Bulletin of Networking, Computing, Systems, and Software – www.bncss.org, ISSN 2186-5140
Volume 11, Number 1, pages 1–6, January 2022

A Survey of the Offensive and defensive in Industrial Control System

Kuan-Chu Lu
Department of Electrical Engineering, Institute of Computer and Communication Engineering
National Cheng Kung University
Tainan, Taiwan
kclu@cans.ee.ncku.edu.tw

I-Hsien Liu
Department of Electrical Engineering, Institute of Computer and Communication Engineering
National Cheng Kung University
Tainan, Taiwan
ihliu@cans.ee.ncku.edu.tw

Jung-Shian Li
Department of Electrical Engineering, Institute of Computer and Communication Engineering
National Cheng Kung University
Tainan, Taiwan
Jsli@mail.ncku.edu.tw

***Abstract*—With the rapid development of the Industrial Internet of Things, the key infrastructure has been transformed from a closed system to an open one and has provided huge benefits, such as reliability, scalability and remote connectivity. But relatively, it also exposes the originally isolated security system to global cybersecurity threats, Therefore, when the ICS system is controlled remotely, a safe and secure method needs to be established, prevent hackers from attacking, and prevent the ICS system from malfunctioning or being invaded by malicious viruses when the ICS system is attacked, causing unprecedented economic losses in the country. In order to protect the country's important economy and security, it is necessary to have an in-depth understanding of the tools that can protect the security of the system, prevent attackers from invading the ICS system. This study will investigate tools and techniques to discover ICS system vulnerabilities or weaknesses, provide a comparison of different defense methods, and give security recommendations to protect the ICS system.**

Keywords*—*Industrial Control System*、*Internet of Things*、*Industrial safety

I. Introduction

Industrial Control System (ICS) is a control system from a computer organization, contains supervisory control and data acquisition (SCADA) system, distributed control system and machine control operation process system. These systems are widely used in many key infrastructures and private enterprises in daily operations, including departmental communications such as energy plants, reservoirs, transportation industries, and chemical plants, as long as there is any communication failure or broken situation in these departments, it may have a great negative impact on our lifestyle. Therefore, the importance of ICS information security has attracted considerable attention from every country in the world [1].

The Zero Day Initiative (ZDI) team made an in-depth study on the security of today's SCADA HMI, a careful analysis of all SCADA software vulnerabilities that have been revealed and fixed between 2015 and 2016, this also includes 250 vulnerabilities notified by the ZDI project. Trend Micro found that these vulnerabilities are mainly divided into several categories: 20% memory corruption, 19% poor management of login credentials, lack of authentication/authorization mechanism and insecure default value of 12%, And 9% of code injection vulnerabilities, all are vulnerabilities that can be prevented by safe programming habits, as shown in Figure 1. Based on the above-mentioned vulnerability methods, hackers may hack into the SCADA system to collect information such as plant equipment configuration drawings, Critical Thresholds and device settings and other data, and then engage in follow-up attacks, the main reason is that the PLC is a set of programmable software. By downloading a new program, the PLC can be reconfigured and run. In normal circumstances, it is usually directly connected to the PLC via a network cable or LAN, and is used with an engineering station to download new programs.

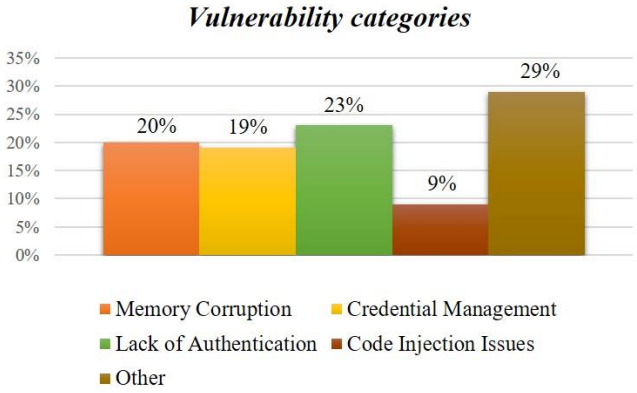

Fig. 1. Vulnerability Survey Diagram [10]

Therefore, the attacker may interfere with and harm the communication between the engineer station and the PLC, and may cause great injure to the entire SCADA system. Take the Stuxnet virus as an example, which once targeted Iran's nuclear facilities [2][3], As well as the computers of workstation personnel in Ukrainian power plants being remotely manipulated, they will all take advantage of this special vulnerability and download malicious programs to the PLC. Most of the existing work is concentrated on HMI-PLC and PLC field device communication [4][5][6][7][8] through Modbus, DNP3 and other agreements. The HMI is a terminal demonstrate device, Which generally displays the condition of the PLC and control process graphically. HMI enables the operator to interact with the PLC and provide some commands for it. In addition, the entire process output, alarms, and events of the equipment in the field are displayed on the HMI.

It can be seen that ICS systems are mostly managed through HMI software, and this type of software is usually installed on a computer with a network connection, Therefore, HMI is one of the main targets of SCADA system attacks. However, the vulnerability of HMI may face the problem of malware intrusion, according to a Trend Micro report, several major well-known ransomware viruses such as Ryuk (20%), Nefilim (14.6%), Sodinokibi (13.5%) and

LockBit (10.4%), it accounts for more than half of all ICS ransomware infection cases in 2020[10].

We can see that the advancement of the ICS system has led to an incremental improvement in the number of malware attacks. However, defensive security devices that can resist intrusion by attackers such as SIEM, Intrusion Prevention System (IPS), firewalls, Intrusion Detection System (IDS), honeynet. Governments and enterprises respond to cyber-attacks by authority control, restricting IP and antivirus software to resist potential threats. However, antivirus software usually only detects well-known malicious software programs to prevent vulnerabilities that invade computers and devices. But with the endless changes in malware attacks, one day it will be invaded by malware programs. Therefore, we will discuss the currently commonly used defense methods and industrial control system safety guidelines to resist possible threats, but different information security equipment has various differences and structures, Therefore, this research will collect different on-site attack cases and try to propose an architecture diagram for discussion. The second section introduces the ICS system security assessment process, ICS architecture and communication protocol, the third section organizes the attack tools, types, and cases study by other research, the fourth section collects and compares the used defense tools, types and functions, and discusses how to attack and defend. And discuss and conclude in the last section, and suggest how to prevent and ensure the stability of the system.

II. BACKGROUND

A. *Evaluation Process*

This study proposes an evaluation process method for research architecture and ICS security[11][12][13], as shown in Figure 2. We introduce the basic structure of ICS and ICS communication protocol, since the ICS system has developed to the fourth generation, it is an independent controller system, a distributed control system, a networked control system and an Internet of Things control system. Considering that there will be many network attacks and malicious software intrusion in the future, we will discuss the attack analysis of the ICS system in Chapter 3 and propose various types of attack techniques. The reports of attacks against units in different countries confirm that ICS attacks have a very serious impact on a country. This study shows the urgent need to protect the ICS system, Therefore, analysis and discussion are conducted based on the attacked country (industry), the type of attack, and the vulnerable of ICS architecture.

In Chapter 4, we discuss defenses, such as the comparison of different defense methods such as firewalls, IDS, IPS, etc., as well as the detection and prevention of these attacks and the identification of vulnerabilities in the system. In addition, many international organizations, such as IEEE, National Infrastructure Protection Center (CPNI), American Gas Association (AGA) and other international organizations, issue security guidelines for ICS systems, and suggest how to prevent the system from being threatened. Finally, the conclusion of Chapter 5 will discuss the issues between attack and defense and make suggestions to ensure system stability and security.

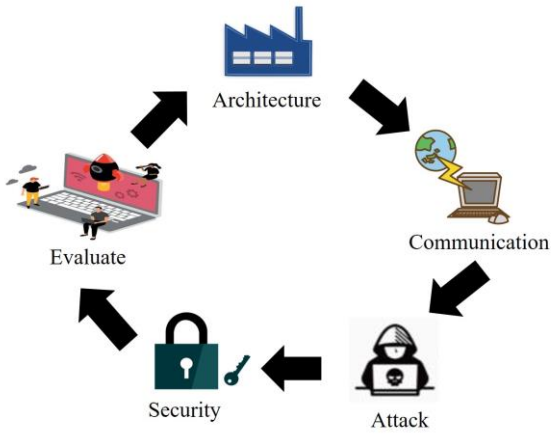

Fig. 2. Security Assessment

B. *ICS Architecture*

The system architecture based on information network technology in Industrial Control Systems (ICS), Monitoring personnel can find remote terminal units through the monitoring screen of the HMI whether there is any abnormal report system, allows the monitoring personnel to control the various equipment systems of the workstation in real time. The SCADA system continues to expand rapidly, With the development of network technology, the monitoring distance is better than before. Application areas include energy facilities, water resources facilities, automobile manufacturing, chemical plants, etc., all of which are monitored and managed through the SCADA system [14].

The ICS is mainly composed of HMI, Supervision Console, Wireless, Data Historian, SCADA Server, Remote Terminal Unit, PLC, Router, Work Station, as shown in Figure 3 [15].

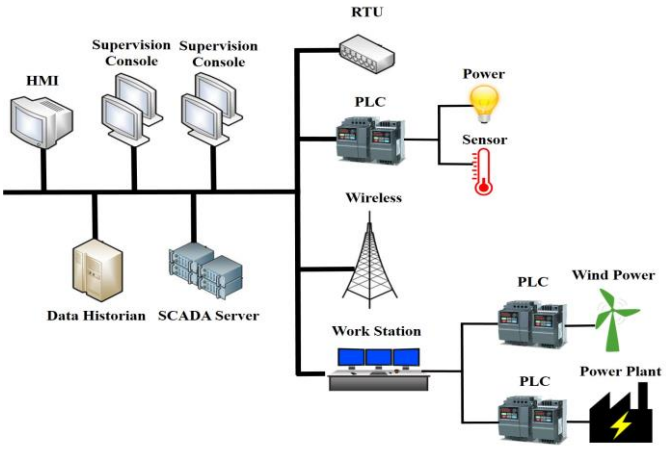

Fig. 3. ICS Framework

C. *Communication Protocol*

The communication protocol is mainly the provision of data narration and exchange through communication links. The ICS communication protocol plays a key role in the MTU-RTU interaction, initially, the instrument and the protection relay allowed the use of RS232 or RS485 for remote communication, but due to scalability issues, it has now moved to a more advanced protocol [16].

Since the ICS system is composed of many devices, if each device uses a vendor-specific agreement, it will not communicate with other devices. Each supplier has a specific ICS communication protocol and has its own rules and communication programs, but these rules and communication programs may have some technical problems due to data presentation and address conversion. Therefore, in order to support interoperability and cost efficiency, some open standards have been proposed [17]. The open protocol improves the availability and interoperability of equipment, minimizes dependence on suppliers, optimizes costs, and simplifies technical support, the following will introduce and discuss the protocols commonly used in industrial control systems, such as Modbus, DNP3, Profibus, etc. The methods of attacks and the cases are shown in Table 1.

- Modbus is a transmission protocol developed by Gould Modicon, which is an application layer messaging protocol for Modicon programmable controllers [18]. In the Modbus protocol, the ASCII transmission mode is used to transmit messages between the Client station and server stations (field devices) through serial communication lines. The newer Modbus TCP protocol provides connections between Modbus networks and IP interconnected Modbus networks. The TCP variant allows the master device to have multiple outstanding transactions, and allows the device to communicate with and send to multiple master devices. Attacks on Modbus systems and networks can have a variety of effects, from sporadic interruptions of field devices (sensors and actuators) to large-scale interruptions, and even loss of control in the case of deceiving the master station. For example, Chen at el. [19] used CPS TestBed to implement attacks (MiTM attacks and DoS) to analyze the security of the Modbus/TCP protocol.
- DNP3 (Distributed Network Protocol) is a communication protocol used between equipment components of an automation system [20], which was developed by Harris Corporation in 1993. The motivation of DNP3 protocol is to obtain openness and interoperability between RTU and MTU and programmable logic controller (PLC). In the layered architecture of the DNP3 protocol, the application layer specifies the data packet design, services and procedures of the application layer[21]. Lu et al. [22] proposed a cryptographic-based design to enhance the security of the DNP3 protocol. The author observes that the upgraded DNP3 protocol can overcome replay attacks and man-in-the-middle (MitM). This method consists of four stages: communication protocol, critical update, key agreement, identify authentication.
- PROFIBUS is a fieldbus standard used in automation technology, n 1987, the German Federation (BMBF) started a cooperation project with the goal of promoting a serial field bus that can meet the basic needs of field device interfaces. The function is that the data communication between MTU and RTU is a cyclic process. MTU reads RTU input data and writes RTU output data. The earliest one proposed in PROFIBUS is PROFIBUS FMS. which is a complex communication protocol designed for demanding communication tasks and is suitable for general communication tasks of industrial equipment [23].

TABLE I. SIMULATION ATTACK TYPES

Attribute	Modbus	DNP3	Profibus
Organization	Gould Modicon	GE-Harris Canada	BMBF Germany
Year	1979	1993	1989
Source	Open source	Open source	Commercially available
Offensive	DoS, MiTM [19]	replay, MiTM attack [24]	DoS, DDos
Security state	No authenticati on and encryption mechanism	Including authentication and encryption mechanism.	Including authentication and encryption mechanism.

III. OFFENSIVE CLASSIFICATION

Rcently, the number of security-related attacks on SCADA systems has increased dramatically. Threats like Stuxnet, Aurora, Maroochy [25] [26] give society a clear idea of how much harm a powerful opponent can cause to the public. These systems are expected to run uninterrupted, so they cannot be upgraded without affecting their productivity. Moreover, most of the communication happens on the network, making it vulnerable to network security attacks. We also emphasize that the vulnerable ICS devices in each threat, such as programmable controllers (PLCs), MTUs, and RTUs, still use the old version of SCADA software and cannot be updated, Therefore, these are vulnerable to well-known vulnerabilities. To analyze SCADA-specific attacks, we searched available databases. The RISI[27] database is the only database that lists specific SCADA attacks. Other current databases of vulnerabilities include NVD [28], ICS-CERT [29], WhiteSource [30]. They observed that more than 80% of the vulnerabilities can only be exploited on the Internet.[28] This is caused by insecure and legacy operating systems. In Table 2, we summarized some of the SCADA security incidents with greater impact. The table highlights the countries and industries that reported attacks. It lists the methods of launching the attack and the vulnerable SCADA components.

In addition, 20% of attacks on critical infrastructure are unknown [31]. As time goes by, attackers begin to use more sophisticated techniques to undermine the security of the SCADA system, so the threat is getting bigger [32]. So far, attackers have mainly focused on high-level systems, such as human-machine interfaces and communication protocols. But what is surprising is that field device firmware development is the least concerned research area [33].

The complexity of cyber-attacks against ICS mainly includes two aspects: attack methods and attack tools. According to the Industrial Control System Cyber Kill Chain [36], cyber attackers do not target the SCADA system in a single incident and vulnerability, but use a series of efforts to achieve access and provide sufficient information to design

effects. Firstly, a fundamental and critical step is to discover the ICS devices exposed on the Internet [37]. Then, the attacker will use the infected device as a gangplank to further probe the whole ICS network [38]. Finally, using these acquired knowledge, attackers can have a predictable impact on ICS by bypassing or affecting the security mechanism, and realizing a real cyber-physical attack [39]. Consequently, in particular network communication based on the ICS protocol, plays an important role in the process of network attacks. In terms of attack tools, since the Stuxnet virus in 2010 [40], a variety of ICS-targeted viruses have been detected, such as BlackEnergy, Duqu, etc. [41]. Even the concept of a virus for ICS devices was discussed and tested. [42], other research discusses the methods of simulated attacks and the cases are shown in Table 3. Most of them use DDOS, DOS, spoofing, Replay, Malware attacks to simulate attacks.

In this study, we can find that the main attacks are launched through the Internet, entering the ICS system for manipulation or theft of funds. In addition, the simulated attack methods in other research are similar to actual attacks, because these attack methods may cause serious damage to the information system or cause significant losses to users. Therefore, as long as master these main types of attacks, we can conduct defense prevention and education. However, with the general technical awareness and the current global security situation is not mature, such attacks may become easier. The next chapter will introduce the defense methods of other research, and discuss a defense method that this review study believes is most suitable for understanding the attacker's thinking.

TABLE II. MAJOR TYPES OF ATTACKS

Item	Using	Vulnerable	Author
Russia-Siberian gas pipeline exploded	Malware	Controller	RISI (1982)[27]
Lithuania Nuclear Power Plant Virus	Malware	RTU	RISI (1992)[27]
Australia-Wastewater Control System	Unauthorised Remote Access	Communication protocol	Slay et al. (2007)[34]
U.S.-Car manufacturer hacked	Malware	Communication Protocols	RISI (2012)[27]
Germany-Steel Plant Cyber Attack	Unauthorised Remote Access	Access to SCADA network	Lee et al. (2014)[35]

TABLE III. MAJOR TYPES OF ATTACKS

Item	Use tools	Using	Author
Wind power plant	OMNeT++	DDoS, spoofing attacks	Queiroz et al. (2011)[43]
Power plant	MAlsim based	Malware simulation	Leszczyna et al. (2008) [44]
Stuxnet on a power plant	MATLAB, Emulab	Malware experimentation	Genge et al. (2012) [45]
Power Control Systems - Resilience	Data statistics	DoS, Data logging	Dondossola et al. (2009) [46]
Tennessee Eastman chemical process	Simulink/Stateflow, HLA, NS2, OPNET, OMNeT++	DDoS, Network	Davies et al. (2009) [47]
Tenessee Eastman	Analytical, simulation	Replay attack	Mo et al. (2014) [48]

IV. DEFENSIVE STRATEGY SELECTION

Many international organizations, such as IEEE, Centre for the Protection of National Infrastructure (CPNI), American Gas Association (AGA), North American Electric Reliability Corporation (NERC) and National Institute of Standards and Technology (NIST), Industrial Automation and Control System Security (ISA) and others often publish security ICS implementation guidelines, and it is recommended that the industry follow these safety guidelines. Security tools such as Core IMPACT and Immunity CANVAS all have some kind of ICS module [46], They have legitimate information security professionals, especially penetration testers, to test the ICS system and ensure that they can resist existing known vulnerabilities. There are two problems with this method. For example, these tools can be used illegally. They are regarded as dual-use tools for attack and defense. Through comprehensive testing, all parties are prepared to ensure that they are not threatened. On the contrary, they have the opportunity to be attacked, as mentioned in the third chapter, the script may have the point of attack.

These tools cannot provide a wide range of ICS attacks. It should be said that penetration testers cannot prove that the SCADA system is completely secure, every time a new vulnerability is discovered, new requirements will continue to be developed in the penetration testing software. The preventive systems used in general IT networks (such as IDS, firewalls, IPS, and SIEM) are also effective when used to protect ICS corporate networks [49]. These systems can be used to protect ICS and control networks, but they must be customized according to the types of data (such as protocols) that exist in this environment. Companies like Tofino provide security solutions for specific ICS and control networks.

And ICS Honeynets are virtual simulations of real ICS systems, which are used to prevent hackers from attacking real systems, the honeynet is very suitable for collecting various realistic statistics, such as current hacker attack trends, methods, tools, hacker's geographic location and number of attacks and other analysis information. Although there is almost no statistical information available for these new systems, they are likely to prove the scale of the attack on the ICS system and the complexity of the attackers. But ICS Honeynets does provide information that can help improve the security of the ICS system. It is also useful in many other industries, and there are no obstacles in the ICS system [50]. The comparison of defense methods is shown in Table 4. As a result, ICS cybersecurity researchers rely mainly on the development of software and simulation hardware to create an ICS attack environment. As shown in Table 5, for the defense methods used in other research

simulation environments, use firewalls, IDS, IPS and other methods to defend against malicious attacks such as Malware, Replay, DDoS, and MiTM, by understanding these methods, we can learn how ICS chooses a suitable defense method, and analyze and evaluate the security of the system.

TABLE IV. TYPES OF DEFENSIVE COMPARISON

Item	Test Environment	Record Attack	Block IP Adress
FireWall	×	×	✓
IDS	×	×	✓
IPS	×	×	✓
SIEM	×	×	✓
Core IMPACT	✓	×	×
Honeynets	✓	✓	✓

TABLE V. COMPARISON OF DEFENSIVE METHODS AGAINST OFFENSIVE

Item	Malware	Replay	DDoS	MiTM
FireWall	×	✓	✓	✓
IDS	×	✓	✓	✓
IPS	×	✓	✓	✓
SIEM	×	✓	✓	✓
Core IMPACT	×	✓	×	✓
Honeynets	✓	✓	✓	✓

V. CONCLUSION

This study is aimed at studying the ICS system environment, discussing that the Internet connection has changed the threat of the overall ICS system, it is urgent to plan a good security assessment process and strategy to protect the network security of the system from threats and attacks. This study reviews current research and literature on major cyber-attacks, including environmental configuration and other methodologies. These techniques can be used to determine the scale of an attack that can reveal vulnerabilities in the system. This all helps system developers and suppliers to make assessments when planning the system, and system users or clients can also understand security regulations and comply with relevant laws and regulations, Due to the rapid changes in the trend of cyber threats, the adoption of security technologies will be relatively forced by new threats. Therefore, the defense technology and evaluation of the network need to be constantly evolving to respond to the threats of attackers. Some organizations, such as IEEE, CPNI, AGA, NERC, NIST, ISA, etc., often publish security ICS implementation guidelines. It is recommended that the industry strictly follow. At the same time, the functions and attributes of various defense technologies are compared. Finally, this study believes that the honeynet will be a defense method suitable for industrial control systems. The honeynet can predict whether it has a vulnerability crisis through the test environment, and it can also track the attacker's address and record actions, and predict the attacker's next attack method to ensure the stability and operation of the ICS system.

ACKNOWLEDGEMENTS

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 110-2218-E-006-013-MBK.

REFERENCES

[1] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436.

[2] Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), 29.

[3] Zhioua, S. (2013). The middle east under malware attack dissecting cyber weapons. International Conference on Distributed Computing Systems Workshops, 11-16.

[4] P. Huitsing, R. Chandia, M. Papa, S. Sheno. (2008). Attack taxonomies for the Modbus protocol, International Journal of Critical Infrastructure Protection, 1(0), 37-44.

[5] W. Gao, T. Morris, B. Reaves, D. Richey. (2010). SCADA Control System Command and Response Injection and Intrusion Detection, eCrime Researchers Summit, 1-9.

[6] Pietre-Cambacédes, L., Tritschler, M., & Ericsson, G. N. (2010). Cybersecurity myths on power control systems: 21 misconceptions and false beliefs. IEEE Transactions on Power Delivery, 26(1), 161-172.

[7] Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Im, E. G., Yao, Z. Q., & Wang, H. F. (2012). Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems, 1-8.

[8] Morris, T. H., & Gao, W. (2013). Industrial control system cyber attacks. In Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research, 22-29.

[9] P. Maynard, K.M. Laughlin, B. Haberler, Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks, in: Proceedings of the Second International Symposium on ICS & SCADA Cyber Security Research, 30-42.

[10] Trend Micro. (2020). Report on Threats Affecting ICS Endpoints. [online]. Available: https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-endpoints.pdf [Access date: 9. 11. 2021]

[11] Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection, 34, 100433.

[12] Abou el Kalam, A. (2021). Securing SCADA and critical industrial systems: From needs to security mechanisms. International Journal of Critical Infrastructure Protection, 32, 100394.

[13] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[14] Townsend, J., Badar, M. A., & Szekerces, J. (2016). Updating temperature monitoring on reciprocating compressor connecting rods to improve reliability. Engineering Science and Technology, an International Journal, 19(1), 566-573.

[15] Trend Micro. (2017). Why Do Attackers Target Industrial Control Systems? [online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/why-do-attackers-target-industrial-control-systems [Access date: 9. 12. 2021]

[16] M. Uzair, Communication methods (protocols, format & language) for the substation automation & control. [online].Available:https://www.eng.uwo.ca/people/tsidhu/Documents/project%20report%20Uzair.pdf [Access date: 9. 12. 2021]

[17] T. Sheldon , McGraw-Hill's Encyclopedia of Networking and Telecommunica- tions, McGraw-Hill Professional, 2001 .

[18] D. Upadhyay, S. Sampalli, SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations, Comput. Secur. 89 (2020) 101666, doi: 10.1016/j.cose.2019.101666 .

[19] Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L., & Kundur, D. (2015). Implementing attacks for modbus/TCP protocol in a real-

time cyber physical system test bed. In 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability, 1-6.

[20] Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2014). The SCADA review: system components, architecture, protocols and future security trends. American Journal of Applied Sciences, 11(8), 1418.

[21] Mahapatra, K. C., & Magesh, S. (2015). Analysis of vulnerabilities in the protocols used in SCADA systems. International Journal of Advanced Research in Computer Engineering & Technology, 4(3).

[22] Lu, Y., & Feng, T. (2019). Cryptography Security Designs and Enhancements of DNP3-SA Protocol Based on Trusted Computing. Int. J. Netw. Secur., 21(1), 130-136.

[23] SMAR. (2021). What is PROFIBUS? [online]. Available:https://www.smar.com/en/profibus [Access date: 9. 12. 2021]

[24] East, S., Butts, J., Papa, M., & Shenoi, S. (2009). A Taxonomy of Attacks on the DNP3 Protocol. In International Conference on Critical Infrastructure Protection, 67-81.

[25] Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), 29.

[26] Slay, J., & Miller, M. (2007). Lessons learned from the maroochy water breach. In International conference on critical infrastructure protection, 73-82.

[27] RISI. (2015). RISI Online Incident Database [online]. Available:https://www.risidata.com/index.php?/Database [Access date: 9. 12. 2021]

[28] I.T. Laboratory. (2000). National vulnerability database[online].Available:https://nvd.nist.gov/general [Access date: 9. 12. 2021]

[29] CISA.(2021). ICS-CERT Advisories [online].Available:https://us-cert.cisa.gov/ics/advisories [Access date: 9. 12. 2021]

[30] WhiteSource.(2021). WhiteSource Vulnerability Database [online].Available: https://www.whitesourcesoftware.com/vulnerability-database/ [Access date: 9. 12. 2021]

[31] Ogie, R. I. (2017). Cyber security incidents on critical infrastructure and industrial networks. In Proceedings of the 9th International Conference on Computer and Automation Engineering, 254-258.

[32] Chan, A. C. F., & Zhou, J. (2013). On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. IEEE Communications Magazine, 51(1), 58-65.

[33] Zhu, R., Zhang, B., Mao, J., Zhang, Q., & Tan, Y. A. (2017). A methodology for determining the image base of ARM-based industrial control system firmware. International Journal of Critical Infrastructure Protection, 16, 26-35.

[34] Slay, J., & Miller, M. (2007). Lessons learned from the maroochy water breach. In International conference on critical infrastructure protection, 73-82.

[35] Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber attack. Industrial Control Systems, 30, 62.

[36] SANS.(2015). The Industrial Control System Cyber Kill Chain [online].Available: https://www.sans.org/white-papers/36297/ [Access date: 9. 12. 2021]

[37] Bou-Harb, E., Debbabi, M., & Assi, C. (2014). On fingerprinting probing activities. computers & security, 43, 35-48.

[38] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.

[39] Kalogeraki, E. M., Polemi, N., Papastergiou, S., & Panayiotopoulos, T. (2018). Modeling SCADA attacks. In Smart Trends in Systems, Security and Sustainability 47-55.

[40] Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), 29.

[41] Yao, Y., Sheng, C., Fu, Q., Liu, H., & Wang, D. (2019). A propagation model with defensive measures for PLC-PC worms in industrial networks. Applied Mathematical Modelling, 69, 696-713.

[42] Spenneberg, R., Brüggemann, M., & Schwartke, H. (2016). Plc-blaster: A worm living solely in the plc. Black Hat Asia, 16, 1-16.

[43] Queiroz, C., Mahmood, A., & Tari, Z. (2011). SCADASim—A framework for building SCADA simulations. IEEE Transactions on Smart Grid, 2(4), 589-597.

[44] Leszczyna, R., Fovino, I. N., & Masera, M. (2010). Simulating malware with MAlSim. Journal in computer virology, 6(1), 65-75.

[45] Genge, B., & Siaterlis, C. (2014). Physical process resilience-aware network design for SCADA systems. Computers & Electrical Engineering, 40(1), 142-157.

[46] Dondossola, G., Garrone, F., & Szanto, J. (2009). Supporting cyber risk assessment of power control systems with experimental data. In IEEE/PES Power Systems Conference and Exposition, 1-3.

[47] Davies, A., Karsai, G., Neems, H., Giani, A., Sinopoli, B., & Chabuksawar, R. (2009). TRUST for SCADA: A simulation-based experimental platform. presentation[online]. Available: https://slideplayer.com/slide/3377726/ [Access date: 9. 12. 2021]

[48] Mo, Y., Chabukswar, R., & Sinopoli, B. (2013). Detecting integrity attacks on SCADA systems. IEEE Transactions on Control Systems Technology, 22(4), 1396-1407.

[49] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436.

[50] Pothamsetty, V., & Franz, M. (2005). Scada honeynet project: Building honeypots for industrial networks. Cisco Systems, Inc. [online] http://scadahoneynet.sourceforge.net/ [Access date: 12. 9. 2021].