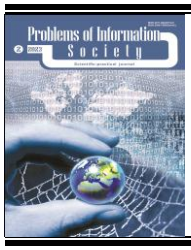

www.jpis.az

14 (2)
2023

Cybersecurity analysis of industrial control systems

Ramiz H. Shikhaliyev

Institute of Information Technology, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

ramiz@science.az

orcid.org/0000-0002-8594-6721

ARTICLE INFO

http://doi.org/10.25045/jpis.v14.i2.06

Article history:
Received 8 February 2023
Received in revised form
11 Aprel 2023
Accepted 13 June 2023

Keywords:
Industrial control systems
Cybersecurity
Vulnerabilities
Threats
Cybersecurity measures and means

ABSTRACT

The current frontiers in the description and simulation of advanced physical and biological Industrial control systems (ICS) used to control various critical industrial and social systems. ICS integrates modern computing, communication, and Internet technologies. The integration of these technologies makes ICS open to the outside world, which makes it vulnerable to various cyber-attacks. ICS's cybersecurity is becoming one of the most important issues due to the significant damage caused by cyberattacks to organizations and society. This article analyzes the cybersecurity issues of ICS. In particular, an analysis of the main components and architectures of the ICS, security aspects of the ICS, vulnerabilities, and threats to the cybersecurity of the ICS, as well as measures and means to ensure the cybersecurity of the ICS, is carried out. The analysis will help to give some insight into the cybersecurity issues of ICS and identify various research objectives necessary to ensure the cybersecurity of ICS.

1. Introduction

Industrial control systems are of great importance for the management of critical infrastructures. ICS is a set of interconnected subsystems. There are various types of ICS, such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and other systems that perform control functions (Mehta and Reddy, 2015). Typically, the ICS collects data from the sensors and the operating data of technological processes, and analyzes it, and then display them. ICS differs from traditional information management systems in that they control physical objects.

Traditionally, ICS is physically isolated from the external environment and based on special equipment, software, and communication protocols, while cybersecurity issues are not taken into account. ICS was developed taking into account reliability and security, which consisted of the physical protection of access to the network and consoles of the control system (Russel, 2015). This approach has led to problems in ensuring the cybersecurity of ICS. Because ICS integrates computing, communication, and Internet technologies to provide their mobility and scalability. ICS is becoming more and more open due to the use of public communication networks for data transmission, such as the Internet, which allows the implementation of remote access tools. These allow users to respond to emergencies on ICS remotely, as well as remotely maintain and monitor ICS. In ICS, commercial equipment, operating systems, and Internet protocol stacks are increasingly used. Therefore, ICS becomes public and vulnerable to new types of cyber threats, and the likelihood of critical cybersecurity issues increases. At the same time, cyberattacks on ICS may create significant risks to human health and life, as well as cause serious damage to production, national economy and environment.

The aim of this article is to analyze the cybersecurity of ICS. To achieve this goal, several research areas are identified, for example, an analysis of the main components and architectures of ICS, security aspects of ICS, various vulnerabilities and threats to ICS, and measures and tools for ensuring the cybersecurity of ICS. The

analysis carried out will help to give some idea of the problems and take measures to improve the cybersecurity of ICS, as well as determine the objectives of future research on the cybersecurity of ICS.

2. ICS's components and architectures

For an effective analysis of the cybersecurity of ICS, it is necessary to consider the main components and architectures used in ICS. These components are used in both SCADA and DCS architectures. Moreover, depending on the functional purpose of ICS, the components can interact in different ways. Several standard architectures are defined by standardization organizations such as ISA (International Society of Automation: www.ISA.org), NERC (North American Electric Reliability Corporation: http://www.nerc.com), AGA (American Gas Association : www.AGA.org), etc. These architectures describe the different layers of the system in terms of network and operations.

Typical ICSs contain multiple control loops, user interfaces, and remote diagnostic and maintenance tools. To create them, protocols of a multilayer network architecture are used. The user interfaces are applied for monitoring and set points setting, control algorithms, and controller parameters setting. The user interfaces may include clients of SCADA servers or directly connected to the control network and display process status information. Remote diagnostic and maintenance tools are used to detect, prevent, and recover from failures.

The control loop uses sensors, actuators, and controllers (such as PLC, - programmable logic controller) to control certain controlled processes. To configure the PLC - the control server, which is software, is used. PLCs are capable of managing complex processes in both DCS and SCADA systems. PLCs are capable of solving complex logic to control process functions and communications generated by the control server. In most cases, PLCs are connected to lower-level devices, such as sensors and actuators.

The management server hosts all control logic and device network configuration applications. In addition, the management server hosts some real-time monitoring services. Typically, the management server is connected directly to the management devices through the management network. The SCADA system uses a SCADA server, which is a central device, to perform the monitoring, control, and object data model functions for process assets.

Modern sensors and actuators are smart enough to collect data and transmit it to PLCs and monitoring services. Sensors and actuators interact with the field side of the process, where analog communications are required for data acquisition and local control.

The ICS can be hierarchically divided into different network levels such as the corporate network, the control network, and the field network. SCADA components interact at different levels and are interconnected through network components, depending on the context of use and regardless of the topology. The support of IT protocol management components enables IT network components to be customized to meet SCADA requirements such as availability, and performance remotely. The control network connects the upper layer (dispatching control, control server, and monitoring services) with controllers and remote terminals. The field network connects sensors, actuators, and other devices to PLCs or other controllers. The use of a dedicated network for these devices avoids the direct connection of sensors and other devices to the PLCs. Furthermore, various communication protocols are used for establishing connections between controllers and devices, as well as between the devices themselves.

The SCADA system may have a different architecture, which depends on the control object. However, a typical SCADA system architecture consists of three main parts, such as the control center, field sites, and network environment (Figure 1) (Byres et al., 2004).

The control center is used to collect, maintain, and monitor the control object and controls the sending of instructions by the SCADA system to all peripheral devices. The control server hosts the DCS or PLC dispatching control software, which communicates with the control devices of the lower level of the APCS network. The SCADA server monitors and manages remote terminal devices and PLCs located at remote field sites. The human-machine interface is software and hardware that allows operators to monitor the status of the controlled process, change the target by changing control settings, and manually override automatic control operations in emergencies. The Data Historian is a centralized database for auditing all SCADA process information. The stored information is used for various analyses and process control statistics needed for corporate-level planning. The I/O server is used to collect, buffer, and provide access from control subcomponents, such as PLCs, etc., to process information. In Figure 1 is shown typical SCADA system architecture (Byres et al., 2004).

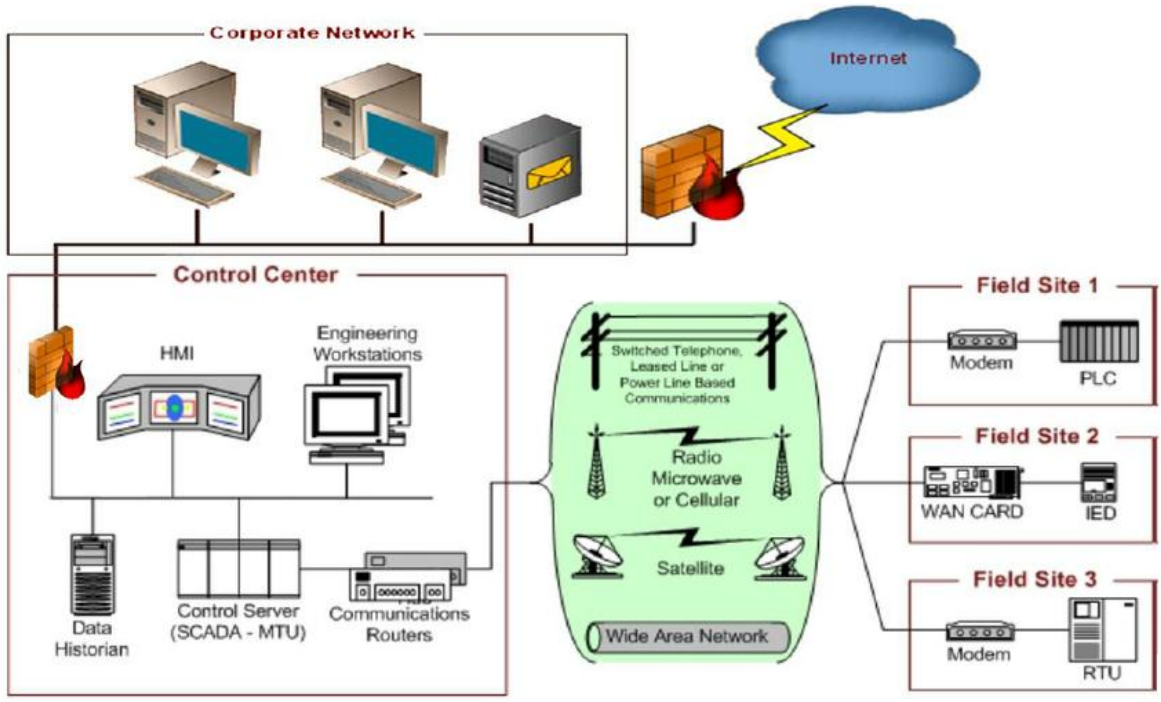

Fig. 1. Typical SCADA system architecture

Field side components are used to monitor field devices, receive instructions from master stations, and control field devices that are directly connected to them. The remote terminal unit (RTU) is designed to support remote SCADA stations. If it is impossible to use wired communication, RUTs are connected using wireless interfaces. The PLC is designed to perform the logic functions previously performed by electrical equipment such as switches, relays, and mechanical timers/counters. In the SCADA system, PLCs are often used as field devices as they are more costeffective, versatile, and flexible than RTUs. Intelligent electronic devices (IEDs) may be intelligent sensors/actuators that have the intelligence necessary to communicate with other data acquisition devices and perform local processing and control.

The network environment is responsible for connecting all field devices to the SCADA system control center and connecting the SCADA control network to the corporate control network. The field network links sensors and other devices to PLCs and other controllers. The messages transferred between the sensors and the controller are uniquely identified for each of the sensors. The control network connects the dispatching control level to the lower-level control devices. Routers relay messages between two networks. They are used to connect the local network to the global network, as well as to connect SCADA servers and RTUs via a long-distance network. Firewalls protect network devices by monitoring and controlling communication packets according to predefined filtering policies. They enable different strategies for separating the SCADA control network. Modems convert digital data into an analog signal for transmission over a telephone line to enable communication between devices. Remote access points are used to remotely access and set up a SCADA system control network in locations where wired communication is not available.

DCS is used to monitor and control physical systems in real time within a specific geographic location. A typical DCS architecture is shown in Figure 2 (Stouffer et al, 2007). It consists of devices and network segments distributed over different levels, namely the control level, intermediate control level, and field level. At the dispatching level, system operators use human machine interface (HMI) applications to send requests over the management network to management servers. These requests require the receiving device to provide process data or propagate process set points to lower levels.

The control server, in turn, requests process data or sends process set points to subordinate control servers at intermediate control levels. Control servers in the lower intermediate layer poll data or send process set point to edge control systems, i.e., field level devices such as PLCs that receive input from sensors and send output by generating electrical signals to control actuators. The edge control system can communicate with digital sensors or actuators over a network called a field bus. In Figure 2 is shown typical DCS architecture (Stouffer et al, 2007).

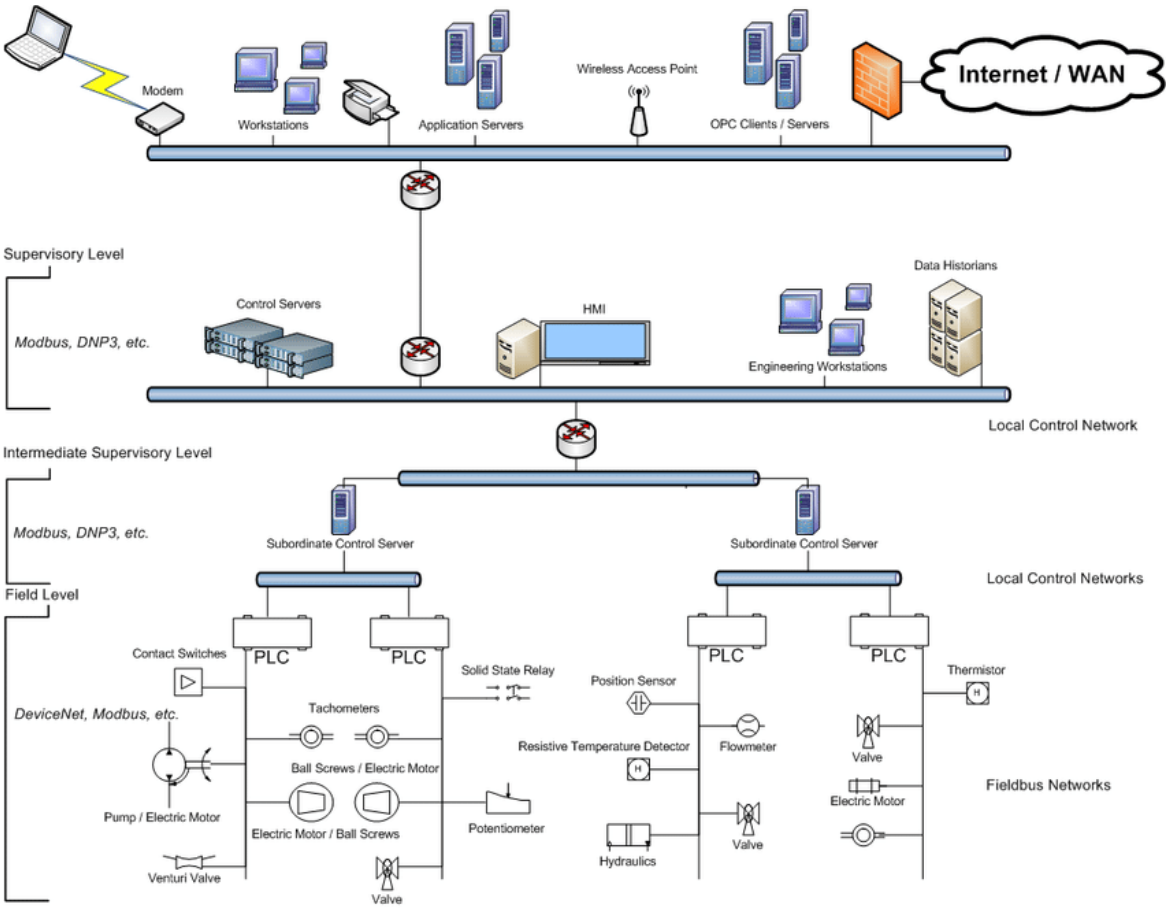

Fig. 2. Typical DCS architecture

Control networks communicate using protocols, such as ModBus (ModbusIDA Website), Fieldbus (Berge, 2002), Distributed Network Protocol version 3 (DNP3) (DNP Users Group, 2007), etc., while field bus communication is implemented using protocols such as DeviceNet (https://www.elprocus.com/devicenet-architecture) or ModBus.

3. ICS security aspects

To ensure the cybersecurity of ICS, that is, to determine any security mechanisms or countermeasures against cyber-attacks, it is important to understand the security aspects and requirements of ICS. The NIST working group issued a guide on ensuring the safety of ICSs, (Stoufler, et al., 2014), from which three main aspects of the safety of ICSs can be distinguished.

Availability means that the products and services provided meet customer or regulatory requirements. In the context of high performance, any deterioration in availability leads directly to financial losses and dissatisfied customers. Real-time access to data assets is paramount to managing system operations. System availability requirements are also an important design factor. The unavailability of system assets or the interruption of control operations leads to the loss of the functions of the object. In the case of critical infrastructure, this leads to economic and human damage. Therefore, some ICSs use redundant components running in parallel to provide continuity when the main components are unavailable.

Integrity refers to ensuring unauthorized changes to data to be made. To guarantee data integrity, it is necessary to be able to detect unauthorized data manipulation. Security measures must be implemented in such a way as to maintain the integrity of the system during normal operation, as well as during cyberattacks. Integrity is a very important aspect of ICS, where false actions are possible due to changed data. Integrity concerns all components of the ICS, such as PLC programs, data sharing, and SCADA software databases.

Confidentiality refers to the concealment of the content of information from those who do not have the right to receive it. Confidentiality in control systems means keeping sensitive process data inaccessible to unauthorized users and assets. ICSs contain sensitive parameters and data, such as production formulas, the system plans, maintenance

plans, PLC programs, device address lists, etc. They can be used by competitors or malicious groups for targeted attacks or simply to collect company data.

In SCADA, the availability and integrity are given higher priority for security rather than the confidentiality. However, with the development of PCS and its becoming part of the global Internet of Things, PCS assets are increasingly interacting with a human user to manage personal data, and in this case, privacy becomes a critical goal.

4. ICS cybersecurity vulnerabilities and threats

Today, in connection with the introduction of IT technologies into ICS, they have become an object of cybersecurity. SCADA cybersecurity vulnerabilities can have multiple sources. This is due to the growing need to consolidate company data and access it remotely in real-time. Remote maintenance is currently carried out on common platforms based on IT technologies. Connecting through standard IT technologies exposes ICSs to vulnerabilities they are unable to defend against. The exploitation of these vulnerabilities can lead to denial of service, unauthorized process control, breach of integrity and confidentiality, loss of reputation, and so forth.

Since ICSs are segmented on a large scale into different levels of networks, it is almost impossible to guarantee the invulnerability of network nodes to cyberattacks. Specifically, in the case of SCADA systems, where data sharing is performed in a geographically distributed, large-scale infrastructure. APCS protocols are not resistant to incorrect communication packets, therefore, connections between ICSs networks and the outside world significantly increase the likelihood of cyber-attacks, leading to ICSs failure. At the same time, cybersecurity threats are also associated with an increase in the number of attacks on ICSs due to the adoption of Internet technologies.

Today, Ethernet networks are widely used in ICSs as field buses. They are used as a common network infrastructure and enable the use of IP layers. Additionally, the source of vulnerabilities is the convergence of ICS protocols for working in IP networks. Vulnerabilities in the design and implementation of ICS networks and communication protocols can lead to privacy attacks that aim to obtain unauthorized ICS data. Besides, the received data, such as passwords, PLC configurations, can be used to reproduce some of the SCADA operations. Availability threats may be caused by denial of service (DoS), and integrity threats may be caused by manipulation, masquerade, etc. (Conpot—ICS/SCADA Honeypot, http://conpot.org/).

In traditional information management systems, vulnerabilities can be fixed regularly by applying patches published by software developers. However, in the ICS, due to availability and security limitations, it is not possible to take such protective measures. This difference in the ability to respond to vulnerabilities is one of the main risks of ICSs. Insufficient user training and a lack of awareness of cybersecurity risks can represent another significant vulnerability.

ICSs are vulnerable to malware that can be used by attackers intentionally, and can also inadvertently enter the ICS through other infected systems or devices. In any case, the damage and impact on organizations and society due to the failure of processes controlled by ICS can be significant.

A threat is any circumstance or event that can adversely affect an organization's operations (including mission, function, image, or reputation), organization assets, individuals, other organizations, or the nation via an information system through unauthorized access, destruction, disclosure, alteration of information, and/or denial of service (Spitzner, 2003). When considering cybersecurity, threats from the adversary must be taken into account, for example, the adversary can snoop on network traffic to obtain sensitive information for further use. SCADA cybersecurity threats can come from multiple sources, such as hostile countries, terrorist groups, competitors, contractors, and disgruntled employees. In addition, the threats of human error, malfunctions, and failures of equipment and networks must be taken into account. These threats and threat actors can be classified as external or internal.

External threat actors include foreign intelligence services, hackers, industrial spies, cyberterrorists, and organized crime. These actors, for political or economic reasons, may carry out attacks for information gathering, espionage activities, or to disrupt technological processes.

Internal threats include network and operational problems, disgruntled employees, and careless or poorly trained staff. Internal threats are no less dangerous than external ones because some of these threats are beyond the organization's control, such as network and hardware misconfigurations.

Social engineering threats and insider threats tend to be ignored compared to typical security

threats. Social engineering is a technique used to manipulate people into giving away personal information such as passwords (Spitzner, 2003). With the help of social engineering threats, hackers can collect the necessary information about the location of devices, and types of controllers, and track them in more depth.

One of the dangerous cyber threats of SCADA is that factory default passwords are built into the hardware and software. Security options are disabled by default, meaning there is no way to change these passwords during the installation of SCADA components. Thus, the installation of components in the ICS is unsafe and security risks arise. For example, the Stuxnet worm abused such a strong password in the Siemens WinCC SCADA product that controlled uranium enrichment centrifuges in Natanz (Nicolas, 2011). Another threat is that authentication information, including passwords, is often unencrypted and can be discovered by cyber attackers in plain text in memory or intercepted from messages. Improper management of the security policy, including the daily behavior of employees, also poses a threat to the security of ICS.

The NIST 800-82 Security Guide for ICSs (Stoufler, et al., 2014) discusses the main threats and vulnerabilities. The document also provides security countermeasures to mitigate the risk associated with process control vulnerabilities and threats.

5. ICS cybersecurity measures and means

To ensure the cybersecurity of ICS, various measures and tools are used, including various security guidelines and standards, intrusion detection and prevention systems, firewalls, cryptographic algorithms, monitoring systems, risk analysis systems, incident analysis systems, authentication, authorization, and integrity management systems.

The IEC 62443 standard is officially called ISA99 industrial automation and control systems security, which is a guiding document for the application of IT security in ICSs, including hardware and software systems such as SCADA, DCS, PLCs, HMIs, and network sensors and devices. IEC 62443 has four main categories of requirements, such as general requirements, policy and procedure requirements, system requirements, and component requirements. IEC 62443 introduces Security Assurance Levels (SALs) for ICSs and the specific security controls that need to be implemented for each SAL (https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu). Security levels are assessed for each functional area. Moreover, seven functional requirements are used, for example, control of identification and authentication, control of use, data integrity, data confidentiality, limited data flow, timely response to an event, and availability of resources.

IEC 62351 is an eleven-part power system management security standard that covers all security aspects of power system communications. The first and second parts are technical specifications that address security issues in power management systems. The fourth, fifth, and sixth parts are published as technical specifications on how to implement security in power management communication protocols such as MMS, IEC61850 over TCP/IP. In addition to the security standard for communication protocols, the remaining parts of the IEC 62351 standard beginning from seven to eleven cover security policies, access control mechanisms, key management, audit trails, and other important infrastructure security issues (Line et al., 2011).

The US National Security Agency Center for System and Network Analysis published a guide in 2010 entitled "Framework for Assessing and Improving the Security Posture of Industrial Control Systems." This guide proposes a cost-benefit analysis approach to prioritizing safeguards by identifying network security improvements that provide the greatest benefit for a given cost. The process of assessing the potential damage incurred as a result of the compromise of network assets of ICSs or network channels is considered. Once a prioritization list has been created, a cost-effective risk management approach can be applied to address system vulnerabilities.

The National Institute of Standards and Technology (NIST) has initiated a project on the safety of ICSs using NIST SP8053 (Katzke et al., 2006). The goal of this project is to apply the Federal Information Processing Standards (FIPS) (National Institute for Standards and Technology, FIPS 199, 2004, National Institute for Standards and Technology, FIPS 200, 2006) to ICSs as part of federal systems. FIPS 199 and FIPS 200 for federal systems define security measures such as access control, awareness and education, audit and accountability, security assessment, configuration management, identification and authentication, and incident response. These requirements are introduced in a special publication of the NIST standard 800-82 (Stoufler, et al., 2014) on the safety of ICSs.

Ensuring the security aspects of the ICS, which were discussed above, can be implemented using cryptographic algorithms. To do this, it is necessary to introduce cryptographic algorithms into the structure of the ICS, which allow ensuring the integrity and confidentiality of data, message authentication, and non-repudiation of actions performed in the control system. However, the use of cryptographic measures in an ICS environment can be very costly in terms of resource consumption. In addition, problems in the application of cryptographic methods in ICSs are associated with the storage, distribution, and updating of cryptographic data embedded in the components of the control system. Therefore, the management of cryptographic keys is a priority for cryptographic systems in ICSs. A key management system is a set of operations that includes key generation, randomization, secure storage with restricted access for unauthorized persons, key distribution, key renewal, and key binding to an encrypted message (Lee et al., 2008).

Organizations can mitigate threats and reduce risk to the production environment by implementing a comprehensive monitoring infrastructure for the process control network. With an effective monitoring infrastructure in place, organizations can not only detect problems earlier but also mitigate the consequences before any real damage occurs and recover faster from an incident, regardless of its nature. However, before implementing any monitoring infrastructure or even considering a specific solution, organizations should assess the risk and threat exposure of their network and devices.

Many monitoring proposals have focused on revising enterprise solutions such as intrusion detection systems (IDS) for ICS/SCADA environments (Zhu et al., 2010). Since SCADA uses specialized protocols such as DNP3 and Modbus for real-time operation and reliability, traditional IDS and IPS do not meet the need for monitoring malicious events in SCADA. Therefore, discovery rules and monitoring mechanisms have been created specifically for SCADA systems and networks, taking into account the specification of communication protocols. The new rules and mechanisms are mainly based on attack signatures, anomaly detection, probabilistic models, system specifications, and the behavior of ICSs' components (Cheung et al., 2007). A lot of research has been done in this area to tune IDS/IPS. For ICSs, the focus is on defining discovery models based on protocol specifications (Wojciech, 2013, Niv and et al., 2013). A problem with implementing such techniques in SCADA is the difficulty in managing the distribution of IDS/IPS agents across all system components and networks in a large-scale system without compromising system performance. Another problem with implementing IDS/IPS in ICS has to do with the post-detection response. Generally, when an intrusion attempt is detected, the target system is shut down and restarted in safe mode by reconfiguring the attacked parts. However, such responses cannot be applied to ICS, since it can be used by an attacker to shut down a process as a response to a false positive intrusion.

6. Conclusion

Today, ICSs are widely used in the management of critical systems. The ICS integrates modern computing, communication, and Internet technologies. The use of these technologies in ICSs makes them vulnerable to cyberattacks. Therefore, ensuring the cyber hazard of the ICS becomes a very urgent task. The solution to this problem involves analyzing the cybersecurity of the ICS.

This article was devoted to the analysis of cybersecurity issues of ICS, in particular, various components and architectures of the ICS, security aspects of the ICS, vulnerabilities, and threats to the cybersecurity of the ICS, as well as measures and means to ensure the cybersecurity of the ICS. To effectively analyze the cybersecurity of an ICS, it is necessary to have a good understanding of the functions of the main components of the ICS, as well as the architecture of the ICS. These components are used in SCADA and DCS architectures. At the same time, depending on the functional purpose of the ICS, the components interact differently. Analyzing the cybersecurity of the ICS will help take preliminary measures to improve their cybersecurity.

Acknowledgments

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA).

References

American Gas Association : www.AGA.org

ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels, https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu

Berge J., Fieldbuses for Process Control: Engineering, Operation, and Maintenance. ISA, 2002, 468 p.

Byres, E. J., Franz M., and Miller D. (2004) The Use ofAttack Trees in Assessing Vulnerabilities in SCADASystems, International Infrastructure Survivability Workshop (IISW'04), IEEE, Vol. 4, 2004.

Cheung, S, et al. (2007). Using model-based intrusion detection for SCADA networks. Proceedings of the SCADA security scientific symposium. Vol. 46. 2007.

Conpot—ICS/SCADA Honeypot, http://conpot.org/

DeviceNet: Architecture, Message Format, Error Codes, Working & Its Applications, https://www.elprocus.com/devicenet-architecture

DNP Users Group. Distributed Network Protocol Specification. 2007.

International Society of Automation: www.ISA.org

Katzke, S. and Stouffer K. (2006). Applying NIST SP 800-53 to Industrial Control Systems, ISO EXPO

Lee, S., Choi, D., Park, C., and Kim,S. (2008). An Efficient Key Management Scheme for Secure SCADA Communication, World Academy of Science, Engineering and Technology, vol. 45, 2008.

Line, M. B., Tondel, I. A. and Jaatun, M. G. (2011). Cyber security challenges in Smart Grids, in Innovative Smart Grid Technologies (ISGT Europe), 2nd IEEE PES International Conference and Exhibition on, pp. 1-8.

Mehta B.R., Reddy Y.J. (2015). Industrial Process Automation Systems, 657 p., https://doi.org/10.1016/C2013-0-18954-4

Minimum Security Requirements for Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 200, March 2006. Framework for Improving Critical Infrastructure Cybersecurity. NIST February 2014.

Modbus Organization. Modbus Application Protocol Specification. ModbusIDA Website.

Nicolas, F., Murchu, L. O. (2011). W32.Stuxnet Dossier. Cupertino, CA, USA: Symantec.

Niv, G., and Wool, A. (2013). Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. International Journal of Critical Infrastructure Protection 6(2): 63-75.

North American Electric Reliability Corporation: http://www.nerc.com

Russel, J. (2015). A brief history of SCADA/EMS., http://scadahistory.com/

Spitzner, L. (2003). Honeypots: Catching the insider threat. In: The 19th Annual Conference on Computer Security Application (ACSAC). pp. 304–313.

Standards for Security Categorization of Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 199, February 2004.

Stouffer, K., Falco, J., and Scarfone, K. (2007) Guide to Industrial Control Systems Security.

Stoufler, K., Lightman, S. and Abrams, M. (2014). Guide to industrial control systems Security NIST special publication 80082.

Wojciech, T. (2013). Native support for Modbus RTU protocol in Snort intrusion detection system." New Results in Dependability & Comput. Syst. AISC 224 (2013): 479-487.

Zhu, B., and Sastry, S. (2010). SCADA—Specific intrusion detection/prevention systems: A survey and taxonomy. In Proceedings of the 1st Workshop on Secure Control Systems (SCS), Stockholm, Sweden, 12 April 2010.