Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model

Taras Lechachenko[1], Ruslan Kozak[1], Yuriy Skorenkyy[1], Oleksandr Kramar[1] and Olena Karelina[2]

[1] *Ternopil Ivan Puluj National Technical University, 56 Ruska St, Ternopil, UA46001, Ukraine*
[2] *Akamai Technologies Poland, Kraków, ul. Opolska 100, PL31-323, Poland*

Abstract

Number and variety of smart manufacturing systems using digital twins for virtualisation and improved control of production are growing fast. Augmented reality interface may serve as an enabler for human creativity inclusion into the product lifecycle and simultaneously contribute to the worker well-being in spirit of the Industry 5.0 principles. Such an integration of a human into industrial platforms requires careful conceptualisation and development of the secure-by-design augmented reality-enhanced interface for industrial digital twins, which is the focus of this research. Threat modeling and vulnerabilities prioritization for AR-enabled industrial digital twins compliant with the Industry 5.0 are performed by an analytical hierarchy process within STRIDE threat modeling methodology using the TODIM method. The security controls and mitigation actions have been identified, the respective threats and vulnerabilities were ranked to optimize decision-making for the AR-enabled industrial digital twin design.

Keywords

Industry 5.0, Industrial Digital Twin, Augmented Reality, IoT Security, Threat Modeling

1. Introduction

Present-day industrial digital twins (IDT) are tools in digitization and optimization of various industrial systems [1-6], and may benefit from such novelties as augmented reality (AR) and virtual reality (VR) technologies [7]. Realistic 3D models of products and equipment can be interacted with and may have rich functionality. Implementation of these technologies offer unique benefits for smart manufacturing as they can be used to model, control and improve the production processes, enhance knowledge transfer and collaboration of employees. The industrial internet of things (IIoT) gives manufacturers a comprehensive view of the current state of the production line, characterizes and controls the ongoing processes in real time.

Smart manufacturing is expected to assure high performance to justify investments done for designing, operating and protection of IIoT. In the transformation, digital twins [8] offer many benefits but also pose some challenges, such as ensuring security, privacy, and ethical standards, as well as dealing with the complexity and accuracy of the models. Importantly, with the widespread use of smart technologies in various domains, ensuring information security becomes vital. Software architecture and information security measures are to be designed appropriately to protect both businesses and individuals from data breaches that can have serious consequences.

Smart manufacturing can provide a variety of data, including physical material data and visual data, process control data and machine data, etc. These data types are to be clearly distinguished, as they require different mechanisms for harvesting, transmitting, pre-processing and storage. To securely

[1]Proceedings ITTAP'2023: 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, November 22–24, 2023, Ternopil, Ukraine, Opole, Poland
EMAIL: taras5a@ukr.net (A. 1); ruslan.o.kozak@gmail.com (A. 2); skorenkyy.tntu@gmail.com (A. 3); kramaroitntu@gmail.com (A. 4), okarelin@akamai.com (A.5)
ORCID: 0000-0003-1185-6448 (A. 1); 0000-0003-1323-0801 (A. 2); 0000-0002-4809-9025 (A. 3); 0000-0002-8153-2476 (A. 4), 0000-0002-5628-9048 (A.5)

manage data from the cyber-physical system of low-resource IoT devices, the streaming large-scale data exchange platform has to be properly designed [9]. Information security and privacy protection, which involve ensuring that data is kept confidential, immutable and accessible, and preventing unauthorized access and manipulation, become the critical requirements and deserve special attention in the context of Industry 5.0.

2. AR-Enhanced Digital Twin Design for Smart Manufacturing

In transition to the Industry 5.0 model, a manufacturing company necessarily implements a human-centered approach into all processes. This includes modeling, engineering, production and management, as well as decision support systems [10, 11]. Human factor determines effectiveness at both design level and operational level, thus setting specific requirements to technological development of the manufacturing facility. Among different aspects, which are to be taken into account, the cognitive ones for human operators and decision-makers are of the utmost importance. These determine, *i.a.*, performance of the manufacturing facility, quality of the product, well being and psychological satisfaction of the personnel. It is crucial to provide, along with collaborative solutions in the workplace, efficient and intuitive interfaces for human-machine interaction. As such an interface, the AR-enabled one has unmatched potential [12]. Such an AR interface can be an indispensable enabler for digital twin implementation (Figure 1) and control of the physical equipment in the factory floor in real time [13, 14].

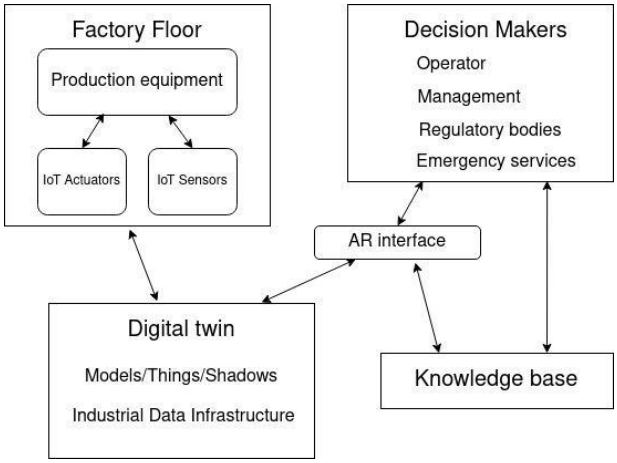

Figure 1: Block diagram representation of a production facility with AR-enhanced industrial digital twin.

It may superimpose an information layer with characteristics, not accessible to a human perception but provided to the industrial digital twin by IoT sensors and display in a timely manner the analytical layer important for informed decision making. Controls may be integrated into AR interface to steer production equipment with embedded IoT actuators [15, 16]. AR interface is also a good solution for making the diffusion of knowledge potential [17-19] more smooth and natural from one professional to another and enable collaboration in diverse teams. The feedback in trainee-trainer interaction [18] will be immediately put in context due to connection of the AR-module to both digital twin and the content of the knowledge base.

We consider modules of the digitized industrial platform and processes of its interaction with the user and the knowledge base, shown in Figure 2, a minimal necessary set for a smart manufacturing facility. The detailed composition of these modules may differ, depending on the production system specification and the stakeholders' requirements, however, this block diagram allows both designing the software architecture and analyzing inherent vulnerabilities to mitigate risks inherent to IIoT components and systems.

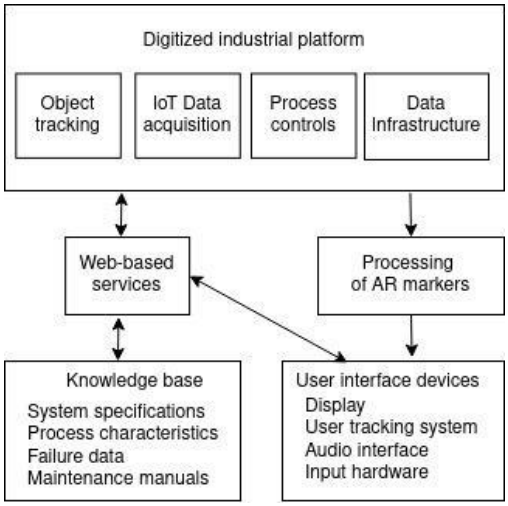

Figure 2: Interconnections within smart manufacturing AR-enhanced digital twin.

3. Cybersecurity Analysis for Smart Manufacturing Digital Platform

As already mentioned, the security layer for an industrial digital twin in cloud/edge environments is to be carefully designed and properly developed. Protection of the IDT as a whole and each IoT device in particular requires addressing multiple information security and cybersecurity threats. Harvested data and processed information in IDT is a valuable business asset, therefore proper security measures are to be designed and enacted.

Since the digital twin operates with sensitive data and privacy data as part of cyber-physical systems, best security practices that are in compliance with industry standards and laws should be adopted by default. One of the most crucial phases of the system development life cycle, secure-by-design implies that security requirements must be identified in order for engineers to create a high-quality, economically viable, and secure system.

In the information security and cyber security domains, threat modeling is a method for determining security needs. It allows the identification of security requirements, finding threats and vulnerabilities, assessing their impact and severity thus making possible the prioritization of viable solutions and measures. A range of applications of this method includes software and networks, IoT components and industrial processes. The STRIDE [20] threat modeling methodology has been used to identify and characterize threats and vulnerabilities inherent to the IDT and to personal data of users. We have composed the general data flow diagram and the threat model shown in Figure 3 for the industrial data platform architecture depicted in Figure 2, for which applications and technologies are examined in paper [21].

For the purposes of this research the specific group of elements (marked in red) have been identified to be analyzed to address extended attack surfaces that IDT and IoT devices might face due to incorporating AR-layer into IDT architecture. It has been studied whether there are threats and risks to the industrial data platform and the data processed in the system imposed by the integrated AR-layer.

Table 1 summarizes descriptions of the corresponding threat and mitigation measures. The suggested countermeasures will help software engineers and security experts in the processes of design and improvement of the industrial data platforms.

The types of security threats have been identified for each element of the specific group within the IDT architecture data flow diagram along with countermeasures that should be put into place to mitigate security risks following the STRIDE methodology. While the STRIDE methodology has been used as a high-level approach to identify the threats and define respective countermeasures, the OWASP IoT Top Ten might be leveraged from low-level perspective to model specific security threats and risks as well as to guide the selection of tests used to evaluate IoT attack surfaces and associated vulnerabilities [22].

Considering the Digital Twin architecture data flow diagram depicted on Figure 3, we adapted the OWASP IoT Top Ten and identified the groups of security practices and controls called to mitigate security threats and risks the IoT devices might encounter.

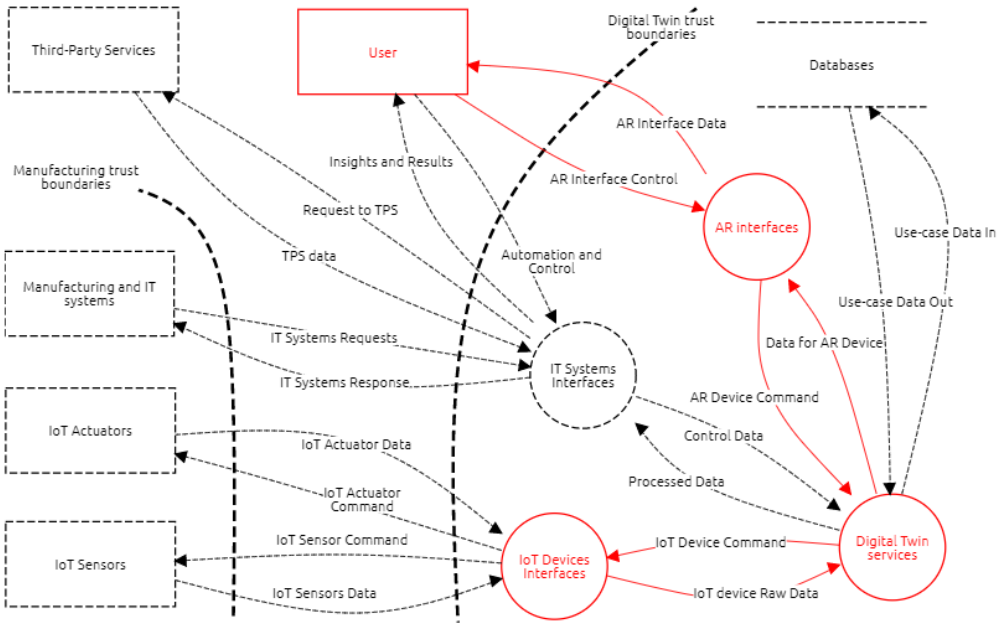

Figure 3: Data flow diagram for AR-enabled Industrial Digital Twin architecture.

A left-shift approach to information security in the development and use of IDT and IoT devices helps ensure that sensitive data and privacy-related information are protected against the ever-increasing threat of cyber-attacks targeting the IoT-empowered industrial systems. The solution provides the necessary traceability in cyber security and privacy audits to demonstrate compliance with the relevant regulations.

Table 1
Security threats and countermeasures for the designed industrial data platform

Type of Security threat	Analyzed components	Proposed countermeasures
Spoofing (claiming a false identity)	AR interfaces IoT Devices Interfaces, Digital Twin services, User	Encryption usage, Strong cryptographic protocols: PGP, AES, SHA-2, TLS 1.2 / 1.3, Strong authentication mechanisms: MFA, biometric auth, certificate pinning, OAuth
Tampering (malicious modifications of data or process)	IoT Device Command / Raw Data, Data for AR Device / Control, AR Interface Data / Control AR interfaces, IoT Devices Interfaces, Digital Twin services	Security Labeling, Secure communication protocols, Proper authorization mechanisms, Data hashing and signing
Repudiation (denial of taking an action or recognising an event occurrence)	AR interfaces IoT Devices Interfaces, Digital Twin services, User	Logging and audit trails
Information Disclosure (leakage of the sensitive data)	AR interfaces IoT Devices Interfaces, Digital Twin services, IoT Device Command / Raw Data, Data for AR Device / Control,	Proper authorization mechanisms, Encryption usage, Strong cryptographic protocols: PGP, AES, SHA-2, TLS 1.2 / 1.3,

	AR Interface Data / Control	Secure coding best practices
Denial of Service (unavailability of an asset, service or network resource for purposive users)	AR interfaces IoT Devices Interfaces, Digital Twin services, IoT Device Command / Raw Data, Data for AR Device / Control, AR Interface Data / Control	Antimalware software, Security applications, Redundancy
Elevation of Privilege (gaining unauthorized access or privileges)	AR interfaces IoT Devices Interfaces, Digital Twin services	Proper authorization mechanisms, Principles of least privilege, Logging and audit trails, Access certification

Table 2 captures the corresponding vulnerability descriptions and mitigations. By understanding these vulnerabilities and implementing effective mitigation strategies, engineers can build a robust security posture that protects their IoT ecosystems.

Implementing additional security controls to handle the extended attack surface for IDT and IoT devices will require the prioritization of the proposed countermeasures and mitigation actions. The following chapter provides the approach of tradeoff decision-making regarding the most valuable security controls during the development process of secure-by-design smart manufacturing which is empowered by AR-equipments.

Table 2
Security vulnerabilities and mitigations for IoT devices

Vulnerability	Mitigation action
Insecure network services	Network isolation for IoT devices. Periodic vulnerability assessment. Secure network protocols.
Insecure ecosystem interface	Strong authentication of IoT endpoints. Access control to sensitive APIs and interfaces. Encrypted communication channels between IoT devices / ecosystem.
Lack of secure update mechanism	Updating and patching all software and components used in IoT devices. Vulnerability monitoring components used in the IoT ecosystem. Hold back from the legacy technologies.
Use of insecure or outdated components	Updating and patching all software and components used in IoT devices. Vulnerability monitoring components used in the IoT ecosystem. Hold back from the legacy technologies.
Insecure data transfer and storage	Using encryption to protect sensitive data during transmission and storage. Using secure protocols.
Lack of device management	IoT devices integration with asset management, bug tracking and patch management systems. Unique device credentials and enforcing access controls.
Insecure default settings	Changing default configurations during initial IoT devices setup. Disabling unnecessary services and ports.

4. Multi-criteria decision making based on AHP and TODIM methods

Ranking of components captured on the data flow diagram (Figure 3) in terms of the STRIDE threat model was conducted using the TODIM [24, 25] method and intuitionistic fuzzy sets [26]. The evaluations for the TODIM method were provided by experts with a minimum of five years of

experience in the field of cybersecurity. Those experts have been asked to utilize a linguistic variable scale presented in Table 3. For this purpose, linguistic variables on the ranking scale, as presented in the paper [27], were modified, and the scale defined in Table 3 has been applied.

Table 3
Intuitionistic linguistic variables

Linguistic term	IFNs
Critical Impact (CI)	[1.00; 0.00; 0.00]
High Impact (HI)	[0.85; 0,05; 0.10]
Medium-High Impact (MHI)	[0.70; 0.20; 0.10]
Medium Impact (MI)	[0.50; 0.50; 0.00]
Low-Medium Impact (LMI)	[0.40; 0.50; 0.10]
Low Impact (LI)	[0.25; 0.60; 0.15]
Miserable Impact (Msl)	[0.00; 0.90; 0.10]

The algorithm of the TODIM [24] method is as follows. Let $\{a_1, a_2, ...a_m\}$ be a set of alternatives, $\{c_1, c_2, ...c_n\}$ be a set of criteria with their corresponding $\{w_1, w_2, ...c_n\}$ weights satisfying the condition $w_i \in [0,1]$ and $\sum_{i=1}^{n} w_i = 1$. We construct a matrix $a = \left[d_{ij} \right]_{m \times n}$, d_{ij} where represents the evaluation of alternative $a_i (i = 1,2,...m)$ based on criterion $c_j (j = 1,2,...n)$. Let's assume that $w_{jk} = w_j / w_k$ are the relative weights for each criterion c_j, c_t where $w_k = max(w_j) \quad k, j = 1,2...,n$. The TODIM method consists of the following steps:

1. Normalization $a = \left[d_{ij} \right]_{m \times x}$ into $a' = \left[d'_{ij} \right]_{m \times x}$.

2. Calculation of alternative a_i dominance over a_t alternative based on criterion c_j. In this case, consider the factor ρ as a mitigating factor for loss effects. Thus, the calculation is as follows:

$$\delta(a_i, a_t) = \sum_{j=1}^{n} \upsilon_j(a_i, a_t) (i, t = 1,2...,m)$$

$$\upsilon_j(a_i, a_t) = \begin{cases} \sqrt{w_{ik}(d_{ij} - d_{tj}) / \sum_{j=1}^{n} w_{jk}} & if\ d_{ij} - d_{tj} > 0 \\ 0 & if\ d_{ij} - d_{tj} = 0 \\ -\frac{1}{\rho} \sqrt{(\sum_{j=1}^{n} w_{jk})(d_{ij} - d_{tj}) / w_{jk}} & if\ d_{ij} - d_{tj} < 0 \end{cases} \quad (1)$$

Where $\upsilon_j(a_i, a_t)(d_{ij} - d_{tj} > 0)$ represents an advantage and $\upsilon_j(a_i, a_t)(d_{ij} - d_{tj} < 0)$ represents a loss.

3. Calculation of the overall evaluation by the formula:

$$\delta(a_i) = \frac{\sum_{t=1}^{m} \delta(a_i, a_t) - min\left\{ \sum_{1}^{m} \delta(a_i, a_t) \right\}}{max\left\{ \sum_{1}^{m} \delta(a_i, a_t) \right\} - min\left\{ \sum_{1}^{m} \delta(a_i, a_t) \right\}} \quad (2)$$

4. Selection of the best $\delta(a_i)$ alternative with the highest value.

Table 4
TODIM ranking of components for the designed industrial data platform

Name of component	Coefficient	Position
Digital Twin Services	1	1

AR interfaces	0.92	2
IoT Devices Interfaces	0.87	3
AR Interface Data / Control	0.53	4
Data for AR Device / AR Device Command	0.35	5
IoT Device Command / Raw Data	0.14	6
User	0	7

Table 4 displays the ranking results of the AR-enabled Digital Twin system components with respect to the STRIDE threats using the TODIM method. The results of ranking shows that major efforts and activities within the secure-by-design approach should be made to the process components of IDT architecture as well as to their respective security controls and mitigations. The implementation of the countermeasures for the data flow and external user components might be deprioritized or delayed for the next system release in case of tough budget or project timeline.

Another important separate task in the context of Industry 5.0 is the prioritization of vulnerabilities for IoT (Table 2) devices, the implementation of which will enable engineers and data architecture designers in the Industry 5.0 sector to proactively prevent their occurrence through the efficient allocation of resources for their mitigation. Effective budget allocation in accordance with vulnerability prioritization will determine the priority of allocating funds to tools and techniques for their reduction.

This work implemented the prioritization of vulnerabilities for IoT devices using the Analytic Hierarchy Process (AHP) method developed by Thomas Saaty [23]. For the purpose of the vulnerability prioritization, three experts with specialized education in the field of cybersecurity and a minimum of 5 years of professional experience within companies of this profile were meticulously selected. Table 5 displays vulnerability ranking assessments by three experts using the Analytic Hierarchy Process methodology.

Table 5
AHP vulnerability ranking assessments for IoT

Vulnerability	Expert 1	Expert 2	Expert 3
Insecure network services	0.0000037	0.0000096	0.0000010
Insecure ecosystem interfaces	0.3465259	0.4901828	0.7605106
Lack of secure update mechanism	0.0000095	0.0000104	0.0000126
Use insecure or outdated components	0.6237466	0.4901828	0.1396856
IInsecure data transfer and storage	0.0000005	0.0000010	0.0000019
Lack of device management	0.0000113	0.0000058	0.0000126
Insecure default settings	0.0297022	0.0196073	0.0997754

Table 6 presents the ranking of averaged pairwise comparison values from three experts in the AHP.

Applying the AHP method to the prioritization of vulnerabilities for IoT components within IDT architecture revealed that the vulnerabilities such as the insecure ecosystems interfaces, useinsecure or outdated components, and insecure default settings should be treated with the highest priority while developing AR-enabled IDT systems.

Table 6
AHP ranking of vulnerabilities for IoT

Vulnerability	Position	Coefficient
Insecure ecosystem interfaces	1	0.5324064
Use insecure or outdated components	2	0.4178717
Insecure default settings	3	0.0496949
Lack of secure update mechanism	4	0.0000108
Lack of device management	5	0.0000099

Insecure network services	6	0.0000048
Insecure data transfer and storage	7	0.0000012

5. Conclusions

Augmented reality interfaces have immense potential as an enabler for human creativity inclusion into the product life cycle according to the Industry 5.0 principles. Augmented reality assets can support virtualisation of manufacturing lines and further implementation of the industrial digital twins. This may be accompanied with extension of the attack surface for the industrial data platform. Proper implementation of a secure-based approach to the industrial digital twins design is to be considered a priority.

An approach for developing a secure-by-design augmented reality-enhanced interface for industrial digital twins is proposed. As a result of threat modeling the specific group of elements have been analyzed to address extended attack surfaces that the IDT system might encounter due to incorporating AR-layer into its architecture. Threat modeling and vulnerabilities prioritization for AR-enabled industrial digital twins compliant with the Industry 5.0 are performed by an analytical hierarchy process within STRIDE threat modeling methodology using the TODIM method. The security controls and mitigation actions have been identified, the respective threats and vulnerabilities were ranked by using AHP and TODIM methods to optimize decision-making for the AR-enabled digital twin design.

The prioritized vulnerabilities and implementing effective mitigation strategies will let engineers build a robust digital twin ecosystem as well as aid security experts in speeding up and saving means on the design and upgrade of the IoT-powered manufacturing systems and its constituent parts.

6. Acknowledgements

This work was partially supported by the European Institute of Technology through the project “Smart Manufacturing Innovation, Learning-labs, and Entrepreneurship” (HEI grant agreement No 10044).

7. References

[1] A. Ilic, E. Fleisch, Augmented Reality and the Internet of Things. Auto-ID Labs White Paper WP-BIZAPP-068, 2016. DOI: 10.3929/ethz-a-010833302.

[2] C. Qiu, S. Zhou, Z. Liu, Q. Gao, J.Tan, Digital assembly technology based on augmented reality and digital twins: a review. Virtual Reality & Intelligent Hardware 1 (2019) 597–610. 597–610. DOI: 10.1016/j.vrih.2019.10.002.

[3] J. Egger, T. Masood, Augmented reality in support of intelligent manufacturing – A systematic literature review 2020 140 106195. DOI: 10.1016/j.cie.2019.106195.

[4] O. Kramar, Y. Drohobytskiy, Y. Skorenkyy, O. Rokitskyi, N. Kunanets, V. Pasichnyk, O. Matsiuk, Augmented Reality-assisted Cyber-Physical Systems of Smart University Campus, 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT) 2 (2020) 309-313.

[5] Y. Yin, P. Zheng, C. Li, and L. Wang, A state-of-the-art survey on Augmented Reality-assisted Digital Twin for futuristic human-centric industry transformation. Robot. Comput.-Integr. Manuf. 81 (2023) 102515. URL: https://doi.org/10.1016/j.rcim.2022.102515.

[6] V. Siatras, N. Nikolakis, K. Alexopoulos, An augmented reality framework for visualization of Internet of Things data for process supervision in factory shop-floor. Procedia CIRP (2022) 107 1162-1167. DOI: 10.1016/j.procir.2022.05.125.

[7] R. Azuma, M. Billinghurst, G. Klinker, Special section on mobile augmented reality. Computers & Graphics 35 (2011) vii–viii.

[8] C.K. Lo, C.H. Chen, Ray Y. Zhong, A review of digital twin in product design and development. Advanced Engineering Informatics 48 (2021) 101297. URL: https://doi.org/10.1016/j.aei.2021.101297.

[9] Y. Drohobytskiy, V. Brevus, Y. Skorenkyy, Spark structured streaming: Customizing kafka stream processing. 2020 IEEE Third International Conference on Data Stream Mining Processing (2020) 296-299.
[10] V. Vijayakumar, F. Sgarbossa, W.P. Neumann, A. Sobhani, Framework for incorporating human factors into production and logistics systems. International Journal of Production Research, 60 (2022) 402-419.
[11] F. Sgarbossa, E.H. Grosse, W.P. Neumann, D. Battini, C.H. Glock, Human factors in production and logistics systems of the future. Annual Reviews in Control, 49 (2020) 295-305 .
[12] S. Ke, F. Xiang, Z. Zhang, Y. Zuo, An enhanced interaction framework based on VR, AR and MR in digital twin. Procedia CIRP 83 (2019) 753-758. DOI: 10.1016/j.procir.2019.04.103.
[13] D. Mourtzis, V. Siatras, J. Angelopoulos, Real-time remote maintenance support based on augmented reality (AR). Applied Sciences 10 (2020) 1855. DOI: 10.3390/app10051855.
[14] R. Geng, M. Li, Z. Hu, Z. Han, R. Zheng, Digital Twin in smart manufacturing: remote control and virtual machining using VR and AR technologies. Struct Multidisc Optim. 65 (2022) 321. URL: DOI:10.1007/s00158-022-03426-3.
[15] C. Li, P. Zheng, S. Li, Y. Pang, C. K. M. Lee, AR-assisted digital twin-enabled robot collaborative manufacturing system with human-in-the-loop. Robotics and Computer-Integrated Manufacturing 76 (2022) 102321. DOI:10.1016/j.rcim.2022.102321.
[16] Y. Cai, Y. Wang, M. Burnett, Using augmented reality to build digital twin for reconfigurable additive manufacturing system. Journal of Manufacturing Systems 56 (2020) 598-604. DOI:10.1016/j.jmsy.2020.04.005.
[17] V. Pasichnyk, N. Kunanets, M. Nazaruk, A. Bomba, Y. Bilak, Modeling the redistribution processes of knowledge potential in the formation of the professional competency system. IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine (2019), 197-200. DOI: 10.1109/STC-CSIT.2019.8929793.
[18] V. Pasichnyk, A. Bomba, M. Nazaruk, N. Kunanets, The dynamics simulation of knowledge potentials of agents including the feedback. J. Phys.: Conf. Ser. 1840 (2021) 012020. DOI 10.1088/1742-6596/1840/1/012020.
[19] A. Bomba, T. Lechachenko, M. Nazaruk, Modeling the Dynamics of "Knowledge Potentials" of Agents Including the Stakeholder Requests. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education IV. ICCSEEA. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer (2021), Cham. DOI: 10.1007/978-3-030-80472-5_7
[20] R. Khan, K. McLaughlin, D. Laverty, S. Sezer. STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings Institute of Electrical and Electronics Engineers Inc. (2018) 1-6. DOI: 10.1109/ISGTEurope.2017.8260283.
[21] P.K. Reddy, V.Q. Pham, B. Prabadevi, M. Liyanage. Industry 5.0: A Survey on Enabling Technologies and Potential Applications. Journal of Industrial Information Integration 26 (2021) 100257. DOI: 10.1016/j.jii.2021.100257.
[22] G. Lally, D. Sgandurra, Towards a Framework for Testing the Security of IoT Devices Consistently. In: Emerging Technologies for Authorization and Authentication. Saracino, A., Mori, P. Eds. ETAA 2018 Lecture Notes in Computer Science, Volume 11263 (2018). Springer, Cham. DOI: 10.1007/978-3-030-04372-8_8.
[23] T. Saaty, What is the analytic hierarchy process? Springer Berlin Heidelberg.1988 109-121.
[24] J. Wang, G. Wei, M. Lu, TODIM Method for Multiple Attribute Group Decision Making under 2-Tuple Linguistic Neutrosophic Environment. Symmetry 10 (2018) 486. DOI: 10.1080/17509653.2017.1349625
[25] T. Lechachenko, T. Gancarczyk, T. Lobur, A. Postoliuk, Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. CEUR Workshop Proceedings 3468 (2023) 250-256.
[26] K.T. Atanassov, Intuitionistic fuzzy sets. Physica-Verlag HD. 1999. 1- 137
[27] B.D. Rouyendegh, The Intuitionistic Fuzzy ELECTRE model, International Journal of Management Science and Engineering Management, 13:2 (2018) 139-145. DOI: 10.1080/17509653.2017.1349625.