

Selected Topics on Information Management in Complex Systems: Editorial Introduction to Issue 24 of CSIMQ

Erika Nazaruka*

Department of Applied Computer Science, Riga Technical University,
1 Setas Str., Riga, LV-1048, Latvia

erika.nazaruka@rtu.lv

Complex systems consist of multiple interacting parts; some of them (or even all of them) may also be systems [1]. While performing their tasks, these parts operate with multiple data and information flows. Data are gathered, created, transferred, and analyzed. Information based on the analyzed data is assessed and taken into account during decision making. Different types of data and a large number of data flows can be considered as one of the sources of system complexity. Thus, information management, including data control, is an important aspect of complex systems development and management.

According to ISO/IEC/IEEE 15288:2015 [2], “the purpose of the Information Management Process is to generate, obtain, confirm, transform, retain, retrieve, disseminate and dispose of information, to designated stakeholders...”. Information management strategies consider the scope of information, constrains, security controls and information life cycle [3]. This means that information management activities should be implemented starting from the level of primitive data gathering and ending with enterprise-level decision making [3].

The articles, which have been recommended by reviewers for this issue of CSIMQ, present contributions in different aspects of information management in complex systems, namely, implementation of harmful environment monitoring and data transmitting by Internet-of-Things (IoT) systems, analysis of technological and organizational means for mitigating issues related to information security and users’ privacy that can lead to changes in corresponding systems’ processes, organization and infrastructure, as well as assessment of potential benefits that a controlled (i.e. based on the up-to-date information) change process can bring to an enterprise.

The *first* article “Emerging Tools for Design and Implementation of Water Quality Monitoring Based on IoT” by Inna Skarga-Bandurova, Yana Krytska, Artem Velykzhanin, Lina Barbaruk, Oleksandr Suvorin and Mikhail Shorokhov presents a discussion on implementation of real-time IoT-based systems for surface water monitoring. The main issue here is related to real-time data gathering in the harmful environment and transferring them to the monitoring application. The authors’ contribution (the definition of an overall strategy for the development and implementation of such systems) includes identification of three stages focused on variables to be monitored, discussion of monitoring system development from logical, technological and

* Corresponding author

© 2020 Erika Nazaruka. This is an open access article licensed under the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>).

Reference: E. Nazaruka, “Selected Topics Information Management in Complex Systems: Editorial Introduction to Issue 24 of CSIMQ,” *Complex Systems Informatics and Modeling Quarterly*, CSIMQ, no. 24, pp. I–II, 2020. Available: <https://doi.org/10.7250/csimq.2020-24.00>

Additional information. Author’s ORCID iD: E. Nazaruka – <https://orcid.org/0000-0002-1731-989X>, PII S22559922000137X.
Received: 28 October 2020. Available online: 31 October 2020.

physical aspects, as well as analytical models and decision-making algorithms for real-time and long term monitoring.

The *second* article, entitled “Smart Home Voice Assistants: A Literature Survey of User Privacy and Security Vulnerabilities” by Khairunisa Sharif and Bastian Tenbergen contributes results of systematic literature review on user privacy and security vulnerabilities of Intelligent Voice Assistants (IVAs). IVAs (Apple’s Siri, Amazon’s Alexa, Microsoft’s Cortana, Google’s Assistant and others) have almost an unlimited access to users’ confidential information expressed, for instance, during conversations in the vicinity of the device or conducting users’ tasks. Unawareness of IVAs users regarding the access can be a potential source of enterprise confidential information leakage. As the result of literature analysis, the authors have outlined the essence and reasons of six major IVA’s vulnerabilities and discussed possible countermeasures to these vulnerabilities. The presented information can be used by professionals while analyzing potential solutions for secure IVAs and potential threats related to the confidential data of enterprises.

The *third* article “Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from GDPR” authored by Johannes Wichmann, Kurt Sandkuhl, Nikolay Shilov, Alexander Smirnov, Felix Timm, and Matthias Wißotzki presents a research on a way for implementation of policies and regulations on issues related to enterprise information security by using not technological but organizational means, i.e. by using enterprise architecture frameworks and management. The authors present a comparison and an analysis of how existing architecture frameworks can help in mitigating information security related risks, in general, and personal data protection related risks, in particular. The authors also describe a case study from a financial industry related to creation of a General Data Protection Regulation (GDPR) compliant enterprise. The authors prove that detailed enterprise architecture framework helps in systemic identifying of critical assets and processes, threats, risks and countermeasures.

The *fourth* article “Potential Benefits of Enterprise Architecture Management in the Digital Transformation Process” by Ralf Härting, Christopher Reichstein, Kurt Sandkuhl, Nathalie Hoppe, and Hakkan Yesilay illustrates advantages of application of enterprise architecture management to the digital transformation process of an organization. The results of digital transformation of an organization are intelligent business processes and the use of efficient modern technologies (e.g., Cloud and Mobile Computing, IoT). However, the transformation process requires proper understanding and information-based management of the enterprise architecture. The authors have conducted a survey where 178 middle-level managers of different German companies took part. The statistical processing of the survey results showed that the indicators IT Landscape, Internal Business and EAM Establishment positively and significantly influence the benefits of EAM in the digital transformation.

The CSIMQ editorial team would like to thank all the authors for their contribution and all the reviewers of this issue for their valuable comments and improvement recommendations regarding the submitted articles.

References

- [1] J. Ladyman, J. Lambert, and K. Wiesner, “What is a Complex System?” *European Journal for Philosophy of Science*, vol. 3, pp. 33–67, 2013. Available: <https://doi.org/10.1007/s13194-012-0056-8>
- [2] ISO/IEC/IEEE, “15288:2015 Systems and Software Engineering – System life cycle processes”, Standard, ISO, 2015. Available: <https://www.iso.org/standard/63711.html>
- [3] A. Pickard, G. Roedler, and R. Madachy, “Information Management,” *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*, v. 2.2, R. J. Cloutier (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology, 2020. BKCASE is managed and maintained by the Stevens Institute of Technology Systems Engineering Research Center, the International Council on Systems Engineering, and the Institute of Electrical and Electronics Engineers Computer Society. Available: [https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_\(SEBoK\)](https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK))