Network Telemetry Security Strategy and Design

Author: Moses Odejobi

Advisors: Dr. Farzad Moazzami, Dr. Richard Dean, Dr. Mulugeta Dugda, Wondimu Zegeye

Morgan State University, Electrical and Computer Engineering Department

ABSTRACT

The paper presents background, strategies, and architectures for security solutions for networked telemetry. This will be an overview of the nature of networked security and strategies for security designs which includes NIST guidelines 800-53, 800-82, IBM Redbook, and security design principles.

Key words: *Telemetry Networks, Risk Assessment; ICS-SCADA; Network Security*

Introduction

Today's drive for Networked Telemetry faces the challenge of cyber security threats faced by traditional government and commercial enterprises. Emerging Telemetry Networks faces conventional cyber vulnerabilities coupled with field layer telemetry structures that are especially vulnerable to attacks. Nevertheless, modern day network analysts and managers have devised renewed means to tackle these prevailing challenges. Of the different modern solutions, design strategies such that those that utilize SCADA/ICS models, e.g., the NIST/ICS – 20 Controls which involves layering, zones, and boundaries are popular. This study therefore reviews security design strategies such as NIST guidelines 800-53, 800-862, IBM Redbook, and a range of security design principles.

Morgan's strategy for protecting Networked Telemetry

Morgan's strategy for protecting Networked Telemetry has proposed approaches developed for ICS/SCADA networks from NIST 800-82 coupled with traditional cyber approaches in NIST 800-53. These are captured below.

Here we consider the ground station to comprise traditional enterprise network and Supervisory Command and Data Acquisition (SCADA) systems. SCADA systems are one of the most widely extensively used Industrial Control Systems (ICS) that enable controlling and monitoring of process equipment on multiple sites which spread over large distances (Rakas et al., 2020) [15]. SCADA systems are cyber physical systems with communication networks interfacing the monitoring and control system with the hardware and these could have multiple supervisory systems, Programmable Logic Units (PLCs), Remote Terminal Units (RTUs), Human Machine Interface (HMIs), process and control instrumentation, sensors, and actuator devices over a large

geographical area. SCADA systems make use of both new and legacy systems including traditional information systems (Vincent Urias, Brian Van Leeuwen, and Bryan Richardson, 2012) [26]. SCADA systems are not only as vulnerable as any other networked computer systems, but their legacy systems create another layer of threat. Since many of these systems have existed for decades, their cybersecurity risks are unknown and challenging to analyze as well. These SCADA systems resemble much of the Networked Telemetry systems that we intend to model and therefore represent a good starting pointsecure.

Due to their architecture, strict real-time specifications, network traffic functionality and complex application layer protocols, there are security threats relevant to SCADA systems in particular (Rakas et al., 2020) [15]. As a result, specialized intrusion detection systems (IDSs) are desired to secure modern SCADA systems. In order to achieve the required performance of a real-time system operating continuously with the behavior of coexisting system failures, environmental conditions, human errors, and cyber-attacks, there are three important factors to be considered for the design of SCADA-specific IDSs: hierarchical architecture, network traffic properties, and cyber vulnerabilities and attacks [26-106]. Having dedicated independent hierarchical architecture in SCADA systems, industrial control networks are characterized by different protocols and physical standards. SCADA physical and cyber security are converging these days. The forthcoming fourth-generation SCADA systems adopt Industrial Internet of Things (IIoT) and the Future Internet (FIN) technologies like cloud/fog computing, big data analytics, mobile computing, etc [59].

In this paper, we are envisioning visualizing the current Telemetry Network Security with the idea of building a general telemetry cybersecurity network testbed which initially combines traditional network security controls with an Industrial Control Systems (ICS-SCADA) structure built with telemetry components. Figure 1 Below is a block diagram of the telemetry network design that we envision.

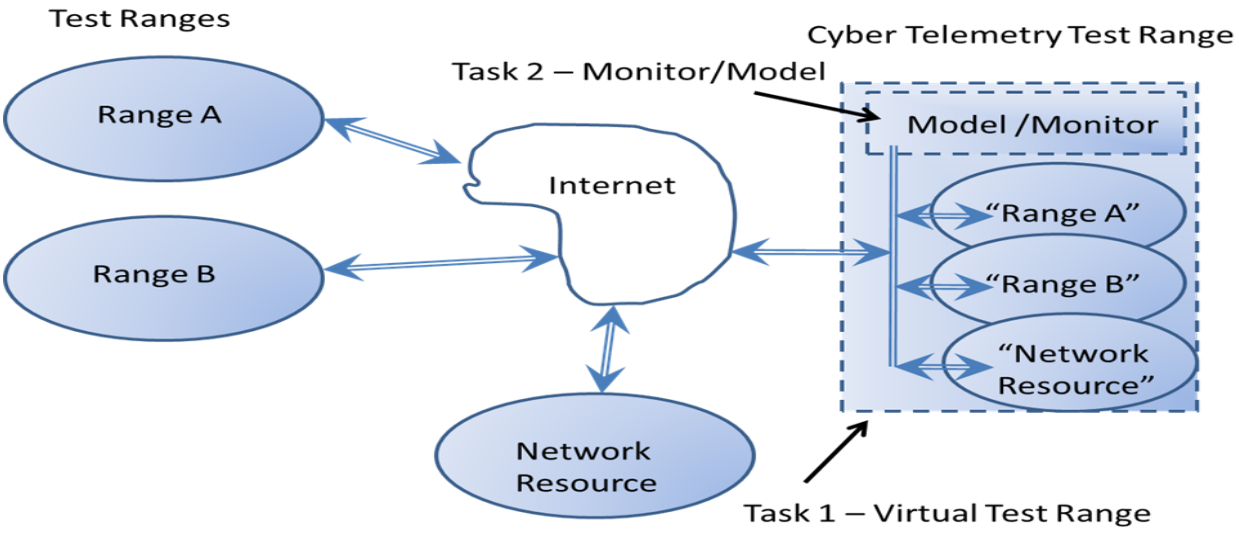

Figure 1. Telemetry Security Design Block Diagram

The proposed telemetry security design highlighted and captured below mainly show the network security aspect in different zones of the telemetry network; in addition, it focuses on security and network controls and how it is adopted to defend the network's confidentiality, integrity, and availability from threats. The details are captured in Figure 1 and in the explanations that follow.

Figure 2. Telemetry Security Design Highlights

Figure 3 below is the more detailed version of Figure 1 which focuses on security and network controls to defend the network's confidentiality, integrity, and availability from threats.

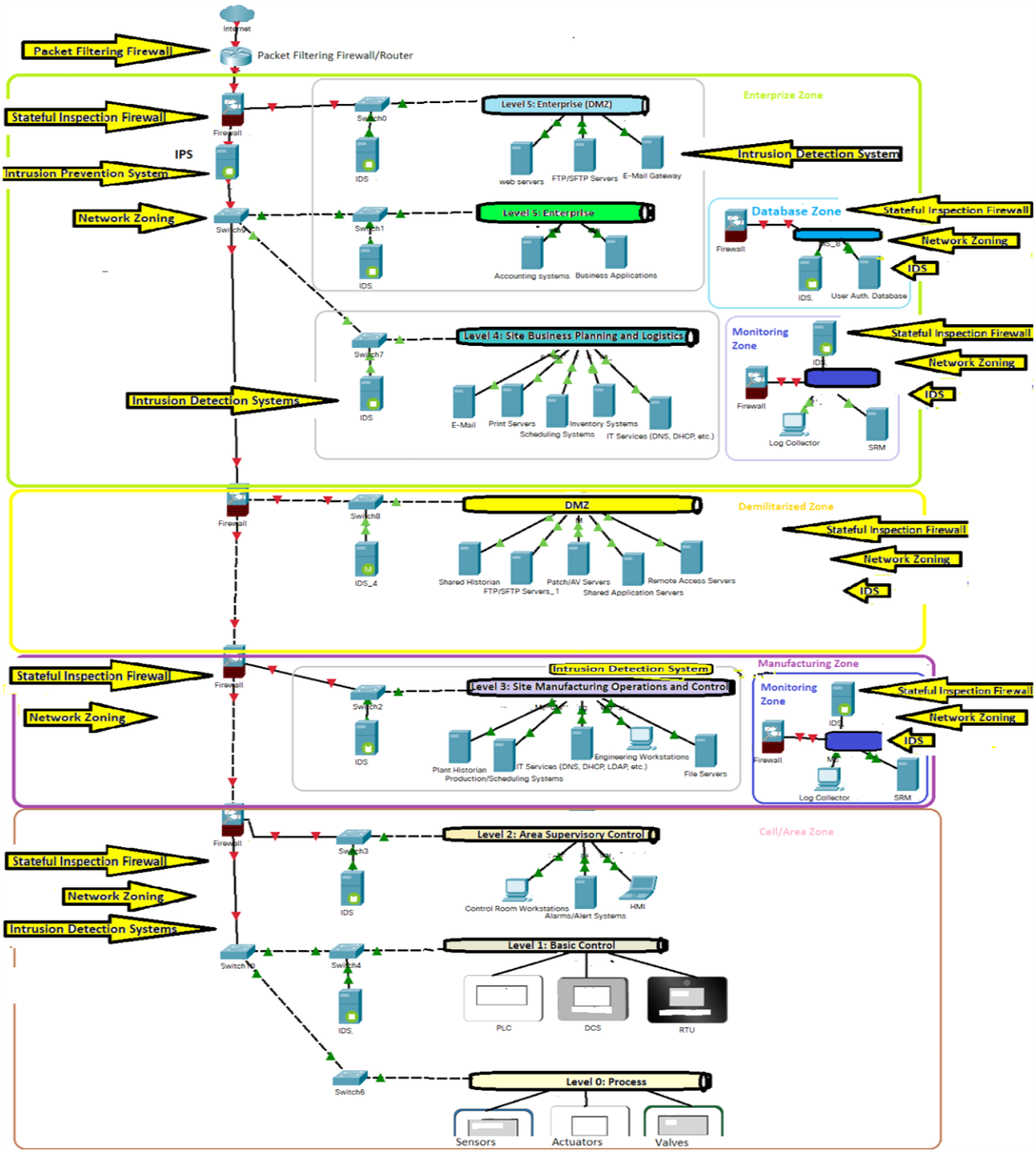

Figure 3. Telemetry Network Security Design

NIST 800-53

The NIST 800-53 is a set of security controls that are designed for protecting the information systems of an organization against a wide range of threats [1]. These controls have demonstrated their effectiveness across several leading organizations in reducing the risk of financial losses, data

breaches, and security incidents [1]. According to [1], these controls are made of 20 critical control which is required under the Office of Management and Budget (OMB) Circular A-130 [2] and the Federal Information Security Modernization Act (FISMA) [3] to be used by organizations in protecting information systems.

Controls

Access Controls are used to address controls in the family of AC, these controls are implemented across organizations and systems [4]. Access control protects an organization's information system by restricting unauthorized access to information systems or resources [5]. In the AC family, the information flow is enforced to control the release of sensitive information, and separation of duties (SoD) is implemented to ensure individuals who administer audit functions are separate from those who administer access control functions [5], [6]. The effective use of access control in organizations reduces the risk of unauthorized access and destruction or modification of sensitive information [7].

Awareness and Training as mentioned in NIST 800-53 is used in addressing the controls in the family of AT [1]. NIST 800-53 emphasized that to implement security policies and procedures, literacy training and awareness have to be provided to the employees on the type of threats that exist and how to protect themselves from this attack [1]. The training is done base on the role of the employees in order to familiarize them to the threats [8]. Through this training, security incidents can be reduced significantly [9]. According to NIST 800-53, audit and accountability are implemented in the organization's system to address the controls in the AU family, these are used to assess event loggings, the content of the audit records to identify the user that caused the event, time and date, and ensuring that users cannot deny that they have access to the informations; these are critical controls that are used to investigate any security incidents, breaches or changes to applicable laws [1]. The three pillars of information security are assessment, authorization, and monitoring which are used to address controls in the CA family. These security controls work together to regularly assess information systems against any security risk [10]–[13], and according to NIST 800-53, for any information to be put into production they must be authorized by the organizations to ensure that they meet the security system requirements, the organization system are also regularly monitored for any signs of unauthorized access [1].

The NIST 800-53 also discusses configuration management which is under the CM family of controls [1]. These are used to establish configuration baselines to track and restore any changes to the system configuration [14]. Contingency planning is used to address control in the CP family, this is used to develop and implement plans to recover the information system from any form of disruptions like natural disasters, power outages, and cyber-attacks [15]. NIST 800-53 mentioned that contingency plans must be developed for all critical information systems, including training for employees on how to respond to information systems disruptions [1]. The Identification and Authentication which is under the IA family of controls, are a set of control which are designed to verify the identity of a device or user before granting access to the information system [16]. According to NIST 800-53, this can be done through multi-factor authentication to privileged accounts and non-privileged accounts, and individual authentication with group authentication [1]. Incidence response protects the information system from the risk of human errors, cyberattacks,

and natural disasters [17]. The IR family of controls is used to respond to and recover from a security threat [1]. According to NIST 800-53, to respond to incidents, employees have to be trained in handling Incidents, monitoring incidents, and reporting incidents [1]. Maintenance is another essential control mentioned in NIST 800-53 [1]. Maintenance is used to keep information in the system in good working order; maintenance of the information system guard against software bugs, hardware failures, and configuration errors [18].

Media protection restrict access to information stored on physical media such as USB drive, hard drives, and CD from unauthorized access, handling, and exposure to sensitive information [1]. The PE is a cornerstone of organization security and information system [1]. According to NIST 800-53, this ensures that the physical infrastructure that stores critical data and systems are well protected, and robust access control is put in place against theft and vandalism [1]. NIST 800-53 emphasized that the PL family of control is an integral part of securing organizations and information systems against cyber-threats, through security controls, risk assessment, and continuous monitoring strategies [1]. The PL family of controls is crucial in coordinating and implementing security controls across organizations and information systems [2], [19]. In protecting organizations and information system, NIST 800-53 identify the PS family of controls as critical to ensuring that individuals with access to critical system and sensitive data are well-vetted [1]. Robust security clearances are also instituted to ensure that only authorized individuals have access to classified information [1]. The PT family of controls is also an effective control in protecting the information system from identity theft and breaches [20]. Similarly, Risk assessment is essential in protecting the information system as it helps in identifying, evaluating, and prioritizing the potential risk to information systems. Not only that, the SA family of control ensures the integrity and security of the organizations and information systems through thorough evaluation of technology solutions and vendors that are needed for information security [1]. The SC control family protects the communications that they use in the information system from cyber-threats [21]. In NIST 800-53, the SI family of controls is designed to ensure that the information system produces accurate, complete, and reliable information [1]. The SR control family is focused on mitigating risks that arise from their supply chains [1].

NIST 800-82

Network Segmentation and segregation

Network segmentation and segregation is the practice of partitioning the ICS into security domains and dividing it into smaller networks [22]. According to NIST 800-82, this is done to protect the ICS network from attacks and unauthorized access through the limitations placed on systems that are open to the internet, as network segmentation and segregation are one of the most effective concepts that an organization can use in protecting the ICS [22]. In partitioning the ICS networks, factors such as uniform policy, management authority and level of trust are considered [23]. The NIST 800-82 indicate that the purpose of network segmentation and segregation is to minimize the number of people who have access to sensitive information, while also ensuring that an organization can operate smoothly without obstruction [22]. This can be achieved through various techniques which are VLANS which is a logical network created in a single physical network, the Unidirectional gateways, and the Encrypted Virtual Private Network (VPN) [24]. Irrespective of

the technologies that are chosen, a common theme that cut across these concepts is the application of technology at more than the network layer, using the principles of need-to-know basis and least privilege, based on security requirement information and infrastructure needs to be separated, and instead of blacklisting whitelisting should be implemented [22].

Boundary Protection

Boundary protection is devices that are used in controlling the flow of information between the ICS network and other networks, such as the internet, corporate network, and vulnerability points [25]. These are used to protect against malicious cyber adversaries gaining access to the ICS networks to disrupt business functions and critical infrastructure. According to NIST 800-82, boundary protection control include routers, gateways, firewalls, encrypted tunnels, mail gateways, and network-based malicious code analysis [22]. Establishing boundary protection protects the ICS from outside threats as it provides the external domains with restricted access [26].

Firewall

In ICS network security control, the firewall is an important security control that controls the flow of network traffic between networks by using different security methods [22], [27]. Firewalls are used by corporate networks to restrict connection from and to the internal networks that are performing sensitive functions such as human resources and accounting [28]. Through the use of firewalls organizations can restrict unauthorized access to resources and organization systems [27]. According to NIST 800-82 firewalls are generally classified into three which are Stateful Inspection Firewalls, Packet Filtering Firewalls, and Application-Proxy Gateway Firewalls [22]. The packet filter is essentially routing devices that contain access control, according to NIST 800-82 the packet filter operate at layer 3 (network) of the ISO/IEC 7498 model, while the stateful inspection firewalls are packet filter that operates based on the awareness of OSI model layer 4 (transport), the application proxy gateway firewalls filter traffic based on some specific rules such as protocols or specified applications [22].

Logically Separated Control Networks (LSCNs)

In protecting the ICS from authorized access, the LSCNs can be used to separate the ICS system from other networks, such as the Internet, and the corporate network, this is usually done through physical and logical separation [28]. Firewalls serve as an effective instrument in that are used to control the traffic between other networks and ICS networks, communication can only be established between a corporate network and an ICS network if there is a demilitarized zone network (DMZ) that has been established [29].

Network Segregation

In protecting the ICS against security threats, network segregation is very important as this can be used as a medium for preventing unauthorized access between distinct network segments [22]. Thus, in this, an examination is carried out on the various strategies for achieving network segregation.

Dual-Homed Computer/Dual Network Interface Cards (NIC)

The use of Dual-Homed Computer/Dual Network Interface Cards (NIC) is a means of creating connections between one network and another [22]. Through this dedicated NIC, network segregation can be achieved by physically separating the networks, this will reduce the risk of data leakage or unauthorized access, as such the NIST 800-82 states that all the connections between the two networks should be through the firewall [22].

Firewall between Corporate Network and Control Network

A significant security improvement can be achieved through the introduction of two-port firewalls between the control networks and the corporate network [22]. According to [22] a firewall controls the traffic between two networks. With an effective and well-configured firewall, unauthorized access and attacks on the control network will be greatly reduced. This provides a significant improvement over non-segregated networks, as the NIST 800-82 opined that the configurations of this firewall should allow traffic for specific services should pass through, and the firewall should be monitored and kept up to date [22].

Firewall and Router between Corporate Network and Control Network

The use of a router and firewall provides a more sophisticated combination [22]; according to NIST 800-53 explanation the router is placed in front of the firewalls which provides packet filtering services in line with the set security policies while the firewall is responsible for scrutinizing incoming and outgoing traffic, enforcing access controls and blocking unauthorized access [22]. The combination of these provides a robust boundary that governs the flow of data and ensures security [22].

Firewall with DMZ between Corporate Network and Control Network

The use of firewalls with DMZ provides a significant improvement, as the establishment of DMZ in corporate and control networks serves as an intermediary and adds an extra layer of security between these two critical networks [30]. Creating a DMZ prevents direct access to control systems that are sensitive [31].

Paired Firewalls between Corporate Network and Control Network

According to NIST 800-82, the use of paired firewalls is a variation of the firewall with DMZ [22]. In this, two firewalls are positioned in tandem between the control network and corporate network to enhance security by ensuring layered protection [22].

Recommended Defense-in-depth Architecture

According to NIST 800-82, to bolster ICS security, multilayer security measures should be created to minimize the impact of failure [22].

References

[1] N. J. T. Force, "NIST Special Publication 800-53 Revision 5–Security and Privacy Controls for Information Systems and Organizations," Technical Report. Computer Security Division, Information Technology …, 2020.

[2] OMB A-130, "Managing Information as a Strategic Resource," Office of Management and Budget Memorandum Circular A-130, 2016. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[3] FISMA, "Federal Information Security Modernization Act (P.L. 113-283)." Congressional Research Service, 2014. [Online]. Available: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[4] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho, "Cyber-Risk Management Planning Using NIST CSF v1. 1, NIST SP 800-53 Rev. 5, and CIS Controls v8," in *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS*, IEEE, 2021, pp. 19–24.

[5] S. H. Somepalli, S. K. R. Tangella, and S. Yalamanchili, "Information Security Management," *HOLISTICA–Journal Bus. Public Adm.*, vol. 11, no. 2, pp. 1–16, 2020.

[6] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, 2020.

[7] J. V. Tojimamatovich, "CONCEPT AND ESSENCE OF INFORMATION SECURITY," *Web Synergy Int. Interdiscip. Res. J.*, vol. 2, no. 4, pp. 643–647, 2023.

[8] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013," *NIST Spec Publ*, vol. 800, no. 53, p. 10, 2022.

[9] A. K. Gill, P. Zavarsky, and B. Swar, "Automation of Security and Privacy Controls for Efficient Information Security Management," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, IEEE, 2021, pp. 371–375.

[10] R. S. Ross, "Assessing security and privacy controls in federal information systems and organizations: building effective assessment plans," 2014.

[11] K. L. Dempsey *et al.*, "Information security continuous monitoring (ISCM) for federal information systems and organizations," 2011.

[12] K. L. Dempsey, V. Y. Pillitteri, C. Baer, R. Niemeyer, R. Rudman, and S. Urban, "Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment," 2020.

[13] S. Brooks, S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, *An introduction to privacy engineering and risk management in federal systems*. US Department of Commerce, National Institute of Standards and Technology MD …, 2017.

[14] S. S. Fortunato, "Risk Management in ICS/SCADA Systems to Enhance Security within the Energy Sector," PhD Thesis, Utica College, 2020.

[15] M. I. Malik, A. Ibrahim, P. Hannay, and L. F. Sikos, "Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions," *Computers*, vol. 12, no. 4, p. 79, 2023.

[16] P. Grassi, M. Garcia, and J. Fenton, “Digital identity guidelines,” National Institute of Standards and Technology, 2020.

[17] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, “How integration of cyber security management and incident response enables organizational learning,” *J. Assoc. Inf. Sci. Technol.*, vol. 71, no. 8, pp. 939–953, 2020.

[18] J. T. Force and T. Initiative, “Security and privacy controls for federal information systems and organizations,” *NIST Spec. Publ.*, vol. 800, no. 53, pp. 8–13, 2013.

[19] M. Nieles, K. Dempsey, and V. Y. Pillitteri, “An introduction to information security,” *NIST Spec. Publ.*, vol. 800, no. 12, p. 101, 2017.

[20] E. McCallister, *Guide to protecting the confidentiality of personally identifiable information*, vol. 800. Diane Publishing, 2010.

[21] M. Souppaya, J. Morello, and K. Scarfone, “Application container security guide,” National Institute of Standards and Technology, 2017.

[22] K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security,” *NIST Spec. Publ.*, vol. 800, no. 82, pp. 16–16, 2011.

[23] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” *Comput. Secur.*, vol. 89, p. 101677, 2020.

[24] Z. Drias, A. Serhrouchni, and O. Vogel, “Analysis of cyber security for industrial control systems,” in *2015 international conference on cyber security of smart cities, industrial control system and communications (ssic)*, IEEE, 2015, pp. 1–8.

[25] B. Galloway and G. P. Hancke, “Introduction to industrial control networks,” *IEEE Commun. Surv. Tutor.*, vol. 15, no. 2, pp. 860–880, 2012.

[26] S. Ponomarev and T. Atkison, “Industrial control system network intrusion detection by telemetry analysis,” *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2, pp. 252–260, 2015.

[27] W. Zegeye and M. Odejobi, “Telemetry Networks Cyber Security Architecture,” International Foundation for Telemetering, 2022.

[28] S. Ponomarev, *Intrusion Detection System of industrial control networks using network telemetry*. Louisiana Tech University, 2015.

[29] T. Macaulay and B. L. Singer, *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.

[30] K. Stouffer, J. Falco, and K. A. Kent, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology. US Department of Commerce, National Institute of Standards and Technology, 2008.

[31] Y. S. Vasiliev, P. D. Zegzhda, and D. P. Zegzhda, “Providing security for automated process control systems at hydropower engineering facilities,” *Therm. Eng.*, vol. 63, pp. 948–956, 2016.