A Brief Introduction to Cybersecurity Landscape in Industrial Control Systems; Practitioners View

Mihai RĂUȚĂ, Victor GÂNSAC, Olivia COMȘA
Safetech Innovations
mihai.rauta@safetech.ro, victor.gansac@safetech.ro, olivia.comsa@safetech.ro

Abstract: With the exponential growth of the Internet and the number of devices able of controlling complex industrial processes, hardware equipment that uses standard IP protocols for transporting data specific to industrial processes, there is an increased incidence of attacks targeting industrial critical infrastructures. If in the past the attackers were persons from inside the industry, often angry dismissed employees, in the last period these attacks are mainly carried out by the players in the field of industrial espionage, terrorist groups or rival nation-state.

The security technologies and measures used in the Industrial Control Systems (ICS) are in vast majority of the cases common with those used in the information technology (IT) business infrastructure, but if in the latter case this falls on the confidentiality, integrity and data availability, in the case of industrial processes governed by ICS the integrity and resilience of the industrial process itself must be ensured in the first place. Data loss is far less important than the catastrophic interruption of the mission–critical industrial process with adverse consequences on environment and life in general.

The paper will briefly review the specific terms used in industrial network systems and will detail some of security challenges and vulnerabilities associated with ICS infrastructure. In the end we will present methods and technologies used to better secure the critical infrastructure environment and some of the activities Safetech Innovations SA performs in this field for its beneficiaries. It present a practitioner point of view with deep involvement in securing important critical infrastructures, from IT to energy, oil, gas and utilities.

Keywords: Cybersecurity, ICS, SCADA, Critical Infrastructures, OT/IT, CERT, Security Challenges, Resilience

INTRODUCTION

The increased role of the Internet and of the number of devices able of controlling complex industrial processes, hardware equipment that uses standard IP protocols for transporting data specific to industrial processes facilitate the access to information but also generate an increased incidence of attacks targeting industrial critical infrastructures. If in the past the attackers were persons from inside the industry, often angry dismissed employees, in the last period these attacks are mainly carried

out by the players in the field of industrial espionage, terrorist groups or rival nation-state *[Baldini et al., 2020]*.

In the case of rival nation-state driven attacks, we may presume that the attacker's goal is to sabotage or even destruct of an entire mission-critical industrial segment. We can mention here the attacks that were targeted against the energy distribution infrastructure in Ukraine in December 2015 and 2016 *[Hemsley & Fisher, 2018]* or against the Iran's uranium enrichment industry in June 2010. All those hacks were highly sophisticated, persistent and precisely targeted (APT), using cutting edge technologies and exploiting vulnerabilities never publicly exposed until the very moment of the incident. They represent a growing category of attacks intended to sabotage mission-critical infrastructure where there is almost no international norms and laws *[Dar, 2019]* to address nation-state sponsored cyberwarfare. More than that, investigators are rarely able to trace hacks back to individuals and they point to faceless attack groups and the nations they live in. It is similarly difficult to connect hackers to governments, despite evidence indicating such connections. Attribution difficulties give victim countries pause before they name an attacker or retaliate, and create plausible deniability for malicious governments. However, in spite of the challenges attribution poses, ATP attacks have served specific nation-state interests and is not difficult to finger point to this countries *[Park et al., 2011]*.

Without drawing any conclusions, it is easy to glimpse a common denominator specific to attacks against industrial critical infrastructures. The security technologies and measures used in the Industrial Control Systems (ICS) are in vast majority of the cases common with those of the information technology (IT) business infrastructure, but if in the latter case this falls on the confidentiality, integrity and data availability, in the case of industrial processes governed by ICS the integrity and resilience of the industrial process itself must be ensured in the first place. Data loss is far less important than the catastrophic interruption of the mission-critical industrial process with adverse consequences on environment and life in general. Among the security experts and consultants dealing with critical infrastructures it is clear that it is not sufficient to deploy ordinary information IT security measures, such as perimeter protections using firewalls, security network segmentation using routers and access lists or application protections using intrusion prevention systems (IPS).

Similarly, unlike what happens with standard IT systems, in industrial systems it is dangerous to transfer a solution directly from one system to another, as the characteristics of the second may include factors that make such a direct integration vulnerable *[Collantes & Padilla, 2017]*. All this means that a detailed knowledge of hardware equipment and of the associated protocols involved in industrial processes and more specifically in operational technology (OT) is crucial in understanding which weak points, attack vectors and possible defensive measures should be taken into account when implementing or enhancing an industrial control system.

In the pages below we will briefly review the specific terms used in industrial network systems and detail some of the security challenges and the vulnerabilities associated with ICS infrastructure. In the end we will present methods and technologies used to better secure the critical infrastructure environment.

DEFINING TERMS: OT, ICS, SCADA – COMMONS AND DIFFERENCES

Operational Technology (OT) refers to computing systems that are used to manage industrial operations as opposed to administrative operations. Operational systems include production line management, mining operations control, oil & gas monitoring etc.

Industrial control systems (ICS) is a major segment within the operational technology sector. It comprises systems that are used to monitor and control industrial processes. This could be mine site conveyor belts, oil refinery cracking

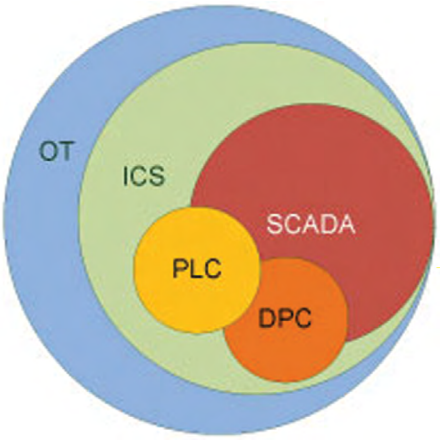

Fig. 1: *SCADA versus OT/ICS*

towers, power consumption on electricity grids or alarms from building information systems. ICSs are typically mission-critical applications with a high-availability requirement.

Most ICSs fall into either a continuous process control system, typically managed via programmable logic controllers (PLCs), or discrete process control systems (DPC), that might use a PLC or some other batch process control device.

ICSs are often managed via a Supervisory Control and Data Acquisition (SCADA) systems that provides a graphical user interface for operators to easily observe the status of a system, receive any alarms indicating out-of-band operation, or to enter system adjustments to manage the process under control.

SCADA systems display the process under control and provide access to control functions. A typical configuration is shown in ***Figure 2***.

The main components are:

• SCADA display unit that shows the process under management in a graphic display with status messages and alarms shown at the appropriate place on the screen. Operators can typically use the SCADA system to enter controls to modify the operation in real-time. For instance, there might be a control to turn a valve off, or turn a thermostat down.

• Control Unit that attaches the remote terminal units to the SCADA system. The Control unit must pass data to and from the SCADA system in real-time with low latency.

• Remote terminal units (RTUs) are positioned close to the process being managed or monitored and are used to connect one or more devices (monitors or actuators) to the control unit, a PLC can fulfil this requirement. RTUs may be in the next room or hundreds of kilometers away.

• Communication links can be Ethernet for a production system, a WAN link over the Internet or private radio for a distributed operation or a telemetry link for equipment in a remote area without communications facilities.

There are some seminal changes happening in the OT world at the moment. Organizations want to leverage their OT assets for business purposes, they want to be agile and have the ability to make modifications to their OT configurations. They want to take advantage of new, cheaper, IP sensors and actuators. They want to leverage their corporate identity provider service to authenticate operational

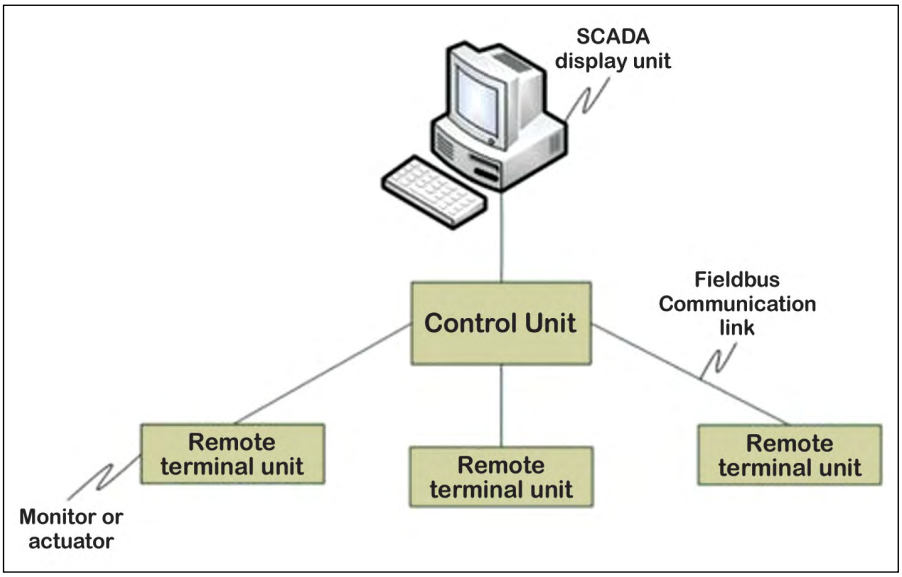

Fig. 2: *Typical SCADA Configuration*

personnel *[Williamson, 2015]*. It's an exciting time for operational technology systems but very challenging from security point of view.

ICS SECURITY CHALLENGES

With the recent high-profile security incidents, briefly presented in the introduction chapter, it is becoming clear that there is a need to implement better security for critical infrastructure providers. Of even more pressing need is the transition from old, serial-based networks ICS protocols to more modern IP-based infrastructure or encapsulating ICS protocol's functionalities in IP protocol. This move requires the incorporation of IT network security controls and procedures in some non-critical part of the industrial network and defining a new controls and security methodologies for mission-critical part of the ICS network *[Lourenço & Marinos, 2020]*.

Equally challenging is the continued failure of leading PLC vendors like Siemens, ABB, Schweitzer, GE, Honeywell and others to patch security vulnerabilities on their systems. And, even for systems where patches have been developed, the age of devices in network, sometimes up to 30 years, and the inability of client companies to service their field systems, means that it is very difficult if not impossible to bring down some industrial processes in order to update the hardware equipment with latest security patches in order to address known vulnerabilities *[Safetech Innovations, n.d.]*.

The critical infrastructure space use specialized systems with protocols that are not normally found on business or IT networks. A brief sample of these OT protocols includes:

- MODBUS, which enables commands to PLCs or gives reporting units (RTUs) the ability to provide data to management systems.
- DNP3, which allows for the migration of serial communications over Ethernet.
- ICCP, which is often used to link independent systems operators (ISOs) to power generators and distributors so that the ISOs can know how much capacity exists and what kind of demand exists in the system.

As an example, electrical companies have clean data centers that can support off-the-shelf devices. However, equally often, the companies who support electrical production and distribution infrastructures have facilities in areas with extreme temperature variance, dust and dirt and challenging electrical current. In such scenarios, dedicated hardware solutions is needed that supports these environmental requirements. More than that, general purpose security solutions which runs on IT security physical or virtual appliances lack support for technology and SCADA protocols used *[Lourenço & Marinos, 2020]*.

Almost all SCADA protocols come from pre-IP era where communications were either analogic or digital-serial. The limited distance between SCADA devices and speed of communications based on serial protocols are today solved by reincarnation of the protocols using the IP addressability and TCP/UDP transport stacks. This pose a very high risk of attacks against SCADA protocols, which were never designed with security in mind but only functionality, and also attacks against IP and transport protocols itself, like in any other well-known IT protocol.

The use of air gaps has eroded or disappeared altogether, thanks to increasingly intertwined OT and IT. In most of the SCADA implementations the associated network is designed to have a firewalled connection with IT corporate network in order to provide access for management reports and statistics, SCADA application updates and patches. This pose a very high risk of unauthorized access knowing that almost any corporate network is connected to Internet. Putting a firewall and an IPS between OT and IT is insufficient for the security requirements of the critical infrastructure industry because malware, APTs and other more sophisticated attack vectors have already proven capable of breaching security perimeters of power companies and not only *[CyberX, n.d. (a)]*.

Insiders with legitimate access to ICS networks include employees, contractors and 3rd party integrators. Since most ICS networks don't have any authentication or encryption mechanisms

that restrict user activity, any insider has unfettered access to any device in these network. This includes the SCADA applications and the critical controllers responsible for the entire lifecycle of industrial processes. Even if there are external "secure" remote network access methods in place for employees, **3rd party integrators and contractors, like client-to-site VPN solutions, loss of credentials or endpoint devices itself pose a serious risk to the ICS infrastructure**. More than that, there is no such thing like 100% secure software application, meaning the VPN client itself could be vulnerable *[CyberX, n.d. (b)]*.

Another risk is represented by the human mistakes which are inevitable and can be very costly. **For many organizations the risks associated with human error can be more serious than the insider threat**. In some cases, it is considered the biggest threat to the ICS system. Human errors can include incorrect settings, configurations and PLC programming errors causing hazardous changes in the process flow. Human error can cause vulnerabilities that can be exploited by external adversaries. A common example includes temporary connections setup for integrators that remain open after a project has ended *[CyberX, n.d. (b)]*.

Some human error scenarios can occur when employees use "creative measures" to get their work done. Like the case of employees that need to remotely connect to ICS networks, but are not provided with secure access. They can set-up unauthorized remote connections on their own. These unsanctioned connections can become infiltration points and expose the industrial network to external attacks.

Securing ICS networks from external and internal threats is a significant challenge since many do not have any authentication or authorization procedures in place. Most also lack controls to enforce access policies, security policies or change-management policies. In addition, there are no audit trails or logs that capture changes and activity to support forensic investigations. As a result, when operational disruptions occur, it is very difficult to determine if they were caused by a cyber-attack, a malicious insider, human error or mechanical failure. This lack of visibility and controls limits the ability of operations staff to respond to events in a timely manner, raising the overall costs associated with operational disruption and mitigation efforts *[Perelman, 2016]*.

SECURITY SOLUTIONS FOR CRITICAL INFRASTRUCTURES

To defend critical infrastructure networks, companies today require security procedures and solutions that can combine multiple protection technologies: firewall and IPS with support for SCADA exploits, antimalware, but more important the ability to analyze deep into SCADA packets and identify attempts to run commands on PLCs or attain data without appropriate permissions. In order to protect against external threats, malicious insiders and human error, real-time visibility into industrial control system networks is paramount for ICS security. Industrial organizations must monitor all activities, whether executed by an unknown source or a trusted insider, and whether authorized or not. Monitoring the changes made to industrial controllers like PLCs, either over the network or on the device itself, is the most effective way to detect unauthorized activities caused by ICS threats *[Lourenço & Marinos, 2020]*.

Specialized ICS monitoring technologies can provide the deep, real-time visibility required to identify suspicious or malicious activity. Latest security monitoring solutions, build around machine learning and finite-state machine technologies, can provide the baseline of industrial process and could detect any abnormal deviations inflicted by either malicious activity or by human error process incidents. In order to not interfere with the industrial process the ICS real time monitoring technologies should be non-intrusive, meaning that they should just analyze the SCADA traffic without modifying or restricting any part of it *[CyberX, n.d. (a)]*.

For the most security demanding part of the ICS network where the process itself is controlled and take place, and because the

air gap between IT and OT has proven not to be effective against the most sophisticated attacks, there are security technologies and solutions that can create a replica of all the SCADA systems required to the IT management for statistics and reporting purposes. Those solutions and technologies use data diode devices as unidirectional gateways and SCADA protocol application proxies in order to create a physical read only channel from within IT networks to SCADA systems. **Such read-only channels disrupt any attack against productions systems from Internet or corporate networks and provide maximum security to the missioncritical processes** *[CyberX, n.d. (b)].*

Not less important are the security methodologies, procedures and user awareness. Companies must invest in employee trainings in order to rise the security awareness and minimize the human error risk.

SAFETECH INNOVATIONS SECURITY SOLUTIONS AND SERVICES FOR CRITICAL INFRASTRUCTURES

Safetech Innovations SA (www.safetech.ro) is one of the market leaders on Cyber Security/ Information Security in Romania. Safetech is a security solutions implementer and integrator, which offers a complete range of cybersecurity services and solutions, including Security Monitoring and Incident Response Services, Penetration Testing for different types of infrastructures, as well as, SOC/CERT services and innovative R&D projects. In the area of critical infrastructure security and resilience, Safetech implement mature, secure, resilient and performing solutions developed by the most known technology providers from all over the world and innovative solutions developed in-house based on the previous experience.

Safetech Innovations SA has an experienced team of experts which assure performing, high quality, resilient and secure solutions and services for critical infrastructure industries to contribute to the digital transformation of society, industry and services. A short presentation of the company and its capabilities is included below.

SAFETECH INNOVATIONS founded, owns and operates a private Computer Security Incident Response Team (CERT) / Computer Emergency Response Team (CSIRT) known as **STI-CERT**, which is accredited by Trusted Introducer (https://www.trusted-introducer.org/directory/teams/sti-cert.html) at European level (since 2015) and which provides to its customers, including

Fig. 3: *Safetech Key Assets [source: Safetech Website]*

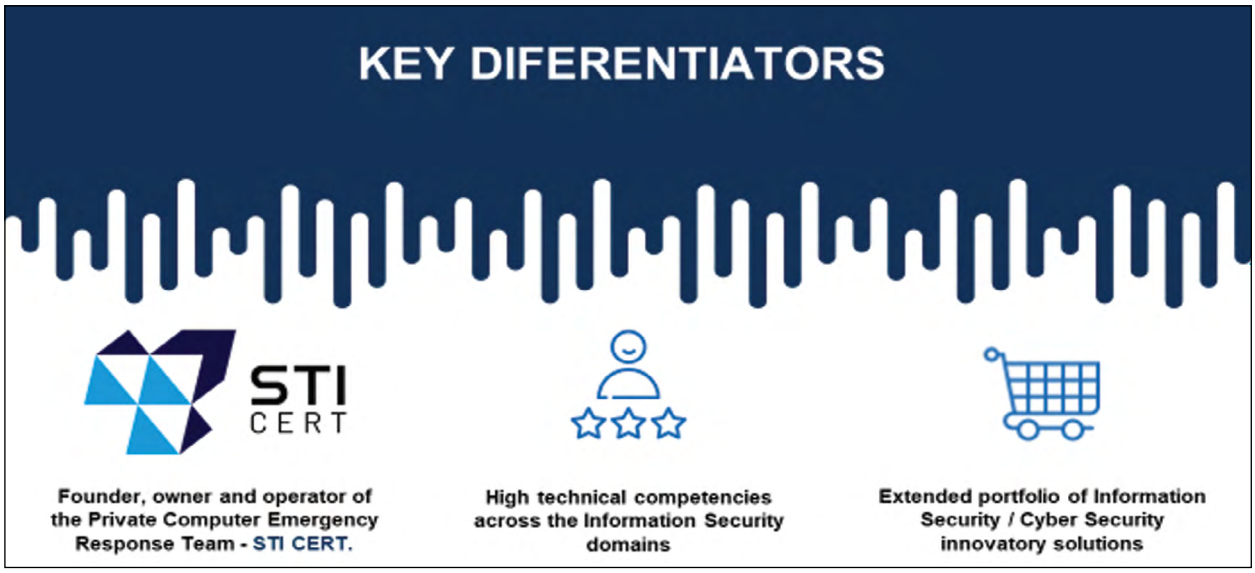

Fig. 4: *Key Diferentiators [source: Safetech Website]*

owners of Critical Infrastructures, Security Monitoring and Incident Response Services, Penetration Testing, Security Consultancy – to name the most representative ones.

Safetech team members have extensive hands-on experience and deep understanding of Information Security practice with a strong technical skillset in managing heterogeneous IT infrastructures and solid IT administration background.

Safetech experience comes from important and relevant projects conducted during the last ten years in Government – Public Sector, Banking & Insurance sector, Energy, Gas, Oil and Public Utilities sector, from Romania or abroad.

Also, the company is accredited as **Official Provider of Penetration Testing** for Arcelor Mittal, Raiffeisen Bank International Group, ING Business Shared Services BV Amsterdam – Bucharest Branch etc.

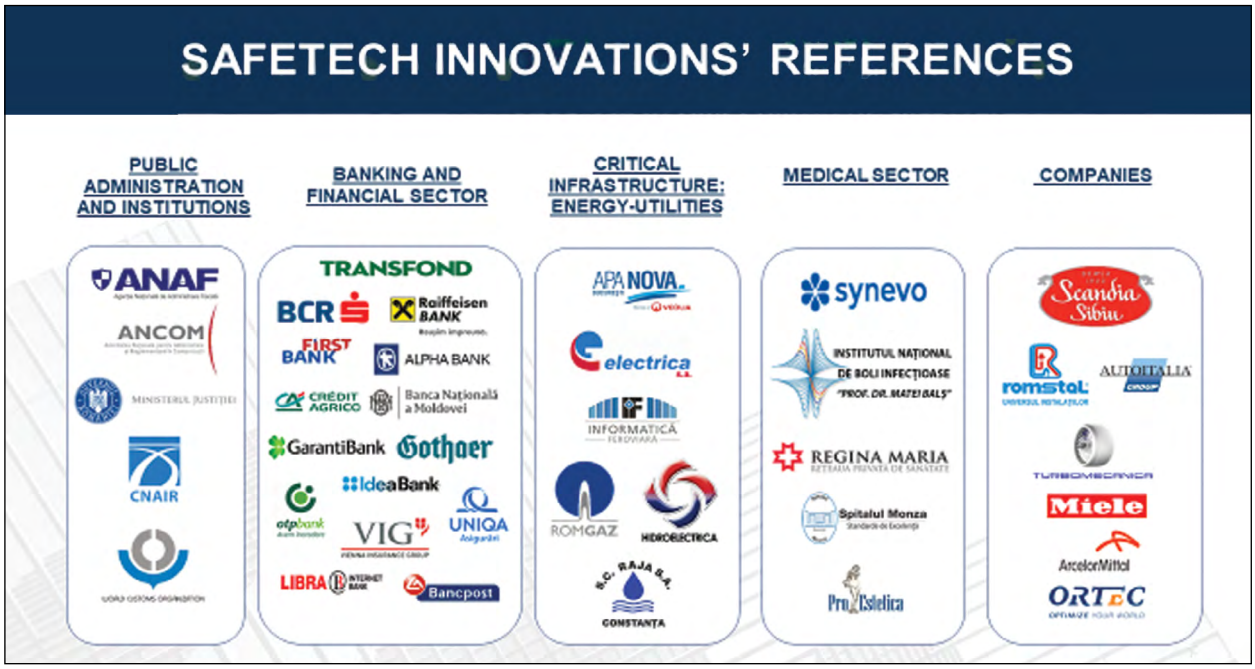

Fig. 5: *Safetech Innovations References [source: Safetech Website]*

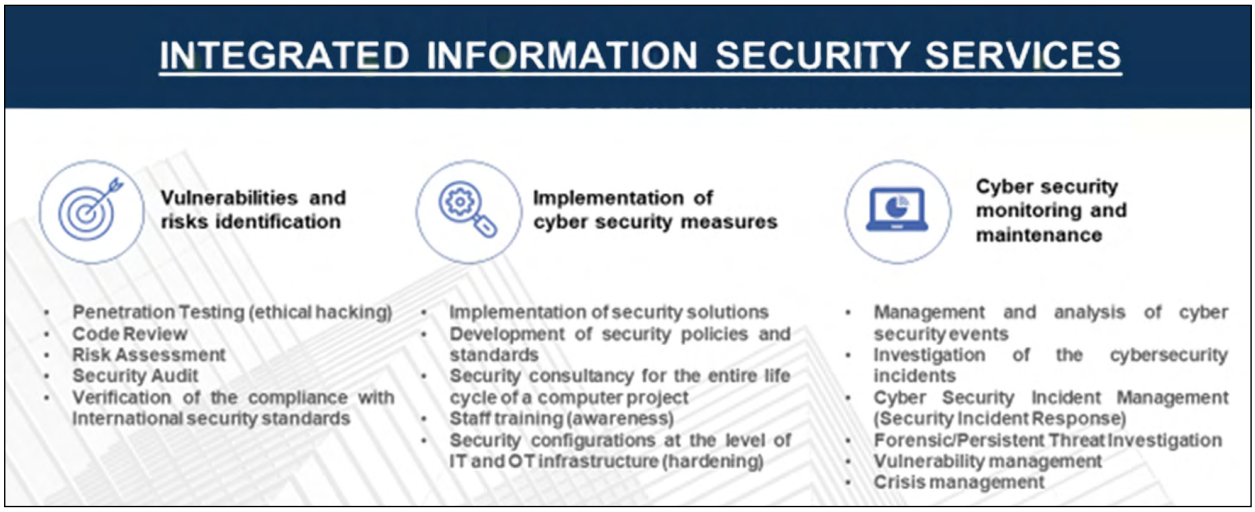

Fig. 6: *Integrated Security Services [source: Safetech Website]*

■ **SAFETECH also developed projects abroad for institutions, such as:**

- World Customs Organization (Belgium), Security Innovation (USA);
- Intrasoft International (Luxembourg), Arcelor Mittal (Luxembourg, Duisburg);
- National Bank of Moldova, Legal & General (Netherlands);
- Ministry of Justice – Security Testing Project MCIS (Moldova);
- Centre for e-Governance – e-Government platform security testing (Moldova).

■ **SAFETECH INNOVATIONS:** is the first Romanian company and one of the few in Europe, registered as a member of the NATO INDUSTRY PARTNER ROSTER and partner in the NATO Industry Cyber Partnership (NICP) – (http://www.nicp.nato.int/relatedactivities/index.html) and one of the 4 companies in the world and the first in Eastern Europe accredited by HID Global Security for Global Professional Services • Has a signed collaboration partnership with the Romanian National Computer Security Incident Response Team – CERT-RO • Has implemented the first project devoted to building security culture in universities, "Improving processes and educational activities in the bachelor and master programs in ICT by creating an information security lab" • Has significant

Fig. 7: *Safetech innovative Cyber Security Solutions [source: Safetech Website]*

Fig. 8: *Safetech Relevant Certifications [source: Safetech Website]*

cooperation with ENISA in the area of IT/OT and critical infrastructures security and resilience.

SAFETECH INNOVATIONS was invited and participated in the last years at: the CYBER EUROPE, the pan-European exercise to protect EU Critical Infrastructures against coordinated cyber-attack, organized by ENISA, at CYBER COALITION, organized by the NATO COMMUNICATION AND INFORMATION AGENCY (NCIA), at CyDEx, cyber security exercises organized under the auspices of National Center Cyberint.

Safetech team is one of the most certified cybersecurity team in Europe and stands out by the ability to discover vulnerabilities by simulating cyber-attacks and is constantly concerned in this regard to improve its theoretical and practical skills.

Also, Safetech team has other leading vendors' accreditations, as:

Fig. 9: *Safetech Quality Standards [source: Safetech Website]*

• HID Professional Services (our company, Safetech, is one of the 4 companies accredited by HID Global Security for Global Professional Services and first in Eastern Europe).

• CCSP – CheckPoint Certified Collaborative Support Provider.

• CCSA – CheckPoint Certified Security Administrator.

• CCSE – CheckPoint Certified Security Expert.

• CCSI – CheckPoint Certified Security Instructor.

• CPSC – Check Point Partner Sales Certification.

Performing services and solutions are sustained by research projects which develop innovative solutions to be used by the company and to be implemented to our partners and customers.

One of the most recent initiative is the project "SafePIC – Center of Excellence for Cyber Security and Resilience of Critical Infrastructure" having the aim to develop innovative solutions, products and services for the increase of interoperability and cybersecurity resilience of critical infrastructures. Several other projects in the area of ICS SCADA cybersecurity, interoperability, cyber range, simulation and E&T are developed together with prestigious research, academic and industrial partners *(Safetech Innovations, n.d.]*.

Safetech Innovations SA is committed to contribute to the increase of critical infrastructures security and resilience which are vital to our life and society.

REFERENCE LIST

Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., Neisse, R., Nordvik, J., Papameletiou, D., Reina, V., Ruzzante, G., Sanchez Martin, J., Sportiello, L., Steri, G. & Tirendi, S., (2020). Cybersecurity, our digital anchor. In: Nai Fovino, I., Barry, G., Chaudron, S., Coisel, I., Dewar, M., Junklewitz, H., Kampourakis, G., Kounelis, I., Mortara, B., Nordvik, J. & Sanchez Martin, J. (eds.), EUR 30276 EN, Publications Office of the European Union, Luxembourg. ISBN 978-92-76-19957-1, DOI: 0.2760/352218, JRC121051

Collantes, M. H. & Padilla, A. L. (2017). Protocols and Network Security in ICS Infrastructures. Spanish National Institute for Cyber-security

CyberX (n.d. (a)). CyberX Report: NIST Recommendations for IoT & ICS Security. An Executive Summary. Available at: <https://cyberx-labs.com/resources/nist-recommendations-for-iot-ics-security/>

CyberX (n.d. (b)). CyberX Whitepaper: Addressing the MITRE ATT&CK for ICS Matrix. How CyberX's Agentless Security Platform Protects against ICS Threat Actor Tactics and Behaviors. Available at: <https://cyberx-labs.com/resources/addressing-the-mitre-attck-for-ics-matrix/>

Dar, Z. S. (2019). Cyber War & International Law. Research paper, Jacobs University Bremen. DOI: 10.13140/RG.2.2.24187.57129

Hemsley, K. E. & Fisher, E. R. (2018). History of Industrial Control System Cyber Incidents. Idaho National Laboratory, U.S. Department of Energy National Laboratory

Lourenço, M. B. & Marinos, L. (eds.) (2020). ENISA Threat Landscape 2020 – Cyber espionage. European Union Agency for Cybersecurity (ENISA). ISBN: 978-92-9204-354-4, DOI: 10.2824/552242

Park, D., Summers, J. & Walstrom, M. (2017). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. Henry M. Jackson School of International Studies, University of Washington. Available at: <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>

Perelman, B. (2016). The Top 3 Threats to Industrial Control Systems. Available at: <https://www.securityweek.com/top-3-threats-industrial-control-systems>

Safetech Innovations (n.d.). Centrul de excelență pentru securitatea cibernetică şi reziliența infrastructurilor critice (SafePIC). Project, available at: <https://www.safetech.ro/safepic/>

Williamson, G. (2015). OT, ICS, SCADA – What's the difference?. Available at: <https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference>