ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

Improving the Security of SCADA Systems In Important Infrastructures: A Thorough Analysis And Possible Solutions

[1]Dr. R Rambabu, [2]Shaik Nazeeruddin, [3]Suda Guna Shekhar, [4]Paladugula Hari Veera Sai, [5]Pitta Saireddy,

[1] Professor, Department of CSE, Rajamahendri Institute of Engineering & Technology, Bhoopalapatnam, Near Pidimgoyyi, Rajahmundry, E. G. Dist. A.P 533107.

[2,3,4,5] Student, Department of CSE, Rajamahendri Institute of Engineering & Technology, Bhoopalapatnam, Near Pidimgoyyi, Rajahmundry, E. G. Dist. A.P 533107.

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. In addition to system-level security flaws, SCADA protocols are often intrinsically vulnerable. They could not have taken necessary security measures. They often rely on "security by obscurity" or seclusion from public networks, which is in contrast to that. Hackers looking to infiltrate SCADA equipment may easily exploit the underlying protocols in the absence of security techniques like as authentication and encryption. The authors highlight the need of improving the security of SCADA devices by drawing attention to the problems with their security and the issues that have not been handled. In addition, the article assesses SCADA networks, delving further to discuss the available security methods to thwart assaults on these networks. Critical infrastructure, cybersecurity, and the protection of industrial control systems are all related terms. I.

INTRODUCTION

Computing and communication have both seen tremendous growth during the last 20 years. Any system may be deemed critical if its weaknesses develop into dangers that have the ability to disrupt societal structures, energy sectors, security frameworks, healthcare systems, and other parts of society. Society, the economy, and general stability are all at risk when a system's operations are unavailable or malfunctioning. When it came to protecting infrastructure, environmental concerns had always taken center stage [1]. Cyberattacks, however, have changed the conversation to additional dangers and losses because they are real. Threat actors seek for vulnerabilities in networks and the Internet. Due to the high risk of cyberattacks on critical infrastructure, new security measures have been developed. Lack of availability or malfunction Society, the economy, national stability, and many other infrastructures may be severely damaged or destroyed by the domino effect of a single CI's failures [2]. Although innovative, powerful attacks are inevitable, traditional security systems try to accommodate recognized evolving dangers. That is why, to combat these dangers, it is essential to use flexible security measures. Problems with security and open questions in this area are the focus of this essay. Several factors contribute to the ever-increasing number of cyber threats that target SCADA systems. These include the increasing sophistication of these systems, the continuous efforts to modernize them, the demand for real-time operations and distribution, and the complex architecture of these systems, which comprises multiple components. Improving SCADA systems to meet the demands of future architectural developments is crucial for enabling complicated tracking of integrated and linked systems. Some commercial manufacturers have developed dedicated firewalls for SCADA systems, while others have improved their existing firewall capabilities to accommodate SCADA protocols. While open-source firewalls have shown to be successful in IT networks, their use in SCADA networks has received less attention [3]. The authors highlight the significance

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

of safeguarding SCADA devices by illuminating the security vulnerabilities and unsolved difficulties around them. Going above and beyond, the essay examines SCADA networks and talks about the security solutions that are now available to prevent assaults on SCADA networks. Important facilities and systems rely on SCADA systems for control and data acquisition. The writers examine SCADA networks, frequent assaults on SCADA networks, protocols for SCADA networks, and important infrastructure for SCADA networks, along with solutions to these problems, in the sections that follow.

SCADA NETWORKS SCADA

systems are often complex networks with many parts. Based on who operates them, these systems are classified into one of three categories. You may find them completely automated by software and hardware, completely manual by human engineers and technicians, or hybrid, with some parts controlled automatically and others by humans. Many SCADA systems are required to complete all of these tasks[4]. 1. Devices that interact with the field: Local control devices, such as actuators for valves and motors, as well as control switch boxes; Sensors that measure and report power, flow, pressure, and temperature. 2. Machines in operation: The SCADA system regulates the valves, pumps, motors, and industrial automation systems. 3. operate PCs: These are the embedded or specialized PCs that receive data from sensor networks, relay it to management systems, and then operate the operational equipment that is linked with it. These computers may get instructions from higher-ups' computers or use sensor data to make judgments autonomously.

4. Computers used for management: terminals equipped with human-machine interfaces. Operators are able to monitor and operate SCADA network devices using the interface provided by these computers. 5. Local and distant network communication: SCADA networks use a variety of mechanisms for communicating. Serial, USB, and bespoke wired networks are used for short-range communication. Communicating across great distances makes use of a variety of protocols, including Ethernet, TCP/IP, WiFi, dial-up networking, cellular packet data, and many more. 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. Since SCADA networks' embedded computers were developed before security became a top priority, they do not have adequate security mechanisms in place [5]. In most cases, the computers that make up the SCADA network are safeguarded by keeping them running the most recent operating systems with the most recent software and security updates. Nevertheless, there are instances when certain SCADA software is incompatible with later versions of operating systems, which hinders PC upgrades and therefore exposes users to security risks. 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. In most cases, specialized gateways link this SCADA network to either an external business network or the worldwide web [7].

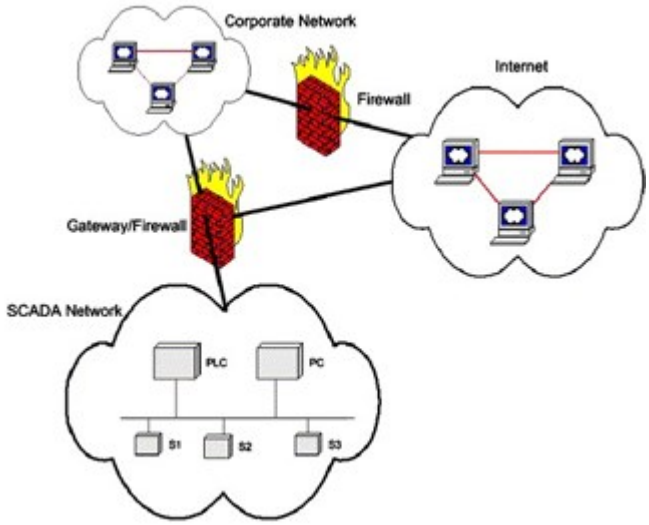

Fig.1: Standard SCADA network structure [8].

These gateways mediate communications between SCADA networks that use the Fieldbus protocol and IP-based networks within the plant. Their responsibilities include bridging the gap between these various networks and translating protocols. 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. Section A: SCADA Network Attacks Manufacturing plant shutdowns, rail delays, and sewage spills are the most common targets of SCADA system hacks. The SCADA industry has to do a better job of strengthening security for both old and new equipment. Particularly with regard to local SCADA devices, including those installed on plant premises, and remote SCADA devices located outside of corporate networks, this improvement must be implemented in a way that guarantees profitability. Upgrades to current SCADA systems may make them more secure by allowing them to control their own communications, detect and report suspicious data flows or illegal access, and integrate full policy management. By bolstering their defenses against the vast majority of cyber attacks, these innovations help to elevate SCADA equipment' security status[9]. Using a SCADA firewall with a virtual isolated network to prevent intrusions is option B. To prevent unauthorized changes to the SCADA system, remote devices may be protected using the SCADA firewall. Also, SCADA systems installed on a factory floor or any other non-remote site may benefit from this. 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. • Protecting against intrusion attempts made over wireless networks, the Internet, or the company network. Protect against packet floods and Denial of Service attacks by enhancing security. • The capacity to monitor and control modifications to filtering policies. • The ability to detect and report suspicious traffic, probes, or attacks. Many unsafe SCADA systems are now connected to the internet, exposing their vulnerabilities, as mentioned above. A SCADA firewall (VCN) virtual closed network might solve this problem. A Virtual Closed Network (VCN) is an option for developers who want to set up communication protocols that restrict device connections to only the most necessary ones. The permitted protocols, the parties with whom the device may communicate, and the ports that must be kept open are all detailed in the communication protocols. The firewall uses these recommendations to filter incoming communications before they are processed by the device. The firewall creates a virtual private network by imposing certain restrictions on the device's ability to communicate. Hackers may use a plethora of password-cracking techniques, such as using stolen credentials, dictionary attacks, or default passwords, in order to infiltrate a system that does not have a firewall. Such attacks may be prevented on the same machine 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. The specific needs of the manufacturing process[13], the nature of the machinery, and concerns about compatibility all play a role in the protocol selection process. The American Gas Association's AGA-12 standard states that there are 150–200 SCADA protocols. The vast majority of these standards were proprietary protocols created by certain companies. Common open standard protocols have gradually gained acceptance in the business. Despite the prevalence of open protocols, several trade associations still push for wider adoption of their own standards within the industry. Here are a few examples of commonly used forms of communication: (A) Modbus: PLC SCADA protocols Modbus is a popular and long-standing protocol for serial communication in industrial automation due to its ease of use and reliability [15]. The Modbus protocol has the following features: it may communicate over Ethernet (Modbus TCP) or serial (Modbus RTU). In most cases, the SCADA system acts as the master and the PLCs as the slaves in this master/slave protocol. Distributed Network Protocol 3, or DNP3, is an overview of a protocol that is often used in the energy and utility industries for remote monitoring and supervisory control and data acquisition (SCADA) purposes [16]. Notable features include DNP3's comprehensive support for serial and TCP/IP connectivity. 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. Features: IEC 60870-5 is compatible with a wide range of communication methods, including balanced and unbalanced techniques. The electric power sector often use it for communication with equipment like as PLCs and

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

remote terminal units (RTUs)[17]. D. EtherNet/IP: Short Introduction: EtherNet/IP is a popular industrial Ethernet protocol for usage in process control and manufacturing. Features: EtherNet/IP allows devices such as PLCs to connect to regular Ethernet networks since it is an open protocol. It finds widespread use in contexts where instantaneous command and data transfer are of the utmost importance [18]. E. Profibus: A General Overview: Profibus is a fieldbus communication protocol that allows for the communication of various automation devices, such as PLCs and sensors, in industrial automation. Features: Profibus PA and DP are both used for process automation, and Profibus provides fast communication that works well with applications that have complicated network designs [19]. F. CANopen: Introduction: CANopen is a CAN bus-based communication protocol that finds widespread usage in automation and motion control. Features: CANopen is a well-known protocol for real-time communication between devices such as PLCs, sensors, and actuators; it is widely used in applications that need exact timing [20]. The requirements of the industrial process and the compatibility of the devices will determine which of these protocols is best. Figure 2 shows the use of industrial communication protocols in 2019[14]. Each protocol has its own set of advantages and disadvantages, so enterprises may choose the one that works best for their SCADA system-to PLC communication needs.

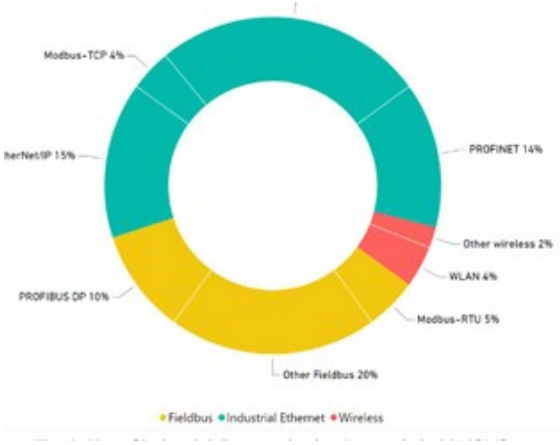

Fig. 2. Use of Industrial Communication Protocols in 2019[14]

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]. Once these substations are coupled to transformers, the supply pathways go to the consumers. Several authors place the inception of the SCADA system in the 1960s. The evolution of SCADA systems was classified by Alexandru [22] as a shift in architecture and technology. A. The Shift from Monolithic to Cloud-Based SCADA Architectures Revealed 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. All sorts of gadgets and sensors make up the Internet of Things (IoT), which allows for data collection from faraway places by connecting to the SCADA master over wireless LAN. The collected data is then uploaded to the cloud so it may be analyzed later. These systems not only integrate easily and are easy to use, but they also quickly scale data, are highly available, efficient, and cost-effective [23].

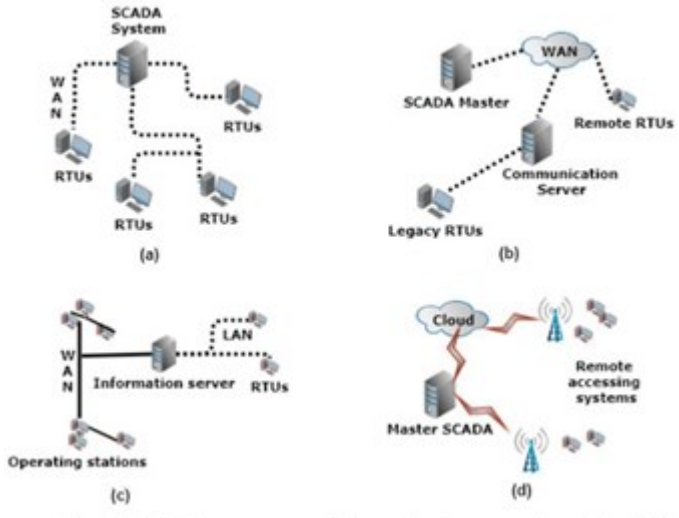

Fig. 3. SCADA system evolution: (a) 1st generation; Monolithic

System control and data acquisition (SCADA) systems with second-generation remote terminal units; third-generation distributed SCADA systems The fourth generation of networked SCADA systems are internet of things (IoT) cloud-based SCADA systems [24]. B. Cyber assailants targeting SCADA-based Foundational systems Cybersecurity is now the top priority for both the government and NGOs. In most cases, malicious software known as "Trojan horses" is used to launch attacks using email attachments and links. They seem real, so it's hard to tell them apart. A nuclear power facility and two US utilities were affected by the 'SLAMMER' worm in 2003. '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. An additional threat is the existence of insiders who have broken into the organization. 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. It becomes more difficult to distinguish between legitimate and fraudulent companies due to these assaults. Another sophisticated kind of cyberattack is a man-in-the-middle threat. It infects computers by interfering with their ability to communicate with one another and by sending harmful virus in the process. As seen in Table 1, there have been many cyberattacks against CIs [25]. Improving existing SCADA systems is crucial for managing the massive volumes of data generated by the growing Critical Infrastructure (CI) and the Internet of Things (IoT). For example, current cloud computing approaches can collect massive amounts of data produced by wide and sophisticated grids [26]. The current cloud infrastructure, according to CISCO's assessment,

struggles with the magnitude, variety, and speed of the generated data. Furthermore, the direct uploading of data to the cloud for storage, processing, and analysis necessitates a high-capacity data transmission capability[27]. Consequently, the emergence of cloud computing has tackled several common challenges linked with cloud-based SCADA systems. It enables temporary data storage and processing at the network's periphery, diminishing the volume of data transmitted and stored in the cloud. This strategy provides an enhanced resolution for applications that are sensitive to delays. However, integrating CI data with cloud computing systems is impeded by stringent security prerequisites, low latency demands, and seamless integration with high-availability services. A pivotal concern is the deficiency of effective and robust privacy and user authentication mechanisms on cloud platforms, where data replication management and screening are limited. Hence, the implementation of essential data security methods and protocols becomes imperative, coupled with comprehensive control over authentication and authorization procedures[28]. Table 1. Different forms of cyber attacks on critical infrastructure[25].

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

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

important infrastructure SCADA system security is a top priority in this digital age because to the prevalence of cyber attacks and the important nature of process and operation integrity. This in-depth study examines the weaknesses of SCADA systems, focusing on the issues of inadequate security measures and out-of-date protocols. To protect vital infrastructures from cyber-terrorist attacks and make sure they can withstand them, the authors correctly point out how important it is to strengthen the security of SCADA equipment. The transition from single-system designs to SCADA architectures that use cloud connection exemplifies how quickly technology is advancing. The protection of critical infrastructure based on SCADA systems from cyberattacks is one area where new issues have emerged as a result of this growth. Robust security solutions that are specifically designed for SCADA systems are urgently needed due to the increasing number of complex cyber threats, including 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. In order to prevent any invasions and data breaches, it is crucial to implement secure communication protocols and rigorous 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. To ensure social stability, economic prosperity, and national security in an ever-more-connected world, this research concludes that strengthening the security and resilience of SCADA systems is crucial for protecting vital infrastructures from cyber attacks.

REFERENCES

[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.

[5]. S. Cunningham, "Cyber security for industrial control systems," Power Eng. (Barrington, Illinois), vol. 115, no. 11, pp. 142–146,2011, doi: 10.2524/jtappij.69.1205.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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,

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.

[16]. Agrawal, K. K. ., P. . Sharma, G. . Kaur, S. . Keswani, R. . Rambabu, S. K. . Behra, K. . Tolani, and N. S. . Bhati. "Deep Learning-Enabled Image Segmentation for Precise Retinopathy Diagnosis". *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 12s, Jan. 2024, pp. 567-74, https://ijisae.org/index.php/IJISAE/article/view/4541.

[17]. Samota, H. ., Sharma, S. ., Khan, H. ., Malathy, M. ., Singh, G. ., Surjeet, S. and Rambabu, R. . (2024) "A Novel Approach to Predicting Personality Behaviour from Social Media Data Using Deep Learning", *International Journal of Intelligent Systems and Applications in Engineering*, 12(15s), pp. 539–547. Available at: https://ijisae.org/index.php/IJISAE/article/view/4788

[18]. 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.

[19]. 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.