COIA 2022

PROCEEDINGS

of the
8th International Conference on

CONTROL AND OPTIMIZATION WITH INDUSTRIAL APPLICATIONS

Volume I

24-26 August, 2022
Baku, Azerbaijan

ISBN 978 – 9952 – 37 – 860 – 3
ISBN 978 – 9952 – 37 – 861 – 0 (Volume I)

MINISTRY OF DIGITAL DEVELOPMENT
AND TRANSPORT
OF THE REPUBLIC OF AZERBAIJAN

BAKI DÖVLƏT UNİVERSİTETİ
BDU
1919
BAKU STATE UNIVERSITY

IAM
Institute of Applied Mathematics

The 8th International Conference on Control and Optimization with Industrial Applications, 24-26 August 2022, Baku, Azerbaijan

RESEARCH OF CYBER RESILIENCE OF CRITICAL INFRASTRUCTURES OF SCIENCE TRANSFORMED BASED ON INDUSTRY 4.0 APPLICATIONS

T. FATALIYEV[1], S. MEHDIYEV[2]

[1,2]Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku
t.fataliyev@gmail.com

1. Introduction

In modern times, the basic technologies of Industry 4.0 are widely used in various areas of the scientific community: in physical experiments, supercomputer calculations of theoretical models, social research, genetic engineering, etc. In such a scientific environment, its science infrastructure has been formed based on the use of the Internet of Things (IoT), cyber-physical systems (CPS), artificial intelligence (AI), cloud solutions, big data analytics, and digital twins, smart cities, etc. In this context, the implementation of critical and security-sensitive tasks required special attention to the reliability of systems with characteristic cyber resilience problems. Unlike cybersecurity, which focuses on assessing the likelihood of incidents and preventing possible security threats, cyber resilience is primarily focused on maintaining the targeted behavior and performance of these infrastructures in the face of cyber incidents. The main purpose of this work is to study the problems and develop ways to solve the cyber resilience of critical infrastructures of the scientific environment.

2. Cyber resilience as a current problem of critical infrastructures

Modern systems, regardless of their functional purpose, are characterized by the introduction of cyber components into their structures. However, such integrated structures, being exposed to numerous cyber intrusions or cyberattacks, required effective solutions to protect against them. Solving the problems of continuous and fault-tolerant operation in the face of such risks is especially important for critical infrastructures on which the security of the country, its economy, health, and safety of the population depends. As it becomes more complex, the scientific environment also acquires the system properties of critical infrastructures, such as cyber resilience, manageability, self-organization, proactive cybersecurity, and adaptability [4]. Each of these properties is the subject of cybernetic research, and each subsequent feature makes sense only if there is a previous one. Cyber resilience is the ability of a system to anticipate, withstand, recover and adapt to adverse conditions, loads, and attacks that use or are activated by cyber resources. Although cybersecurity is an integral part of a system security strategy, it does not always protect against sophisticated cyberattacks. In contrast, cyber resilience is a broader concept that includes ensuring business continuity, securing critical processes, identifying potential threats, managing risks, minimizing attacks, and implementing procedures against cybersecurity incidents. It allows the system to continue its normal operation without interruption during and after disruptive events such as cyberattacks or technical failures [6]. Cyber

resilience is used by many organizations to refer to organizational resilience against cyber incidents, hacks, and DDoS attacks. Thus, many organization-level cyber resilience measures focus on a combination of so-called cyber hygiene practices (eg, avoiding public Wi-Fi networks, creating strong unique passwords, etc.) and incident response. The problem area of cyber resilience overlaps with the areas of security and fault tolerance. This means that many of the metrics defined for security or fault tolerance may be relevant to or adapted for cyber resiliency. In this context, some problems of cyber resilience in the Science 4.0 environment are considered, in which there are qualitative transformations of the scientific community based on Industry 4.0 applications. Modern science is a complex corporate system based on interconnected smart subsystems: buildings, infrastructure, resources, research environment, CPS, management, integrated security, etc. [1]. The integrated Science 4.0 model can be represented as consisting of critical infrastructures for various purposes. Here, critical infrastructure refers to the physical resources, services, information technology systems, networks and infrastructure assets that, if damaged or destroyed, could have serious consequences for critical scientific functions. Keeping them secure, reliable and resilient to cyberattacks has become critical, requiring innovative and creative cybersecurity and resilience solutions. In the Science 4.0 environment, different types of threats can be encountered. These can be threats related to information security, data privacy and cybersecurity related factors. Although cybersecurity is becoming an integral part of the security strategy in the scientific community, however, protection against complex cyberattacks is not always provided, when unauthorized access to information can lead to undesirable consequences. Thus, guaranteeing the cyber resilience of critical Science 4.0 infrastructures, that is, ensuring the purposeful operation of the system when exposed to attacks from cyberspace, is an urgent problem that requires preventive solutions. Cyberattacks are a very real threat to Science 4.0, which is based on the use of innovative technologies and especially the Internet. It should be noted that for such an environment, the cybersecurity landscape is complex and constantly changing. As you know, cybersecurity is associated with the protection of information assets and systems in three areas: confidentiality; integrity and availability. Conducting a risk assessment is an important part of determining what cybersecurity measures need to be implemented and to what extent in order for protection to be cost-effective and sustainable. A large part of any risk assessment should be to identify threats and vulnerabilities. In turn, in order to assess cybersecurity risks, it is first necessary to determine which assets need to be protected. After that, potential vulnerabilities and threats to these assets are identified accordingly. Thus, it is necessary to take into account not only three aspects of security, but also risk groups on which protection should be based: employees, resources, processes and technologies. A number of studies on the security issues that arise from the application of advanced technologies show that the Science 4.0 environment can also face various types of threats [2, 3]. In the Science 4.0 environment, different types of threats can be encountered. These can be threats related to information security, data privacy and cybersecurity related factors. Although cybersecurity is becoming an integral part of the security strategy in the scientific community, however, protection against complex cyberattacks is not always provided, when unauthorized access to information can lead to undesirable consequences. Thus, guaranteeing the cyber resilience of critical Science 4.0 infrastructures, that is, ensuring the purposeful operation of the system when exposed to attacks from cyberspace, is an urgent problem that requires preventive solutions.

3. Conceptual issues of ensuring the cyber resilience of critical infrastructures of science

To ensure comprehensive security and thus cyber resilience of critical Science 4.0 infrastructures, the following problems should be solved:

- Management of security, protection and privacy;
- Building security, uninterrupted power supply, climate control, video surveillance, access control;

- Cyber security networks, data centers, automated control systems for scientific experiments, resources, tools and equipment;
- Data privacy, protection of personal information, compliance with the General Data Protection Regulation (GDPR);
- Security of infrastructure for information support of science;
- Security policy and procedures, security audit and reporting;
- Analytical monitoring, attack modeling, controlled DDoS testing, etc.;
- Automation of processes with extensive use of IoT, FSC, AI, big data analytics and other advanced technologies in providing integrated security;
- Development of smart and cyber-immune IT solutions to ensure cyber resilience;
- Employee cybersecurity awareness and training;
- Cooperation with domestic and international organizations, etc.

Let's consider some conceptual issues of ensuring cyber resilience. Risk prevention measures can be divided into three categories: a) preventive, b) real-time, and c) post-incident. For the effective implementation of risk mitigation measures, it is considered most effective to use a dynamic approach, in which individual security measures work effectively together and compensate for each other's shortcomings. The use of defense in depth can become one of the most effective tools for preventing attacks at various levels. When considering attack options concerning defense-in-depth, it is important to consider how controls can be circumvented. This requires finding the weakest link in the security system and further strengthening this link to reduce the risk. Note that in recent years, a progressive concept of cyber immunity for a secure digital environment has been developed, which opens up new prospects for Science 4.0 security [5]. Similar to the immune system of living organisms, cyber-immune IT solutions are created initially protected from a whole class of cyber threats, and consist of elements that constantly monitor unusual system behavior and warn of suspicious activity. For example, the architecture of KasperskyOS is based on dividing objects into many isolated modules. All interactions between them are controlled at the level of the microkernel and the internal security system: they allow only those actions that were indicated at the stage of system development. In conclusion, it should be noted that at present, the technological solutions of Industry 4.0 open up prospects for a new qualitative transformation of science within the framework of a single concept of Science 4.0. The analysis performed shows that this problem requires, along with multiple solutions, the provision of integrated security for critical infrastructures of science. Research in this direction confirms not only the relevance of the problem but also emphasizes its complexity.

Keywords: Industry 4.0, Science 4.0, Critical Infrastructure, Risk, Cybersecurity, Cyber Resilience.

AMS Subject Classification: 68M11.

References

[1] Fataliyev T.Kh., Mehdiyev Sh.A., Integration of cyber-physical systems in e-science environment: state-of-the-art, problems and effective solutions, *I.J. Modern Education and Computer Science*, 2019, pp.35-43.

[2] Jamai I., Azzouz L.B., Sadane L.A., Security issues in Industry 4.0, *International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp.481-488.

[3] Ismagilova E., Hughes L., Rana N.P. et al., Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework, *Information Systems Frontiers*, 2020, Open Access.

[4] Petrenko S.A., *Kiberustojchivost' Industrii 4.0*, Sankt-Peterburg, Izdatel'skij Dom "Afina", 2020, 256 p.

[5] Petrenko S.A., Makoveichuk K.A., Olifirov A.V., Concept of cyber immunity of industry 4.0, *CEUR Workshop Proceedings*, 2019, pp.93-99.

[6] Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R., *Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*, NIST Special Publication, 2019, 205 p.