DOI: 10.2507/33rd.daaam.proceedings.xxx

INDUSTRIAL CYBER SECURITY ASPECTS IN ICS APPLICATIONS

Mladen Babić, Miloš Stanojević, Gordana Ostojić, Srđan Tegeltija & Stevan Stankovski

This Publication has to be referred as: Babić, M[laden]; Stanojević, M[iloš]; Ostojić, G[ordana];Tegeltija S[rđan]; & Stankovski, S[tevan] (2022). Title of Paper, Proceedings of the 33rd DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/33rd.daaam.proceedings.xxx

Abstract

Regarding already growing technological progress and the new industrial revolution, Industry 4.0, every day there is a bigger need of using security systems in Industrial Control Systems. Using closed or open architectures, which are connected locally or over the Internet, is much more vulnerable in terms of outside or inside attacks in terms of gathering pieces of information or just sabotage. In this paper, we make a survey of possible concepts which are used to eliminate the possibility of cyber-attacks on Industrial Systems. We will also make a classification of CPS Domains, Attacks, Defences, Research-trends, Network-security, Security level implementation, and Computational Strategies.

Keywords: CPS; ICS; Security; Vulnerabilities; Industry 4.0;

1. Introduction

In the last decade, the development of various types of Cyber-Physical Systems (CPS) are growing exponentially which is resulting in their wider application. These systems can be found in daily life as a part of transport systems, oil, gas and electrical energy distribution, medicine, household appliances, and a lot of other systems. Many of these systems are used in processes that are endangering humanity and the environment and at the same time in processes that are improving the quality of life. For all these reasons, these systems are considered critical and they must be resilient to failures and all kinds of attacks which are proven to be very challenging to achieve.

As there is not yet an official definition for Cyber-Physical Systems (CPS), it can be described as a system that is used for monitoring and controlling the outside world. They are considered a new generation of embedded control systems that are interconnected [1]. Also, CPS can be defined as IT systems, integrated into the physical world applications [2]. More and more industries, such as energy, military, auto industry, and medical are starting to depend on and to leverage CPS. CPS can be named differently based on an area of application. One of the most known CPS is Supervisory Control and Data Acquisition (SCADA) systems, which are used for example in Smart Grid and Industrial Control Systems (ICS). In the wide spectrum of systems in which CPS are present, in this paper, the accent will be on Industrial Control Systems

(ICS). This paper contains an analysis of potential attacks on these systems, systems vulnerabilities, threat mitigation, and the proposal for securing these systems.

2. Industrial Control System

The main responsibility of Industrial Control Systems (ICS) is the acquisition, control, and monitoring of several types of industries such as the auto industry, pharmaceutical, nuclear power plants, water systems, sewerage, and many others. ICS is composed of several control units with different capabilities that work together to achieve a common goal. The most used control unit is the Programmable Logic Controller (PLC). PLC is nothing more than a microprocessor designed for continuous operation in difficult working conditions [3]. This controller is connected to the real world through sensors and actuators. Such controllers may have wireless and/or wired communications, depending on the system to be controlled. They can also be connected to desktop computers located in the control center, which serves to monitor and control the entire system. These systems are expected to be resistant to all types of attacks, whether those attacks are external or performed by insiders. Lack of or weak security in ICS systems can lead to catastrophic consequences depending on the area of application. For example, if there was a problem in the security of the ICS used in a nuclear power plant, it would pose a great threat both to the broader and narrower environment. Therefore, ICS are not yet ready to be connected to the Internet [4]. In order to better understand the system and create better protection, it is possible to divide the entire system into three parts: cyber, cyber-physical, and physical [5]. The physical part of the system represents all components that are in direct contact with the real world, such as sensors and actuators. Cyber and cyber-physical parts of the system have no connection with the real world and they represent software, communication as well as monitoring systems. These two mentioned parts of the system share some common functionalities, but the key difference between them is the way of interaction with the physical part of the system. The cyber-physical part communicates directly with the physical part, while the cyber part does not communicate directly. The cyber-physical part is the mediator between the cyber and physical parts. Cyber, cyber-physical and physical parts of ICS are shown in figure 1.

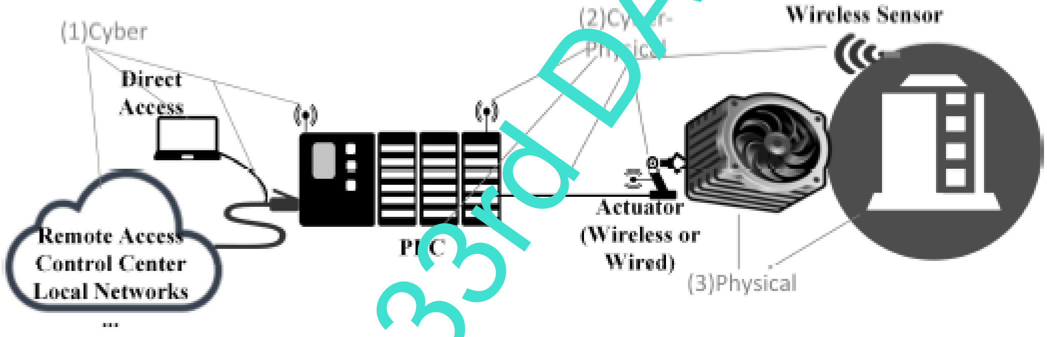

Fig. 1. Possible division of ICS [5]

3. Security threats

In order to create a secure system, first it is necessary to understand potential threats to that system [6]. System is considered safe if it meets the following three requirements: confidentiality, integrity and availability. The first step is to understand what is threat. One of the possible threat definition is that the threat is „a set of circumstances that has the potential to cause loss or harm“[7]. Each threat can have five different factors.

- First is the threat source, it represents the attacker. Attacks can be intentionally performed by an individual or a group of people, they can be accidental, for example through legitimate ICS components, or they can be environmental threats that include natural disasters (floods, earthquakes), disasters caused by humans (fires, explosions) or infrastructure failures (power or telecommunications failure).
- Second factor is the goal that is gained by performing the attack. Targets can be ICS applications and their components or users.
- The third factor is motive. Attackers usually have a number of different motives such as espionage, criminal, terrorism or perhaps political.
- Method of attack is the fourth factor. The attack can be based on one or more of the following four mechanisms: interception, interruption, modification or fabrication [8].
- The fifth factor represents the consequences of a possible attack. Consequences can be for confidentiality, integrity, availability, privacy, or safety.

In most cases, insiders participate in the attacks, because they are fully aware of the system (the source) and have the knowledge to attack the system and harm its normal functioning. Another attack example can be a capable customer who aims to reduce the utility bill by tampering with physical equipment or entering false information to deceive the utility company and thereby cause financial damage. Also, hostile organizations could cause a cyberwar against a nation by remotely attacking critical infrastructures such as nuclear power plants, gas pipelines or other facilities with the help of malware and thus causing power utility shutdowns, sabotage or environmental pollution. Another example of an attack would be to tamper with the data that the sensor measured and sent to the control center.

4. System vulnerabilities

The most frequent method in the last few decades for implementing security in almost all ICS was "security by obscurity". The focus was on creating reliable systems, while security was not so important. The reason for this is that these systems were isolated from the outside world and were therefore considered secure. Perhaps the best example of such systems is the auto industry. ICS is demanding more and more connection to the Internet than ever before and almost every part of today's systems relies on communication technology. For example, an ICS that controls the operation of an industrial utility is connected to a control center that is connected to the internet. Until 2001, most attacks on ICS were from the inside, but with the beginning of the Internet era, attacks started coming from the outside world as well [9]. Also, to speed up data transfer, many field devices are directly connected to the Internet [10], [11], [12], [13], [14], [15], [16], [17] and [18]. System vulnerabilities can also be observed as three types: cyber, cyber-physical, and physical.

4.1. Cyber vulnerabilities

The first area of interest needed investigation for determining cyber vulnerabilities is communication between ICS components. ICS uses standard protocols such as TCP/IP and ICCP. As these protocols are vulnerable, it makes ICS vulnerable. TCP/IP communication, although it has been studied for many years, still has some shortcomings in terms of security [19]. Another protocol used is Remote Procedure Call (RPC), which also has data security problems, which was exploited by the well-known Stuxnet attack. Wired communication in ICS uses fibre-optic and Ethernet. Local networks are usually based on Ethernet and therefore have problems with message interceptions and man-in-the-middle attacks [20]. For example, an inside attacker could tamper messages with false data or reveal confidential information [21] and [22]. Security problems can also occur if the ICS uses short-range wireless communications. If an employee connects his possibly insecure device to the network, there is a possibility to expose the system to threats, so that an attacker can use his device to attack the system through the employee's device. Another area needing investigation when cyber vulnerabilities are the subject is software. One of the most popular attacks is the attack on databases and all the records in them. Databases containing important data can be directly or indirectly connected to ICS servers, which is the reason why this vulnerability exists. Also, emails can be one of the most common ways of attack. Via email, it is possible to send malware that will later spread through the network. In the end, we should pay additional attention to the devices that are connected to the internet as well as to the local network, such as servers in control centers, laptops and mobile phones of employees, through which malware can be inserted into systems [23].

4.2. Cyber-physical vulnerabilities

The area of observation is the connectivity between the cyber and physical components of ICS. The most used communications are Modbus and DNP3 protocols for monitoring and sending commands from the control center to sensors and actuators. As Modbus has shortcomings in terms of data transmission security, it exposes ICS to various types of attacks. Because it has no encryption capability, the system is exposed to espionage [24]. Also due to the lack of data validation, the integrity of the data is questioned [25]. The authenticity of the sent data is not taken into account, so manipulation of the transmitted data can occur on the source. As a consequence, the actuators can receive wrong data which can lead to their misbehavior, or the sensors can send wrong data to the controller [26]. It is similar to the DNP3 protocol, it does not have any mechanized encryption or authentication. Direct access to remote devices such as PLCs used in smart grids can also be problematic. Furthermore, in today's systems more and more PLCs are directly connected to the internet. Another area of vulnerabilities refers to Operating System (OS) vulnerabilities. Applications used to manage and monitor field devices run on a general-purpose OS. If the OS or the specified application has flaws, they can be a potential risk for an attack on field devices. The well-known Stuxnet attack used two flaws in Windows OS, Print Spooler Service and Windows Server Services for the attack. The third and final area for vulnerabilities refers to Software vulnerabilities. Programs running on a general-purpose OS for controlling and monitoring controllers can be an opportunity for attack. Simatic WinCC is an example of such a program, which is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system developed by Siemens. During the Stuxnet attack, the first step was to find a vulnerable computer on which WinCC software is running [27].

4.3. Physical vulnerabilities

Physical exposure of many ICS components is a problem for system security. A soil moisture measurement system can be observed as an example. It can consist of multiple sensors at different locations powered by solar panels so that they can measure the desired values and send the measured values to the control center. If the solar panels are stolen, the sensors no longer have the necessary power and the control center is left without the necessary data.

5. Improvements of security in ICS

One of the main directions in improving ICS security is the improvement of security in communications protocols. Even if protocols are used to connect the system to the Internet or if they are used to connect system hardware locally, some standard protocols are Modbus, DNP3, TCP/IP. The main directions in improving security in ICS communication protocols are: Cyber, Cyber-Physical and Physical.

5.1. Cyber

The best mechanism to prevent attacks is to use an encryption mechanism in all ICS networks. One of the problems with encryption is the delay in data transmission that occurs due to data encryption, which can be a big problem in real-time systems. The delay problem that occurs during data encryption can be solved by using an ICS-specific key management solution [27]. In addition, there are studies that say it is possible to use a layered approach to protect important ICS data [28]. This study is based on Hash Chains to create layered protection by dividing it into two zones: high and low-security zones and a lightweight key management mechanism. Thanks to this division, if an attacker gets full access to the low-security level, he will not be able to access the data that is in the high-security level. The next step in security is the constant improvement of OS security. Windows improved its security after the Stuxnet attack, so that this type of attack is no longer a security threat [29]. In addition to the OS and applications used for management and monitoring, ICS must also follow trends and constantly improve their protection measures. Another type of improvement in security protection is standardisation. By following existing security standards when designing an ICS, it can contribute to a greater degree of security. One of the studies provides guidelines for technical controls such as firewalls, IDS and access control, which can influence the increase of ICS security [30].

5.2. Cyber-Physical

The best solution would be to create a new security solution designed exclusively for ICS. That new solution should take into account both the system's communication with the cyber part and the system's communication with the real world. Until now, the solutions have mainly aimed to ensure the reliable functioning of the solution in case of some unintentional problems [6]. Although reliability is a very important feature, malicious cyber-attacks are more possible today than ever, and must be taken into account when creating new ICS security solutions. It is also necessary to increase the security of communication protocols. Secure Modbus framework is one of the solutions [31]. This method of communication ensures authentication, non-repudiation, and obstructs replayed packets. Another problem is related to remote access to field devices. One solution is that only authorised persons can access remote devices [32]. This could be achieved by using one particular computer and through a VPN.

5.3. Physical

National Institute of Standards and Technology provides a list of defence-in-depth physical controls [30]. Examples of which include the protection of physical access, locations, etc.

6. Conclusion

This paper showed the main problems of security in ICS applications. We presented threats, vulnerabilities and possible improvements separated into the cyber, cyber-physical and physical aspects. For each ICS application, it is mandatory to isolate threats, in the last years the main solution for security in ICS was to isolate the system from the outside world, and not to implement security solutions because it was considered safe from an outside attack. Today, more and more industrial systems are connected to the Internet and they are no more isolated from the outside world, this brings a very big risk of attacks and the possibility to interfere in the system process. There are possible improvements that are proposed as the solution to diminish risk in ICS and they are considered in the cyber, cyber-physical and physical aspects. Cyber aspect solutions should implement an encryption mechanism in all ICS networks. Cyber-Physical aspect solution implements a new security framework for Modbus communication protocol which is used for communication between system hardware, and implements security in terms of authorised remote access using VPN to control the ICS. In physical it is only mentioned that NIST provides standardised solutions for lowering the risk of vulnerabilities of ICS.

With the increasing implementation of Industry 4.0 and IoT, there is a need to connect ICS applications to the outside world and this increases the risk of outside attacks on ICS applications which in many ways are real-time applications that need to be isolated and secured from outside attacks. On basis of described aspects we intend to implement every aspect on existing ICS application, and to validate implemented solutions and gather results on which we will make distinction and show results of which solution is easiest to implement and which solution gives us best protection against outside attacks.

7. Acknowledgment

This research was funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia through project no. 451-03-68/2022-14/200156 and the Provincial Secretariat for Higher Education and Scientific Research of Autonomous Province of Vojvodina, Republic of Serbia, through project no. 142-451-2004/2022-01.

8. References

[1] Amin, S.; Schwartz, G. A. & Hussain, A. (2013). In quest of benchmarking security risks to cyber-physical systems. IEEE Network, 27(1), 19-24.

[2] Amin, S.; Litrico, X.; Sastry, S. S. & Bayen, A. M. (2010, April). Stealthy deception attacks on water SCADA systems. In Proceedings of the 13th ACM international conference on Hybrid systems: computation and control (pp. 161-170).

[3] Anderson, R. & Fuloria, S. (2010, October). Who controls the off switch?. In 2010 First IEEE International Conference on Smart Grid Communications (pp. 96-101). IEEE.

[4] Francia III, G. A., Thornton, D., & Dawson, J. (2012). Security best practices and risk assessment of SCADA and industrial control systems. In Proceedings of the international conference on security and management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[5] Humayed, A.; Lin, J., Li, F. & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802-1831.

[6] Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A. & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (Vol. 5, No. 1).

[7] Ankaralı, Z. E.; Demir, A. F.; Qaraqe, M.; Abbasi, Q. H.; Serpedin, E.; Arslan, H. & Gitlin, R. D. (2015, September). Physical layer security for wireless implantable medical devices. In 2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD) (pp. 144-147). IEEE.

[8] Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A. & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (Vol. 5, No. 1).

[9] Byres, E. & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In Proceedings of the VDE Kongress (Vol. 116, pp. 213-218).

[10] Leverett, É. & Wightman, R. (2013, November). Vulnerability inheritance programmable logic controllers. In Proceedings of the Second International Symposium on Research in Grey-Hat Hacking. GreHack 2013 Grenoble, France.

[11] Slay, J., & Miller, M. (2007, March). Lessons learned from the Maroochy water breach. In International conference on critical infrastructure protection (pp. 73-82). Springer, Boston, MA.

[12] Stankovski, S., Ostojic, G., Baranovski, I., Babić, M.& Stanojević, M. (2020). The Impact of Edge Computing on Industrial Automation, 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2020, pp. 1-4.

[13] Klašnja, N.; Sremčev, N.; Vukelić, Đ.; Simeunović, N. & Lazarević, M. (2019). Optimization of Cable Harness AssemblySystems Based on Lean Concept Application. International Journal of Industrial Engineering and Management, 10(1), 115.

[14] Anišić, Z.; Veža, I.; Suzić, N.; Sremčev, N. & Orčik, A. (2013). Improving product design with ips-dfx methodology incorporated in PLM software. Tehnicki vjesnik/Technical Gazette, 20(1).

[15] Ostojic, G., Lazarevic, M., Stankovski, S., Cosic, I. & Radosavljavic, Z. (2008). Radio frequency identification technology application in disassembly systems, Strojniski Vestnik/Journal of Mechanical Engineering, 54 (11), 759-767.

[16] Tegeltija, S.., Lazarević, M., Stankovski, S., Ćosić, I., Todorović, V. & Ostojić, G. (2016). Heating circulation pump disassembly process improved with augmented reality, Thermal Science, 20, 611-622.

[17] Stankovski, S., Ostojić, G., Šaponjić, M., Stanojević, M.& Babić, M., (2020). Using micro/mini PLC/PAC in the Edge Computing Architecture, 19th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2020, 1-4.

[18] Ostojic, G., Stankovski, S., Vukelic, D., Lazarevic, M., Hodolic, J., Tadic, B. & Odri, S. (2011). Implementation of automatic identification technology in a process of fixture assembly/disassembly, Strojniski Vestnik/Journal of Mechanical Engineering, 57 (11), 819-825.

[19] Harris, B. & Hunt, R. (1999). TCP/IP security threats and attack methods. Computer communications, 22(10), 885-897.

[20] Francia III, G.; Thornton, D. & Brookshire, T. (2012, June). Cyberattacks on SCADA systems. In Proc. 16th Colloquium Inf. Syst. Security Educ (pp. 9-14).

[21] Paukatong, T. (2005, August). SCADA security: A new concerning issue of an in-house EGAT SCADA. In 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific (pp. 1-5). IEEE.

[22] Wang, W. & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. Computer networks, 57(5), 1344-1371.

[23] Cardenas, A. A.; Roosta, T. & Sastry, S. (2009). Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. Ad Hoc Networks, 7(8), 1434-1447.

[24] Alcaraz, C. & Zeadally, S. (2013). Critical control system protection in the 21st century. Computer, 46(10), 74-83.

[25] Fovino, I. N.; Carcano, A.; Masera, M. & Trombetta, A. (2009). An experimental investigation of malware attacks on SCADA systems. International Journal of Critical Infrastructure Protection, 2(4), 139-145.

[26] Zhu, B.; Joseph, A. & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing (pp. 380-388). IEEE.

[27] Chen, T. M.,& Abu-Nimeh, S. (2011). Lessons from stuxnet. Computer, 44(4), 91-93.

[28] Choi, D.; Kim, H.; Won, D. & Kim, S. (2009). Advanced key management architecture for secure SCADA communications. IEEE transactions on Power delivery, 24(3), 1154-1163.

[29] Cao, H.; Zhu, P.; Lu, X. & Gurtov, A. (2013). A layered encryption mechanism for networked critical infrastructures. IEEE Network, 27(1), 12-18.

[30] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

[31] Fovino, I. N.; Carcano, A.; Masera, M. & Trombetta, A. (2009, March). Design and implementation of a secure modbus protocol. In International conference on critical infrastructure protection (pp. 83-96). Springer, Berlin, Heidelberg.

[32] Fernandez, J. D. & Fernandez, A. E. (2005). SCADA systems: vulnerabilities and remediation. Journal of Computing Sciences in Colleges, 20(4), 160-168.