Central Power Research Institute

Vol. 20(1)/35-45, June 2024
ISSN (Print) : 0973-0338
DOI : 10.33686/pwj.v20i1.1168

Power Research

Cyber Security: Perspective of Challenges in Operational Technology Systems in Power Sector

Debottam Mukherjee[1*], Abhijit Lele[1], Anand Shankar[2], T. S. Kiran[1], Bindhumadhava Bapu[1], N. Bharghav[1] and Gurunath Gurrala[3]

[1]Power Grid Center of Excellence, Indian Institute of Science, Bengaluru – 560012, Karnataka, India; debottamm@iisc.ac.in

[2]Power Grid Corporation of India Limited, New Delhi – 110016, India

[3]Department of Electrical Engineering, Indian Institute of Science, Bengaluru – 560012, Karnataka, India

Abstract

The paper explores the cyber security challenges faced by Operational Technology (OT) systems in the power sector, emphasising the need for a holistic approach that includes employee training, contingency planning, attack detection, and resilient protection schemes. It aims to contribute to a deeper understanding of the unique cyber security challenges and requirements of OT systems in power transmission utilities, enabling stakeholders to develop informed strategies, policies, and investments to mitigate cyber risks and enhance the resilience of electrical grids. Moreover, it also highlights the importance of training employees to identify and mitigate cyber threats, fostering a culture of security awareness. It also states how simulation and modelling can facilitate proactive identification and mitigation of potential cyberattacks on critical infrastructure while exploring robust security solutions for Intelligent Electronic Devices (IEDs) and proposes solutions for mitigating these threats. The importance of evaluating adherence to the IEC 62351 standard through dedicated tools and procedures is also emphasized.

Keywords: Cyber-Physical Power Network, Embedded Security, IEC 62351

1. Introduction

The power sector is dependent on "Security by Obscurity" as a measure of cyber-security[1]. However, the advent of the IEC 61850 standard in the year 2003, which is an international standard for the communication and interoperability of power utility automation systems, made reliance on digital technologies for communication. Thus, the interconnected systems pose a significant cyber-security challenge, which concerns grid reliability, operational continuity, and safety. The electrical power grids are classified as critical infrastructure of national importance, and disruptions due to cyberattacks can lead to widespread blackouts, economic losses, and public safety concerns.

Power transmission utility OT systems include control systems like Remote Terminal Units (RTUs) and Supervisory Control and Data Acquisition (SCADA) systems. Sensors and actuators collect data from the field and initiate actions based on control system commands. Human-Machine Interfaces (HMIs) allow operators and engineers to interact with OT systems, visualize data, and control processes. Networking infrastructure connects OT devices and systems, enabling data exchange, remote monitoring, and control. Figure 1 depicts the typical architecture of communication networks falling under the scope of Transmission System Operators (TSO). This architecture is taken from article[2], applicable to Protection and Control Engineers (P and C), and describes the cyber security mechanisms used to protect access to and use of system protection, System Integrity

**Author for correspondence*

Protection Schemes (SIPS), and local substation control and automation.

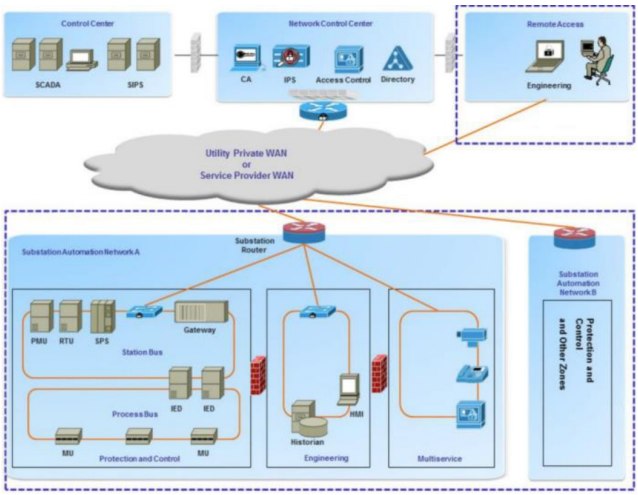

Figure 1. Typical Communication Architecture of TSO[2].

The IEC 61850 specifically focuses on communication networks and systems used in electrical substations and power generation facilities and aims to standardize communication protocols, data models, and system architectures within power utility automation systems. It provides a common framework for exchanging data and information between various devices and subsystems in substations, such as protection relays, bay controllers, RTUs, and HMIs. This made it possible to interconnect the substations and have a centralized control centre for monitoring and control. Thus the TSO like Power Grid Corporation of India Limited (PGCIL) India's transmission owner has built substation automation systems[3] and control centres at the national level[4] and many other states[5] and private players that have similar infrastructure which led to a need for cyber-security in the power system domain.

Cyber security of OT systems within the power transmission domain focuses on protecting critical infrastructure and control systems that manage the transmission of electrical power. Power transmission systems are essential components of the electrical grid, responsible for transporting electricity from power plants to distribution substations and eventually to end users. Ensuring the security of these systems is paramount in maintaining the reliability, availability, and safety of the electrical grid.

Some news stories on the internet demonstrate the increasing attacks on the essential infrastructure "Electric Power Grid". The European Network of Transmission System Operators for Electricity (ENTSO-E) reported a successful cyber intrusion into its office network in March 2020 and is implementing contingency plans to prevent future attacks[6]. In 2017, Saudi Aramco faced a cyberattack, with experts suggesting that an incident could have occurred despite the plant's shutdown. In 2016, Ukraine experienced a second cyberattack, leaving customers without electricity for an hour after disabling an electricity substation. A US report concluded that the virus was delivered via email through spear-phishing, a technique that ends key employees' detailed messages using social media information[6]. In 2014, South Korean nuclear and hydroelectric company Korea Hydro and Nuclear Power was hacked, stealing plans and manuals for two nuclear reactors and the data of 10,000 employees[6]. The North American Electric Reliability Corporation (NERC) reported a 2019 cyberattack on power grids, involving firewall firmware vulnerabilities, causing communication outages between control centers and generation sites. The disruption occurred due to an outside party rebooting firewalls, lasting around ten hours[7]. A UK power grid company, Elexon, has been targeted by a possible ransomware attack, affecting the Balancing and Settlement Code (BSC), a crucial part of the power supply chain. The company uses over one million meter readings daily to compare predicted production or consumption volumes with actual volumes[8].

This paper aims to analyze the cyber security landscape of OT systems in power transmission utilities, distinguishing it from Information Technology (IT) cyber security practices. It identifies the unique challenges, vulnerabilities, and requirements of OT systems, such as legacy infrastructure, interoperability issues, real-time operational constraints, and the convergence of IT/OT networks. Also emphasizes the importance of cross-disciplinary collaboration between IT, OT, cyber security, and regulatory stakeholders in addressing cyber security challenges in power transmission utilities. The paper advocates for a holistic and integrated approach to cyber security governance, risk management, and compliance to safeguard critical infrastructure and ensure grid reliability.

2. Challenges in Operating Technology Cyber Security

The cyber security requirements and measures in OT systems are different from IT systems, as the priority of the system objectives and requirements are different, thus cyber security measures applicable in IT systems may not be suitable for OT systems[1]. The detailed comparison objectives and requirement is tabulated in Table 1 and Table 2 respectively. Table 3 describes the threat landscape for the

power utility domain. Also, digitization and modernization of power grids, including smart grid technologies and advanced metering infrastructure, introduce new cyber security risks. With the growing number of cyber threats affecting OT systems, significant risks to the reliability, safety, and resilience of electrical grids. These threats are becoming more sophisticated, persistent, and diverse, driven by geopolitical tensions, technological advancements, and the expanding attack surface of interconnected OT networks[9].

Cyberattacks that are targeting power grids can take various forms and the mapping of threat to actors is tabulated in Table 4, such as ransomware, malware, phishing, Denial-of-Service (DoS) attacks, Advanced Persistent Threats (APTs), and others. Ransomware attacks are not a major concern for power utilities, as they can disrupt operations and demand ransom payments, leading to extended downtime, financial losses, and potential safety hazards are a major concern but in IT systems the data which is encrypted by attackers is of importance. Malicious software and botnets exploit vulnerabilities in software and network infrastructure, causing disruptions in control systems, data theft, and remote access by attackers will also lead to the stated problem and importance is given to restoring the system rather than data lost, as data is dynamic. Phishing and social engineering are common tactics used by cybercriminals to gain unauthorized access to OT systems[10].

Table 1. Comparison of IT and OT cyber security objectives

Objective	IT Cyber Security	OT Cyber Security
Confidentiality	Protect sensitive data and information from unauthorized access or disclosure.	Preserve operational data and control signals to prevent unauthorized manipulation.
Integrity	Ensure the accuracy and reliability of data by preventing unauthorized modification or tampering.	Maintain the integrity of operational data and measurements to support safe and reliable processes.
Availability	Ensure systems and services are accessible and operational when needed, minimizing downtime.	Maintain the availability and performance of systems to prevent disruptions to critical operations.
Authentication	Verify the identity of users, devices, or entities accessing IT systems to prevent unauthorized access.	Authenticate the identity of users and devices interacting with OT systems to prevent unauthorized control or manipulation.
Authorization	Grant appropriate permissions and privileges to users based on their roles and responsibilities.	Authorize access to OT systems and functions based on operational requirements and safety considerations.
Non-repudiation	Provide evidence that actions or transactions cannot be denied or disputed by the parties involved.	Ensure that operational actions or control commands cannot be repudiated or disputed in industrial processes.
Resilience	Enhance the ability of IT systems to withstand and recover from cyber incidents or disruptions.	Build resilience in OT systems to maintain operational continuity and recover from cyber-physical threats.
Compliance	Ensure compliance with relevant laws, regulations, and standards governing cyber security and data protection.	Comply with industry-specific regulations and standards for safety, reliability, and cyber security in industrial environments.

Table 2. Comparison of cyber security requirements for IT and OT systems

Requirement	IT Systems	OT Systems
Access Control	Implement Role-Based Access Control (RBAC) mechanisms to restrict access to authorized users based on their roles and responsibilities.	Enforce strict access controls to OT networks and devices, limiting access to essential personnel and trusted devices only.
Encryption	Encrypt sensitive data at rest and in transit using strong cryptography algorithms and secure communication protocols (e.g., TLS/SSL).	Encrypt communications between OT devices and control systems to prevent eavesdropping and tampering with operational data.
Patch Management	Regularly update and patch IT systems with security updates, patches, and fixes to address known vulnerabilities and mitigate potential security risks.	Follow a cautious approach to patch management in OT environments, carefully testing and validating updates before deployment to prevent disruptions to critical operations.

Table 2. Continued...

Requirement	IT Systems	OT Systems
Network Segmentation	Segment IT networks into separate zones or subnetworks based on security requirements and data sensitivity, implementing firewalls and access controls between zones.	Implement network segmentation in OT environments to isolate critical control systems from enterprise networks and external threats, reducing the attack surface and limiting the lateral movement of attackers.
Intrusion Detection	Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic, detect suspicious activities, and block malicious intrusions in real-time.	Implement specialized intrusion detection and prevention mechanisms tailored for OT environments, including anomaly detection, signature-based detection, and protocol whitelisting to identify and respond to cyber threats effectively.
Incident Response	Establish incident response plans and procedures to detect, analyze, and respond to cyber security incidents promptly, minimizing the impact on IT systems and data.	Develop comprehensive incident response capabilities for OT environments, including procedures for isolating compromised systems, restoring operations, and recovering from cyber incidents while ensuring the safety and reliability of industrial processes.
Physical Security	Implement physical security measures, such as access controls, surveillance cameras, and security guards, to protect IT infrastructure and prevent unauthorized access to data centres and server rooms.	Enhance physical security for OT assets, including substations, control rooms, and field devices, to safeguard against physical tampering, sabotage, or theft that could disrupt critical operations and compromise grid reliability.

Table 3. Cyber security threat landscape

Element	Related Elements
Threat Actors	• Nation-State Actors: APTs, Supply Chain Attacks • Cyber Criminals: Ransomware, Phishing • Terrorist Groups: DoS/DDoS • Insider Threats: All Cyber Threats
Cyber Threats	• Ransomware: Data Breaches, Power Outages • APTs: Data Breaches, Equipment Damage • DoS/DDoS: Power Outages • Phishing/Spear-Phishing: Data Breaches • Supply Chain Attacks: Data Breaches, Power Outages
Vulnerabilities	• Legacy Systems: Ransomware, APTs • Lack of Segmentation: APTs, Lateral Movement • Inadequate Access Controls: All Cyber Threats • Insufficient Monitoring and Detection: Delayed Response to All Threats
Potential Impacts	• Power Outages: Caused by Ransomware, DoS/DDoS, Supply Chain Attacks • Equipment Damage: Caused by APTs • Data Breaches: Caused by Ransomware, Phishing, APTs • Loss of Public Trust: Result of Any Impact
Mitigation Strategies	• Risk Assessment: Addresses All Vulnerabilities • Network Segmentation: Mitigates Lateral Movement • Regular Patching: Reduces Legacy System Vulnerabilities • Access Control and Monitoring: Prevents Unauthorized Access, Detects Threats • Incident Response Planning: Prepares for and Mitigates Impacts of Cyber Threats
Standards and Regulations	• NIST Framework: Addresses All Elements • IEC 62443: Focuses on System Security, Relevant to All Vulnerabilities • NERC CIP Standards: Mandatory for Power Utilities, Addresses All Elements

Table 4. Cyber security threat mapped to actors

Cyber Threats	State-sponsored Hackers	Cyber criminals	Other Hacktivists	Most Insiders	Script Kiddies	Organized Crime Groups	Terrorist Organizations	Other Competitors	Cyber Warfare Units	Advanced Persistent Threats (APTs)	Rogue Hackers	Cyber Espionage Groups
Malware	X	X		X	X	X				X	X	
Phishing		X	X			X						
Social Engineering		X	X	X		X						
DoS/DDoS Attacks	X	X				X			X			
Insider Threats				X								
Zero-Day Exploits	X					X				X		
MitM Attacks	X					X						
SQL Injection						X						
XSS			X			X						
Data Breaches	X	X		X		X	X					X
Ransomware	X	X				X	X					
Cryptojacking		X				X						
IoT Vulnerabilities	X	X		X		X						
Supply Chain Attacks	X	X				X						
Credential Stuffing		X				X						
DNS Spoofing/ Poisoning						X						
Brute Force Attacks	X	X				X						
APTs	X					X				X		
Physical Security Compromises		X		X		X	X					
Emerging Tech Threats	X	X		X	X	X	X	X	X	X	X	X

Supply chain risks are also growing, as attackers exploit vulnerabilities in third-party software, hardware, and service providers to gain access to critical infrastructure. Compromised supply chain components can introduce backdoors, malware, or counterfeit firmware into OT systems, undermining their security and integrity. Zero-day exploits targeting previously unknown vulnerabilities in OT software and firmware pose significant challenges for power utilities, as they often lack timely patches and mitigation measures. Insider threats, including disgruntled employees, contractors, or vendors, represent an ongoing risk to OT systems in the power sector, as they may abuse their privileged access to OT infrastructure to sabotage operations, steal intellectual property, or compromise system integrity[11].

Nation-state-sponsored cyber espionage and sabotage activities are also posing significant risks to power utilities, involving advanced persistent threats and coordinated cyber

campaigns aimed at infiltrating OT networks, compromising control systems, and causing widespread disruption to critical infrastructure[12]. However, gold-plating the IT measure onto OT requirements is not the correct measure. The problems associated with the gold-plating of IT measures are tabulated in Table 5.

Table 5. IT Gold plating for OT cyber security

IT Cyber Security Measures	Gold Plating for OT Cyber Security
Network Segmentation	Implementation of overly complex network segmentation that disrupts OT workflows or hinders operational efficiency.
Patch Management	Enforcing strict patch management policies without considering the impact on OT systems' availability or reliability.
Antivirus and Endpoint Security	It is deploying traditional antivirus solutions designed for IT environments that may not adequately protect specialized OT devices and control systems.
Intrusion Detection Systems	Installing intrusion detection systems that generate excessive false positives, leads to alert fatigue and overlooking genuine threats in OT environments.
Security Information and Event Management (SIEM)	Implementing SIEM solutions tailored for IT networks that may not effectively capture or analyze OT-specific security events and anomalies.
User Access Controls	Enforcing stringent user access controls that restrict operational personnel's ability to perform critical tasks or respond to emergencies promptly.
Encryption	Encrypting OT communication channels with protocols or algorithms unsuitable for real-time control systems, leading to latency issues or communication failures.
Vulnerability Scanning	Conducting vulnerability scans on OT systems without understanding their unique architecture and operational requirements, resulting in disruptions or outages.
Incident Response Planning	Developing incident response plans solely based on IT incident scenarios, overlooking the specialized processes and requirements of OT environments.
Security Awareness Training	Providing generic security awareness training to OT personnel without addressing specific threats, vulnerabilities, and operational risks.

3. Limitations and Potential Remedies in Operational Technology

One important shortcoming is the legacy nature of OT infrastructure. Many systems created decades ago lack the security features and protocols required for today's threat environment. Outdated software, unpatched vulnerabilities, and inadequate network segmentation make them easy targets for attackers. The integration of IT and OT systems complicates matters even more. As smarter technologies are integrated into the power grid, the distinction between operational and informational realms becomes blurred. This convergence opens up new attack routes, allowing criminals to exploit IT weaknesses to infiltrate and disrupt vital OT operations.

Furthermore, poor cyber security practices worsen the issue. Budgetary limits, a lack of awareness, and limited experience can result in ineffective security measures. Weak password management, unmonitored networks, and inadequate incident response skills make utilities vulnerable to basic hacks. The implications of these flaws can be severe. Cyberattacks can affect electricity grids, resulting in extensive outages and economic losses. Malicious actors can disrupt grid operations, potentially causing equipment damage, cascading failures, and even personal harm.

The likelihood of data breaches increases the risk of disclosing sensitive information and affecting system integrity. Addressing these issues demands an extensive approach. Upgrading outdated systems, creating strong cyber security standards, and fostering a security-conscious culture are critical initial steps. Furthermore, coordination among utilities, governments, and cybersecurity professionals is critical for sharing best practices and developing effective mitigation solutions. Only via such collaborative efforts can the power sector negotiate the hazardous landscape of cyber threats and assure a secure and resilient grid in the future. The essential steps connected with building a complete cyber security environment in power system OT operations can be divided into the following subsections.

3.1 Comprehensive Cyber Security Program and Employee Training

The incorporation of technology into power systems has created a security gap, leaving them vulnerable to cyberattacks. To eliminate these risks, a complete solution

that includes people, procedures, and technology is required[13]. This includes building a robust cyber security policy, deploying data encryption, network segmentation, and access controls, and emphasizing employee training and awareness. Training sessions should teach employees how to identify phishing attacks, social engineering tactics, and password hygiene. Simulated cyberattacks can help evaluate workforce readiness and identify areas for improvement. Fostering a culture of security and reporting suspicious activity without fear of punishment is critical for early detection and response. Risk assessments based on international standards such as ISO27001 or IEC 62443 offer a formal framework for detecting, assessing, and prioritizing security threats in all assets and systems.

Risk evaluations help create contingency plans for power systems, outlining recovery processes, communication protocols, and personnel responsibilities in case of a cyberattack. These plans are regularly tested and refined to ensure a smooth response during a crisis. Stakeholder collaboration, sharing information and best practices, is crucial for collective defense against sophisticated attacks. Cyber security is an ongoing process that requires continuous monitoring, adaptation, and investment to protect critical infrastructure[14].

3.2 Advanced Cyber-Physical Modelling Framework for Contingency Planning

Advanced Cyber-Physical Modelling (ACPM) frameworks are critical for protecting the power grid. These frameworks generate a digital duplicate of the power system, combining cyber and physical components to better comprehend cascading effects and enhance contingency planning. The foundation consists of mapping various power sector databases and consolidating information on physical assets, communication networks, software settings, and security measures. The cyber dependencies are removed, revealing hidden links between IT systems and crucial infrastructure[15]. The system automatically generates a cyber-physical dependency model, which depicts the interaction between cyber activities and their physical repercussions. A threat vulnerability database powers the framework by storing information about known cyber threats, their prospective attack paths, and the vulnerabilities they exploit. As new threats surface, the database adapts, keeping the architecture constantly updated. The ACPM framework evolves into a larger automation-driven model, simulating various cyberattacks in real-time, and predicting their impact on the physical grid. This proactive approach allows utilities to identify and address weaknesses before they are exploited in real-world attacks.

The ACPM framework employs complex algorithms to assess cyber threats, including possible infrastructure damage, economic losses, and public safety hazards. It optimizes resources and customizes security measures to maximum impact. The framework also suggests security countermeasures based on known vulnerabilities and dangers, such as network segmentation or software patching. This constant cycle of assessment and development assures grid resilience in the face of emerging threats. The ACPM framework also supports "What-if" scenarios for thorough risk assessment, allowing utilities to examine contingency preparations and suggest areas for improvement[16]. This proactive method enables grid managers to make educated judgements, resulting in a speedy and effective reaction to intrusions. ACPM frameworks, which integrate cyber and physical factors, provide a glimpse into the future of grid security, enabling utilities to safeguard critical infrastructure and ensure a secure power supply for future generations.

4. Testbed for Evaluating the Cyber Security of Operations

cyber security testbed provides a controlled environment in which to evaluate vulnerabilities, train workers, and develop effective power system defence techniques. These virtual sandboxes imitate power systems, allowing researchers and operators to test "what-if" scenarios without jeopardizing real-world infrastructure[17]. The process begins with the design and development of a basic testbed, which includes simulated power generation, transmission, and distribution components linked to communication networks. Simple assault scenarios are launched to test detection and response systems, and the testbed is augmented and enhanced as operators acquire experience. The simulation repertoire grows to include semi-coordinated attack scenarios that resemble real-world techniques in which attackers combine various vulnerabilities for maximum impact. The apex of testbed progression is coordinated attack scenarios, in which planned attacks target various weaknesses throughout the cyber-physical system. By witnessing such complex scenarios, operators can refine their incident response plans, ensuring a coordinated and effective defence.

Cyber security testbed is a critical instrument for increasing capacity and training individuals to detect and respond to cyberattacks. They offer hands-on experience, which promotes improved decision-making in real-world scenarios. Testbeds also encourage stakeholder collaboration, allowing utilities, government agencies, and cyber security professionals to share expertise and build joint protection measures[18]. Building robust testbeds is a continuous process that enables the power sector to shift from reactive defence to proactive anticipation. Testbeds protect vital infrastructure by constantly changing and adapting, ensuring power systems' security and resilience.

5. Cyber Security in Substation Automation System

Substation Automation Systems (SAS) are critical for power grid management, but they also offer a substantial cyber security risk. To maintain grid resilience, a comprehensive cyber security plan is required. This includes categorizing devices based on their usefulness and criticality, enacting specific security policies, and implementing role-based access control, secure communication protocols, and strong password management. Regular firmware updates and vulnerability patches are also necessary[19]. Cyber security testing is required throughout the lifetime, including Factory Acceptance Tests (FAT) and Site Acceptance Tests (SAT), which comprise vulnerability assessments, penetration testing, and protocol conformance tests for IEDs. Dedicated testing frameworks, such as the Common Vulnerability Scoring System (CVSS), can determine the vulnerability of Smart Protection System (SPS) devices to targeted assaults. Understanding acceptable communication patterns and bespoke automation for alarm generation can provide early warnings of potential attacks.

Risk mitigation for downstream IEDs receiving inputs from SPS devices is critical, which includes vulnerability evaluations and penetration testing to avoid exploitable entry points. Regular reviews of security rules, monitoring logs for suspicious activity, and incorporating emerging risks into testing methods are all necessary. Collaboration with cyber security professionals and participation in information-sharing forums can help build defences against emerging threats. A multi-layered approach, which includes device grouping, policy enforcement, rigorous testing, and constant monitoring, may help SAS establish a strong cyber security posture, ensuring the security and resilience of the power grid[20].

6. Embedded Systems Security for Field Devices

The increased reliance on linked field equipment in critical infrastructure needs strong embedded system security. A diversified strategy encompassing several methodologies and continual innovation is essential. Data collecting and surveying methodologies serve as the foundation, with known vulnerabilities, industry best practices, and open-source tools such as Ghidra and Binwalk identifying possible weaknesses and attack routes[21]. Penetration testing with these tools reveals hidden vulnerabilities and informs future mitigation measures. Modern methodologies such as fuzzing and symbolic execution generate complete baselines, providing a solid foundation for security assessment. Minimum testing criteria and procurement requirements based on established standards assure uniform security across all devices. Mandatory secure boot, code signing, and anti-tamper procedures improve the overall security posture. Automating methods and documenting the process allows for efficient mass testing and reproducibility. Advanced fuzzing techniques and machine learning for anomaly detection enhance threat identification. Blockchain-based Firmware Databases offer tamper-proof storage of known vulnerabilities specific to different field device types.

Developing innovative testing techniques and technologies that are customized to the specific problems of field devices remains critical. Research into hardware-based security features, side-channel analysis techniques, and advanced fuzzing algorithms can reveal previously unknown vulnerabilities. Additionally, automated reverse engineering techniques designed for IEDs can speed up vulnerability detection and analysis, saving significant time and money. By combining existing techniques, creative ideas, and constant development, we can create a strong security environment for embedded systems in field equipment. This maintains the dependability and resilience of essential infrastructure, protecting sensitive data and operations from cyberattacks. Remember that security is a continuous journey, not a one-time destination. We can protect the field by putting forth consistent effort and collaboration, ensuring confidence and reliability in the gadgets that power our interconnected world[22].

7. Machine Learning-based Intrusion/Attack Detection and Mitigation Systems

Machine learning is a potential solution to intrusion detection and mitigation in OT systems. It expands on the Policy Framework for Intrusion Detection in OT Systems, improving security beyond standard signature-based detection. The model is based on past operational data, network traffic patterns, and known vulnerabilities unique to the Industrial Control System (ICS) under protection. Testbeds that simulate realistic ICS environments are critical for training and testing these models, allowing researchers to assess their efficacy and discover potential flaws[23]. These testbeds also function as training areas for security officers.

However, machine learning for OT security faces several hurdles, including data availability and quality, integration into existing OT infrastructure without affecting operations, and ongoing retraining and adaptation owing to the always expanding threat landscape. Mitigation strategies include data augmentation, federated learning, security by design, continuous monitoring, and threat intelligence feeds[24]. Machine learning can be used to protect vital infrastructure, assure smooth industrial processes, and defend against cyberattacks by constructing strong models, using realistic testbeds, and adopting effective mitigation mechanisms.

8. Develop Cyber Resilient Protection Strategies based on the IEC 61850 Standards Framework

The worldwide standard IEC 61850 provides a solid framework for creating cyber-resilient protection strategies in power systems. However, reacting to the changing cyber threat scenario necessitates harnessing the experience of industry specialists, creating specific skill sets, and constantly upgrading compliance procedures. The IEC TC WG15 working group, made up of experienced engineers, security experts, and researchers, is critical for detecting potential attack routes and devising mitigation techniques. Investing in skill development for engineers and operators is critical, with training programs covering cyber threats, secure coding methods, and incident response processes. Fostering a culture of security awareness within firms is also critical. Finally, adapting and continuously evolving compliance procedures is necessary. Regular vulnerability assessments, penetration testing, and secure communication protocols are crucial elements to achieve cyber-resilient implementations of IEC 61850 [25].

A cyber resilient protection scheme can be created on the IEC 61850 standard by leveraging existing knowledge, developing specific skill sets, and embracing continuous development[19]. This enables the reliable and secure functioning of electricity grids, protecting critical infrastructure from an ever-changing threat scenario.

9. Evaluation of the IEC 62351 Standard using Tools and Procedures

The IEC 62351 standard, which is a critical component of cyber security in power systems, must be continuously evaluated to address new threats. This can be accomplished through a multifaceted approach that includes harnessing the experience of IEC TC WG15, the body responsible for the standard, and undertaking a detailed examination of the standard. This analysis should look into the effectiveness of its security advice, coverage, and alignment with current cyber threats. Tools such as gap analysis frameworks and threat modelling can help discover potential flaws and areas for development[1]. Key implementation suggestions should be prepared, providing practical assistance on how to efficiently apply the standard and customize it to unique industry needs. Collaborating with stakeholders ensures that these recommendations are feasible and actionable.

The implementation and testing of IEC 62351 processes for compliance are critical, necessitating internal expertise, specific testing equipment, and standardised procedures. Collaboration with accredited laboratories improves the evaluation process. Understanding IEC 62351's limitations enables targeted improvements and the creation of complementary security measures. Contributing findings to the IEC TC WG15 promotes continuous improvement. IEC 62351 remains a strong basis for cyber security in power systems, allowing the industry to keep ahead of evolving threats and protect vital infrastructure[26].

10. Conclusion

Cybersecurity is a serious challenge in the energy sector. Cyber threats to the energy delivery systems can not only

impact national security but also have a socio-economic impact. Looking at this critical importance of cyber security, the Power Grid Centre of Excellence in Cyber Security (PGCoE) is set up to drive a vision of securing the national power grid and build a roadmap to address the technology advances and the ever-evolving needs of the sector. PGCoE is tasked to build technologies towards building a resilient energy delivery system capable of detecting cyber incidents while sustaining critical functions. The primary drivers for PGCoE are but are not limited to (a) Building a culture of security (b) Assessing and monitoring risks in the energy sector (c) developing and implementing new protective measures to reduce risks and (d) sustaining security improvements. The operational model of PGCoE is to engage with academic institutions, industries, research labs and organizations in the power sector to identify short-term problems and long-term challenges to carve out a roadmap towards fulfilling the vision of a secure and resilient power grid.

11. References

1. Schlegel R, Obermeier S, Schneider J. A security evaluation of IEC 62351. J Inf Secur Appl. 2017; 34:19-204. https://doi.org/10.1016/j.jisa.2016.05.007
2. Malko J, Lis R. Cyberbezpieczen'stwo systemo'w zabezpieczen' i sterowania. Prz Elektrotech. 2016; 1:182-5.
3. Ministry of Power. Powergrid inaugurates remote operation of 250th sub-station [Internet]; 2021. Available from: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1768492
4. Ministry of Power. Haryana chief minister dedicates national transmission asset management centre of power grid to the nation [Internet]; 2015. Available from: https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=120012
5. The Times of India. Remote control at 22 state power sub-stations [Internet]; 2022. Available from: https://timesofindia.indiatimes.com/city/mumbai/now-remotecontrol-at-22-state-power-sub-stations/articleshow/93199340.cms
6. Macola IG. The five worst cyberattacks against the power industry since 2014 [Internet]; 2020. Available: https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/
7. Dean C. How and why power grid cyberattacks are becoming terrorists' go-to [Internet]. Available from: https://energycentral.com/c/iu/how-and-why-power-grid-cyberattacks-are-becoming-terrorists-go
8. M. Phil. UK power grid biz suffers outage after cyber-attack [Internet]; 2020. Available from: https://www.infosecurity-magazine.com/news/uk-power-grid- biz-suffers-outage/
9. Hollerer S, Brenner B, Bhosale PR, Fischer C, Hosseini AM, Maragkou S, *et al*. Challenges in OT security and their impacts on safety-related cyber-physical production systems. Digital Transformation, Springer; 2023. p. 171-202. https://doi.org/10.1007/978-3-662-65004-2_7
10. Scarfò AA. The cyber security challenges in the IoT era. Security and resilience in intelligent data-centric systems and communication networks. Elsevier; 2018. p. 53-76. https://doi.org/10.1016/B978-0-12-811373-8.00003-3
11. Jesus V, Josephs M. Challenges in cybersecurity for industry 4.0. Innovation in manufacturing through digital technologies and applications: Thoughts and Reflections on Industry 4.0; 2018. p. 61. Availa from: https://research.aston.ac.uk/en/publications/innovation-in-manufacturing-through-digital-technologies-and-appl
12. Parsons D. The state of ics/ot cybersecurity in 2022 and beyond. Survey Report; 2022.
13. He W, Zhang Z (Justin). Enterprise cybersecurity training and awareness programs: Recommendations for success. J Organ Comput Electron Commer. 2019; 29(4):249-57. https://doi.org/10.1080/10919392.2019.1611528
14. Krumay B, Bernroider EWN, Walser R. Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. Secure IT Syst. 2018; 11252:369-84. https://doi.org/10.1007/978-3-030-03638-6_23
15. Zonouz S, Davis CM, Davis KR, Berthier R, Bobba RB, Sanders WH. SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures. IEEE Trans Smart Grid. 2014; 5(1):3-13. https://doi.org/10.1109/TSG.2013.2280399
16. Mouelhi S, Laarouchi ME, Cancila D, Chaouchi H. Predictive formal analysis of resilience in cyber-physical systems. IEEE Access. 2019; 7:33741-58. https://doi.org/10.1109/ACCESS.2019.2903153
17. Ukwandu E, Farah MAB, Hindy H, Brosset D, Kavallieros D, Atkinson R, *et al*. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors. 2020; 20(24):7148. https://doi.org/10.3390/s20247148 PMid:33322224 PMCid:PMC7764257
18. Hahn A, Ashok A, Sridhar S, Govindarasu M. Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans Smart Grid. 2013; 4(2):847-55. https://doi.org/10.1109/TSG.2012.2226919
19. Moreira N, Molina E, Lázaro J, Jacob E, Astarloa A. Cyber-security in substation automation systems. Renew Sustain Energy Rev. 2016; 54:1552-62. https://doi.org/10.1016/j.rser.2015.10.124
20. Hong J, Liu CC, Govindarasu M. Integrated anomaly detection for cyber security of the substations. IEEE Trans

Smart Grid. 2014; 5(4):1643-53. https://doi.org/10.1109/TSG.2013.2294473
21. Hwang DD, Schaumont P, Tiri K, Verbauwhede I. Securing embedded systems. IEEE Secur Priv Mag. 2006; 4(2):40-9. https://doi.org/10.1109/MSP.2006.51
22. Manifavas C, Fysarakis K, Papanikolaou A, Papaefstathiou I. Embedded systems security: A survey of EU research efforts. Secur Commun Netw. 2014; 8(11):2016-36. https://doi.org/10.1002/sec.1151
23. Abubakar A, Pranggono B. Machine learning based intrusion detection system for software defined networks. 2017 Seventh Internat Conf Emerg Secu Technol, UK: Canterbury; 2017. https://doi.org/10.1109/EST.2017.8090413
24. Liu H, Lang B. Machine learning and deep learning methods for intrusion detection systems: A survey. Appl Sci. 2019; 9(20):4396. https://doi.org/10.3390/app9204396
25. Hong J, Nuqui RF, Kondabathini A, Ishchenko D, Martin A. Cyber attack resilient distance protection and circuit breaker control for digital substations. IEEE Trans Ind Informat. 2019; 15(7):4332-41. https://doi.org/10.1109/TII.2018.2884728
26. Todeschini MG, Dondossola G, Terruggia R. Impact evaluation of IEC 62351 cybersecurity on IEC 61850 communications performance [Internet]; 2019. Available from: https://www.cired-repository.org/items/b238105f-1dc9-4db0-8098-629200f0164a