Introducing the Profession of Cybersecurity Specialist for Automated Command-and-control Systems

Ella Magdalena CIUPERCĂ, Alexandru STANCIU
National Institute for Research and Development in Informatics - ICI Bucharest
ella.ciuperca@ici.ro, alexandru.stanciu@ici.ro

Abstract: Currently, our society is experiencing an acute need to ensure the security of critical infrastructures with respect to cyber incidents that can disrupt their normal operation and thus create major socio-economic turmoil and financial loss. Industrial control systems have become the main target for coordinated cybersecurity attacks, and the number of threats has increased with the complexity of the new technologies. Cybersecurity requires both advanced technological solutions and human skills to effectively prevent known threats but also be efficient against unknown vulnerabilities. Consequently, there is a need to train and recognize the professionals that perform cybersecurity activities in order to protect critical infrastructures. This paper presents the introduction of the profession of cybersecurity specialist for automated command-and-control systems in the Romanian Classification of Occupations.

Keywords: cybersecurity, critical infrastructures, industrial control system, SCADA, cybersecurity specialist.

INTRODUCTION

Every day, we are exposed, consciously or not, to threats originating from cyberspace. The number of cyber threats has increased with the complexity of new technologies. They involve new risks that can have a serious impact on an industrial control system (ICS) or process, with a multitude of hostile actions such as maliciously disrupting an information infrastructure, stealing restricted information, and many others.

It is recognized that critical infrastructures have always been the most sensitive, vulnerable area of any system or process. Therefore, no matter how well they are protected, they will always have a degree of vulnerability, usually being the first to be targeted when the aim is to destabilize or even destroy a system or process (Alexandrescu & Vaduva, 2006).

Cybersecurity incidents targeting ICS have become increasingly severe over time,

https://doi.org/10.54851/v4i2y202201

demonstrating the dynamic nature of threats to industrial systems. Attacks have also evolved until cyber threats have become increasingly difficult to detect and extremely persistent. Industrial networks are vital components within industrial control systems, and as such, in the event of a successful cyber incident, the consequences can be devastating.

OVERVIEW OF INDUSTRIAL CONTROL SYSTEMS

Industrial control system is a general term now used in the technical field to designate a collection of individual control or supervisory systems and other hardware equipment that work together to automate or operate industrial processes. The aim of ICS is to make day-to-day operations more efficient and autonomous, with minimal input from human workers. In each industrial field, such as manufacturing, chemical processing or food production, the ICS is tailored and configured for the specific processes of that field. An ICS is composed of various electrical, mechanical or hydraulic components that work together in order to manage an industrial process. The command-and-control part of the system may be fully automated or may include a human in the control loop.

An industrial control system might include a variety of components such as programmable logic controllers (PLCs), remote terminal devices (RTUs), intelligent electronic devices (IEDs), process safety systems (PSSs), and could be implemented as a distributed control system (DCS), industrial automation and control system (IACS) or supervisory control and data acquisition (SCADA) system.

The communication protocols are used in real-time for data transfers and are developed to interconnect the systems, interfaces, and instruments that make up the industrial control system. A number of protocols were developed to communicate over RS-232/485 interfaces at low speeds of 9.6 kbps to 38.4 kbps, but over time they have evolved to operate over Ethernet networks using TCP and UDP protocols.

The performance of the task (process) is controlled by a software application running inside the controller. The local view panel or human-machine interface (HMI) device allows the operator to view process values and modify how the controllers operate. ICSs may include software components for managing the processing logic, as well as graphical user interfaces (GUIs) for human operators that are implemented on the HMI. The execution of the control task is recorded in a database called History (E. D. Knapp & Langill, 2014).

ICS can be configured to operate in open-loop, closed-loop and manual modes (Stouffer et al., 2015). The difference between open-loop and closed-loop systems is that whereas in open-loop control systems the output is determined by preset settings, in closed-loop systems, the output acts on the input in order to maintain the desired target. In the manual mode, the operator exerts complete control over the system. In general, an ICS is composed of several control loops in which a controller (or regulator) is responsible for maintaining compliance with the process specifications, human-machine interfaces (HMIs) and maintenance and diagnostic tools using various network protocols.

ICS are used predominantly in utility industries (electricity, water and wastewater, oil and gas), as well as chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace and durable goods) and transportation facilities.

The first generation of ICSs was implemented with basic equipment with analytical electronics and programmable logic controllers (PLCs), thus it included simple supervisory control and data acquisition (SCADA) systems. However, as the technology advanced in the 1990s and 2000s with high performing microprocessors and programmable integrated circuits, and with ever-increasing computing and storage power, more advanced control systems begun to be implemented in various industries, including manufacturing, transport, oil and gas, water and smart grids. In these computerized control systems, the controlled objects are managed by a specialized supervisor component, which includes both hardware and software components in a unified system (Zhang, 2010).

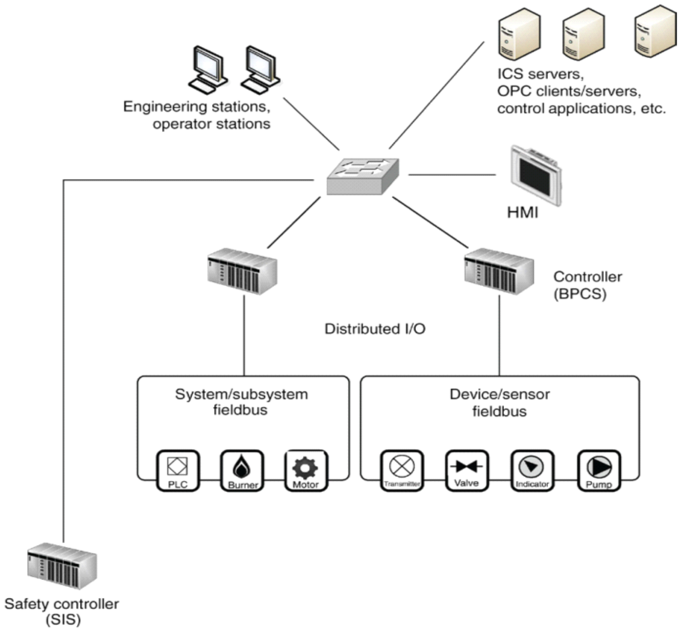

Fig. 1: *Example of an ICS (Knapp & Langill, 2014)*

THE NEED FOR CYBER SECURITY ON AUTOMATED CONTROL SYSTEMS

Cyberattacks are designed to be as difficult to detect as possible or even impossible and use unknown vulnerabilities that cannot be protected against. Well-known examples of this are Stuxnet and Flame, both of which have been carried out over long periods of time without being detected, although their payloads were designed for different purposes: Stuxnet was designed to induce irreparable failures in centrifuges for obtaining enriched uranium, while Flame was designed to collect security information to enable subsequent cyberattacks.

The security of industrial networks can be disrupted by the deliberate intervention of an individual or organization, by a specific act of cyber governance, it can be the side effect of a computer virus that just happened to spread from a business network to an ICS server, the deliberate sequence of a faulty network card, or the result of random circumstances, but unfortunately combined to generate disruptive effects.

Thus, cybersecurity activities require both human skills and advanced technological solutions. Tools that facilitate automated anomaly detection and graphical monitoring of system parameters are needed to effectively prevent known threats but also to provide some degree of security and protection against an unknown vulnerability.

There is a distinct difference between industrial networks and enterprise networks, which may require specific skills and techniques for an attacker. Although an attack on an industrial network is theoretically a simple task, nevertheless it requires specialized knowledge and more resources to be made available to the attacker. Obviously, an attack on industrial networks does not always bring a major direct benefit as an attack on a financial services or sales network. But despite this, attackers still exist and could be differentiated into several classes. For instance, The US Government Accountability Office (GAO) has identified the following classes. (Stouffer et al., 2008):

- Hackers who are interested in individual recognition of their skills and prestige;
- Spammers and botnet operators who may have the same motivation as hackers

but usually are more interested in lucrative exploits;
- Criminal groups seeking to obtain money, using ransom or theft;
- Phishers using identity theft;
- Malware and spyware authors;
- Intelligence services that target critical infrastructures;
- Industrial spies who are in the pursuit of the acquisition of intellectual property from companies and/or competitive nations.

Usually, the critical systems of an industrial network are protected behind heavily layered defenses making a simple attack extremely difficult. However, there are many ways in which an attacker can exploit the vulnerabilities of an industrial system, of which the enterprise network is one the most prominent target, but other vectors of attack include the SCADA systems and even the demilitarized zones. Securing an industrial network, therefore, starts with understanding how an attack can win and then putting in place the necessary defenses.

To complicate matters, the simple demarcation of industrial networks into separate zones may be counterproductive as there are many enclaves that need to be isolated and secured, and if one system is vulnerable and there is a lack of protection and isolation between systems, this vulnerability could be exploited further. Additional complications are introduced by smart networks. The sheer scale of smart grid deployment makes these networks easily accessible, both physically and digitally. In addition, a smart grid communicates with multiple systems that are logically separated into enclaves. Thus, a smart grid breach can open many entry points into different areas of the industrial network (E. Knapp & Langill, 2011). An easy system to attack the SCADA DMZ is through the business network. Potential vulnerabilities are expected to be found in every component of the industrial system, including automated control systems. Therefore, the effect of an intrusion could be a benign minor disturbance caused by a malfunctioning HVAC, but it could be a more severe outcome such as shutting down the plant or the critical infrastructure.

The majority of experts recommend a defense in depth with several layers of intrusion detection and protection in order to discourage the attackers and make their task as difficult as possible. Therefore, companies should focus on the whole rather than any one aspect of their operations from floor to executive. It is recommended that the first step is to establish safety policies. Next, risk and security assessments are required, followed by the selection, installation and activation of remedies. Neglecting the security mode of the switch is not indicated. This is especially true when a thorough defense system is used. Switches become another layer of security. Also, educating employees about security is an indispensable measure for any company using a control system (Adams, 2014).

Securing industrial control systems against cyberattacks should be a priority for the proper functioning of critical infrastructures (power generation and distribution, water distribution, etc.). A cyberattack on an industrial SCADA control system can result in loss of control, shutdown, damage to facilities and alteration of the final product, with devastating consequences. Critical infrastructure-specific automated command and control systems require internet connectivity to run smoothly. But once implemented, critical infrastructures become vulnerable to cyberattacks because they are insecure by design.

It is therefore imperative to have people specialized in ensuring the cyber security of these types of exchanges, which are essential for any community. The niche specialization of these specialists can be enhanced as threats, risks and vulnerabilities diversify by offering additional training programmes.

CHARACTERISTICS OF THE SCADA CYBERSECURITY SPECIALIST PROFESSION

Taking as a premise the fact that technology has produced major changes in the way professional activities are carried out and has implicitly produced substantial changes in the labor market, we consider it important to periodically carry out analyses on the opportunity of introducing new occupations in the Romanian Classification of Occupations (COR).

Thus, in order to implement solutions to combat or mitigate the effects of cyberattacks on industrial control systems, specific skills and competencies are required to perform the necessary activities, such as managing cybersecurity solutions for operational environments within ICS, analyzing the specifications and designing the security architecture of the ICS, defining and modeling the threats and vulnerabilities of the ICS, developing the risk management plan, the prevention and response actions after the materialization of a threat, assessing and prioritizing potential threats and the actions required to mitigate the damage of any kind. Working in the field of automated command and control systems therefore requires the acquisition of niche skills to ensure the undisturbed operation of critical reference infrastructures.

Based on the awareness of the urgency of the digital transformation in all sectors of activity, ICI Bucharest met the need for training of the workforce in the ICT field by identifying new occupations in its field of competence and took the initiative to introduce in the Romanian Classification of Occupations the occupation of cyber security specialist for automated command-and-control systems, in accordance with Order no. 270/273/2002 of the Minister of Labor and Social Solidarity and of the President of the National Institute of Statistics on the procedure for updating the nomenclature of the Romanian Classification of Occupations, contributing decisively to the official status of this profession of great importance for the proper functioning of critical infrastructures.

This approach involved the preparation of a memorandum addressed to the Ministry of Labor and Social Solidarity, which included details on the description of the contexts, the occupation, the importance of the roles and responsibilities of such a specialist and the points in which his/her activity is particularized in relation to other experts in similar groups, as well as studies carried out by economic agencies with interest in the labor market, from which the need to update the current qualifications emerged.

The description of the occupation we have introduced involved identifying the COR code, describing the occupation in terms of roles and responsibilities and the tools needed to carry out the profession, specifying the elements of occupational safety, the programme, how to enter the profession and the skills required, etc. as follows:

Specialist in cyber security for automated command and control systems/ COR code 252303

Duties and responsibilities:

- Participates in the implementation of cybersecurity solutions for specific work environments for automated command-and-control systems;
- Operates cybersecurity solutions for specific working environments for automated command and control systems;
- Manages maintenance and user support (help-desk level 1, or 2) for security and data networking solutions for operational environments specific to automated command and control systems;
- Monitors cybersecurity events, log management tools, early detection tools and vulnerability assessment solutions and indicators of compromise;
- Administers tools to monitor the stability and security of data networks in the specific automated command-and-control systems environment;
- Analyses data, logs, and behaviors in specific working environments of automated command-and-control systems and related data networks for early identification of abnormal situations and potential cyber security incidents;
- Alerts the management team and all members of the response team upon identification of a cyber security incident in the monitored work environment;
- Enforces cybersecurity policies and procedures for the industrial automated command-and-control system;
- Applies a set of support and response measures in the event of a cybersecurity incident being identified;

- Coordinates third-party maintenance for hardware, software and telecommunications services for industrial control systems and related managed assets.

Tools and work instruments used:

- Equipment, data networks, installations and devices that are part of an automated command-and-control system;
- Equipment, data networks and specialized software applications designed to ensure cyber security in automated control systems;
- Equipment, installations and devices for the replication of the operation of automated command-and-control infrastructures in a controlled environment and related data traffic;
- Computing equipment, data networks and software applications composing a virtual environment intended to simulate the operation of automated command-and-control systems and related data traffic;
- Dedicated software applications designed to replicate or simulate in a virtual environment the operation of automated command-and-control systems and related data traffic;
- Libraries of functions and virtual objects of the automated command-and-control system type for the replication or simulation in a virtual environment of the operation of the automated command-and-control system and related data traffic;
- Dedicated equipment and software applications for the management of automated command-and-control systems;
- Methods, methodologies and procedures for the replication or simulation in a virtual environment of the operation of automated command-and-control systems and related data traffic;
- Dedicated equipment and software applications for detection and analysis of data traffic in controlled or virtual command-and-control automated system environments;
- Dedicated equipment and software applications for cybersecurity management in automated command-and-control system environments, replicated or simulated infrastructures in controlled or virtual environments;
- Libraries of functions and virtual objects for replication or simulation of cyber security incidents in automated command and control systems;
- Methods, methodologies and procedures for virtual replication or simulation of cyber security incidents involving automated command-and-control systems and related data traffic;
- Software applications for reporting and alerting human personnel to cybersecurity incidents in automated command and control systems;
- Methods, methodologies and procedures for an adequate response to cybersecurity incidents involving automated command-and-control systems infrastructures.

The Cyber Security Specialist for Automated Command and Control Systems is required to have the following credentials:

- An undergraduate degree in information and communication technology (e.g., automation, computer science, systems engineering, industrial engineering, etc.);
- A certification from specialization programme approved by the National Qualifications Authority.

The level of training required to practice the occupation:

- Qualification level according to the National Qualifications Framework (NQF) – 6;
- Reference level according to the European Qualifications Framework (EQF) – 6;
- Corresponding educational level according to ISCED - 2011 (educational programme code) – 6.

Competences:

- Understanding of the global safety context for automated control systems;

- Ability to understand system specifications and design logic of industrial control system security architecture;
- Ability to identify, assess and prioritize industrial control system cyber security vulnerabilities;
- Ability to validate industrial control system cybersecurity;
- Ability to manage and oversee cybersecurity solutions for operational environments within industrial control systems: application of job-specific cybersecurity standards.

ICI Bucharest's initiative to introduce in the Romanian Classification of Occupations the occupation of cybersecurity specialist for automated command-and-control systems was supported by analyses carried out by significant actors in the field (Safetech, ARPIS) and endorsed by the General Secretariat of the Government.

CONCLUSIONS

In this paper, we have introduced the profession of cybersecurity specialist for automated command-and-control systems which has been included in the Romanian Classification of Occupation. Following the presentation of the main characteristics of the industrial control systems, the need for cybersecurity specialists in this domain was highlighted. Further, we have presented the duties and responsibilities as well as the tools and instruments that are required for performing the expected work.

The occupation of cybersecurity specialist for automated command-and-control systems, code 252303, proposed by the National Institute for Research and Development in Informatics – ICI Bucharest, was accepted by the Ministry of Labor and Social Solidarity by Order 38/82/2022, published in the Official Gazette No 142 of 11 February 2022.

ACKNOWLEDGMENT

This work was funded from the project *„Cybernetic polygon for industrial control systems (ROCYRAN)”* (*„Poligon cibernetic pentru sisteme de control industrial (ROCYRAN)”).*

REFERENCE LIST

Adams, T. (2014). *SCADA System Fundamentals* (Course No: E01-007). Continuing Education and Development, Inc.

Alexandrescu, G., & Vaduva, G. (2006). *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*. Editura Universității Naționale de Apărare 'Carol I'.

Knapp, E. D., & Langill, J. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Knapp, E., & Langill, J. (2011). *Industrial Network Security.* Retrieved from https://www.safaribooksonline.com/library/view/-/9781597496452/?ar

Stouffer, K., Falco, J., & Scarfone, K. (2008). Guide to industrial control systems (ICS) security. *NIST Special Publication 800*(82). National Institute of Standards and Technology.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security. National Institute of Standards and Technology. *NIST Special Publication*, *800*(82), Revision 2. National Institute of Standards and Technology.

Zhang, P. (2010). *Advanced Industrial Control Technology.* William Andrew.