Final Scientific Programme
G5744 ARW: “Cybersecurity of Industrial Control Systems (ICS)”

List of Abstracts

No.	Authors	Title	Abstract
1	**R. Alguliev**	**Some actual problems of the formation and comprehensive security of cyber-physical systems in Azerbaijan**	Issues of creating cyber physical systems (CPSs) in various spheres in Azerbaijan under the influence of the 4th industrial revolution is being considered. In this regard, some actual scientific and practical problems and their conceptual solutions for ensuring the smart security of critical CPSs are outlined.
2	**G. Sadovsky**	**Computer and Network Security in an Increasingly Complex World**	The talk reviews the highlights of computer and Internet security and the implications for industrial control systems. I discuss the growth of the cybercrime industry, the components of incident and security attack surfaces, our urrent situation and how we are responding to it, and some special considerations that are introduced by physically dispersed industrial control systems
3	**M. Maj**	**Cyber fortress - cybersecurity simulation game.**	Cyber Fortress is a strategic simulation game in cybersecurity area. The main idea and the task during the game is to build the best cybersecurity system to prevent players' organizations against the most likely threats and to effectively react during the incident mitigation phase. Game is a perfect tool for building cross-cutting skills and team communication. It allows choice and testing different strategies and tailor cybersecurity budget to organization needs and specificity.
4	**K. Szefler**	**Cybersecurity threat scenario for a hypothetical nuclear power plant facility.**	The presentation will guide the viewers through each step of the attack scenario taking place in a hypothetical nuclear power plant facility. The attack utilises an exploit for a programmable logic controller found by our cybersecurity laboratory. It disturbs a connection to the PLC and as it will be shown in the presentation, execution of it could have negative effect on the operation of the plant. Tedious task of an adversary to hack into the plant has been mapped to the MITRE ATT&ACK® framework to provide formalized description of the employed tactics and techniques. The standardized scenario creates an excellent tool for both awareness and technical education.
5	**K. Waedt**	**Cybersecurity Education Programme & Laboratories - Joint Industry and Universities Cooperation**	The presentation will address some of the cybersecurity training programmes related to the R&D projects SMARTEST ("smart" model based security testing), ABAC (Attribute Based Access Control) and SMARTEST2 but also cybersecurity trainings that are proposed by Framatome GmbH and have also been provided in other countries. These trainings target different staff from industry, e.g. (1) line/project management and marketing/quality assurance for trainings of one to three days, (2) technical staff specific trainings, related to cybersecurity of Safety and Operational I&C and Electrical Power Systems (EPS) or (3) trainings for cybersecurity staff working at NPP sites or at utility headquarters.

6	**B. Jerman-Blažič**	**The overall web security and the presence of vulnerabilities in the web spaces of 30 European countries**	The presented study explore at large the state of the security of the web space over all Internet, but the main focus is to reveal what are the real factors that shape the level of web security in particular country population. The web space of 30 European countries is explored and compared regarding the identified factors that influence on the presence of number of web vulnerabilities and higher level of insecurity of the whole space. A specific platform for scanning and inspecting the web sites all over the internet was designed and applied by respecting the ethical rules for scanning web servers. Basic innovative properties of the vulnerability scanning tool Vulnet are described. Collected data with the Vulnet tool are processed and the web pages are classified according to the level of present vulnerabilities based on calculated scores that consider both the server core web version and the plug-ins vulnerability. The studied web space shows different level of web security which is related to the pace of digital advancement. Running WCMS in web site is a positive risk factor for the presence of higher vulnerability and insecurity, the presence of plug-ins is a also a risk factor for a higher insecurity. Higher level of digital skills within a country's population is a negative factor for web insecurity, lower price for internet access as a measure of the internet affordability is a negative factor for web insecurity. The briefly presented methodology is an original result from own development and is based on inclusion of original solutions that enable large Internet scanning in relatively short period of time. The study of 30 European countries and their web spaces regarding the state of the security and the identified dependences from different factors is an original and is unique in that respect in the known literature.
7	**O. Illiashenko; V. Kharchenko**	**Theoretical and practical issues of security management systems in the context of Industry 4.0.**	The methodology of analysing integrated security management system considering features of manufacture industry 4.0 is discussed. The following aspects security and safety (S&S) model are taken into account: (a) level of technologies (information, operation, ecological), kinds of S&S (physical security, information and cybersecurity, functional and ecological safety). The structure of multilevel S&S management systems with separate channels of monitoring, control and joint support of decision making is analysed. Industrial cases are discussed.
8	**M. Mammadova; Z. Jabrayilova**	**Architecture of an intelligent health and safety management system for workers employed on offshore oil and gas platforms**	Oil and gas companies have an urgent need for technologies that provide real-time complete and reliable information about the actual state of health and safety of personnel. The concept based on IoT and e-health solutions for the development of a system of continuous remote monitoring of safety and health of employees simultaneously linking them to the context of the environment is proposed. The architecture of a three-level geographically distributed intelligent health management system for workers on remote offshore oil and gas platforms has been developed.

9	**T. Mammadov**	**New cyber realities in securing Critical Information Infrastructures**	As its observed global pandemic brought new realities with it. As most of the people started to work online it observed with two main issues: In one hand fast growing online platforms, markets and so on technical solutions in other hand spreading out cybersecurity and feeling it almost in our daily life. Having less time to adapt new technologies and security rules people who started to work online and connect secure network from a non-secure network also became a thread for the sensitive networks. So, pandemic realities brought new cyber realities in securing and managing networks in critical information infrastructures. And this reality brought a new risk which haven't measured and considered before. Taking into account all new realities, critical information infrastructures, their identification and evaluation models, security issues of these infrastructures, as well as the segregation of critical infrastructures by degree of importance requiring a comprehensive and new approach. Our presentation is about the need of the "update" classic approach to cybersecurity in critical infrastructures taking into account new risks and threats.
10	**S. Mahmudova**	**Development of an intelligent software system to ensure cyber security through ontology.**	This study reviews software security, etc. It studies the methods for the analysis of software security. The problems of software protection are identified. The risks for software projects, their management, determination and categories are studied. Software development process includes the construction of an agreed structure for software development. The article describes the ontology of cybersecurity based on standards. The main concepts related to cybersecurity problem and their relationships are reviewed. It studies basic structure, concept, etc. of intelligent software system to ensure cybersecurity
11	**M. Hashimov**	**Personal data security problems in smart city environment.**	The concept of smart city is considered as a promising solution to provide effective services to citizens through information and communication technologies. However, the data sensed through various devices when using smart city services poses problems for the security of citizens personal data. To this end, the article analyzes the issues of personal data security in the smart city environment and presents suggestions to solve them to some extent.
12	**V. Kharchenko; H. Fesenko; I. Kliushnikov**	**UAV fleet based monitoring of critical infrastructure objects: planning of application considering failures and cyberattacks.**	The structure and tasks of systems for monitoring of pre- and post-accidents of critical infrastructure objects (SMA CIO) such as a NPP based on UAV fleet (UAVF) are discussed. The matrics for planning of UAVF application, dependability modelling and assessment considering failures and cyberattacks on Internet of Drones resources are described. The results of development and research of UAVF and SMA dependability models analysed. Case study for NPP SMA are discussed.
13	**F. Abdullayeva**	**Cybersecurity issues of some class Unmanned Aerial Vehicle systems: A survey.**	The application of Unmanned Aerial Vehicles in various areas created problems in the field of cybersecurity, privacy, safety. Gaps in the security system of UAVs allow them to be easily hijacked. The article analyses the security issues of UAVs, reviews their attacks scenarios, and proposes a fuzzy

			approach to the automatic selection of effective mechanisms to prevent identified attacks. The Drone Backbone Model has been developed to show the impact of attacks on UAVs at different levels. The Backbone Model allows a numerical assessment of the impact of the attack on the system.
14	**O. Valikhanli**	**Methods of detecting cyber-attacks on Unmanned Aerial Vehicles: A survey**	As the use of Unmanned Aerial Vehicles (UAVs) increases, so does the number of cyber-attacks on them. Thus, some of the main cyber-attacks on UAVs such as GPS Spoofing, Denial of Service (DoS), Man-In-The-Middle (MITM) and etc. are researched. Existing countermeasure methods against this kind of attacks are analyzed. Proposed methods against each attack are compared with each other. Advantages and disadvantages of such methods are described as well.
15	**R. Ibrahimov; F. Abdullayeva,**	**Comparative analysis of methods for detecting unmanned aerial vehicles**	The widespread use of UAVs in both the national and military spheres has made them the focus of industrial organizations. However, the use of drones has seriously affected the privacy of personal data, posed a threat to states, national institutions, nuclear power plants, historical sites. One way to reduce this threat is to detect malicious drones. The article analyses the existing methods in the detection of malicious drones and proposes a new approach to their detection.
16	**A. Moens**	**Cybersecurity of critical European IT infrastructures: GEANT and NRENs**	Under the newly proposed EU legislation on cybersecurity the NIS-2 Directive, the European Research and Education network GÉANT will most likely be appointed critical infrastructure, just like all National Research and Education Networks (NRENs). Being in the scope of the NIS directive implies that an organisation will have to adhere to strict international standards. Together with the European NRENs GEANT has started preparing for things, building upon the work done over the past 3 years in the GN4-3 security innovation program. In recent years GÉANT has developed a security baseline for Research and Education that enables the R&E community to get a coherent overview of the maturity of information security in their organisation and networks. The baseline is based in international standards such as ISO 27001 and NIST and has proven very valuable in practice. The global R&E community has developed and agreed upon a number of standards for identity management and incident management, such as SIRTFI for identity federations and the SIM3 model for security incident management as run by the Trusted Introducer program. In this talk I will give an overview of the most relevant and practical standards for identity management and security management and illustrate these with examples for use.
17	**C. Spirito**	**Cyber Threat Assessment Methodology for Autonomous and Remote Operations for Advanced Reactors**	The next generation of *Advanced Reactors* include planned capabilities for both Autonomous (operating without human interaction for a set period-of-time) and Remote (operating with human interaction from a separate physical location) Operations. Existing Nuclear Reactor architectures include a set of safety and security constraints tightly coupled with

			personnel policies and procedures. As *Advanced Reactors* are fielded with these new *Autonomous* and *Remote* operational capabilities, the architectures and associated infrastructure services and components will perceivably expand the overall attack surface and risk calculations with regards to safe and secure operations. This paper is part of an FY21 work program focused on ensuring *Advanced Reactor* designs are informed with threat-based guidance on design and operation of Secure Architectures with a specific focus on the deployment of *Autonomous Systems in support of Advanced Reactor Operations.* The next phase of this research program is to complement produce a methodology for assessment of the cyber threat against these architectures as well as a catalogue of *Use Cases* to support the *Advanced Reactor* community in their implementation of *Autonomous* and *Remote Operations*.
18	**J. Suchorab**	**Vulnerability research of programmable logic controllers using fuzz testing method.**	The presentation will focus vulnerability research of programmable logic controllers. Being one of the most popular vulnerability discovery techniques, fuzz testing was chosen as a testing method. The aim of the study was to prove the effectiveness of fuzz testing in the search for vulnerabilities of programmable logic controllers. The research was undertaken in order to develop a specific fuzz testing methodology allowing to test the security of industrial protocols stack implementation in firmware of this devices. A fuzzing laboratory testbed has been designed with the purpose of conducting various fuzzing tests. The presentation will describe the theoretical fundamentals of the fuzz testing and will walk through the systematic methodology of testing. The process of discovering and investigating a zero-day vulnerability in a Siemens S7-1500 series PLC will be discussed as it served as a basis for establishing the methodology. Lastly, several case studies will be introduced, that will share technical details of the vulnerabilities found using the presented methodology and pinpoint the effect and potential consequences that the exploitation of the vulnerable device may have on the whole industrial process that relies on PLCs.
19	**B. Watson**	**Open inference networks**	Both ad hoc and structured networking of IoT devices leaves ample opening for cybersecurity issues – made worse by the relatively limited computing power available for cyber defence. In this work, we consider a robust inferencing architecture/structure which can be used for complex event processing (CEP) of “normal” IoT events, but also cyber security (threat) events.
20	**M. Hashimov; R. Alakbarov**	**Cyber security problems in cloud-based SCADA systems**	The article explores the conceptual model and security issues of cloud-based SCADA systems which is widely used in the monitoring and management of the oil and gas industry. It highlights existing vulnerabilities that could restrict the security of cloud-based SCADA systems. For this purpose, this article analyzes security problems and risks in the use of cloud-based SCADA systems and provides recommendations for their solution.

21	**W. Graniszewski**	**A Cybersecurity Testbed for Industrial Control Systems**	Recently, cybersecurity issues of Industrial Control Systems (ICS) have focused the attention of many stakeholders. Among them there are academia and the scientific community. The industry has developed numerous control systems and devices like Programmable Logic Controllers (PLCs), distributed control systems (DCS), Supervisory Control And Data Acquisition (SCADA). These systems control plants and exchange data using several dedicated communications protocols, e.g. Modbus, Fieldbus, Industrial Ethernet, etc. In the beginning, in the 1970s and 1980, legacy systems were designed with assumption that these systems will be not accessible from outside of a plant. The introduction of the Internet and integration of Operational Technology (OT) with the company's business networks segmentation of both was one of the cybersecurity requirements. One of the first standards within this area was coordinated by the International Society of Automation (ISA) as ISA95, Enterprise-Control System Integration, which based on the Purdue Reference Model. During the last decades, ISA95 naturally evolved to ISA/IEC 62443 standard. A natural development of ICS and integration with other business systems increase cybersecurity threats. To evaluate different devices, communication protocols, topologies, and also for training objectives, there is a tremendous demand for ICS testbeds. At Warsaw University of Technology (WUT), Faculty of Electrical Engineering (EE), we have integrated several elements of industrial equipment and systems with business infrastructure. We use this environment to test different attacking scenarios and collect data to evaluate different machine learning algorithms, particularly Convolutional Neural Networks (CNN). Keywords — industrial control systems, cybersecurity, industrial security control, safety, supervisory control and data acquisition (SCADA), machine learning algorithms, convolutional neural networks (CNN).
22	**G. Visky**	**Cyber environment for maritime sector**	This presentation introduces an environment for cyber-related education and maritime-related cyber research that is flexible enough to adapt to specific needs. The proposed environment has enormous potential in education and research, but it can be used in cyber exercises as well. The introduced environment aims not to provide sailing-related experience but focuses on the consequences of cyber attacks and how to react to those attacks. Furthermore, the environment offers a maritime-related climate for cyber experts to conduct experiments.
23	**A. Iqbal, J. Olegård, O. Popov**	**On the Beckhoff PLC Security and Forensic Analysis**	The advent of smart buildings and smart cities has increased the use of Operational Technology (OT) and Industrial control systems (ICSs). Recent trends of cyberattacks on OT of various sorts demands more attention for forensic and security analysis of such environments. The paper studies and examines a case of a widely used PLC, the Beckhoff CX9020 PLC, from a digital forensic perspective. Initially, a PLC is configured to log as many activities as possible using the available options. The next step is to test a set of

			basic cyberattacks on the PLC. Finally, we devise a framework for a forensic acquisition and analysis of the system. Apparently, while the system supports certain evidence gathering in the form of logging, it appears that this evidence is insufficient to make more definite conclusions about the nature of the cyberattacks. Finally, a discussion follows that covers the general impact and eventually a few possible improvements to the forensic readiness of the basic system.
24	**S. Akleylek**	**Cyber Security Challenges and Opportunities in Quantum Era**	In this talk, we give a brief survey on the importance of post-quantum cryptography by describing current approaches in cyber security. The talk provides details on applied cryptography for cyber security. Then, we discuss the computationally hard problems used in post-quantum cryptographic schemes focusing on lattice-based and code-based cryptography. The focus will be given to NIST Post-Quantum Cryptography Standardization Project in view of cyber security applications, formal analysis/verification and performance.
25	**B. Nabiyev**	**Investigation of computer incidents for cyber-physical infrastructures in industrial control systems Digital forensics for ICS/PLCs.**	Industrial Control Systems (ICS) are complex systems of sensors, hardware, programmable logic controllers, and communications that are linked together to perform monitoring and control tasks in a variety of industries. ICS has a wide range of critical applications and infrastructures it is means delay or shutdown of these systems can lead to irreversible consequences. For example, SamSam, Shamoon, Stuxnet, and Triton are just a few of the popular viruses that target ICS. They did a lot of damage. However, ICS has poses a number of issues that make it particularly difficult to defend against determined attackers. For investigation, defeating, and preventing cybersecurity attacks we need to do the right digital forensics for ICS.
26	**C. Spirito**	**Incorporating Cyber Denial and Deception Capabilities into the Nuclear and Radiological Domains**	Ensuring the safe operation of elements within the Nuclear and Radiological Domains requires a proven approach to handling the cyber-security risk that is associated with the use of interconnected digital systems. The most common approach to this problem is to implement cyber-security best practices into the design of domain systems and field a cyber-defense capability centered on detection and response to anomalies that may indicate that a cyber-attack has taken place. One capability suite that is not often included within these best practices is Cyber Denial and Deception (D&D), the ability to use the manipulation of facts and fictions to engage with an ever-clever set of cyber actors and prevent them from carrying out their mission objectives against your infrastructure. This paper provides an entry point for those not familiar with the practice of D&D and how these capabilities can be incorporated into the Nuclear Energy Domain.
27	**B. Watson; L.Watson; D. Blaauw**	**Glass box data science on ATT&CK**	In this work, we demonstrate an alternative visualization of the MITRE ATT&CK framework for ICS, using formal concept lattices to highlight deep structures. ATT&CK comprehensively shows threat actors' tactics, techniques and procedures, but there remain further connections which

			are not found without exploratory data science. Lattices provide glass-box data science/machine learning – highlighting the relationships between threat actors, as well as differences that can be used for attribution.
28	**U. Glaesser; Z. Zohrevand**	**AttackTracker: Dynamic Attack Scoring using Distributed Local Detectors.**	Complex cyber-physical systems necessitate advanced analytic methods for situational awareness of physical and cyber threats to support supervision and decision-making processes. We explore here a scalable and unsupervised end-to-end framework for online intrusion detection in stream data from supervisory control systems used in the continuous operation of critical infrastructure**.**
29	**L. Sukhostat**	**Anomaly detection in industrial control system based on the hierarchical hidden Markov model.**	An approach based on the Hierarchical Hidden Markov Model (HHMM), which is applied to detect anomalies in the industrial control system (ICS), is proposed. Signals of the system components are fed to the proposed model input. The model can correlate events occurring relatively far from each other. Each of the latent states is an independent probabilistic model so that each state is also an HMM. The approach is evaluated on two datasets: ICS actuators and sensors measurements dataset and a network traffic dataset. HHMM can detect abnormal activity in both physical and network systems.
30	**S. Mehdiyev**	**On monitoring the technical condition and technological safety of functional elements of the corporate cyber-physical infrastructure**	During operation, cyber-physical systems (CPSs) are constantly exposed to a wide range of factors that affect their technical condition in different ways. With increasing interaction in the CPSs environment, physical systems become more and more susceptible to security vulnerabilities. The key issues for ensuring the safety of the CPSs are as follows:Understanding the threats and possible consequences of attacks. Determination of the unique properties of CPSs and their differences from the security of traditional information systems.
POSTER Session			
31	**T. Bayramova**	**Analysis of modern methods for detecting vulnerabilities in software for industrial information systems.**	Errors and vulnerabilities in software are analyzed and problems of their detection are considered. Existing modern methods of vulnerability detection using artificial intelligence technologies are studied. In addition to detecting these cybersecurity vulnerabilities in a timely manner, it specifies the correct choice of software development technologies, methods and operating conditions to prevent them.
32	**T. Fataliev; N.N. Verdiyeva**	**Science 4.0: Complex security problems and solution mechanisms.**	It is supposed to consider the conceptual issues of the reconstruction of science as a corporate environment of Science 4.0 based on the key technologies of Industry 4.0 - Internet of Things, Cyber-Physical Systems, Artificial Intelligence, Cloud computing, Big Data analytics and other Smart solutions; eScience considered to be the technological base of Science 4.0; research of complex security problems and their solution mechanisms within Science 4.0.

33	**S. S. Ojagverdiyeva**	**About a Comprehensive Approach to Ensuring the Children's Safety in Terms of Industry 4.0.**	This study provides information on the concept of the safety of children's data environment. It highlights the concept of Children 4.0, which offers a comprehensive approach to ensuring the safety of data included in databases (medical data safety, spatial data safety, etc.) through wearable devices. This approach is also very important in protecting children's personal data. Keywords. Industry 4.0, Wearable, sensors, IoT, child safety, Children 4.0, smart things.
34	**R. Shikhaliyev**	**Some approaches to intellectual monitoring of industrial control systems cyber security.**	For security of the modern industrial control systems (ICS) basic protective tools can be used. These tools can protect against common attacks and be sufficient for low-risk systems. The required security level of the ICS be ensured by constantly monitoring. With increase of the monitoring data volume, increase the costs of ICS resources consumption, as well as the data analysis becomes more complicated. It is necessary to intellectualize the security monitoring of the ICS. The purpose of this article is to study the approaches to intellectualization of monitoring the security of ICS.
35	**F. Aghayev; M. Gulara**	**Risk analysis and assessment of the level of security of the educational system in Education 4-0.**	The article shows the problems of information security in Education 4.0, identifies the most vulnerable spots in the e-education system. The analysis of the reasons for the violation of information security is carried out, and the main directions of protection of the e-education system are shown. The need to protect educational resources from unauthorised access is substantiated by analysing the state of the problem and existing approaches to ensure information security. The article describes a model for assessing the security of an e-education system based on an indecipherable correspondence processing algorithm. Possible threats in the e-education system and actions to eliminate these threats have been identified. The results obtained can be used by tutors and the administration of e-education to ensure the protection of educational content.
36	**K. Hashimova**	**Problems of intelligent network management of smart billboards on the IoT platform in Industry 4.0**	AI plays a special role in new technologies used to develop advertising and marketing. It plays a special role in improving effectiveness and marketing, has had its say in the business market, and this process continues. A quick search for any product on Internet search engines is an indispensable process for the marketing market. It is possible with the help of artificial intelligence to provide a virtual environment, street advertising, the required product or service promptly, at a high level, considering the individual characteristics of the customer. In the modern world of cyber-physical systems, machines created using intelligent algorithms facilitate human labour in almost all areas. Intelligent management of a network of smart billboards on AI research in advertising and marketing has a positive impact on economic development. The article discusses the use of artificial intelligence in advertising, the principle of their work, the processes of applying new technologies in this area. The article analyzes scientific researches of the problems on the topic, their solutions, generalization of the results and the method of a systematic

			approach.
37	**Bikes Agayev**	**A methodology based on cyber physical systems platform for assessment of the safety of acoustic noise pollution**	Acoustic noise pollution is currently a global environmental problem. Many citizens are interested in the following question: what is the level of noise pollution where I live, work or travel? Does it meet standards? An ordinary citizen cannot monitor noise by standard methods. This process is complicated, and required equipment is expensive. However, the computing, communication and sensory functions of modern mobile phones allow monitoring. To do this, they need simple and straightforward methodologies. The article proposes a simple monitoring methodology. A number of experiments are being carried out.
38	**K. Dashdamirova**	**Cyber socio-technological problems of the networked society and their analysis**	The article analyzes the evolutionary history of industrial revolutions, and points out the beginning of building a "Society 5.0" or "Super Intelligent Society" in some countries. Moreover, the current state of digital technologies affecting the technological and social development of society is analyzed, the socio-technological problems of the Internet in a networked society are studied. It is shown that many innovations that Industry 4.0 brings to the life of a networked society will exacerbate many problems.
39	**G. Nabibayova**	**Analysis and research of the impact of Industry 4.0. challenges on demographic processes**	In order to solve the problem posed in the article, the characteristics of the Industry 4.0 (Fourth Industrial Revolution) are considered. In addition, the possibility of threats to the data security of an electronic demographic decision support system (DSS) from attackers in the context of Industry 4.0 is considered, since the attack risks for them is very high. It is found out that damage to these data will impact on the course of demographic processes in the region. Solution ways of arisen problems are indicated.
40	**I. Alakbarova**	**On one approach for detecting social relationships by analyzing video images in e-government**	Video surveillance systems are installed wherever it is important to ensure public safety. Determining social relationships by observing the behavior of citizens is a very complex process. The article proposes a new approach for identifying social relations based video analysis. Keywords: video surveillance system, videimages, big data, social relations, video analytics.