Cyber Security for SCADA Systems in Power Systems

[1]M.GuruMaheswara Reddy,[2]M.S. Sujatha,[3]NalisettyNikhila, [4]M.Manohar, [5]B.Vidya Sagar [6]Nimmanapalli Babu Reddy and [7]Madapuram Anusha

[1,2,3,4 , 5 and 6] Department of Electrical and Electronics Engineering,
Mohan Babu University, Tirupati, India

[5]Teegala Krishna Reddy Engineering College
Hyderabad, Telangana, India

Abstract:-In recent years, SCADA has been integrated into power systems to achieve automation at many phases, including generation, transmission, and distribution. This process makes the Smart Grid better in a big way. However, the excessive integration of SCADA systems into the Smart Grid comes at the expense of cyberattacks, which can result in significant losses in terms of money, confidence, and even lives. In the past, these cyberattacks with ransom demands led to prolonged blackouts in places like the Ukraine, Natanz, Mumbai, the United States, etc. Therefore, ensuring an uninterrupted power supply for the consumers and defending the entire Smart Grid System from these kinds of attacks are the essential tasks.

Confidentiality, Integrity, and Availability (CIA) of the sensitive information that is being transported between the two end terminals, from the sensors to the Substation, can be taken care of in order to protect it. The Cyber Security Management System (CSMS) is the suggested remedy for this, and it contains the remediation steps to be taken after an attack (to get back to the fully functional state), protocols to be followed, standards for the hardware and software to be maintained, and instructions on how to deal with updates, security patches, and zero-day attacks, among other things. Along with these safeguards, other attacks, including DDoS (Distributed Denial of Service), CSRF (Cross-Site Request Forgery), XSS (Cross-Site Scripting), and MITM(Man in the Middle), Spoofing, Tampering, Ransomware and others are discussed in this paper.

Keywords: ***SCADA system, Smart Grid, Cyber Security, Cyber-attacks, CIA triad, Cyber Security ManagementSystem (CSMS).***

INTRODUCTION

SCADA (Supervisory Control and Data Acquisition) systems are essential to the smooth running of vital infrastructure and industrial facilities. Critical infrastructure companies have frequently adopted SCADA/ICS to automate process control and data collection [16]. These systems have been raised to high-value targets for attackers attempting to damage industrial operations. Unfortunately, many ICS are not built to withstandthreat, andtheartactors are increasingly focusing their attention on these systems [1]. A successful attack on the system, have the ability to disrupt internal processes, cause financial losses, and even take lives [2].

The Industrial network attacks are not extremely complex.By using current industrial device setup flaws, network, and OS vulnerabilities, threat actors might use a variety of attack models [3].

Most security professionals who have done Vulnerability Analysis and Penetration Testing(VAPT) found that the external defence against outside threats is inefficient and industrial networks are not properly isolated from operational financial systems.

Stuxnet (2010), Shamoon (2012), Dragonfly (2014), Black Energy (2015), Triton (2017), and Wannacry(2017) are a few well-known attacks.

Protecting SCADA systems from assaults that could result in a denial of service and financial loss is crucial for Power Systems. In this study, the protection strategies are explored.

1. Cyber Attack Surface of SCADA Systems

Security of these systems has become essential since SCADA Systems were introduced to industry and were automated. Security threats exist for any firm or organization that employs SCADA systems, from small enterprises to the federal government. These threats have the potential to have a profound influence on the local community and economy.

According to a study by the ICS security firm Dragos, and it was found that 26% of those advisories were about zero-day vulnerabilities. This situation is concerning because there was a high possibility that attackers who used zero-day threats in their attacks would succeed.

Incorrect input validation, cross-site scripting (XSS), stack-based buffer overflows, the use of default creds, and excessive hardware resource consumption (i.e., DoS) problems are all features of the majority of assaults.

1.1 Attack Surfaces for Scada Systems

Human Intervention in the system is typically the first step in a successful attack. Only products that belong on Monitoring systems, Engineering workstations, operational panels,core field devices, and industrial network equipmentthemselves are affected by the shortcomings, which account for 77% of the identified vulnerabilities, according to the research [5] [6].

The majority of the time (approximately 75% of the time), an attack is based on a networkvulnerabilities, whereas the remaining weaknesses could only be used by attackers who had direct access to the targeted system physically or locally [7] [8]. Loss of control and loss of vision are the effects of the attacks against SCADA. In these, 5% of advisories could only cause a loss of vision (but no loss of control), 2% could cause a loss of control, and 50% are linked to theflaws that might cause both a loss of the control over the operating system [4].

1.2 Common SCADA security issues and threats

1.2.1Old software

The fact that SCADA systems usually use obsolete software with inadequate security is one of their most critical problems. Most of this sort of software lacks fundamental security features like user/system authentication and data integrity checks, which makes it possible for attackers to utilise ICS components as targets for a range of assaults.

1.2.2 Misconfigured Netwrok

The Network component is typically set improperly in systems. Industrial network firewalls typically fail to identify or stop malicious activities carried out by outside attackers, allowing them to gain access to OT systems.

In some instances, industrial environment operators have improperly installed remote-access servers or SCADA systems are connected to unaudited dial-up lines, which might provide attackers with access to both the corporate LAN and the OT network [9] [10].

1.2.3 Default configuration

Hackers are well aware that threat actors frequently attempt to exploit devices with factory settings in place. Attackers can readily locate and attack more OT systems connected to the same network using a device's factory defaults, including default passwords. [13] [14].

1.2.4 Unencrypted communications

Virtually any legacy,the lack of encryption in ICS and industrial protocols gives opportuanity for threat actors to eavesdrop on communications, steal credentials, and launch man-in-the-middle attacks [11] [12]. Attackers may use unencrypted way of communication protocols to target workstations, ICS, and HMI in order to distribute malicious software. One method is to push rogue updates that can compromise these components[15].

1.2.5 DDoS attacks

Threat actors could use DDoS attacks on vulnerable, unpatched, online-exposed, and insufficiently secured systems to attempt to breach OT systems.Hackers may find it quite simple to find these systems use the search engines like

Shodan.Attackers have access to all the data that could be utilised to locate a possible victim that has been made public online thanks to the well-known search engine [16].

2.Cyber Attacks on SCADA Systems

The ICS has grown to be one of the primary targets of sophisticated cyberattacks during the past ten years. The discovery of "Stuxnet," the first malware that was known to the general public, at the uranium enrichment facility in Natanz, Iran, in 2010 marked a turning point in the history of ICS cybersecurity. Since then, a tonne of additional, more advanced malware and tools have surfaced in various parts of the globe, some of which were purportedly created by nation-states as weapons of war[1].

2.1 STUXNET(2010): The Stuxnet malware targeted Iranian facilities. The attack is thought to have started from a USB drive belonging to a worker. The attack avoided cyber defence technologies for years and employed worm-type malware to target specific SCADA devices and change PLCs. The virus made extensive use of zero-day vulnerabilities and was built to automatically identify its targets before attacking them. The malware physically damaged the gas centrifuges that are used to separate radioactive material, and it especially targeted PLCs that enable automation of the electromechanical operations utilised in Natanz's plant to operate machinery and industrial processes.

2.2 WANNACRY(2017): At least 100,000 organisations, including energy firms, telecoms, banks, and governmental agencies, were impacted by this international attack, which occurred in 150 different nations. The attack used data encryption and a Bitcoin ransom demand to target ICS machines using the Microsoft Windows operating system. The control server (with the historian), the operator station, and the engineering stations were all impacted by the attack on the OT system's IT side in the industrial setting. Due to a lack of access to process data, the affected facilities had to shut down partially, however the assets of Levels 1 and 0 were unaffected (PLCs and actuators).

2.3 Colonial Pipeline (2021): One of the largest oil pipelines in the US, the US Colonial Pipeline, was the target of the attack. The energy firm was forced to shut down its entire fuel distribution pipeline for 6 days after the pipeline was the target of a ransomware attack. The DarkSide organisation was responsible for this ransomware attack. Instead than focusing on the operating systems, DarkSide operators addressed the commercial side, which suggests that their goal was to make money rather than to shut down the pipeline.

3. Cybersecurity Measurements for SCADA

Design, scope, and implementation of a Cybersecurity Management System (CSMS) typically depend on the size and complexity of a business, and more significantly, the infrastructure it uses. In order to acquire a thorough grasp of what needs to be handled, analysis and adherence to recognize relevant international standards, frameworks, and models would be a great place to start when building an organization's CSMS[12].

Some Physical Security and Disaster Recovery Standards and Guidelines

- **NERC CIP-014-2 Standard for Physical Security**

This provides utilities with guidance on how to protect key physical assets.According to cip-014-2, organisations must identify and safeguard transmission stations, transmission substations, and key control centres that, if physically attacked and rendered inoperable or damaged, could cause interconnection instability, uncontrolled separation, or cascade.

- **.NERC Physical Security Guideline for the Electricity Sector**

Any vulnerability assessment should consider the threats to physical security, as well as the consequences of those risks. This recommendation focuses on creating procedures for evaluating physical security vulnerabilities that result fromefficient planning and can lessen the effects of extreme events.

- **ISO/IEC 2703157**

This offers comprehensive instructions on how to handle ICT components to guarantee businesspersistence. It describes the concept and guiding principles of ICT ready for business continuity and offers a framework of strategies and procedures to improve ICT readiness inside an organization.

3.1 Cybersecurity Standards and Guidelines Developed for the Electricity Sector

- **NIEC 6244359 series of standards**

The IEC 62443 series was created to ensure industrial automation and control system security throughout their lifecycle. It includes guiding frameworks for effectively improving an organization's ICS defensive posture.

- **ISO/IEC 27001 and ISO/IEC 27019 standards**

The specifications for an information security management system are laid forth in the International Organization for Standardization (ISO)/IEC 27001 standard. Additionally, ISO/IEC 27019 offers guidelines for process control systems used in the energy utility sector to regulate and observe production, based on ISO/IEC 2700261.

- **NIST Cybersecurity Framework**

The National Institute of Standards and Technology Cybersecurity Framework (NISTCSF) is voluntary guidance for organisations to increase manage and reduce security risks based on existing standards, guidelines, and practises.

3.2 Cyber Security Management System

A CSMS is the collection of all the interconnected cybersecurity elements of an organizations to ensure that policies, security standards, and objectives that can be created, implemented, communicated, and evaluated to ensure an organization'scybersecurity status. A CSMS assists organizations in identifying and assessing cybersecurity risks, as well as reducing them as effectively as possible. A CSMS should be a continuously evolving iterative process with at least three fundamental steps reflectingthe overall logic[1]:
1.Risk Analysis
2.Addressing Risk
3.CSMS Monitoring and Improvement

3.3 Life Cycle of an OT Cybersecurity Management System

3.3.1 Risk Analysis

Cyber risks, such as the possibility of harm or loss as a result of unauthorized entry,disclosure,modification,disruption, use or destruction of IT, OT, or information assets, should be identified and analyzed in order to address them correctly and appropriately. A risk assessment is commonly recommended to be performed before and after any significant change to an organization's structure and processes, after any OT changes, and after any significant cybersecurity incidents during post-incident action.

Identification and qualitative or quantitative estimation are the two parts of risk assessment. Risk identification refers to the process of identifying and characterizing risks, whereas risk estimation refers to the process of comparing a risk to predefined risk criteria to determine its significance.Risk assessment entails calculating an inherited score for a risk based on its likelihood, impact, and residual score, as well as estimating how current mitigation measures reduce the risk.

International Standards for Risk Management

- **ISO 3100064 standard**

Guidelines of risk management for ISO 31000: This defines risk management principles, as well as a framework and a process.. It can assist organizations in increasing the likelihood of achieving their goals, improving the identification of opportunities and threats, and effectively allocating and using risk management resources.

- **ISO/IEC 2700565 standard**

Information technology - Security techniques - Information security risk management, ISO/IEC 27005: This standard is intended to aid in the implementation of information security using a risk management approach and supports the general concepts specified in ISO/IEC 27001.

3.3.2 Network Security Management

The cornerstone of an industrial network security management is building and maintaining ICS networks that are secure by design. Secure by design implies that OTnetworks should be segregated into meaningful zones andsegments defined by network purpose and function.

In OT networks of high criticality, physical segregation is highly recommended or should at least be considered, though logical segregation should be ensured by firewalls in all instances[13] .

3.3.3 CSMS Improvement

The enhancement step focuses on the CSMS's need to effectively address internal and external threats, the most recent vulnerabilities, changes in risk tolerance, and legal requirements. During this stage, the organisation should assess whether the identified cybersecurity risks are adequately managed and whether risk mitigation measures are adequate. In the event of inconsistencies, the CSMS should be modified to meet the organization's cybersecurity strategic goals and expectations. Furthermore, the organisation should think about conducting an external audit of the CSMS to ensure that its design and implementation adhere to international standards, best practices, and guidelines. Organizations should review and improve their CSMS at least once a year, or more frequently if significant organisational changes occur.In sum, the CSMS takes a comprehensive approach to cybersecurity, assisting in the protection of the OT and the entire organization from OT-specific risks as well as vulnerabilities that are more prevalent, such inadequately trained employees or inefficient procedures. A CSMS reduces the threat of constantly evolving risks by constantly adapting to changes both inside and outside an organisation. As a result, putting in place and maintaining a CSMS can significantly improve an organization's resilience to cyberattacks.

4.Remediation Methods

Defending SCADA systems

Applying vendor-released security patches and upgrades is a need for businesses that employ ICS/SCADA systems in their infrastructure to maintain their systems up to date. Operators of critical infrastructure are required to put security measures in place to protect themselves from cyberattacks, some of which are based on the NIST guide on ICS security[8].

These are some of the recommended methods:

- **Virtual patching**can be implemented in the system to avoid the vulnerabilities that arises due to usage of the outdated OS's and the software applications. This method also avoids the loss in production work, as there is no downtime while the systems installs it's updates. [14].
- **Network segmentation**is very important in any industrial network, as it's protects the systems core network being visible to the malicious attacker. Basically, the Internet network i.e outer network is partitioned from the inner core network by the implementation of the Demilitarized Zone(DMZ). This also helps prevention of malware spread and sensitive data exposure.[6].
- **Separation of ICS network from the corporate network**, this helps to prevent the sensitive data explosureusing adequate security measures like firewalls in order to prevent the lateral movement of attacks from one to another.
- **Untrusted Removable Devices**, many malwares seek their way into the system through the removable usb and hard-disks. Thus, it's advised to not to insert the unknown removable devices into the system.
- **Authorization and User accountsManagement**, this Access Control management is very useful for maintaining the sensitive data

from being sabotaged by the unauthorizedpersons and leaking out of the company.[15].

Power grids are critical infrastructure that necessitates a comprehensive approach to cybersecurity management to ensure maximum electricity security and availability. Adequate cybersecurity protection for the electricity sector necessitates a systematic, ongoing process of cybersecurity management. The process's fundamental activities include establishing a cybersecurity programme, assessing and treating risks, and regularly evaluating, monitoring, and improving cybersecurity within an organization.These activities should be carried out in a cyclical manner. Although general organizational cybersecurity management should ideally be an all-encompassing (i.e., covering OT and IT) component of a general risk management programme (that also includes traditional physical security, business continuity, and disaster recovery), in the case of TSOs and DSOs, running a dedicated cybersecurity programme for an ICS makes sense, as ICS are increasingly becoming a target for cyberattacks. Because cybersecurity management is still a developing concept, energy and other utility organizations can implement a number of relatively simple, cost-effective, and simple-to-understand best practices.Following recognized international standards and tools can lead to a comprehensive understanding of what needs to be addressed and how. Furthermore, given the financial, regulatory, and legal constraints, a phased approach to strengthening cybersecurity for TSOs and DSOs in developing countries may be the only way to proceed.

5. Conclusion

The attack surface and common weaknesses in the SCADA, IED, and communication systems used in the Smart Grid were explored in this paper. The case study on the infamous attacks on the power systems around the globe is finished. The Cybersecurity Management Systems (CSMS) is suggested for the changes to be made and the Standards of the hardware that must be upheld in the System to prevent future assaults. Additionally, the Risk analysis that is present and the Remediation techniques that are to be performed are swiftly mentioned.

REFERENCES

[1] World Bank. 2022. Strengthening the CybersecurityofElectricity Grids: Context and Good Practices for Transmission and Distribution System Operators. © World Bank.

[2] Marín-López, A.; Chica-Manjarrez, S.; Arroyo, D.; Almenares-Mendoza, F.; Díaz-Sánchez, D. Security Information Sharing inSmart Grids: Persisting Security Audits to the Blockchain. Electronics 2020, 9, 1865.

[3] IEEE Research Paper on"Utility of SCADA in Power Generation and Distribution System".2017.

[4] Appiah-Kubi, J.; Liu, C.C. Decentralized Intrusion Prevention (DIP) Against Co-Ordinated Cyberattacks on Distribution Automation Systems. IEEE Open Access J. Power Energy 2020, 7, 389–402.

[5] Suciu, G.; Sachian, M.A.; Vulpe, A.; Vochin, M.; Farao, A.; Koutroumpouchos, N.; Xenakis, C. SealedGRID: Secure andInteroperable Platform for Smart GRID Applications. Sensors 2021, 21, 5448.

[6] Chromik, J.J.; Remke, A.; Haverkort, B.R. Bro in SCADA: Dynamic intrusion detection policies based on a system model. In Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR), Hamburg, Germany,29–30 August 2018.

[7] Wang, T.; Long, Q.; Gu, X.; Chai, W. Information FlowModeling and Performance Evaluation of Communication Networks Serving Power Grids. IEEE Access 2020, 8, 13735–13747.

[8] van der Velde, D.; Henze, M.; Kathmann, P.; Wassermann, E.; Andres, M.; Bracht, D.; Ernst, R.; Hallak, G.; Klaer, B.; Linnartz, P.; et al. Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures. In Proceedings of the 6th IEEE International Energy Conference (ENERGYCON), Gammarth, Tunisia, 28 September–1 October 2020.

[9] Zhang, H.; Jin, X.; Li, Y.; Jiang, Z.; Liang, Y.; Jin, Z.; Wen, Q. A Multi-Step Attack Detection Model Basedon Alerts of Smart Grid Monitoring System. IEEE Access 2019, 8, 1031–1047.

[10]Appiah-Kubi, J.; Liu, C.C. Decentralized Intrusion Prevention (DIP) Against Co-Ordinated Cyberattacks on Distribution Automation Systems. IEEE Open Access J. Power Energy 2020, 7, 389–402

[11]Kenyon, R.W.; Maguire, J.; Present, E.; Christensen, D.; Hodge, B.M. Bulk Electric Power System Risks from Coordinated Edge Devices. IEEE Open Access J. Power Energy 2021, 8, 35–44.

[12]Cardenas, D.J.S.; Hahn, A.; Liu, C.C. Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations. IEEE Access2020, 8, 61161–61173.

[13]A. Hahn, et. al., "Development of the Power Cyber SCADA Security Test bed", in Cyber Security and Information Intelligence Research (CSIIR) Workshop, Oak Ridge National Laboratory.

[14] C.Ravariu, A.Srinivasulu, A.Bhargav, "Viral Invasion Flow-Chart for Pathogens With Replication Target in a Host Cell", pp. 33-53, doi: 10.4018/978-1-6684-6434-2.ch002. IGI Global: Recent Advancements in Smart Remote Patient Monitoring, Wearable Devices, and Diagnostics Systems.

[15] C. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cyber security for SCADA ".

[16]S. Siddharth and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system" IEEE PES General Meeting.

[17] M. S. Sujatha, P. Shashank .et. al, "Advanced Protection System for SCADA usingFog Computing", IEEE Access 2022.