



# FACT SHEET

## Industry Cybersecurity and Reliability

### ICCSS INTEGRATED VISION : CYBERSECURITY – RESILIENCE – RELIABILITY

Effective safety and security in chemical and environmental activities play a vital role in society and have become the backbone of public and social security, and economic growth. Digitization in chemical areas and industry activities, and use Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the chemical production, transport and use of chemicals. A large number of chemical installation and their economic significance make the chemical industry particularly vulnerable to terrorist attacks, including cyberattacks. As a result of a cyberattack, release of toxic chemicals or stoppage of flow of chemicals (reagents) to other industries would have serious health, social, economic and ecological repercussions. In practice it could form use of chemical weapons. **Therefore cybersecurity and reliability have become a leading component of any safety and security activities.**

### ICCSS INDUSTRY CYBERSECURITY AND RELIABILITY GOALS

- Building a cybersecurity, resilience and reliability as a whole organizational effort, starting Board level
- Promoting cybersecurity, resilience and reliability culture, nest practices and capacity building by developing and promoting manual for industrial cybersecurity, resilience and reliability
- Offer a series of industry cybersecurity trainings to enhance resilience against cyber threats and reliability awareness
- Partner with a technology providers to demonstrate y show how best practices can be effectively applied with the use of 3rd party software
- Enter international market with ICCSS program on increasing resilience against cyber threats.

### ICCSS INDUSTRY CYBERSECURITY AND RELIABILITY ACTIVITIES

The ICCSS has introduced 6 innovative offers and approaches to enhance industry cybersecurity and reliability. They include:

- 1) National Conference/Training: Cybersecurity and Industry Reliability:** strengthening resilience against cyberattacks and improving reliability in small and medium enterprises (SME) and local government utility companies, to enhance development of professional competences in cyber security of OT and cyber security audits in Polish industry.
- 2) Inauguration of the international Task Force within Working Group on Cybersecurity for Industry 4.0** at the Ministry of Digital Affairs and under the co-ordination International Centre for Chemical Safety and Security (ICCSS), to elaborate Manual of best practices in cybersecurity and reliability in the chemical and energy carriers industries. The international Task Force include partners from Canada, Italy, Ukraine and US.
- 3) Establishment of the international Working Group,** (coordinated by ICCSS) to develop concept of the international university education and training curriculums in cybersecurity for industry.
- 4) Initiative to establish 3 market specialties in industrial cybersecurity and reliability** for technicians, management and policy. The new market industrial cybersecurity specialties focus both on how to operate cybersecurity in IT and OT at industrial sites and on reliability, as the very core of the cybersecurity design. Development and wide implementation of the above professional competences, based on knowledge of legal norms, management and good engineering practices, will be an important instrument to achieve the basic goal: preventing

the cyber-intruder before he stops the industrial installation. The introduction of these market specialties will lower costs of cybersecurity services for Small and Medium Companies (SMI) and local administration.

**5) Roadmap For Raising Cybersecurity Awareness and Responsibility**, to promote partnerships in strengthening cybersecurity in the chemical industry. It focuses on gathering and sharing of the most recent knowledge in terms of procedures, technical solutions and trainings in cybersecurity and reliability. ICCSS connects the subject of automation with the subjects of security of access and corporate architecture.

**6) Trainings on Cybersecurity Awareness and Responsibility** for international organisations, small and medium enterprises (SME), and local government utility companies

## ICCSS OFFER

ICCSS helps integrate cyber-security needs and culture with the cyber-security technical solutions in Industry. We developed an integrated approach to train company Staff on cyber-security, with emphasis on sales teams to prepare them for dialogue with clients on developing background company knowledge and culture on industrial cybersecurity. Our approach provides for: 1) conducting cyber-security training aimed at development of company cyber security culture; 2) assisting to verify resilience against cyber threats; 3) support to introduce best practices and standards.

ICCSS offers unique **training program to increase resilience against cyber threats**. This program addresses and promotes also human behaviour as equally important factor in cyber-security. It supports 'cyber-hygiene', a set of routine measures that, where implemented and carried out regularly by organisations and businesses, minimize their exposure to risks from cyber threats.

For the purpose of strengthening international organisations cybersecurity structures, the ICCSS offers capabilities to comprehensively respond to cyber threats and promotes **Roadmap For Raising Cybersecurity Awareness and Responsibility**.

ICCSS Proposes the following offers/trainings:

- *Offer on Building Awareness about Cyber Threats And Increasing Reliability Against Cyberattacks In The Company*
- *Conference/Training: Cybersecurity and Industry Reliability, for central and local administrations, Small and Medium Companies, and academia*
- *Conference/Training: Cybersecurity and Industry Reliability*

## Contact and further information:

For more details on ICCSS Offers, please visit: [ICCSS Industry Cybersecurity And Reliability Portal](#) and [ICCSS Training Offer](#)

For further information please contact:

1. **Amb. Krzysztof Paturej**, ICCSS President, at: e-mail: [k.paturej@iccss.eu](mailto:k.paturej@iccss.eu)
2. **Mr Adam Paturej**, ICCSS Director of ICCSS cybersecurity and reliability programme, at e-mail: [a.paturej@iccss.eu](mailto:a.paturej@iccss.eu)