countermeasures or remediation procedures at the system development life cycle stage.

7. REFERENCES

1. Goel S, Hong Y, Papakonstantinou V, Kloza D. Security challenges in smart grid implementation. In: Smart Grid Security. Berlin/Heidelberg: Springer; 2015. p. 1-39. https://doi.org/10.1007/978-1-4471-6663-4_1
2. Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Comput Netw. 2020; 169:107094. https://doi.org/10.1016/j.comnet.2019.107094
3. ICS-CERT. Cyber-attack against Ukrainian critical infrastructure. ICS Alert (IR-ALERT-H-16-056-01). Washington, DC: Cybersecurity and Infrastructure Security Agency; 2016.
4. Salazar L, Castro SR, Lozano J, Koneru K, Zambon E, Huang B, *et al*. A tale of two Industroyers: It was the season of darkness. 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA; 2024. p. 312-330. https://doi.org/10.1109/SP54263.2024.00162
5. Dragos. OT cyber threat intelligence: Electric threat perspective. Hanover, MD: Dragos; 2024.
6. Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, *et al*. A review of cyber security risk assessment methods for SCADA systems. Comput Secur. 2016; 56:1-27. https://doi.org/10.1016/j.cose.2015.09.009
7. CVE - Common Vulnerabilities and Exposures (CVE) [Internet]. Available from: https://cve.mitre.org/ (Accessed 2026 Jan 5).
8. Khan R, Maynard P, McLaughlin K, Laverty D, Sezer S. Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid. In: 4th International Symposium for ICS & SCADA Cyber Security; 2016; p. 53-63. https://doi.org/10.14236/ewic/ICS2016.7
9. Huang X, Qin Z, Liu H. A survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis. IEEE Access. 2018; 6:69023-69035. https://doi.org/10.1109/ACCESS.2018.2879996
10. Swain KP, Sharma A, Karkare A, Chakrabarti S, Gryazina E, Terzija V. Network-level vulnerability assessment of synchrophasor measurement devices. IEEE Access. 2024; 12:72491-72503. https://doi.org/10.1109/ACCESS.2024.3403456
11. MITRE ATT&CK [Internet]. Available from: https://attack.mitre.org/ (Accessed 2026 Jan 14).
12. MITRE ATT&CK for ICS [Internet]. Available from: https://www.mitre.org/resources/attck-ics (Accessed 2026 Jan 15).
13. Xu D. Software security. In: Wiley Encyclopedia of Computer Science and Engineering. Hoboken, NJ: John Wiley & Sons; 2008.
14. Jamil AM, Ben Othmane L, Valani A. Threat modeling of cyber-physical systems in practice. In: Luo B, Mosbah M, Cuppens F, Othmane LB, Cuppens N, Kallel S (editors). Risks and security of internet and systems. CRiSIS 2021. Lecture Notes in Computer Science, vol 13204. Springer, Cham. https://doi.org/10.1007/978-3-031-02067-4_1
15. Haider MH, Saleem SB, Rafaqat J, Sabahat N. Threat modeling of wireless attacks on advanced metering infrastructure. In: Proceedings of the International Conference on Mathematics, Actuarial Science, Computer Science, and Statistics (MACS), Karachi, Pakistan; 2019; p. 1-6. https://doi.org/10.1109/MACS48846.2019.9024779
16. Ferrer BR, Afolaranmi SO, Lastra JLM. Principles and risk assessment of managing distributed ontologies hosted by embedded devices for controlling industrial systems. In: IECON 2017 - 43rd Annual Conference of Industrial Electronics Society, Beijing, China; 2017. p. 3498-3505. https://doi.org/10.1109/IECON.2017.8216592

17. Ahn B, Kim T, Smith SC, Youn Y-W, Ryu M-H. Security threat modeling for power transformers in cyber-physical environments. 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2021 Feb 16-18, Washington, DC, USA. https://doi.org/10.1109/ISGT49243.2021.9372271
18. Holik F, Fla LH, Jaatun MG, Yayilgan SY, Foros J. Threat modeling of a smart grid secondary substation. Electronics. 2022; 11(6):850. https://doi.org/10.3390/electronics11060850
19. Ling ER, Ekstedt M. Generating threat models and attack graphs based on the IEC 61850 system configuration description language. SAT-CPS '21: Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical System; 2021. p. 98-103. https://doi.org/10.1145/3445969.3450421
20. Ling ER, Ekstedt M. A threat modeling language for generating attack graphs of substation automation systems. Int J Crit Infrastruct Prot. 2023; 41:100601. https://doi.org/10.1016/j.ijcip.2023.100601
21. Hawrylak PJ, Haney M, Papa M, Hale J. Using hybrid attack graphs to model cyber-physical attacks in the smart grid. 2012 5th International Symposium on Resilient Control Systems, Salt Lake City, UT, USA; 2012, p. 161-164. https://doi.org/10.1109/ISRCS.2012.6309311
22. Suleiman H, Alqassem I, Diabat A, Arnautovic E, Svetinovic D. Integrated smart grid systems security threat model. Inf Syst. 2015; 53:147-160. https://doi.org/10.1016/j.is.2014.12.002
23. Omerovic A, et al. An industrial trial of an approach to identification and modelling of cybersecurity risks in the context of digital secondary substations. In Kallel S, Cuppens F, Cuppens-Boulahia N, Hadj Kacem A editors, Risks and Security of Internet and Systems. CRiSIS 2019. Lecture Notes in Computer Science, vol 12026. Springer, Cham. https://doi.org/10.1007/978-3-030-41568-6_2