CYBERSECURITY AND INDUSTRIAL PLANTS – FOUNDATION OF THE "INDUSTRY 4.0" PROJECT AND A CHANCE FOR POLAND

dr eng. Andrzej Kozak – Office of Technical Inspection, Warsaw
prof. dr hab. eng. Maciej Kościelny – Warsaw University of Technology
dr eng. Piotr Pacyna – AGH-UST University of Science and Technology, Kraków
dr eng. Dariusz Gołębiewski – The Capital Group of Powszechny Zakład Ubezpieczeń SA, Warsaw
amb. Krzysztof Paturej – International Centre for Chemical Safety and Security, Warsaw
dr Joanna Świątkowska – The Kosciuszko Institute, Kraków

1. "INDUSTRY 4.0" AND CYBERSECURITY

A digital world is the heart of and driving force behind the fourth revolution. The Internet of Things,automation of industrial processes, data processing and many other phenomena that bring new technologies are all changing the way modern enterprises function and, indirectly, changing entire economies, societies and states. We live in a physical world which entwines with a digital one. This digital world has an impact on many spheres of human activity, including issues related to security. In today's world, it is not surprising that providing only physical security is not enough to ensure the security of various systems, including installations, objects, appliances and services. Security must be viewed in a holistic way, and cybersecurity plays an essential role in this.

For Poland, along with its large industrial share of the economy, following that trend presents great challenges, but also great opportunities. On the one hand, having industry become reliant on modern digital technology creates a situation where it opens itself up to many new, unexpected threats which can come from many different sources. On the other hand, taking care of cybersecurity, especially industrial control systems, can lead to the creation of new national specialities in the realm of cybersecurity, making cybersecurity one of Poland's possible "export products." We have plenty of advantages in implement this plan, including both great experts and also favourable structure of the economy. Referring to Poland's national interest, the only thing we need is to make this task our strategic objective. If we want to feel safe and develop dynamically, we need to specialise ourselves in the industrial control system branch of cybersecurity.

Many countries lack the measures predisposing them to become leaders in cybersecurity. However, Poland certainly does not belong to that group. Besides its natural potential, currently Poland benefits from favourable external conditions which support achieving a successful transition. Europe is focused on developing European solutions to cybersecurity. There are an ever increasing number of new instruments and mechanisms which support these efforts, including, for instance, the initiative of the European Commission – *Private Public Partnership* in cybersecurity. We should seize that opportunity.

The text was written by representatives of leading Polish academic centres, practitioners, experts and private sector actors. The main goal is to introduce the reader to cybersecurity of industrial control systems and to identify potential steps which should be taken in order to truly enhance security.

2. THE CATASTROPHE OF BAKU PIPELINE – TBILISI – CEYHAN – THE BEGINNING OF THE STORY

On the 6th of August 2008, approximately at 11:00 p.m., there was an explosion of a pipeline close to Erzican city in Eastern Turkey which had begun operating in 2006.[1] The explosion's shock wave was felt in a radius of around 500 meters. The pipeline staff was notified about the inci-

1 *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar, [available: 09.09.2016].

dent only after 40 minutes by one of the guards who was observing the fire on his own. Daily losses were valued at $ 5 million.

It was discovered that none of the components of the well-equipped security system worked properly.[2] The pipeline as a whole was under the supervision of CCTV cameras, pressure and flow of oil sensors, alarms and information about the fire system. The parameters were read up to date by the system and transferred to the central control room over wireless networks or, in the event of communication problems, via emergency satellite connection. The Turkish government blamed separatist communities for this attack and launched a war with them. Three days later, the war in the Caucasus began.

On the 6th of August 2008, there was an explosion of a pipeline in Eastern Turkey. The explosion's shock wave was felt in a radius of around 500 meters. Daily losses were valued at $5 million.

The answer for the question of why the central control room of the pipeline did not receive a single disturbing signal from the explosion region came in the autumn of 2015. A long-lasting investigation revealed that the software of one of the computers responsible for gathering data was modified. Most likely the attackers also disrupted satellite communication, which would explain why the sensors did not transmit the parameters via the backup communication channel. In addition, someone must have deleted the essential 60 hours of recordings from the supervising CCTV cameras.

However, it turned out that one of the cameras, recording infrared image, was attached to a separate network. Thanks to this recording, it is known that a few days before the explosion there were two men strolling along the pipeline, carrying laptops in their hands.

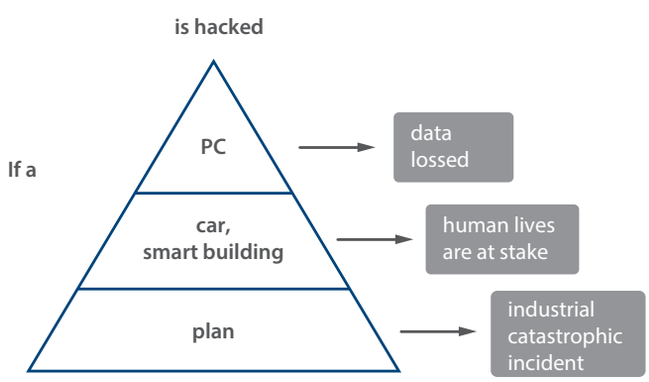
At the same time, according to correlation logs coming from computer systems of the pipeline, someone had scanned the pipeline ICT infrastructure. There were several attempted attacks and one of them appeared to be successful. It turned out that the starting point was the software used by the security cameras for communication purposes. The attackers, after gaining access to the network of cameras, infiltrated the internal network that oversees the pipeline and then they installed the backdoor software on one of the computers running a Windows system (the effect of propagation). At this stage they managed to infiltrate Distributed Control System (DCS) "to blind" an operator and take control over individual valves (the effect of disinformation).As a result of the manipulation of the values corresponding to the pressure in given sections, they caused a rupture of the pipeline, leakage, ignition and an explosion (the effect of damage in physical assets). The catastrophe of the pipeline marks the beginning of a new era in cybersecurity in which digital threats can change the real world.

The attackers installed the backdoor software, they managed to infiltrate Distributed Control System "to blind" an operator and take control over individual valves.

3. CYBERSECURITY OF INDUSTRIAL SYSTEMS – BASIC INFORMATION

Nowadays, digital technology is entering the industry, contributing to the development in control systems. At the same time, this development brings side effects in the form of a threat of unlawful interference into industrial processes caused by cyberattacks. The problem of cybersecurity is well-understood in the IT environment, however the industry, which is not free from cyberthreats, seems to underestimate the situation. The effects of a cyberattack on industrial facilities can be devastating for the property, life, health of employees and the environment.

FIGURE 1. THE GRADATION OF THE EFFECTS OF CYBERATTACKS PRESENTED IN THE FORM OF A PYRAMID OF CYBER INCIDENTS.



A cyberattack can be carried out from all over the world– that is why cyber criminals, especially groups responsible for advanced persistent threats**,** can keep a sense of impunity. Recent attacks on industrial facilities show that the risk of conducting cyberattacks on critical infrastructure on an ideological (terrorism) or political basis is real, because the cost of preparing and carrying out the attack is low in com-

2 British Columbia Institute of Technology, *The Myth and facts behind Cyber Security Risk for Industrial Control Systems*, Report PA Consulting Group, http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf, [available: 06.09.2016].

TABLE 1. COMPARISON OF ICS AND IT SYSTEMS.

	ICS	IT
Operational mode	permanent – 24/7/365	permanent – 24/7/365
	Real time working regime. System reboot severely hampered. Severe results of a system reboot, difficult to compensate.	No real-time working regime. System reboot acceptable. The impact of system reboot can be compensated.
Life span	15-30 years	2-3 years
Communication protocols	De facto standard industrial networks and business solutions, binary protocols.	Based on open standards.
Working regime	Real time working regime. Bounded delays. Limited tolerance for delays.	"Best effort" model. Delays out of control, variable, commonly accepted.
Characterisation of the system	High complexity of a system. Compatible elements. The internal structure of the system, as well as interaction easy to identify. Implementation and configuration errors are occasional or infrequent.	Very high complexity of the system. Elements of different origins, are incompatible in some parts despite open standards. Complex internal structure of the system. Implementation and configuration errors not unusual.
Awareness of cyberrisks	Low awareness of the threats amongst high-level personnel.	Moderate awareness of the threats amongst high-level personnel.
Risk management	Risk analysis and assessment conducted with recognised methods. Extensive expert knowledge. Professional expertise based on experience remains valid for a long period of time.	Risk analysis and assessment is difficult due to the weakness of the methodologies. Expert knowledge – broadly available, but sectorial and selective. Professional expertise based on experience is subject of rapid outdating (depreciation).
The applied protection measures	Security systems model led after IT systems. Weak security, given modern threat vectors of APTs, interference with the system. Security controls become rapidly outdated (loss of efficacy). Lacks effective security in communication protocols.	Multi-level security system. They become quickly outdated, but are frequently updated. Secured communications. The systems satisfyconfidentiality, integrityand availability requirements.
The security policy	System security policies derived from isolation policy. It fulfils process safety objectives.	It recognises connections with external systems. It is well thought, carefully designed, and highly developed. It is complex but addresses IT security objectives.

parison to the cost of using traditional methods, such as sabotage. At the same time, the propaganda effect can be large, while because of the known difficulties in detecting the source of the attack and establishing fault, the political and criminal penalties for perpetrators are negligible or none. Figure 1 presents a gradation of the effects of cyberattacks.

Various terrestrial and wireless data transmission systems are used in vehicles, machine control systems and the so called smart buildings. Those systems, as well as industrial control systems, have existed so far as disparate and isolated systems. Nowadays, they are being developed increasingly often with the use of open platforms. They interface through the telecommunication enterprise networks and employ communications, which is implemented through the public infrastructure as Intranets. There exist increasingly open environments, including industrial ones, more often with remote access, for example, via frequent updates, etc. The immediate benefits resulting from new functional capabilities often begin to overshadow common sense. Approval for cutting-edge technologies resulting from expected new functional capabilities is connected with the ability to estimate the benefits resulting from the introduction of new solutions. At the same time, it is accompanied by a total lack of ability to assess threats, a habit of making an analysis and assessment of cyber risks, and even an awareness of the risk itself.

Due to the universality of knowledge concerning these systems, their software, and the general availability of tools created for the purpose of conducting targeted cyberattacks which are being developed by professional teams, the threat is considerable and cybercrime is a serious challenge. The cyberattacks often remain unnoticed for several months, until we can see their devastating effects.

There exist two broad types of cyberattacks:

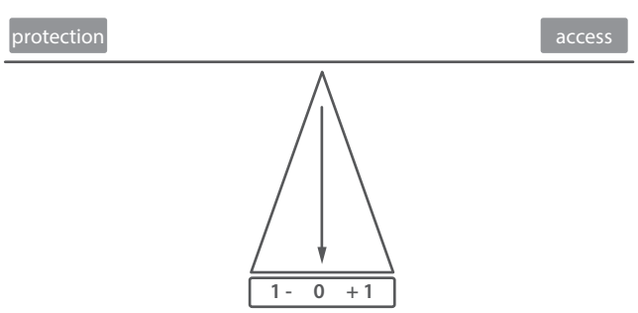
a. The attack causing no harm in physical assets. The main goal of this kind of attack is, among other things, to breach confidence and trust in national authorities, cause social unrest, or reap financial benefits. This kind of cyberattack was carried out against TV5 Monde channel in France on 8-9 April 2015.[3] We can add to this group cyberattacks conducted on banking systems. Generally, these are attacks on ICT systems.

b. The attack aiming at causing harm in physical assets.[4] These are attacks against industrial control systems.

IT systems differ significantly from industrial control systems. Basic similarities and differences are enlisted in Table 1.

It is also important to highlight the differences in how IT and ICS units are located in an organization. Generally, IT has large autonomy. In properly managed organizations, IT units report directly to the Board and employ IT security specialists. ICS departments, on the contrary, are subject to production management and are often scattered over a company. They employ specialists in the field of automation and measurement. The objective of ICS is to maintain operational capabilities of production. These differences cause difficulties in communicating needs which are necessary for the construction of a proper business continuity plan and its effective use. This structure of subordination and divergence of objectives make it more difficult to defend itself against cyberattack.

FIGURE 2. ILLUSTRATION OF THE BALANCE BETWEEN NECESSARY MEASURES FOR THE PROTECTION OF INDUSTRIAL CONTROL SYSTEMS AND ITS ACCESS.



Industrial IT systems constitute business layout, which gathers and processes data from production process, sales and external data coming from sources like: warehouse management, customer relationship management, human resources, finance and accounting, marketing, etc. IT layout is connected with the outside world in many ways. Access can be easily distributed using wireless network or smartphones (the so called BYOD). ICS layout – measurements and control – through transferring current process data outside their own autonomous area, more and more, is being connected to IT layout. It is a physical layout designed to be oriented toward "functionality" rather than "security." It causes a serious threat, and contributes to its vulnerability against cyberattacks.

4. LEGAL STATUS AND CYBERSECURITY STANDARDS

It is very difficult to detect concrete persons responsible for a cyberattack and hold them liable. The attackers very often operate in dispersed groups in different legal systems, and they can be strongly determined. In this case, the most effective way of counterattack is an effective defence which does not decrease significantly the usability of the system. The defence must be based on the principle of "maximum security with reasonable transparency of the access to the system for authorised users."

According to the opinion of the authors of this document, the below documents have the most relevant application in the field of cybersecurity of industrial control systems.

Despite the above-mentioned series of standards, it is worth noticing the other group of norms. The series of norms IEC 62443 provides an integrated environment, which responds to currently known and probable types of vulnerabilities in industrial automation control systems. It includes a wide range of security measures and recommendations for their implementation. The main aim of introducing the IEC 62443 series is to initiate efforts to develop the already functioning, in enterprise, security enhancements to complement security requirements of IT systems and expand them in order to cover the area of industrial automation and to make them internally consistent. It is a matter of fact, that in the environment, one of the most important thing is high availability.

IEC 62443-2-1:2010 defines how to establish a program for the implementation of security systems for ICS. It designates elements, which are necessary to create cyber security management system for ICS (CSMS) and provides guidance for the initial and later development. This is the reason why the norm relates somehow to ISO 31000 which corresponds to risk management, and series of ISO 27000, which describes information security management systems.

3 *ISIS hacks French broadcaster TV5 Monde*, http://www.alphr.com/security/1000604/isis-hacks-french-broadcaster-tv5-monde, [available: 23.08.2016].

4 It is also called *cyber-physical attack*.

TABLE 2. THE MOST IMPORTANT DOCUMENTS IN THE FIELD OF ICS CYBERSECURITY.

Documents with crucial, legal and organisational application in the field of cybersecurity of control systems	
EN ISO 9001;2015	The norm requires, based on the analysis and risk assessment, an approach to quality management which is a reliable balance of opportunities and threats. Currently, cyber risk is perceived as one of the most severe risks, leading to loss of production capacity. Properly developed risk management can effectively and systematically combine the sphere of IT with the area of ICS.
The Directive of the European Parliament and of the Council on providing measures, in order to provide a common high level of network and information security within the European Union.	Annex II includes the list of operators concerned by the Directive, which include, among others, energy and transport.
A series of standards EN IEC 61508 concerning the reliability of electrical and electronic appliances and its software responsible for security.	It is a basic series of standards used widely in the construction of the so-called hardware safety circuits. A cyberattack, carried out against the systems, creates an extremely dangerous situation. At the same time, the working group of the standard included in the document (The 61508 Association, Cyber Security Working Group) recommends to treat a cyberattack as another type of damage, and to identify the probability of the so-called likelihood of a successful cyberattack.

The IEC 62443 standard provides a fairly broad indication of what is included in the industrial automation and control system (IACS). The elements that will be included in an information security management system are: policies and regulations, procedures and best practices, including those relating to personnel, which describe what should be, ultimately, included in safety management system intended to protect automation systems in an organisation.

The IEC 62443 series of norms and accompanying technical documents cover four groups:

1. General plan – concepts and models.
2. Policy and procedures – it defines the rules for establishing and developing the safety program.
3. The system – requirements relating to design process and desired actions.
4. The components – the process of implementation of the system and technical requirements for system's components.

For instance, the main objective of IEC 62443-1-1 is to define security levels for different functionalities of the control system. It includes seven basic criteria: identification and authorisation control (IAC), unified communication (UC), security of integration (SI), data confidentiality (DC), resource description framework (RDF), timing retard elimination (TRE) and resource availability (RA). These seven requirements constitute a base in order to define the levels of security of different functionalities of the system (SL-C).

IEC 62443-1-1 describes the requirements for a proper determination and, subsequently, the implementation of effective and efficient security systems for IACS, while IEC 62443-2-2 includes indications for the requirements relating to the effective use of the security management system.

IEC 62443-3-2 gives an explanation on how to define levels of security encumbered with risk and how to match solutions with proper security functions. IEC 62443-3-3:2013 assumes that a security development program is practiced according to IEC 62443-2-1.

Reliability, contrary to cybersecurity, is a commodity. Reliability can be purchased as a feature of the product. Cybersecurity is a process.

IEC 62443-3-3 gives specific system requirements, which are accredited in seven basic criteria included in the above-mentioned IEC 62443-1-1, along with the identification of requirements for different security levels of the various functions in the control system. The requirements are taken into account during the development and implementation process of the targeted security levels of a control system, in the context of a particular protected resource.

IEC 62443-4-1 describes secondary requirements, which relate to products and solutions. This norm includes the image of system requirements oriented towards subsystems and components of protected system.

It is necessary to distinguish between reliability and cybersecurity. Reliability, contrary to cybersecurity, is a commodity. Reliability can be purchased as a feature of the product. Cybersecurity is a process. This is the reason why there is a need to use tools and methodology corresponding to the rules of process management.

5. THE ANALYSIS OF CYBER RISKS AND THE MOST COMMON WAYS TO CARRY OUT CYBERATTACKS

The analysis of risk is one of the fundamental actions we can take in order to provide an adequate level of cybersecurity. The strategy of risk analysis should be focused, at first, on assessing the nature of a cyberattack and, later, on its classification to one of three groups:

1. Statistical – a random cyberattack. The defence can have a statistical nature which is provided by an antivirus software and a firewall.

2. Semi-statistical – a cyberattack carried out against similar systems or systems with congruous functionalities, for instance, an attack against bank IT systems. Usually, it is not an attack with a specific intention.

3. Hostile – an intentional and purposeful attack causing physical damage.

The hostile attack, conducted against industrial critical infrastructure, can cause the greatest losses, and therefore, the authors of this article claim, that the most significant thing is to focus on defending industrial resources including critical infrastructure.

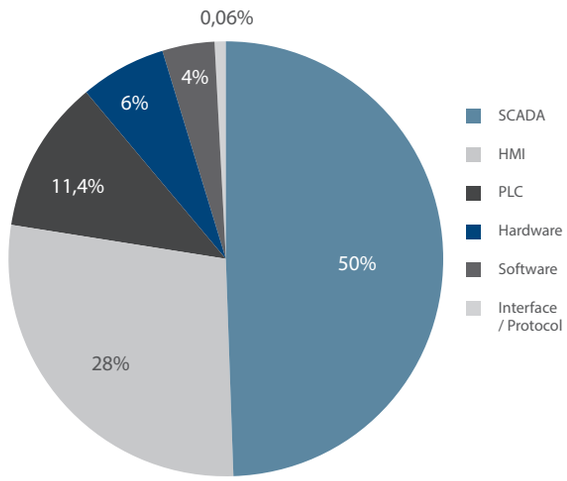
Every risk analysis brings the answer for the following question: "What happened in the past? Why? What are the consequences?" It is necessary to know:

a. The ICS vulnerability to a cyberattack

b. The frequency of attacks on individual elements of the ICS.

The following chart presents the most commonly attacked elements of an ICS.

FIGURE 3. THE MOST COMMONLY ATTACKED ELEMENTS OF INDUSTRIAL CONTROL SYSTEMS AND MEASUREMENTS.
Source 1G. Gritsai et all, *SCADA Safety in numbers*, Positive Technologies 2012, www.ptsecurity.com



In *SCADA Safety in Numbers*, there is a statement of SCADA vulnerability to cyberattacks.[5] The qualitative determinants have been adopted as the scale of vulnerability. According to the following Figure 4, 25% of vulnerabilities are considered critical, and 41% are labelled as high risk.

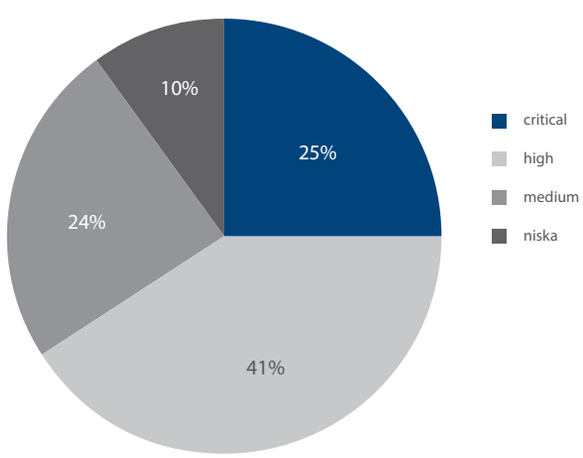
In the analysis of cyber risk there must be two issues taken into consideration: the valuation of actual status and the capabilities of security layouts for:

1. Prevention of cyberattacks.

2. Straightforward defence during a cyberattack.

3. Mitigation and restriction for implications resulting from cyberattacks.

FIGURE 4. VULNERABILITY OF SCADA SYSTEM.
Source 2 G. Gritsai et all, *SCADA Safety in numbers*, Positive Technologies 2012, www.ptsecurity.com



5 G. Gritsai et all, *SCADA Safety in numbers, Positive Technologies* 2012, www.ptsecurity.com.

Cyber risk analysis is a complex process which requires taking into account various functionalities, uncertainties, and events resulting from sources located out of the area of analysis. So far, there is no developed and formalised cyber risk analysis similar to HAZOP, which is commonly used to analyse procedural threats and operational capabilities of industrial installations. The multitude of standards, platforms, models or communication and software techniques used in ICT makes it difficult to develop precise recommendations which would remain relevant despite the progress in IT.

In order to carry out an effective cyberattack, the following conditions must be met:

1. There must be vulnerabilities or weaknesses in the defended system.

2. An attacker needs to have sufficient capabilities to find those weak points.

3. An attacker needs to believe that attack will bring him benefits.

4. The expected benefits drive motivation.

While taking into consideration the first condition, the success of a cyberattack does not depend on the attacker. It is determined by the action or inaction of the attacked actor. Conditions 2, 3 and 4 depend on the attacker, however the defender may provoke an attack. It is necessary for the defence to take into account that there may be more than one attacker in a given moment, and the attack can be low and slow.

Cyber risk analysis is a complex process which requires taking into account various functionalities, uncertainties, and events resulting from sources located out of the area of analysis.

Unfortunately, most cyberattacks are not reported to authorities, which increases the motivation of groups conducting hostile attacks. According to the British Columbia Institute of Technology, only 30% of industrial cyberattacks are reported. Of this group, nearly 50% of reports deal with losses of more than $ 1 million. Most of victims face difficulties in estimating losses.[6]

In a majority of cases, a cyberattack is carried out along the following scheme. An attacker finds gaps in an IT system or firewall, they penetrate the IT system and embed malicious software enabling them to conduct further actions. The main aim of this action is to provoke the effect of propagation, which is getting access to the ICS. In order to fulfil this aim, there are several techniques of profiling a victim, for instance an employee of a company, via social and professional media. An attack is conducted using techniques based on sociological grounds (so called social engineering). From time to time, attackers use the effect of victims' disorientation by sending, previously hoaxed, dedicated message containing a malicious code, like in the spear phishing method.

After gaining access to the ICS, the attacker needs to achieve the so-called disinformation effect. This is based on the manipulation of process data in order to cause an industrial catastrophe or stop the production process (loss in physical assets) in an unnoticed way (blinding), at least for the operator.[7]

Cyberattacks can be conducted also through smartphones.[8] Applications and mobile devices with low security levels can be attacked according to the following scheme – a hacker overcomes the firewall and gains access to the computer workstation. The computer workstation identifies the hacker as a registered user and permits them to exchange information. The hacker gains access to control system and downloads and sends data to the ICS. From this point, the hacker already has the access to critical data and may cause damage to the system.

6. ELEMENTS OF EFFECTIVE SECURITY MEASURES IN THE INDUSTRIAL CONTROL SYSTEMS

Providing security to industrial control and measurement systems against cyberattacks should be based on three pillars. The first one is having a proper corporate architecture in terms of management of cybersecurity in IT systems. The second is a corporate architecture for ICS together with its components and the contact areas with the corporate IT system. It has to be as resistant to cyberattacks as possible. The third pillar is anon-line diagnostics system for identifying cyberattacks and system damages.

Cyberattacks can be conducted also through smartphones.

6 British Columbia Institute of Technology, op.cit…

7 The above-mentioned scheme is described in detail in Kozak A. „European Cybersecurity Journal" vol. 2 issue 4, practical aspect is presented below, while elaborating the case study.

8 The scheme of attack was described in – „Control Engineering Polska", No 4 (120), July/August 2016, p. 80.

6.1. PROTECTION OF IT SYSTEMS

A methodology of protection of the critical infrastructure telecommunication (OKIT[9]) developed in Poland specifies the method for properly implementing a telecommunication safety system in enterprises using installations and systems considered important for the functioning and safety of the economy. The methodology specifies the rules of conduct of ICT systems which support the functioning of critical infrastructures, and assist the people responsible for safety in making decisions, planning and taking decisions connected with the building or modernisation of the ICT safety system. The support particularly concerns itself with questions which require a coordinated use of experts' knowledge in the field and their mutual decision making while performing risk assessments, choosing the right protections, implementing the protections and monitoring the effects of implementation. The methodology has its use both in enterprises which are just thinking of implementing a safety system, as well as in those where it is already implemented and requires a verification whether it meets the requirements in terms of information protection and the needs for protection of systems responsible for transmission, processing and storing of information. The methodology was developed in the Department of Telecommunications at the AGH-UST University of Science and Technology in Krakow. Its important feature is its focus on business needs which means pursuing to fulfil the requirements, including continuity of action as well as implementation of mechanisms, which identify the important and urgent needs in terms of security, their prioritisation, and to choose a solution based on a specific scenario with the possibility to justify the decision making process. The methodology covers six thematic areas: management of the ICT safety system implementation, risk assessment, risk analysis, response to main risks, management of protection implementation, as well as continuous monitoring of the effects of the implementation for an evaluation of the effectivity of the implementations, and an operative monitoring. It refers to standards and norms in terms of ISO and NIST security, and emphasises the value of corporate architecture as an important source of information about the company. The corporate architecture of a company provides key knowledge for performing a proper risk assessment and analysis in order to determine the real needs in terms of protection.

9 P. Pacyna, N. Rapacz, T. Chmielecki, P. Chołda, P. Potrawka, R. Stankiewicz, P. Wydrych, A. Pach, *OKIT. Metodyka ochrony teleinformacyjnych infrastruktur krytycznych*, Wyd. PWN, 2013.

6.2. THE ARCHITECTURE OF INDUSTRIAL CONTROL SYSTEMS

The architecture of ICS is built in a few steps. Step one is to choose the norms, standards, and good engineering practices. In this context, it is good to build it on a complex system of American standards, e.g., NIST 800. The second step is to determine the required level of SAL (Safety Assurance Level) cybersecurity according to IEC 62443-1-1. The next step is to choose the components and to build the ICS. The final step is an analysis of the outcomes and verification of the results of the work. In enterprises managed by critical infrastructure containing the ICS, it is common to use various ICT systems which serve to transmit, process and store information. Connections between the critical infrastructure and ICT systems are becoming significant enough that it can be stated that the protection of the continuity of the action of the infrastructure depends on the resilience to cyber threats also of the IT systems. In the face of that, the cybersecurity of industrial installations mentioned in the title is expanded by the issue considered, until now, as a separate topic – the security of IT systems. Focusing on both of these areas, ICS and IT, helps for a proper management of the cyber risks.

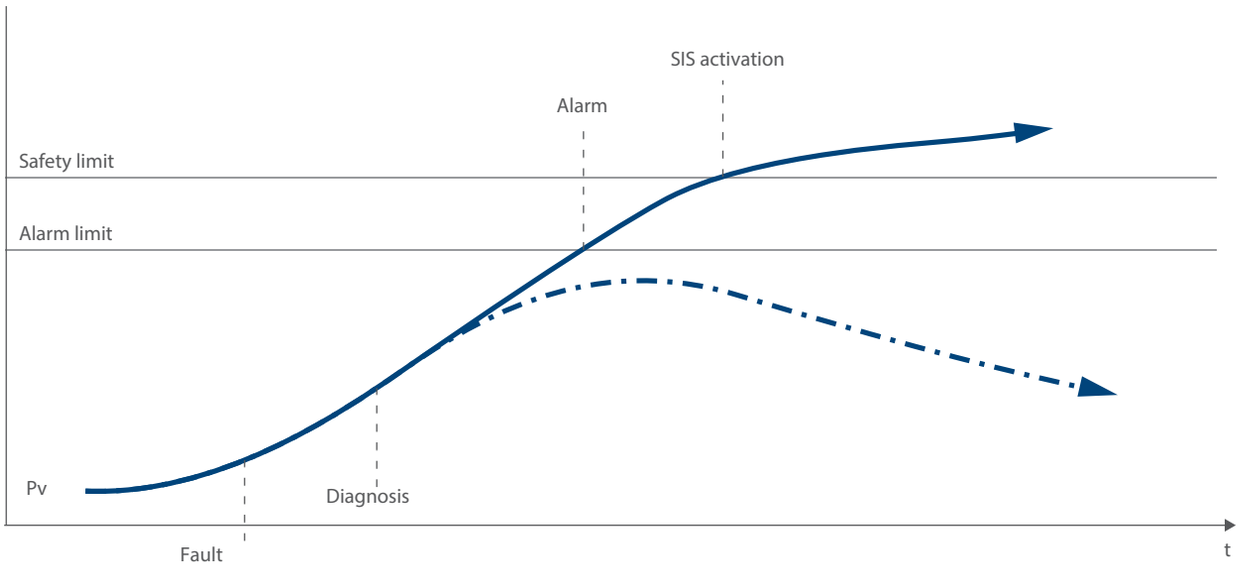
Focusing on both of these areas, ICS and IT, helps for a proper management of the cyber risks.

6.3 ADVANCED ON-LINE DIAGNOSTICS OF THE PROCESS AND CONTROL SYSTEM – IDENTIFYING CYBERATTACKS AND FAULTS

Both faults and cyberattacks carried out from outside and inside are manifested by various changes in the functioning of the process and control systems, differing from their original condition. In automatic control systems of the industrial processes (SCADA, DCS), and also in SIS security systems, an alarm system (AS) is used to identify irregular and emergency conditions. The main disadvantage of an AS is the excess of generated alarms. According to the EEMUA database, the average daily number of alarms in the petrochemical industry is around 1500 and in the power industry around 2000, while, according to the recommendations, it should not exceed 144. Other disadvantages of an AS are substantial delays in the detection of faulty symptoms. Furthermore, the symptoms can be masked or corrected by the control loops. These disadvantages are a result of using a simple limit check to detect the emergency conditions. An AS does not provide any reference about the causes of alarms. This task is assigned to the process operators.

Interpretation of such a large number of alarms appearing in a short period of time causes a serious problem for the

FIGURE 5. EXEMPLARY TREND OF A PROCESS VARIABLE IN A SYSTEM WITH AND WITHOUT DIAGNOSTICS.



operators. An information overload phenomenon occurs in this situation, which then leads to stress. In these conditions, the operators are not able to formulate a correct diagnosis, i.e., to identify the threats. It increases the likelihood of incorrect protective reactions and their results, cumulating with the previously occurring faults, may cause serious malfunction. A mechanism of such a negative (positively charged) feedback was the cause of numerous serious emergencies in nuclear and conventional power plants, and in chemical plants (among the others an explosion in Texaco's Milford Haven refinery in 1994). Furthermore, if a cyberattack is the reason for the control system's malfunction, then an intervention in the control system may change the manner in which the alarm system operates in such a way as to hide from the operator the symptoms of an attack.

An effective recognition of threats (damages, attacks) in control systems requires the use of advanced diagnostics of the process and control system itself, carried out in real time.

An effective recognition of threats (damages, attacks) in control systems requires the use of advanced diagnostics of the process and control system itself, carried out in real time.[10] Damage or attack detection consists of an early discovery of a discrepancy between the current and the referential functioning, represented by quantitative and qualitative models defining the normal condition of the process. Methods of detection based on models help for an earlier damage/attack detection[11] The conclusions concerning the reasons of observed discrepancies (damages, cyberattacks) are conducted on the basis of observed diagnostic signals, which constitute detection algorithm outputs and information included in system databases relating to relations between symptoms and possible threats.[12] A clear process is shown on Figure 5. A diagnosis is the result of automatic reasoning, i.e., a hypothesis about the damage or attack that occurred. Based on hypotheses, a system can also aid the operators by giving them operating instructions in case of an emergency. Thanks to it, they will be able to make fast and effective protective decisions. They should bring the process back to its normal condition. As a result, the safety integrated system is not activated and, thereby, the technological process is neither partially nor entirely stopped. In this way, we avoid major economic losses.

Damage or attack detection consists of early discovery of discrepancy between the current and the referential functioning.

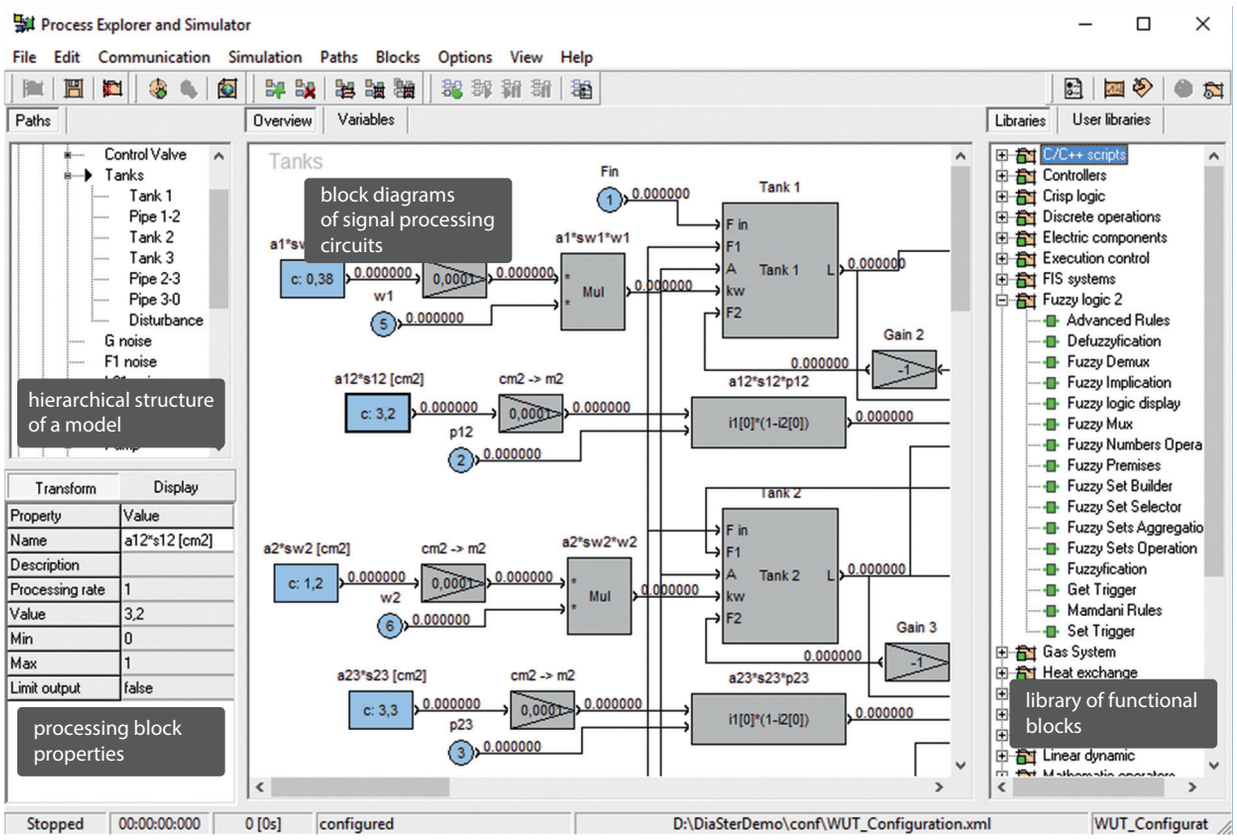
Therefore, we can state that reducing risk in terms of *safety* as well as *security* can be achieved by the use of an advanced system of on-line diagnostics of the process including the components of the process and the control system with measuring equipment and actuators. Such a system, along with the operators' interventions, creates an

10 More: J.M. Kościelny, *Diagnostyka zautomatyzowanych procesów przemysłowych*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2001 (1-418);

11 J. Korbicz, J.M. Kościelny, Z. Kowalczuk, W. Cholewa (ed)., *Fault Diagnosis. Models, artificial intelligence, application, Springer*, 2004, (1-920),

12 J. Korbicz, J.M. Kościelny (ed), *Modeling, Diagnostics and Process Control. Implementation in the DiaSter System*, Springer, 2010, (1-384).

FIGURE 6. PROCESSING MODULE OF PROCESS VARIABLES IN THE FORM OF USER-DEFINED SIGNAL PROCESSING PATHS.



additional protective layer in terms of *safety*.[13] Moreover, the diagnostics system constitutes the last layer where cyberattacks, including sabotage attacks, are possible to be detected if they go through all the other protective layers. Therefore, it makes it possible to reduce the risk in terms of *security*.

The Institute of Automatic Control and Robotics of the Warsaw University of Technology is currently working on a Cyber-Fault-DIAG system – an advanced diagnostic of cyberattacks and damages. This system is intended to be used in the power, chemical, pharmaceutical, steel, food industries and many others. The base for the new system is the experience gained while creating and implementing the advanced systems of diagnostics of damages: DiaSter, AMandD, DIAG, and OSA. The Cyber-Fault-DIAG system will be available either in a full version or in reduced ones assigned either to detect the cyberrisk – Cyber-DIAG, or to detect and isolate the faults – Fault-DIAG.

13 J.M. Kościelny, M. Bartyś, *The Requirements for a New Layer in the Industrial Safety Systems*, 9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SafeProcess 2015, Paris, France, September 2-4, 2015, Volume: 1333-1338, http://www.ifac-papersonline.net/, [available: 06.09.2016].

It is adapted to work with various distributed control systems (DCS) as well as supervisory control and data acquisition systems (SCADA). The diagnostic system receives the measuring process data through digital transmission from the control systems (ICS, SIS), PLC and directly from measuring devices. Usually, the communication is unidirectional – from the measuring and control system to the diagnostic system.

Operating principle of the system, in a nutshell, comes down to:

- monitoring the process and the process control system;
- analysing the available values of the process variables and the control signals in order to validate the operation of control algorithms and the process itself;
- decision making to leave the process in a safe condition;
- identifying the cyberattacks or faults.

In the case of a discrepancy between the normal condition and the observed one, an alarm is sounded and countermeasures are suggested if needed.

The main task of the system is the realisation of advanced functions of the damage and cyberattack diagnostics. The

methods used in order to detect attacks or damages based on qualitative and quantitative models: analytical, neuronal, fuzzy, statistical, as well as heuristic using different relations between the process' variables. Diagnostics reasoning is carried out with the use of a fuzzy logic, according to the optimal method developed in the Institute of Automatic Control and Robotics of the Warsaw University of Technology. Furthermore, the system will be equipped with advanced tools to process the process variables (Figure 6) and to build models needed for on-line diagnostics. The system will be a unique solution on a world scale, including the implementation of a wide range of cutting-edge algorithms in the realm of smart computations used in a software intended for modelling, identification of cyberattacks, detection and isolation of damages. The Cyber-Fault-DIAG system, thanks to its open architecture, can be connected to virtually any automatic control system. Simultaneously, remaining completely independent from control systems, it constitutes a new, unique protective layer against cyberattacks. It is unique because it is neither an IT security system, therefore not known to hackers, nor anICS, therefore not known to automatics, and which, according to experts, will be an industrial standard in the near future.

7. INSURANCE FROM THE CONSEQUENCES AND REPERCUSSIONS OF CYBERATTACKS

While analysing the last decade in the world and in Poland, we notice an increased number of cyberattacks on firms in all industrysectors. Given the possibility of cyberattacks causing huge financial losses and disturbing processes in production companies, industrial automation and control sectors become the centre of interest for cybercrime and cyberterrorism. Insurance companies have noticed a rise of interest in buying security policies which compensate the potential damages connected to loss and display of a company's or client's sensitive data. On the world market, insurers have been offering such protection for many years now. In Poland, the development of security policies in terms of "cyber risk" is still only in its initial phase. However, the observed interest of potential clients in this kind of protection indicates the need for a rapid progress of insurance companies in this subject. Unfortunately, among insurance companies, a subject of security of industrial installations' control systems is still rarely ever mentioned, even though the consequences of an unauthorised access (attack) could be much more crucial than in the case of data loss. PZU LAB, together with external partners, has started research and development (R&D) work in terms of creating a new product, i.e., policies from the effects of a cyberattack on an ICS. The work started with the creation of a methodology for analysing cyber risks, dedicated to industrial customers. Thanks to this methodology, new equipment will be created to aid Polish enterprises in managing cyber risks and, therefore, increase their level of security in functioning.

The development of technology and the Internet creates many new cyber risks which were not known in the recent past, regardless the industry and the size of a firm. The scale of outcomes of a cyberattack ranges from the loss or sale of information, the loss of one's reputation due to a terrorist attack, the damage or destruction of a property (fire, explosion, etc.), or even casualties. That is why we should look into the complex nature of a cyber risk and consider transferring risks onto an insurance company in terms of:

- Cyberterrorism in an industrial area;
- Enemy taking control over decision-making centre, e.g., control system over industrial processes;
- Loss of or damage to technical information, e.g., control system's data base;
- Data leak (trade or personal, with confidentiality clauses);
- Income loss due to a cyberattack;
- Additional expenses to deal with cyberattacks;
- Loss of reputation;
- Expenses connected to bringing the company back to work after a cyberattack.

We should look into the complex nature of a cyber risk and consider transferring risk onto an insurance company.

It is important to highlight that making decisions in terms of insurance protection should be preceded by an in-depth analysis of the risk in order to identify the threats coming from cyber risks. In Poland, there are entities being founded that specialise in this field of expertise. Also, insurance companies notice the weight of the issue and they are creating their own specialty units which support their clients with analysing cyber risks. The development of this kind of added values offered by insurers on a big scale will, most likely, occur in the coming years. External experts and insurers' specialists will be the professional support, and they will share insight on the company's susceptibility to cyberrisk, make analyses, suggest appropriate protection and solutions, and suggest a correct security package, as well as help during liquidation in case of damages.

On the global insurance market, there are modular insuring packages in terms of cyber risks which provide a wide actuarial protection and will protect the entrepreneur in case of compensation claims connected to losses, damages, leakage and the disclosure of information. Within these packages, there are protections available in case of the necessity to cover various expenses like: technical experts, the recovery of data and rebuilding the image of the company.

Providing ICT security requires a team for organisational and technical actions designed to minimise the risk of disturbing functioning and the risk of unauthorised action on systems, ICT networks and the control and measurement instruments.

Cybersecurity of industrial systems and the quick development of technology seem to be favourable towards cybercriminals and state entities specialised in attacks on other country's infrastructure. Particular attention must be paid while dealing with critical data and ensuring its protection, especially in the age of terrorism. Data loss is connected to huge potential losses – trust of business partners and the firm's reputation. Cybersecurity is one of the company's elements of defence, therefore it is recommended to assume the defence in depth strategy. Correct countermeasures require the definition and research of the ICT environment on all of its layers, with the highest one being the classic IT systems and the lowest one being control and measurement instruments and actuators which have an effect on the technological processes.

Any risk analysis conducted by the insurer's experts should, therefore, include an analysis of all three fields of activity of the insured company which is connected to cybersecurity.

1. Business activity – covers mainly the analysis of the corporate architecture. Thereby, it mostly seeks answers to the questions: who, why, in what scope and in which place does someone have access to a particular equipment or to a particular piece of information.
2. Operational activity – a review of the ICS drafts, the meeting points with the IT layer and looking for system's weak points to cyberattacks.
3. Technical activity – the manners and methods of an active and well-organised cyberdefence.

8. DIRECTIONS OF IMPROVING THE INDUSTRY'S RESILIENCE TO CYBERATTACKS

The large number of chemical installations worldwide and their great economic significance make the chemical industry particularly vulnerable to terrorist attacks, including cyberattacks. As a result of a cyberattack, the release of toxic chemicals or stoppage of flow of chemicals (reagents) to other industries would have serious health, social, economic and ecological repercussions.

8.1. IMPLEMENTATION OF CYBERSECURITY POLICIES IN THE EU AND THE US

Countermeasures against cyberattacks on industrial installations, including chemical ones, should be an element of a wide strategy which incorporate co-operation with all potential stakeholders. The EU has not developed a system to protect industries from cyberattacks. It is, in a way, the result of a legal situation since internal security, which includes the subject of cybersecurity, remain within the national competence. EU programmes are divided into two categories: "criminal" and "prevention-care." They are regulated by different articles from the Treaty of the European Union and they remain within the competences of different Directorates. Therefore, the implementation of a single decision-making centre against industrial cyberattack on an EU scale is virtually impossible.

Countermeasures against cyberattacks on industrial installations, including chemical ones, should be an element of a wide strategy which incorporate co-operation with all potential stakeholders.

Until now, United States has developed complex programmes and entire security systems against terrorism which include cybersecurity. In the US, a key focus is assigned to the securityof chemical installations. They have implemented Chemical Facility Anti-Terrorism Standards.[14] The US Department of Homeland Security plays the role of a central supervisory authority over the above-mentioned regulations which include also the cybersecurity of industrial installations. The advantage of the American approach is in linking of the subjects of cybersecurity in the industrial sector, counteracting against terrorism, and providing the Department of Homeland Security with the role as a control centre. Furthermore, US legal regulations include both the aspects of physical security and the strengthening of prevention. This requires, inter alia, the implementation of ICS security in the facilities which, after a review, are assigned to the risk group. The American system is built on close co-operation between state agencies and organisations which represent the consumers of the chemical industry and the industry itself, which foundation is the exchange of information.

8.2. CO-OPERATION IN COUNTERACTING THE CYBERATTACKS IN THE POLISH INDUSTRY

In Poland, there were actions taken on the state level to regulate the growing threat of cyberattacks onto industrial installations. We do not have a centre which coordinates

14 Chemical Facility Anti-Terrorism Standards, Risk-Based Performance Standards Guidance – US DHS, May 2009.

measures against such threats. Such measures were not undertaken by industrial organisations either. We meet cyberterrorism threats with an approach similar to the case of terrorism. We concentrate mainly on physical security and the management of critical situations, i.e. on actions after the incident. This is accompanied by a rather low priority of cybersecurity in industry which is the result of a lack of awareness of the real threat.

The International Centre for Chemical Safety and Security (ICCSS) is planning to develop a partnership to strengthen cybersecurity in Polish industries. It would focus on gathering and sharing the most recent knowledge in terms of procedures, technical solutions and trainings. We want to connect the subject of automation with the subjects of the security of access and corporate architecture. We will share the best solutions in the world using broad international contacts and partnerships. The ICCSS closely co-operates with the US Department of Homeland Security. The ICCSS notices growing needs to implement comprehensive solutions in the area of cybersecurity within Polish industries. The currently used commercial solutions offered by providers of automation systems are not only expensive, but they also prove to be insufficient at ensuring the complete security of a company. A very common mistake is to focus too much on technical matters and underappreciate the importance of the corporate structure, implementation of adequate procedures and relevant training courses.

8.3. ROADMAP FOR RAISING CYBERSECURITY AWARENESS AND RESPONSIBILITY AMONG CHEMICAL INDUSTRY STAKEHOLDERS

In view of the analysis of existing national and international experiences, it is proposed to take active actions towards the creation of a cooperative model between all the stakeholders in the chemical industry, including chemical critical infrastructure. They would include raising awareness of the threats coming from cyberattacks, and implementing effective technical solutions. Such an initiative would constitute a specific kind of roadmap. State agencies, producers and users of the chemical industry including industry associations, economic chambers and social organisations should be partners of this roadmap. The roadmap would be founded on the development of a system of information exchange about threats, as well as a platform for co-operation among all the participants. The initiative of a roadmap for raising cybersecurity awareness and sharing responsibility among users of the chemical industry could be a part of the Polish nationwide program – Local Awareness and Responsibility in Chemical Safety and Security. The main aim of the program is to support local public authorities and private actors to overcome challenges connected with the increasing use of chemicals and easy access to hazardous substances, on the local stage, in terms of production, storage, railway and road transportation of hazardous substances, including chemical compounds, sources of energy and wastes, following the requirements of environmental protection and chemical security. Within this roadmap, a Working Group should function to support the program's implementation with the participation of government, the private sector, industry, civil society and the media. The core objective of the roadmap would be to create a cybersecurity culture. The leading assumption of the roadmap is a statement that the traditional crisis responses are insufficient to battle the challenges resulting from accidents and catastrophes caused by cyberattacks. In order to battle potential cyberthreats, we need co-operation between all entities (a community commitment).

Industrial producers and organisations should have the knowledge and adequate security systems against cyberattacks on industrial systems. The community should participate in the dialogue on the subject of the existing resources and requirements which should be met in order to counteract potential cyberthreats and minimise potential losses.

The Working Group should develop draft standards, guides for good engineering practices, training tips and materials on cybersecurity in the chemical industry.

9. SUMMARY

Cybersecurity is one of the elements of a wide, holistic understanding of "safety and security" in an industry. A satisfactory result can be achieved by implementing these three actions: a proper corporate architecture, the right structure of IT and ICS networks, and an appropriate level of ICS security to potential threats. Such an approach means, inter alia, the continuous monitoring of and reacting to cyber incidents, the documenting of incidents and quick decision making in terms of improvement activities.

1. Cybersecurity is a process and it requires a process-oriented approach, as well as a continuous improvement of the defence system. Risk assessments and analyses enable the evaluation of the influence of undesired incidents on a security system and the assessment of potential damages. This, in turn, is a foundation for protective recommendations.

2. The cybersecurity of "non-computer" systems and circuits should play an essential role as early as the beginning of the designing process of the product . A user of a "non-computer" device like a car, a machine tool with numerical controls, or a tenant in an intelligent building has a negligible chance to defend himself from a cyberattack.

3. We should endeavour to standardise the techniques of analysing cyber risks for ICS and "non-computer" systems.

4. It will be particularly important to provide a high level of cybersecurity for the "Industry 4.0" project – a fourth industry revolution.

5. The advanced on-line diagnostics of damages or cyberthreats in an ICS will be one of the key elements of a solution in the "Industry 4.0." It makes it possible to reduce the risk in ICS connected with cyberthreats. The diagnostics system constitutes the last layer where cyberattacks can be detected if they go through all the other protective layers.

6. The market of insurance policies against the consequences and repercussions of a cyberattack may bring the desired effect in the form of an improvement of industry installations' resilience to cyberattacks and the increase in the level of cybersecurity. Transferring cyber risk to insurance companies will help to compensate the losses caused by a successful cyberattack.

7. A central location for gathering data and monitoring cyber incidents is indispensable, particularly in chemical, petrochemical, power and gas industries. It should also facilitate a flow of information between the institutions involved in cybersecurity.

8. The actions taken within the proposed roadmap to increase awareness of threats of cyberattacks in chemical sector and chemical infrastructure, should be a subject of a wide promotion at the international arena. They should be furthered within the of the development of the Polish specialty worldwide in the area of chemical safety and security, and global summit of chemical safety and security – CHEMSS.

LIST OF ABBREVIATIONS

AS – Alarm System
BYOD – Bring Your Own Device
DCS – Distributed Control System
IACS – Industrial Automation Control System
ICS – Industrial Control System
IT – Information Technology
SCADA – Supervisory Control and Data Acquisition
SIL – Safety Integrity Level
SIS – Safety Integrity System
VLAN – Virtual Local Area Network
WLAN – Wireless Local Area Network

ABOUT THE AUTHORS

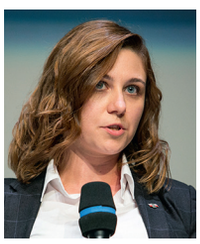
Dr eng. Dariusz Gołębiewski has a graduate degree in automatics. He received his PhD in risk modelling of power engineering facilities from the Gdansk University of Technology. His research and publications deal with critical infrastructure insurance and risk management. He was responsible for risk engineering at PZU. He is the founder and director of risk engineering and industry partnership development at PZU LAB.

Prof. dr hab. eng. Jan M. Kościelny, a Full Professor at the Institute of Automatic Control and Robotics, Warsaw University of Technology. His research interests include the fields of fault diagnosis of Industrial Processes and fault tolerant control systems. He is a member of the Committee of Automatics and Robotics of the Polish Academy of Sciences, Technical Committee TC 6.4: Fault Detection, Supervision, and the Safety of Technical Processes of International Federation of Automatic Control.

Dr eng. Andrzej Kozak does work for the Office of Technical Inspection in Warsaw, Poland. Currently he holds an advisory position to the President of the Office and he specializes in the cybersecurity of industrial control systems. He also is a senior lecturer at the Technical University of Lodz. He graduated from Chemical and Process Engineering of the Cracow University of Technology. He developed further interest in the process engineering, performed research and achieved a PhD degree from the Polish Academy of Sciences. He also is Certified Reliability Professional (CRP). In summery, Dr Kozak has more than 35 years' experience in the safety process industry and safety and security management.

Dr eng. Piotr Pacyna is a professor at AGH University of Science and Technology. His research activities focus on complex systems and security. Piotr was active in R&D projects in the 5th, 6th and 7th EU FP projects as a researcher and project manager. In Polish R&D projects he authored an OKIT methodology, which recognises the value of enterprise architecture in security management. Piotr was a visiting professor at Universidad Carlos III in Spain. He contributed to the International Telecommunications Union (ITU-T). Piotr is a certified PRINCE2 Practitioner and Approved Trainer on project management and TOGAF 9 Certified (Level 2) on enterprise architecture and IT governance.

Amb. Krzysztof Paturej, President of the Board of the International Centre for Chemical Safety and Security, Warsaw, Poland (www.iccss.eu), a career diplomat. Amb. Paturej has international standing in multilateral diplomacy, negotiations, disarmament, and he has vast experience in multicultural relations, development programmes, relations with industry and public society, and risk management strategies. He chaired many international meetings, including, most recently, the Global Summit on Chemical Safety and Security (ww.chemss2016.org) in Kielce, Poland, on 18-20 April, 2016.



Dr Joanna Świątkowska is the Programme Director of the European Cybersecurity Forum, the Chief Editor of the European Cybersecurity Journal and Senior Research Fellow of the Kosciuszko Institute. She is a member of the Advisory Group for Cybersecurity of the Republic of Poland working within the Polish Presidential National Bureau of Security. She has been involved in numerous high profiled national and international cybersecurity initiatives.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is an independent and non-governmental research institute founded in 2000 as a non-profit organization. It closely cooperates with Polish and European scientists, administration representatives and experienced practitioners involved in public and socio-economic activity.

The mission of the KI is to contribute to the socio-economic development and security of Poland and Europe. It strives to be a leader of positive changes, creating and promoting the best solutions for Poland and Europe, as well as for neighboring countries that are now in the process of building states based on the rule of law, civil society and a free market economy.

Krakow office: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: ik@ik.org.pl

More information and comments: Joanna Świątkowska – joanna.swiatkowska@ik.org.pl – tel. +48 515 174 389