International Journal of Advanced Research and Review

www.ijarr.org

IMPROVING THE SECURITY OF SCADA SYSTEMS IN MISSION-CRITICAL INFRASTRUCTURES: A THOROUGH ANALYSIS AND POSSIBLE SOLUTIONS

[1]S. Sarika, [2] Dr.N.Deepak Kumar,

[1]PG Scholar, Dept.of.CSE, Sree Rama Engineering college,Karakambadi road, Tirupati-517507.

[2]Professor, Dept.of.CSE, Sree Rama Engineering college,Karakambadi road, Tirupati-517507.

Abstract

A critical infrastructure concern is the security of supervisory control and data acquisition (SCADA) systems, which are essential for ensuring the resilience and integrity of processes and operations and for maintaining service continuity in the face of hostile and cyber-terrorist attacks. There are system-level security holes, and SCADA protocols are often prone to them as well. Not all necessary security measures may be in place. They often rely on "security by obscurity" or seclusion from public networks, which is in contrast to that. Hackers trying to breach SCADA equipment have an easy target in the protocols that lack security measures like authentication and encryption. In order to demonstrate the need of improving SCADA device security, the authors highlight the security risks and unsolved matters associated with these devices. In addition, the article assesses SCADA networks, delving further to discuss the available security methods to thwart assaults on these networks.

Keywords—Critical Infrastructure, Cyber Security, Industrial control systems security.

INTRODUCTION

Computer and communication technologies have come a long way in the last 20 years. Every system is capable of becoming

be deemed crucial when its weaknesses transform into dangers that have the potential to wreak havoc on social structures, energy sectors, security frameworks, healthcare systems, and many other facets of society. Society, the economy, and general stability may be severely impacted when a system's services are unavailable or malfunctioning. When it came to protecting infrastructure, environmental concerns had always taken precedence [1]. The spotlight has shifted to other dangers and harms, however, since cyberattacks are real. Hackers target vulnerabilities in networks and the Internet. The development of current security solutions has been prompted by the vulnerability of Critical Infrastructure (CI) to cyber assaults.
Lack of availability or malfunction A single CI has the potential to trigger a domino effect of failures that might damage countless other infrastructures as well as society, the economy, and national stability [2]. However, new and powerful attacks are always a possibility, even when conventional security measures try to account for recognized dangers. Therefore, to combat these risks, it is crucial to establish flexible security measures. The paper explores the subject of unanswered questions and security concerns. There has been a steady rise in cyber attacks aimed against SCADA systems, and this is due to things like developing

complex multi-component design, increasing demands for real-time operations and delivery, and continuing attempts to modernize all contribute to the complexity of these systems. It is crucial to create state-of-the-art SCADA systems that meet the needs of upcoming architectural breakthroughs in order to facilitate the complicated tracking of linked and integrated systems. Firewalls designed for SCADA systems or improved by commercial

vendors to manage SCADA protocols are available. The use of open-source firewalls in SCADA networks has not been thoroughly investigated, despite their successful use in IT networks [3]. The authors highlight the significance of safeguarding SCADA devices by illuminating the security challenges and difficulties that have so far not been overcome. In addition to going over SCADA networks, the paper also covers the many security solutions that are available to protect against assaults on these networks. Critical infrastructures rely on supervisory control and data acquisition systems. Following this, the writers provide a brief overview of SCADA systems, protocols, assaults, and critical infrastructure, as well as solutions to these issues.

SCADA NETWORKS

SCADA systems are often complex networks made up of many different parts. Based on who is operating them, these systems are classified into one of three categories. They may be entirely mechanized by software and hardware, entirely hand-operated by engineers and technicians, or a combination of the two, with some human intervention still needed for portion control. Many SCADA systems include[4] to carry out all of these duties. 1. Devices that interact with the field: Local control devices and sensors that report and detect power levels, flow rates, pressure, and temperature; actuators for valves and motors; and control switch boxes. 2. Functional machinery: The SCADA system regulates the actuators, pumps, and valves inside the manufacturing facility. 3. PCs for control: These may be embedded systems or specialized PCs that collect data from sensor networks, relay it to management systems, and then operate the corresponding operational machinery. These machines may get instructions from higher-ups' computers or make judgments autonomously based on data collected by sensors.
Administrative computers: desktops, laptops, and tablets with human-machine interfaces. These workstations allow operators to operate and monitor SCADA network devices using a user interface. Fifthly, SCADA networks use a variety of communication mechanisms, both local and distant. The use of USB, serial transmission, and specialized wired networks allows for short-range communication. Prototypes for long-distance communication include Ethernet, TCP/IP, WiFi, dial-up networking, cellular packet data, and others. Furthermore, SCADA networks are making more and more use of the Internet for remote access and long-distance communication. Embedded systems using real-time operating systems like VxWorks, INTEGRITY, or MQX are a part of SCADA networks, which also include personal computers (PCs). Many of the computers in SCADA networks haven't seen any software patches or upgrades since they were first installed, so they're open to assaults. Due to their antiquated architecture, the embedded computers used by SCADA networks do not have adequate security mechanisms in place [5]. It is common practice to safeguard the SCADA network's PCs by keeping them updated with the most recent operating systems, security patches, and applications. But there are situations when some SCADA software is incompatible with newer OS versions, which prevents the PC from being upgraded and leaves a security hole. It will need a new strategy to fix the security issues with these old PCs and embedded SCADA systems [6]. To aid operators in monitoring the industrial network, modern control centers are equipped with data servers, HMI stations, and additional servers. Directed gateways often link this SCADA network to the internet and/or an external business network [7].

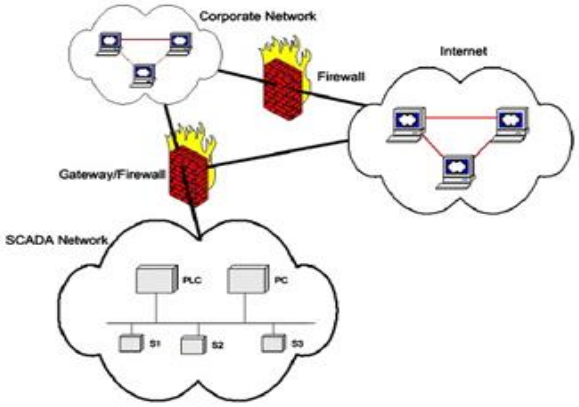

Fig.1: Standard SCADA network structure[8].

Using the Fieldbus protocol, these gateways mediate communications between SCADA networks and IP-based networks within the plant. Protocol translation and facilitating communication between these various networks fall within their purview. In order to improve the gateway's speed while dealing with data items that are transferred across networks, they also use caching technologies. As shown in Figure 1[8], this is a typical SCADA network configuration. A. SCADA network attacks The shutdown of manufacturing plants, delays in rail systems, and spills in sewage systems are the most common targets of assaults against SCADA systems. The SCADA industry has to do a better job of strengthening security for both old and new equipment. It is important to implement this improvement in a way that guarantees a profit, especially for SCADA devices located outside of corporate networks and for SCADA devices on manufacturing premises. Current SCADA devices may be enhanced with new features that allow them to control their connections, detect and notify of suspicious data flow patterns or illegal access, and increase security with full policy management. All of these improvements work together to make SCADA equipment more secure, making them resistant to most cyberattacks [9]. B. Using a SCADA firewall with a virtual isolated network to prevent invasions.

To secure distant devices without modifying the SCADA system, the SCADA firewall may be used. Another possible use is the preservation of SCADA equipment that is installed on a manufacturing floor or in a non-remote location. Firewall software may be used to secure SCADA devices in the future [10]. An essential feature of a SCADA firewall is the ability to regulate the packets processed by the device. • Preventing intrusions into computer systems using wireless networks, the company intranet, or the Internet. Protect against packet floods and Denial of Service attacks by enhancing security. • The capacity to trace and report suspicious traffic, probes, or attacks. • The capability to monitor and control modifications to filtering policies. A lot of SCADA systems that weren't very secure are now online, which exposes their vulnerabilities, as mentioned before. One possible solution is to set up a SCADA firewall (VCN) to create a virtual closed network. The developer must set up communication protocols that restrict the device's connections to just necessary ones in order to choose a Virtual Closed Network (VCN). These protocols define the allowed parties with whom the device may communicate, the protocols that are allowed to run, and the ports that are kept available. The firewall uses these recommendations to filter incoming communications before they are processed by the device. Through the implementation of these rules, the firewall limits the device's ability to communicate and creates an artificial, private network. Attacks using stolen credentials, dictionary attacks, or default passwords could be used by hackers to infiltrate systems without firewalls. get a job. These assaults are often automated, which allows for a multitude of attempts to break passwords. The identical system may prevent similar attacks by setting up a firewall with a trusted host whitelist. Therefore, the firewall will prevent any login attempt by blocking access attempts from hosts that aren't on the whitelist, whether it's by IP or MAC address. References [11] and [12].

SCADA PROTOCOLS

Various protocols are routinely used by supervisory control and data acquisition (SCADA) systems to communicate with PLCs. Considerations for interoperability, the kind of equipment in use, and the specific needs of the industrial process are some of the elements that impact the selection of a protocol. The American Gas Association's AGA-12 standard states that there are 150–200 SCADA protocols. Most of these protocols were private standards that were established by particular companies. Over time, the industry has come to embrace open standard protocols. Even with open protocols, several professional organizations still work to have their standards adopted by the industry more widely. Here are a few examples of commonly used forms of communication: One SCADA protocol for PLCs is Modbus. Summary: Modbus is a very simple and effective serial communication protocol that has been around for a long time and is used extensively in industrial automation [15]. The Modbus protocol has the following features: it may communicate over Ethernet (Modbus TCP) or serial (Modbus RTU). In a normal setup, the SCADA system acts as the master and the PLCs are the slaves; this is how the protocol works. Part B: Distributed Network Protocol 3 (DNP3) Overview: The utility and energy industries are typical users of DNP3 because of its suitability for remote monitoring and supervisory control and data acquisition (SCADA) applications [16]. Features: DNP3 allows for strong communication across a number of channels, including TCP/IP and serial. Features like event reporting and time synchronization make it ideal for use in mission-critical infrastructure.

Section C.IEC 60870-5: Synopsis: The International Electrotechnical Commission (IEC) 60870-5 specifies communication profiles for telecontrol and telesignaling and is a standard for SCADA systems' telecontrol protocols. Specifications: IEC 60870-5 is compatible with a wide range of communication techniques, including

balanced and unbalanced methods. For connecting to equipment like PLCs and remote terminal units (RTUs), it is widely used in the electric power sector [17]. D. EtherNet/IP: A General Overview: EtherNet/IP is a popular industrial Ethernet protocol for usage in process control and manufacturing. Features: PLCs and other devices may interact over regular Ethernet networks thanks to EtherNet/IP, an open protocol. Applications requiring real-time control and high-speed communication often use it [18]. Profibus, in E. Profibus: An Overview, is a Fieldbus communication protocol that is extensively used in industrial automation. It allows for the communication of various automation devices, including PLCs, sensors, and more. Featuring high-speed communication that is well-suited to applications with complicated network topologies, Profibus is compatible with both process automation (Profibus PA) and factory automation (Profibus DP)[19]. In motion control and automation applications, CANopen is a communication protocol that is based on the Controller Area Network (CAN) bus.

The CANopen protocol is well-known for its real-time capabilities and is often used in applications that need accurate timing. It allows devices such as PLCs, sensors, and actuators to communicate with one another [20]. These protocols are just examples; ultimately, the decision is dependent on the requirements of the manufacturing process and the compatibility of the devices involved. Organizations may choose the protocol that best suits their needs for SCADA system-to PLC connection, since each has its own set of advantages and disadvantages. Figure 2 shows the use of industrial communication protocols in 2019[14].

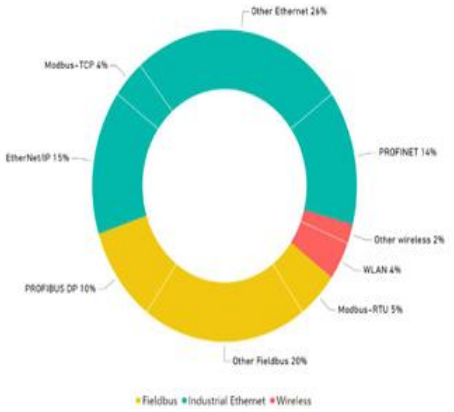

Fig. 2. Use of Industrial Communication Protocols in 2019[14]

SCADA CRITICAL INFRASTRUCTURE

There are several interconnected subsystems that make up the essential infrastructure. Take electricity grid systems as an example, where transformation substations are linked to interconnected high-voltage transmission lines [21]. Afterwards, supply pipes connect these substations to transformers, which in turn link to customers. The SCADA system supposedly had its start in the 1960s, according to many authors. The evolution of SCADA systems was classified by Alexandru [22] as a shift in architecture and technology. A. Revealing the Development: Moving from Symmetrical Systems to SCADA Architectures Connected via the Cloud Based on their functional capacities, the four preceding generations of architecture may be further split, as shown in Figure 3. Conventional SCADA systems using RTUs (Remote Terminal Units) were the norm in the early stages. Phase two of distributed systems development came with the advent of wide-area networks (WANs) connecting RTUs to interaction servers. The third generation of supervisory control and data acquisition (SCADA) systems evolved as a result of the proliferation of automated processes, the proliferation of new equipment suppliers, and the generalization of an ever-expanding industrial environment. The IoT and cloud computing have had a significant impact on the next generation. Connected to the SCADA master via a wireless LAN, the Internet of Things (IoT) comprises a network of interconnected devices and sensors that gather data from distant places. After then, the data is sent to the cloud to be analyzed later. The rapid scalability of data, increased availability, improved efficiency, and cost benefits that these systems provide are in addition to their user-friendliness and smooth integration [23].

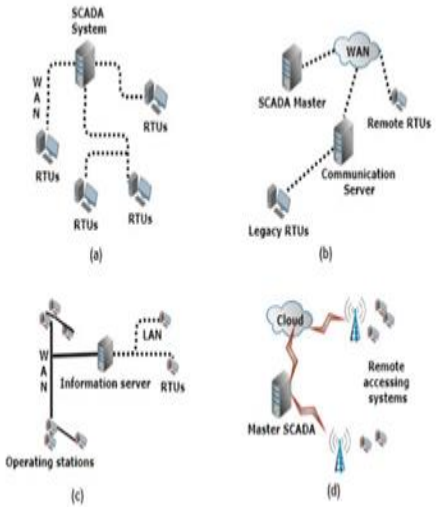

Fig. 3. SCADA system evolution: (a) 1st generation; Monolithic SCADA systems with remote terminal units, (b) 2nd generation; Distributed SCADA systems, (c) 3rd generation Networked SCADA System (d) 4th generation; IOT Cloud-based SCADA System[24].

B. Cyber attacks on SCADA-based Critical infrastructure Both government and NGOs view cyber issues as their primary issue at now.

In most cases, malicious software known as "Trojan horses" is used to launch attacks using email attachments and links. Because they seem real, they are quite difficult to spot. In 2003, the 'SLAMMER' worm infected two US utilities and a nuclear power facility. 'Dragonfly,' the second cyberattack on the energy industry, deployed malware via spam emails. Social engineering is a method by which an attacker may get access to a system and use it for malicious purposes. Internal threats can exist in the form of invaders. Attacks in which the perpetrator is aware of and able to circumvent security measures are considered particularly dangerous. Attacks on sewage management systems have caused sewage floods in many places; one such incident occurred in Queensland, Australia. The intruders started their assault using a USB flash drive [1]. Additional hacking techniques aimed at stealing personal information for financial gain include phishing. One method used in these attacks is to contact consumers via a fake website in order to get their financial details.

Distributed denial of service (DDoS) attacks are distinct types of cyberattacks that aim to overwhelm nodes and servers by flooding them with data and traffic. Differentiating between legitimate and fraudulent entities becomes more difficult as a result of these assaults. Another sophisticated kind of hacking is a man-in-the-middle (MITM) assault. It infects computers by interfering with their ability to communicate with one another and by sending harmful virus in the process. Here are several examples of cyberattacks against CIs, as seen in Table 1. The growing importance of Critical Infrastructure (CI) and the Internet of Things (IoT) highlights the need to improve existing SCADA systems for managing the massive volumes of data generated by these assets. For example, current cloud computing approaches can collect massive amounts of data produced by wide and sophisticated grids [26]. The current cloud infrastructure has problems with the volume, diversity, and velocity of the data that is produced, according to CISCO's observation. The ability to transmit data at large capacities is also required for data uploading directly to the cloud for

processing, storage, and analysis[27]. As a result, cloud computing has emerged to address a number of shared issues associated with SCADA systems hosted on the cloud. It reduces the amount of data sent and stored in the cloud by allowing for temporary data storage and processing at the network's perimeter. For time-sensitive applications, this approach offers a better resolution. However, there are a number of obstacles to integrating continuous integration data with cloud computing systems, including strict security requirements, low latency expectations, and the need for smooth connection with high-availability services. Cloud systems have limited data replication management and screening capabilities, which is a major cause for worry over the lack of strong privacy and user authentication measures. Consequently, it is critical to establish fundamental protocols and techniques for

data security and to exert thorough control over authentication and authorization processes [28]. Cyberattacks on vital infrastructure may take several forms, as shown in Table 1 [25].

Attack	Consequences	Instigation	Attack type	Impact	Sensitivity
Ransomware attacks on SCADA.	Locked PlCs. Spread of ransomware.	Vulnerable PLCs, weak authentication, weak integrity control.	External	Financial loss.	High
Attacks on industrial robots.	Auto execution of malicious node. Altered robot firmware.	Vulnerable OS and web interface, weak authentication.	External	Sabotaged thought, safety threat , financial loss.	High
FDI Attacks on real-time market models and state estimation systems.	Fabricated data, profit gain from selling and purchasing a virtual power.	Vulnerable AMI and sensor network	External	Disrupted smart grid operations, profit loss.	High
Remote attacks on IoT-enabled traffic control systems.	Eavesdropping, remotely controlled traffic lights,	No encryption and authentication mechanisms.	External	DoS attack causing road accidents, loss of credibility.	High
Remote attacks on mission-critical systems on a ship.	Mission-critical systems on acquired ship, compromised navigation system	Weak authentication, weak web interfaces, no network segmentation.	External	Human injuries, financial loss.	High
Attacks on E-Health insurance.	Compromised hospital medical devices.	Vulnerable PMDs and weak authentication.	External	Threat to Human lives,loss of credibility.	High
Phishing attacks on container port systems and devices.	Compromised devices.	Outdates OS, vulnerable network protocols, no network isolation, weak authentication	External	Threat to Human lives,loss of credibility.	High
Spear-phishing attached on smart grid.	Control over SCADA system	Vulnerable OS, weak authentication, no network isolation.	External	Power outage, disrupted servises,loss of credibility.	High
Worm attack on SCADA systems.	Self replication exploited access privilege.	No network isolation.	Internal	Compromised infrastructure, decreased of efficiency.	Medium
Attacks on SCADA honeypots.	Modified devices functionality, pump shut down.	Weak security policies, vulnerable servers.	External	Loss of functionality, disrupted production, devices damage, loss of credibility.	High

CONCLUSION

In this digital age, when cyber risks are significant and process and operation integrity is important, the security of Supervisory Control and Data Acquisition (SCADA) systems in critical infrastructures is of utmost significance. The weaknesses of SCADA systems are thoroughly examined in this paper, with a focus on inadequate security measures and out-of-date protocols. The authors make a valid point about how important it is to strengthen the security of SCADA devices in order to protect vital infrastructures from cyber-terrorist attacks. Changes in SCADA design, from standalone systems to ones that rely on the cloud, demonstrate how quickly technology is developing. Yet, new difficulties have emerged as a result of this development, most notably in protecting critical infrastructure reliant on SCADA systems against cyber assaults. There is a pressing need for strong security solutions that are customized to the specific needs of SCADA systems due to the increasing prevalence of complex cyber threats like as phishing, distributed denial of service attacks, and man-in-the-middle assaults. The use of SCADA firewalls that use virtual isolated networks is one example of an adaptive security strategy that shows promise in reducing cyber threats and strengthening SCADA device defensive mechanisms. Further precautions against such invasions and data breaches include using secure communication protocols and strong authentication procedures. The development of effective countermeasures and resilience plans requires close cooperation between cybersecurity specialists, government agencies, and industry stakeholders as we traverse the intricate terrain of SCADA security. We can strengthen SCADA systems against new threats and keep vital infrastructures safe from cyberattacks by making security improvements a top priority and using cutting-edge technology. The research concludes that in order to

protect vital infrastructures from cyber attacks, improve the security and resilience of SCADA systems. This will help maintain social stability, economic success, and national security in our linked world.

REFERENCES

[1]. [1] H. Altaleb and Z. Rajnai, "Risk assessments Methods and Cyber Vulnerabilities in SCADA systems," Natl. Secur. Rev. Period. Mil. Natl. Secur. Serv., vol. 2, pp. 181–194, 2021.

[2]. J. Jaskolka and J. Villasenor, "An approach for identifying and analyzing implicit interactions in distributed systems," IEEE Trans. Reliab., vol. 66, no. 2, pp. 529–546, Jun. 2017, doi: 10.1109/TR.2017.2665164.

[3]. K. Stouffer, J. Falco, and K. Scarfone, "GUIDE to industrial control systems (ICS) security," Stuxnet Comput. Worm Ind. Control Syst. Secur., pp. 11–158, 2011.

[4]. K. Sayed and H. A. Gabbar, "Scada and smart energy grid control automation," Smart Energy Grid Eng., pp. 481–514, 2017, doi: 10.1016/B978-0-12-805343-0.00018-8. S. Cunningham, "Cyber security for industrial control systems," Power Eng. (Barrington, Illinois), vol. 115, no. 11, pp. 142–146,

[5]. V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," Comput. Secur., vol. 25, no. 7, pp. 498 506, 2006, doi: 10.1016/j.cose.2006.03.001.

[6]. J. Hajda, R. Jakuszewski, and S. Ogonowski, "Security challenges in industry 4.0 plc systems," Appl. Sci., vol. 11, no. 21, 2021, doi: 10.3390/app11219785.

[7]. T. Sauter and C. Schwaiger, "Achievement of secure Internet access to fieldbus systems," Microprocess. Microsyst., vol. 26, no. 7, pp. 331–339, Sep. 2002, doi: 10.1016/S0141 9331(02)00044-3.

[8]. V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," Comput. Secur., vol. 25, no. 7, pp. 498 506, Oct. 2006, doi: 10.1016/J.COSE.2006.03.001.

[9]. D. Ranathunga, M. Roughan, H. Nguyen, P. Kernick, and N. Falkner, "Case Studies of SCADA Firewall Configurations and the Implications for Best Practices," IEEE Trans. Netw. Serv. Manag., vol. 13, no. 4, pp. 871–884, 2016, doi: 10.1109/TNSM.2016.2597245.

[10]. D. Li, H. Guo, J. Zhou, L. Zhou, and J. W. Wong, "SCADAWall: A CPI-enabled firewall model for SCADA security," Comput. Secur., vol. 80, pp. 10.1016/J.COSE.2018.10.002. 134–154, J. Nivethan and M. Papa, "On the use of open-source firewalls in ICS/SCADA pp. http://dx.doi.org/10.1080/19393555.2016.1172283, vol. 25, no. 1–3, 83–93, 10.1080/19393555.2016.1172283.

[11]. K. Ferencz, J. Domokos, and L. Kovács, "Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations," Acta Polytech. Hungarica, vol. 21, no. 4, pp. 7–28, 2024, doi: 10.12700/aph.21.4.2024.4.1.

[12]. E. Tapia, L. Sastoque-Pinilla, U. Lopez-Novoa, I. Bediaga, and N. López de Lacalle, "Assessing Industrial Communication Protocols to Bridge the Gap between Machine Tools and Software Monitoring," Sensors, vol. 23, no. 12, 2023, doi: 10.3390/s23125694.

[13]. W. Staszewski, A. Jabłoński, and K. Dziedziech, "A survey of communication protocols in modern embedded condition monitoring systems," Diagnostyka, vol. 19, no. 2, pp. 53–62, 2018, doi: 10.29354/diag/86409.

[14]. M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," Adv. Comput. Information, Syst. Sci. Eng. - Proc. IETA 2005, TeNe 2005, EIAE 2005, pp. 227–234, 2006, doi: 10.1007/1-4020-5261-8_36. Jan. Apr. 2019, doi: systems," 2016, doi:

[15]. D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Commun. Surv. Tutorials, vol. 22, no. 3, pp. 1942–1976, 2020, doi: 10.1109/COMST.2020.2987688.

[16]. J. Sottile, "Alpha Foundation for the Improvement of Mine Safety and Health," Alpha-Foundation.Org. PROFIBUS Nutzerorganisation e. V. (PNO), "PROFIBUS System Description," p. 30, 2010. National Instruments, "The Basics of CANopen," 2022. [Online]. Available: https://www.ni.com/fi-fi/innovations/white papers/13/the-basics-of-canopen.html.