Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions

To cite this article: Anees Ara 2022 *IOP Conf. Ser.: Earth Environ. Sci.* **1026** 012030

Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions

Anees Ara[1]
[1]*CS department, CCIS, Prince Sultan University, aara@psu.edu.sa*
Corresponding Author: aara@psu.edu.sa

Abstract. Industrial control systems (ICS) play a vital role in monitoring and controlling the plants like power grids, oil and gas industries, manufacturing industries, and nuclear power plants. Present research and development in information and communication technologies have changed the domains of industrial control systems from traditional electromagnetic to network-based digital systems. This domain shift has created better interfaces for communication between physical processes and the control units. Eventually, making the complex process of monitoring and controlling the industries easier, with the help of internet connections and computing technologies. The field instruments such as sensors and actuators and the physical processes in industries are controlled and monitored by programmable logic controllers (PLC), remote telemetric units (RTU), and supervisory control and data acquisition systems (SCADA) with the help of communication protocols. The seamless integration of the information technologies (IT) and operational technologies (OT) make the management of the industrial environment foster. However, the inclusion of new technologies that increase the number of internet connections, the new communication protocols, and interfaces that run on open-source software, brings up new threats and challenges in addition to existing vulnerabilities in these classical legacy-based heterogeneous hardware and software systems. Due to the increase in the number of security incidents on critical infrastructures, the security considerations for SCADA systems/ICS are gaining interest among researchers. In this paper, we provide a description of SCADA/ICS components, architecture, and communication protocols. Additionally, we discuss details of existing vulnerabilities in hardware, software, and communication protocols. Further, we highlight some prominent security incidents and their motives behind them. We analyse the existing state of OT and IT security in SCADA systems by classifying the SCADA components among them. Finally, we provide security recommendations based on current trends and also discuss open research problems in SCADA security.

1. Introduction

The national critical infrastructure includes smart grids, oil and gas industries, nuclear power plants, water supply and waste management, health sector, air traffic control and management systems. These systems are having automation processes monitored and controlled by ICS [1]. In past, ICS were isolated and controlled by proprietary protocols, physically secured not connected to any external networks. But with the advancement of information and communication technologies (ICT) and internet connectivity, the protocols in legacy control systems were replaced by the IP based protocols. As result, it increased in remote accessibility and connectivity of devices and increased business continuity. Further the ICS environment is back up by cloud environment to solve the storage and computational cost issues. The wireless communication technologies evolved to connect between the field devices. All these advancements made ICS systems to have similar characteristics as that of information technologies. However, integration of these open standards of communication technologies and hardware or software

systems leads to enormous threats and vulnerabilities in ICS [2]. The TCP/IP based protocols over insecure communication channels increases the possibilities of cyber-attacks. The usage of new hardware and software from third party vendors opens up new threat vectors. The cloud storage systems by third party providers are another addition to increase the attack surface in ICS [3]. The increasing wireless communication networks in the industrial environments increase the risk of attackers to get connected to devices which are closer in physical proximity.

Remotely connected and assisted operational technologies are increasing exponentially worldwide. Due to aforementioned technologies and increasing cybersecurity incidents in ICS, it was reported in first half of 2021, that one-third of ICS were targeted by malicious activities [3]. Kaspersky reported that 33.8% of ICS machines were targeted, among which 18.2% were internet-based threats, followed by 5.2% by removable devices and 3% by email attachments [3]. Further, Claroty reported 637 ICS vulnerabilities affecting the products sold by 76 vendors. Among these 70.93% vulnerabilities are classified as high or critical. Most of these vulnerabilities affected basic controls (15.23%), supervisory control (14.26%), and operations management (23.55%) [4].

ICS mainly includes supervisory control and data acquisition systems (SCADA) and distributed controlled systems (DCS). The SCADA is widely used to control large scale geographical spread production systems whereas DCS is mostly used to control production systems in local factories [5]. In this paper, the study emphasizes on securing SCADA based industrial control systems. SCADA systems security is one of the critical aspects of national critical infrastructure as it protects the safety and security operations of industrial plants and production systems. The SCADA systems are expected to be available and running 24/7 continuously, as they serve the critical operations in real-time. The security measures applied on IT systems cannot ne same as the SCADA systems as availability of the systems is the grave concern. Any interventions on working operations of these critical infrastructures may lead to serious causalities and human lives [6]. In this paper, a comprehensive survey of the SCADA based ICS security is presented. This study reviews the components, architecture and communication protocols of SCADA systems. An elaboration of security vulnerabilities, threats and attacks on the SCADA systems are discussed. Further, we present the security challenges and security solutions. Finally, we discuss the security standards and compliances that are applicable in ICS. Later, we propose some security recommendations and future research directions in this area.

The rest of the paper is organized as follows: In section 2, the overview of the SCADA architecture is presented, followed by in section 3 the security in SCADA is explained by discussing the security issues and the relevant solutions and recommendations. Finally in section 4 future research directions are highlighted followed by conclusion of the paper in section 5.

2. Supervisory Control and Data Acquisition Systems (SCADA)

In this section we describe the SCADA architecture, its basic components, the communication protocols and the related security concerns and recommendations.

2.1. SCADA Architecture

The main job of SCADA is to collect the information about the field devices in the factories and plants and then store and analyse this information to monitor and control automation processes in the industries. The basic architecture of SCADA includes four levels (see Figure 1):

- ***Level 0***: Process level
- ***Level 1:*** Basic control level
- ***Level 2:*** Supervisory Control
- ***Level 3:*** Operations Management

The data flows upstream from level 0 to level 3 in SCADA architecture. Whereas the control commands are sent downstream from level 3 to level 0, i.e. after the data is analysed and based on the decision making the control commands from operations management are forwarded to Level 0 devices [4].

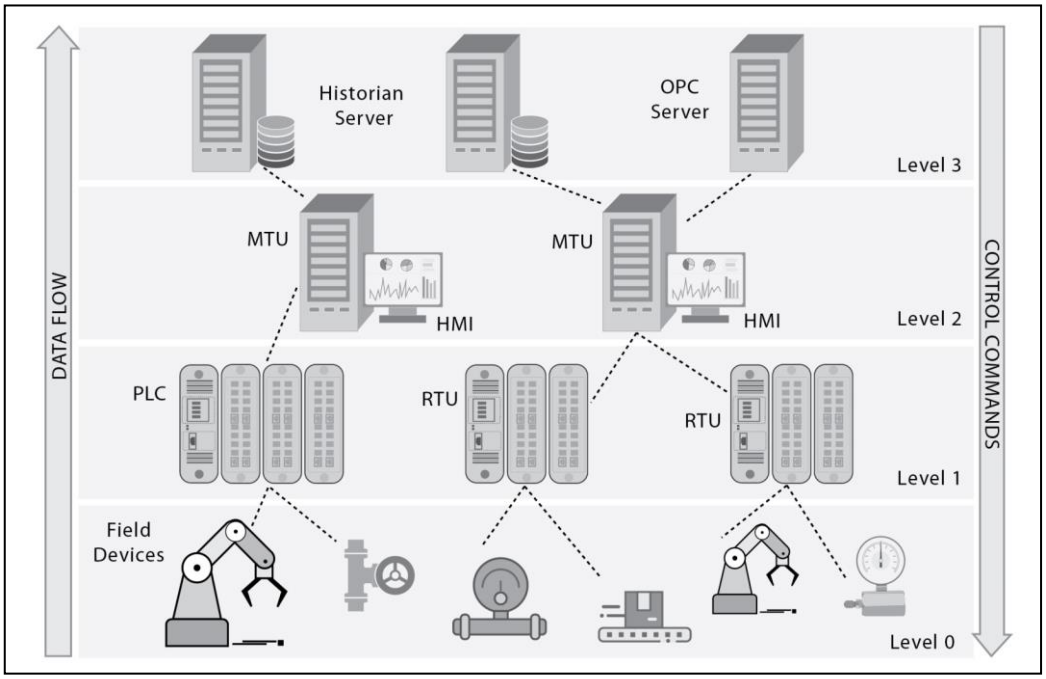

Figure 1. SCADA Architecture

2.2. Components of SCADA

- ***Field Devices:*** These are devices that are deployed in the physical environment that has to be monitored. These devices include sensors to collect the physical data and translate into digital world and actuators that can perform the control actions.
- ***Remote Telemetric Units (RTU):*** These are intelligent electronic devices that send the collected data to MTU. Sometimes in absence of PLC's they also send control commands to actuators.
- ***Programmable Logic Controllers (PLC):*** These are intelligent electronic devices that exchange the collected data to MTU with the control commands that should be sent to actuators. In some cases, the PLC's themselves send suitable commands to actuators based on the logics they are programmed with.
- ***Master Terminal Unit (MTU):*** This is the device that collects all the data from control level terminals and then passes them to supervisory control level. They are responsible for sending control commands to the field devices.
- ***Human Machine Interface (HMI):*** These devices provide the interfaces to the operators to interact with the SCADA system. They can understand the overall schematic diagram of the plant environment. The data collected from MTU is analysed and then appropriate control command is sent to the physical environment.
- ***Servers:*** These are powerful servers that are used to store the data collected from the field devices as databases. OPC servers are special software that acts as an interface between windows software and industrial hardware.
- ***Communication Network:*** The SCADA environment uses numerous communication technologies to communicate between SCADA control room, PLCs, RTUs and other field devices. These communication technologies and devices include, Ethernet, fibre optics, Wi-Fi, satellite, switches, routers, modems etc.

2.3. Communication protocols in SCADA

Based on the aforementioned SCADA architecture, heterogeneous components and their connecting networks, it is evident that one protocol cannot serve the entire purpose. To connect systems efficiently and deliver reliable automation process, the SCADA systems are well equipped with industrial network

protocols, also called as field-bus protocols. There are various industrial network protocols implement in automation industries. However, some of them are very popular, due to ease of use and wide applicability in the market. In this paper, prominent set of protocols, based on their popularity and security concerns are discussed in Table 1.

Table 1. Communication Protocols in SCADA [7], [5]

	Description	**Security concerns**	**Security recommendations**
Modicon Communication Bus (Modbus)	It's an application layer protocol. It is used in both serial and routable architectures. It used for communication between any of the devices such as Sensors, RTU's/PLC's and HMI's in SCADA control room.	Lack of authentication, lack of encryption, Lack of integrity in programming logics at RLU's/PLC's.	This protocol should be used only between known devices. Only expected function codes should be exchanged, any abnormality should be reported.
Inter Control Centre Protocol (ICCP)	IEC60870-6 mostly used for communication between utility control centres using Wide area network (WAN).	It is susceptible to spoofing, session hijacking, lack of authentication, Non-trusted relationships. Accessibility in wide area network.	Penetration testing and patching of ICCP servers is needed. Practice defence-in- depth mechanisms to protect the devices connected in the network.
Distributed Network Protocol (DNP3)	This protocol is used between PLC's and RTU's and also between RTU's and MTU's.	Lack of authentication, and encryptions. Only support given for data frame integrity.	Use of secure DNP3 variant. Penetration testing and patching is needed.
Ethernet for control automation technology (EtherCAT)	It is an Ethernet based protocol used to connect Ethernet based field devices in industries.	Lack of authentication and encryption mechanisms and may lead to packet injections and intrusions.	Intrusion detection mechanisms have to be installed in the industrial network.
Open Platform Communication (OPC)	Set of protocols used to connect the control systems using windows OS.	Flexibility of protocol causes more vulnerabilities to the control systems and may lead attackers to connect through it	Hardening should be applied on the OPC servers to avoid any unwanted communications from attackers.
Common Industrial Protocol (CIP)	It is a peer-peer protocol used to communication between field devices and supervisory control devices.	Unauthorized sessions can be established by attackers. Session hijacking, Message alterations and eavesdropping can happen.	Appropriate authentication and authorization, is needed. Hashes, MACs and digital signatures should be applied.

Additionally, DCS uses vendor specific protocols such as process field net (PROFINET) and process field bus (PROFIBUS) for communication between field devices and high-level devices. Due to the use of vendor specific protocols, DCS is considered to be more secure than SCADA. However, this is true only for large-scale applications [7].

3. Security in SCADA systems

The critical infrastructure based industries are monitored by ICS using SCADA. The operational technologies (OT) are responsible to conduct the seamless automation processes in the industrial

environment with the support of information technologies (IT) and communication network. Both OT and IT technologies work together so that the national critical infrastructure services are available all the time. With the ever growing amalgamation of new technologies, it opens business cases for industries. However, with the growing interconnectivity and remote accessibility of SCADA devices, it brings in new vulnerabilities and increases the threat landscape of ICS [8]. In the following subsections the security vulnerabilities, threats and attacks, security gaols and security solutions are discussed in detail.

3.1. Vulnerabilities, Threats and Attacks

Due to increasing thread landscape in the industrial control systems (ICS), ICS security is continuously gaining attention from various industries including, government, non-government, university researchers, vendors, independent researchers and 3rd party companies [4]. 80% of the vulnerabilities were reported to vendors by external researchers. Table 2, describes the attacks in 2021 as result of the exploitations of the existing vulnerabilities and threats in ICS. For further details on published list of attacks in SCADA/ICS please refer to [9].

Table 2. Some of the key cyber-attacks on SCADA/ICS published in year 2021

Attacks	Year	Consequences & Impact	Reason
Ransom ware attack on colonial pipeline [10]	2021	Impacted the delivery of oil and gas on east coast. May increase the gasoline prices if the impact is continued for long time.	Vulnerable legacy systems and wide spread distributed pipelines operated by any operators.
Oldsmar Water Hack [11]	2021	Attack was conducted using remote desktop sharing app team viewer, changing the sodium hydroxide levels in drinking water. Contamination of the drinking water supply.	Legacy operating systems like windows 7, remote desktop connections and no security hardening.
JBS Attacks [10]	2021	A ransom ware attack was conducted to shut down the distribution service.	Compromised the IT systems by exploring the vulnerabilities in both OT and IT systems

There are several vulnerabilities that extend the attack vectors of ICS systems. The Table 3 describes the vulnerabilities related to hardware, software and communication networks, which comprise the basic components of SCADA systems. Most of the vulnerable and unsecure SCADA devices are discoverable by online search engines like shodan.io and censys.io [12]. The attackers can easily exploit the published vulnerabilities using common vulnerabilities and exposure (CVE) and can plan an organized security attack on the SCADA/ICS systems [12].

Table 3. Vulnerabilities in SCADA/ICS systems [5], [13]

Vulnerability	**Components affected**	**Threat**	**Mitigation**
		Policies and procedure vulnerabilities	
Lack of security controls, policies and procedure	Hardware, Software and communication network	No monitoring on security controls	To maintain the accountability of any actions in the ICS environment, security policies and procedure have to be developed

Lack of authentication and authorization policies	Hardware, Software and communication network	Unauthorized access to the OT and IT environment	An mandatory authentication and authorizations should be done through proper access control policies
Lack of cyber incidence and response plan	Hardware, Software and communication network	The systems will not be able to recover and contain loss	Incident detection and response plans are necessary to take any viable action in a given time
Physical systems vulnerabilities			
Unauthorized access to field devices	Hardware, software and communication network	Unauthorized access to the OT and IT environment	An mandatory authentication and authorizations should be done through proper access control policies
No security hardening and open ports	Hardware and communication network	Unsecure ports and devices can be utilized by malicious insiders to plug-in devices that can upload malwares to the system	Secure hardening should be implemented and all the unnecessary ports should be closed
Lack of security perimeters	Hardware and communication network	Lack of physical security perimeters may lead to unauthorized access and trespassing	All hardware security perimeters should be implanted and software security perimeters like firewalls should be catered.
Architecture and designing vulnerabilities in hardware and software			
Insecure architecture and design	Hardware software and communication network	Insecure architecture may open up unknown loopholes and therefore attacker can exploit these vulnerabilities to get administrators access	The architecture of the ICS systems should start with security in mind from the design phase itself.
Improper data validations in applications facing internet	Hardware, software and hardware	80% of the attacks happen due to the software applications vulnerabilities in ICS. It can lead to complete compromise of the ICS system and data breaches can happen	All the applications run by the SCADA systems should be tested for the user input validations, cross site scripting, and buffer overflow attacks [14]
Communication network vulnerabilities			
Lack of secure industrial communication protocols	Communication network	Most of the communication industrial protocols mentioned in the previous sections lack basic security mechanisms like authentication, integrity and encryptions	Need for secure end-end secure communication protocols to protect the data confidentiality and integrity of operations
Lack of log monitoring	Hardware, software, and communication network	Most of the devices are connected remotely and mostly no logs are recorded	Visibility of the SCADA operations is important to take any actions after security

			incidents. Log monitoring is must.
Inadequate firewall configurations	Hardware, software, and communication network	A lack of firewall configurations may lead to injections of malware from outsiders	Proper firewall rules and policies must be set. Whitelisting is mostly recommended in ICS.

The ICS-CERT have defined a vulnerability coordination process, to timely detect and collect all the vulnerabilities, then conduct a vulnerability analysis, find mitigations and then apply and again continue the cycle. In Table 3, we highlight certain categorizations of vulnerabilities that are prominent in SCADA/ICS environment [5] [13] [15].

3.2. Security Challenges

Due to the combination of heterogeneous OT and IT technologies, the aforementioned list of vulnerabilities add up variety of challenges in SCADA/ICS systems. However, the main challenge is to deal with the people, process and technology [15] in ICS. Following is the list of summarized challenges in SCADA systems:

- Lack of vulnerability assessment and penetration testing techniques. This will lead to inadequate response plan and mitigation strategies.
- Lack of visibility of entire environment. Since the ICS/SCADA systems are wide spread in large scale industries, then there is no log monitoring and accountabilities recorded to know any actions performed by the operators.
- Unsecure communication between OT and IT technologies. The OT technologies use WAN based communication technologies that transmit data in clear text format. So these communications can be exploited by attackers.
- No downtime expected in ICS/SCADA systems. No backup of historian databases. This may affect the installation of software updates and firmware on the legacy systems. Any compromise on the database servers will lead to huge data breach and loss in the revenue.
- Lack of trained personnel and inadequate knowledge about the security standards, policies and procedures.

3.3. Security Goals

In ICS, the security goals of the critical infrastructure can be categorised as follows:

- ***Availability:*** The primary concern of the SCADA systems in ICS is to provide continuously reliable and secure services with high level of assurance. Any security incident should not lead to shutdown of the critical infrastructure. Therefore a graceful degradation mechanism should be applied on process automations.
- ***Integrity:*** The secondary concern in SCADA systems is the correctness of data collection, analysis and the transmission of control logics to the field devices. If any of these is manipulated by any intruders through active man-in the middle attack, this may lead to unexpected errors in the production process and cause fatalities and huge business losses.
- ***Confidentiality:*** The data collected by the sensors from the field environment are time constraint. They don't have to be secured all the time. As the time passes the data becomes absurd. However, the storage data in the historian servers need to be secured from any data breaches. These data contribute in analysing the field environment and in appropriate decision making.
- ***Authorization:*** All the operations or commands given by operators, machine-machine interactions in the SCADA environment should be identified by proper authorizations and access control mechanisms. There should be log monitoring for all the operations conducted on any automation processes.

3.4. Security Solutions and Recommendations

From the previous discussion on security attacks, vulnerabilities and threats in the ICS/SCADA environment, it is evident that there are various security challenges faced by these systems. In this section we provide some security solutions and recommendations so that we can achieve the previous stated security goals in SCADA/ICS systems.

- **Security standards and compliances**: For protecting the ICS in [16], the ICS security related standards guidelines are provided for IT and OT security. IEC 62351 [16] is recommended for data and communication security, IEC 62210 [16] for communications in power systems control and ISO 27000 families of standards is recommended for ICS software and equipment manufactures. For complete details on security compliances and guidelines please refer to National Institute of Standards and Technology (NIST) [5] and European Union Agency for Cybersecurity (ENISA) [16] reports.
- **Need for security maturity models in ICS environment:** The security teams should identify the crown jewels (assets) in their industries and plan a business contingency plan in case of any security incidents. Risk assessment and management should be proactively done. Mitigation plan for the existing vulnerabilities and threats should be implemented.
- **Visibility of the OT and IT operations:** There should be log monitoring done for the IT security team, which should also monitor the OT environment. Network intrusion and Detection and Prevention (IDS/IPS) systems should be installed. Any inappropriate behaviour in the network should raise an alarm and timely actions have to be applied.
- **Network Segmentations and segregations:** Physical and logical network segmentations should be done to prevent any malicious traffic from outside. Network traffic filtering mechanisms such as industrial firewalls should be installed in ICS environments.
- **Defense-in-depth strategies:** The ICS/SCADA systems should adapt defense-in-depth approaches such as security policies, authentications and authorizations, firewall controls, separating mailing servers in DMZ network zones, redundant communication networks, graceful degradations and restricted physical access and encryptions and backup and recovery procedures.
- **Education/trainings and certifications:** The employees/operators working in OT and IT teams should be given enough training on the security guidelines and policies related to authentication and authorization of their roles. The security teams should include members who are qualified and certified Example: ISO 27001, or ISO/IEC 27019:2017 (information security controls for energy utilities) etc [8].

4. Future Research Directions

With the ever-growing need for industrial automations in various sectors and inclusions of new technologies such as cloud computing, Artificial intelligence (AI), Blockchain and distributed infrastructure, their opens new business opportunities and research directions [17].

- **Technological revolution:** Addition of virtualisation, internet of things (IoT) [19], 5G and blockchain technologies brings up new research directions [20] to combine them and propose the standardize schemes to protect the ICS environments [21] [22] [23]. AI techniques have been abundantly used in analysing the behaviour of the network and maximize the capabilities of the network. However, the same AI can be used by attackers to exploit the system faster.
- **Authentication and Authorization:** When the operators and machines are participating in command and control operations in large-scale ICS environment then it becomes difficult to monitor the authentication and authorization controls in remote locations. There is a need for least privilege and accountable authorization mechanisms in these areas, to avoid exploitations by adversaries [18].
- **Third party vendors and open source software:** To reduce the attack surface and increase the visibility of network, trusted, product specific whitelisting should be done. There is need for framework that includes end-end enhanced network monitoring and detection techniques [22]. The open source software used in ICS/ SCADA systems leads to ease of installations and

extensibility of the performance of systems. However, with insecure open source libraries they can lead to malicious code injections and open new vulnerabilities and threats.

Hence there are many challenging research directions that can be considered in proposing new secure schemes that strike a balance between security and performance.

5. Conclusion

Industrial controls systems monitor the national critical infrastructure using the SCADA systems. These systems monitor the critical applications like power grids, transportations, and manufacturing and production industries. The SCADA systems are connected with many heterogeneous devices to monitor and control the automation process in the industries. In this paper, the SCADA architecture, components, communication protocols have been explained. A detailed investigation on the security of SCADA systems with respect to operational and information technologies is conducted. An elaborated discussion on current cyber-attacks their motives, list of vulnerabilities, threats and mitigations, security challenges and respective security goals is presented. Further, based on the discussed security issues, an enhanced list of security solutions and recommendation is given. Finally, future research directions and the need for new security mechanisms are highlighted at the end. In upcoming projects, we would like to propose secure SCADA design and architecture that can provide authenticated data transmission, and secure aggregation in ICS environment.

6. References

[1] Yadav, G., & Paul, K. 2021. Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection, 100433.
[2] Tariq, N., Asim, M., & Khan, F. A. 2019. Securing SCADA-based critical infrastructures: Challenges and open issues. Procedia Computer Science, 155, 612-617.
[3] Kaspersky, I. C. S. 2021. Threat landscape for industrial automation systems.
[4] *Biannual ICS Risk & Vulnerability Report: 1H 2021*, 2021. Accessed online on January 22, 2021. https://security.claroty.com/1H-vulnerability-report-2021
[5] Stouffer, K., Falco, J., & Scarfone, K. 2011. Guide to industrial control systems (ICS) security. NIST special publication, 800(82).
[6] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.
[7] Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Communications Surveys & Tutorials, 22(3), 1942-1976.
[8] Dragos: 2020 ICS cybersecurity: Year in review 2020.
[9] The Repository of Industrial Security Incidents, 2016. Accessed online on January 22, 2021. http://www.risidata.com/
[10] Keary, J. (2022). Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware.
[11] Hunt, J. S. (2021). Countering cyber-enabled disinformation: implications for national security. Australian Journal of Defence and Strategic Studies, 3(1), 83-88.
[12] Ceron, J. M., Chromik, J. J., Santanna, J., & Pras, A. (2020). Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands. arXiv preprint arXiv:2011.02019.
[13] U.S. Department of Homeland Security, ICS-CERT Monitor, Technical Report ICS-MM201210, Washington, DC, 2016
[14] Mathas, C. M., Vassilakis, C., Kolokotronis, N., Zarakovitis, C. C., & Kourtis, M. A. 2021. On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids. Energies, 14(10), 2818.
[15] Mar Bristow SANS 2021 survey: OT/ICS Cybersecurity
[16] ENISA, 2011. Protecting industrial control systems, Annex III. ICS Security Related Standards, Guidelines and Policy Documents, Ed. ENISA

[17] Securing the grid: cybersecurity report in the electricity sector 2020. Accessed online on January 22, 2021. https://nca.gov.sa/files/cres_en.pdf
[18] Faquir, D., Chouliaras, N., Sofia, V., Olga, K., & Maglaras, L. 2021. Cybersecurity in smart grids, challenges and solutions. AIMS Electronics and Electrical Engineering, 5(1), 24-37.
[19] Nasralla, M. M., García-Magariño, I., & Lloret, J. (2020). Defenses against perception-layer attacks on iot smart furniture for impaired people. IEEE Access, 8, 119795-119805.
[20] Zhang, Y., Li, J., Zheng, D., Li, P., & Tian, Y. 2018. Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice. Journal of Network and Computer Applications, 122, 50-60.
[21] Butun, I., Lekidis, A., & dos Santos, D. R. 2020, February. Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities. In ICISSP (pp. 733-741).
[22] Khan, M. A., Nasralla, M. M., Umar, M. M., Khan, S., & Choudhury, N. (2022). An Efficient Multilevel Probabilistic Model for Abnormal Traffic Detection in Wireless Sensor Networks. Sensors, 22(2), 410.
[23] Khan, M. A., Nasralla, M. M., Umar, M. M., Iqbal, Z., Rehman, G. U., Sarfraz, M. S., & Choudhury, N. (2021). A Survey on the Noncooperative Environment in Smart Nodes-Based Ad Hoc Networks: Motivations and Solutions. Security and Communication Networks, 2021.

7. Acknowledgments

My special thanks to Dr. Dhafer Almakhles and Dr. Abdul Hakim AlMajid from Prince Sultan University for their encouragement on this research work. I take the privilege to thank in advance the anonymous reviewers for their valuable comments to improve the quality of paper.