IRASA International Scientific Conference
SCIENCE, EDUCATION, TECHNOLOGY AND INNOVATION
SETI VI 2024
Book of Proceedings

DOI: `https://doi.org/10.62982/seti06.slve.57

CYBERSECURITY ASPECTS OF IMPROVING BUSINESS OPERATIONS OF LEGACY SYSTEMS

Slavimir Vesić[201], *Dobrica Vesić*[202]

Abstract

Legacy information systems show inertness in adapting to changes due to reduced evolutionary ability. In addition to the fact that the modernization of the legacy system is financially demanding, it is also risky. If, due to the high risk, they are unable to withdraw the system from use, the organization decides to continue its maintenance. In such a situation, one of the ways to improve business operations can be through sporadic integration with systems implemented in new technologies. Choosing an adequate integration strategy offers a whole series of challenging aspects that need to be analyzed. What is not paid much attention in practice is the security aspect. In this paper, an analysis of suitable strategies for improving the legacy system, the method of selecting the best alternative and the method of its implementation will be presented on the example of the city's waterworks and sewerage system. Migrating up-to-date data to a legacy system database with minimal software re-engineering can improve the business processes of sales, billing and maintenance of the distribution network necessary to deliver a product or service.

Key words: *Cyber security, legacy systems, data migration, critical infrastructure.*

Introduction

Organizations, like never before, are facing changes in an increasingly turbulent and complex environment. In that environment, there are various intertwined relationships in the market with customers and suppliers, relationships with employees, and between competitors. Various global factors, primarily economic and technological, and local factors such as the legal system and public opinion act on such a single environment. Business information systems as models of real systems display, maintain and change the representation of the state of the business domain for which they were originally designed and put into use [1]. In this way, they enable the organization to be in line with the changes in the environment to which it is exposed, therefore they must continuously evolve. They are very important for the organization

[201] Slavimir Vesić, PhD, Academcian of IRASA, Head of software development, PUC "Belgrade Waterworks and Sewerage", Belgrade, Republic of Serbia, vesic.slavimir@gmail.com
[202] Full Professor Dobrica Vesić, PhD, Senior Research Fellow, Academcian of IRASA, University Business Academy in Novi Sad, Novi Sad, Republic of Serbia, vesicdobrica@gmail.com

because they need to ensure continuous implementation of daily activities, and at the same time provide support when making strategic decisions. In this way, they are strongly correlated with the mission, vision and goals of the organization. If they are a faithful representation of the domain, their influence is significant and therefore it is necessary to pay attention to their long-term health and evolution.

After the development of the information system, it is put into use, when the process of its long-term maintenance begins. Over time, there is a certain gap between business needs and what the system does, so system maintenance is carried out. Over time, maintenance is not enough for the system to keep up with business and other changes, most often technological, so modernization is carried out, which is a more intensive set of activities than maintenance for the system to continue to maintain its evolutionary capability. When the system is no longer able to be modernized, and at the same time there is a big gap between the functionality it offers and business needs, then like any other product, it is withdrawn from use, ending its life cycle. For non-IT people, it seems very simple to remove a system, but practice shows that it is a much bigger problem.

A big part of that problem is the phenomenon of legacy systems. These are systems developed in the past, most often with old or outdated technology, designed and implemented following the methodological settings and development practices of that time [2]. They exhibit great inertia and defy Lehmann's laws of software evolution. Organizations and IT managers would love to get rid of them, but they can't implement it, because it can be very complex and risky. At the same time, legacy systems support core business operations and store decades of valuable knowledge about how a particular job is done. Their difficulty and complexity is that they involve not only legacy software and legacy hardware, but also legacy processes and procedures - "old ways of doing things", which are difficult because they rely on legacy software [3]. With uncontrolled changes in the system, multiple ripple effects can occur that will produce unwanted events in various other parts of the system and potentially generate a large number of errors and failures.

In the following, we will deal with the phenomenon of legacy systems, the cyber security aspects under which such a system will remain in use, as well as its improvement of functionality on the example of PUC "Belgrade Waterworks and Sewerage" through the migration of data into its database with the necessary software reengineering.

Legacy systems

The phenomenon of legacy systems is rather vague and with great variability defined in theory and research from practice. One part of the authors indicates that these are systems with certain shortcomings, difficult to change with numerous defects, bad features, high maintenance costs, etc., but that they have value for the organization [4]–[9]. Seen from the aspect of shortcomings, the legacy systems are:

- systems developed in the past
- consist of legacy hardware, legacy software, legacy business procedures and rules

- support key business processes
- difficult to understand
- hardly use the most modern technologies
- they resist changes
- restrict business operations
- their maintenance is expensive
- risky for replacement
- produce dissatisfaction at all levels of management in the company
- may have inadequate software architecture
- may have little possibility of integration with other systems
- one of the biggest challenges for professionals in the field of information systems.

On the other hand, sensing that perhaps the first group of authors does not see the problem as a whole, but focuses mainly on the shortcomings of these systems, the second group of authors decided to examine the phenomenon in practice. By looking at legacy systems from several different perspectives, insight into their "non-technical" aspects is also possible [10]–[12]. It makes it possible not to observe the phenomenon of legacy systems in isolation, thereby reducing the error in choosing a suitable modernization strategy.

Legacy systems can be viewed from 4 perspectives: developmental, operational, organizational, and strategic. The development perspective is looking at the legacy system from the point of view of the people who developed it and later maintained that system. These are business analysts, designers, architects, programmers, testers, engineers who take care of quality assurance, etc. The operational perspective includes system users, who on the one hand want a functional system, and on the other hand, a system that provides other non-functional requirements (such as interoperability and usability). Therefore, for them, in addition to the fact that it is important that the system provides the necessary functionalities, it is also important that it has the ability to exchange data with other systems, and at the same time that it is relatively easy to use so that it is easy to learn and remember how it works, and even after some time, the user can use it again, without much relearning. The organizational perspective consists of managers who evaluate the impact of the system on the organization, the support of business processes, as well as the possibility to simply slow down the reengineering of business processes when adopting a new business model. The focus of top management is that the system can be adapted to strategic activities, which can lead to changes in the business model in order to ensure the vision, mission and goals of the company. The strategic perspective also considers the costs of lost business opportunities caused by preventing the use of new technologies that the legacy system potentially cannot support.

Experience has shown that there are a large number of failed projects to modernize legacy systems, even after significant investments. For example, Cigna spent $1 billion on IS in insurance, where health insurance was recognized in inappropriate cases, the state of Florida's welfare system showed many errors after implementation, although it was overpaid by $260 million, ARM Corporation, Hilton, Budget Rent A Car and Marriot invested in the project for 4 years, in the amount of 125 million dollars, which

ultimately failed, etc [13]. These are just some of the examples in practice, there are many more, publicly disclosed or not.

Keeping the legacy system in use

In a situation where the organization does not have enough funds and resources to carry out the modernization process or withdraw the system from use and activate a new system, it keeps the existing system. On the one hand, all those risks and unplanned costs arising from the modernization or replacement of the system are eliminated, while on the other hand, there is an increase in the costs of maintaining the legacy system. The results of certain research indicate that even with very high maintenance costs, organizations decide to keep their systems in use, even if they amount to almost 90 billion dollars of planned funds, due to the very high risk of their replacement [14]. In this way, they express their reluctance to accept the risks of a potentially unsuccessful modernization effort or possibly withdrawing the existing system while starting the life cycle of a new system.
Costs are primarily determined by long-term and laborious maintenance, which often leaves development teams working on such systems in a situation to make design decisions that will reduce their effort when working on such a system, which can produce additional maintenance costs in the context of remediation of all newly created ripple effects. This is further increased if the deadlines for implementing the necessary changes are short. Second, costs are directly related to the size of the development community and the available workforce for the development environment in which the legacy system was developed. Some research indicates that about 43% of banking systems are built on COBOL, where 95% of card machines rely on COBOL and about 220 billion lines of code exist in COBOL that are still in use today [15]. To overcome the mentioned problem, the organization often hires older programmers, where some of them have already completed their working lives.

Cybersecurity of legacy systems

When an organization decides to keep a legacy system in use for some time, it needs to be prepared to implement numerous changes that will to some extent adapt the legacy system to a changing environment. We can take the banking business as an example. Although banking information systems still rely heavily on programming languages that were dominant in the past, such as e.g. COBOL, banks saw their business opportunity in offering mobile applications to their customers. Through them, users monitor payments and withdrawals from accounts, make payments, pay credit annuities, and have the possibility to convert monetary amounts from one currency to another if they have a large number of accounts, etc. Mobile applications, especially when we talk about native ones, ie. those that are directly executed on the operating system of a mobile device such as Google Android and Apple iOS, were developed in completely different, modern programming languages, e.g. Java, Objective-C, Swift, etc. The way mobile applications work and their software

architecture encourages banks to invest in the development of software integration elements that will allow these completely diverse systems to function and exchange data. In this way, organizations whose business was limited by the technological capabilities of the legacy system open up a new set of business opportunities and see an opportunity to achieve their goals. Although the user of the mobile application can make a payment through the m-banking application, he has no idea that in the background some of the transaction data that is sent may be input data for COBOL programs that are part of the core banking business.

What has been observed in practice is that when organizations implement such initiatives, they are much more focused on the achievement of business goals and often do not pay attention to a whole set of emerging problems as a result of the use of new technology or software integration with it. Software integration is the process of enabling different subsystems and applications within an organization to communicate and work together. In this context, software integration, on the one hand, can make it possible to use the value of applications within the legacy system in full size, while on the other, very often due to the use of the global network - the Internet, it puts a large number of security challenges from the cyber world in front of the organization.

Due to the highly connected world through technology, organizations that maintain a legacy system and occasionally invest in integration with other systems may face a "Black Swan" phenomenon. The term "Black Swan" means certain dangerous (risky, critical) events that cannot be predicted, but which nevertheless change the course of history [16]. This is easily noticeable in the case of critical infrastructure, which forms the most important part of the overall infrastructure. If its temporary or permanent incapacitation occurs, it will have far-reaching consequences because many infrastructural subsystems are connected [17]. It is a necessary condition for the functioning of the economy and society. The history of cyber attacks on critical infrastructure is characterized by financial losses, the ability to damage physical equipment, and the potential for human casualties [18]. The attack on the electricity network in Ukraine in 2015 was a large-scale attack that caused a power outage for about 225,000 consumers for several hours and prevented the distribution of electricity in the amount of about 73 MWh. The attack took place by taking control of the SCADA system, synergistically acting with a spear phishing attack and installing the BlackEnergy 3 malware [19]. This was followed by other attacks that maintained the intensity of this cyber operation and further compromised ICS operations. In addition to consumer data being stolen through the attack, much of the equipment was damaged during the attack itself [18]. After the attack and the great damage that was done, it took time to restore the system, and then to implement necessary measures to prevent the attack from happening again.

Therefore, a high degree of integration between subsystems can represent a major security challenge, because in this way the possibility of the vulnerability of one subsystem, and thus the entire system, increases. In a certain way, the target for cybercriminals is greater because there are more connection points and more subsystems that need to be constantly updated with software patches and fixes, which

further complicates the implementation of overall continuous monitoring. On the other hand, the organization is expected to have as simple as possible access to all its subsystems, which requires the development of a complex and very secure identity management, often formulated as "one username and one password to access everything". In practice, it is not easy to implement, so it is only a matter of time before one of the attacks will occur that will violate the 3 fundamental concepts of cyber security: confidentiality, integrity and availability.

Organizations that decide to keep the legacy information system in use, and occasionally enable new business functions by using new technology that requires integration, need to strategically approach the problem and, in addition to the expected benefits, fully consider the threats that may arise in the cyber world. Nassim Taleb in his book "The Black Swan, The Impact of the Highly Improbable" emphasizes that risk management is the knowledge to maximally mitigate the impact of unknown (inaccessible, difficult to understand) phenomena to our understanding, and not completely futile attempts to create refined methodologies and scenarios, which reflect in us the delusion that we supposedly clearly see social, economic, and technological trends and that we can therefore forecast them [20]. The same principle can be applied to the risk in cyber security, which is whether and to what extent organizations can prevent threats, and if they do not adequately assess if a breach occurs, to what extent they can mitigate the consequences of a security breach. Such a risk assessment can guide the organization towards choosing an adequate strategy when modernizing the software legacy.

Analysis of cybersecurity aspects of the improvement of the legacy system on the example of the city water utility

When an organization that at the same time wants to keep the legacy information system in production, because it assesses that it cannot currently withdraw it from use or significantly modernize it, decides to apply a new technological solution or to improve its business processes, it is necessary to look at all aspects of such activities. The legacy system and its condition largely depend on all the activities that the organization has implemented up to that point and can vary greatly from organization to organization.

On the example of PUC "Belgrade Waterworks and Sewerage", in the continuation of PUC BWS, we will look at the problem of choosing an adequate strategy for the technological improvement of the legacy system. PUC BWS has a legacy business information system, about 2.5 decades old, developed in the Progress 4GL programming language, which works with the Progress relational database. The version of the OpenEdge environment in which the system was built is 10.2B. PUC BWS has a large number of applications, developed by its forces, the most important of which are: water and sewage invoicing, billing, water meter recording, notification and monitoring of faults in the water and sewage network, procurement planning, procurement implementation, warehouse and material operations, bookkeeping etc. Progress 4GL is a domain-specific language, which means that it performs very well

operations on the domain for which it is designed, such as business applications, because they almost always rely on databases and tables as the concepts in which data is stored. This has also been a requirement that the business world has been putting in front of such systems for years. At the moment when there was progress in technologies and the need for ever-increasing availability of services on different devices, this system and similar ones showed their shortcomings in relation to general-purpose programming languages. On the other hand, in addition to the ownership and long-term tying of the organization to one software producer, a big disadvantage is that it works very hard with concepts for which it was not originally designed. So the producer himself, only if he finds interest, enables ways to expand and enrich the system. Progress OpenEdge technologies are owned by PSC Corporation.

Address data are the most important for the following business operations at PUC BWS: water meter reading, water invoicing (billing), registration and monitoring of repairs to water and sewerage network failures and leakages, records of customers and suppliers, etc. Address data needs to be refreshed periodically, to improve the previously mentioned business operations. The Republic Geodetic Authority, hereafter RGA, is the institution that manages the address system at the level of the Republic of Serbia, and it initiates all changes that occur in address data. For PUC BWS to use the address data, it needs to download it from RGA through software integration.

During 2023, an analysis was conducted and two different approaches to integration were compared. The first approach included the creation of a Web service that would aquire data via the Internet and load it into the legacy system through the RGA IT infrastructure. The second approach included manual data download from the RGA portal and their migration to the database of the legacy system. Both approaches have advantages and disadvantages that are revealed after the analysis from the aspects of costs, current level of knowledge, required level of knowledge, time to reach the required level of knowledge and security aspects. The results are shown in Table 1.

Table 1: comparison integration approaches

Approach	Web services	Migration
Advantages	higher degree of automation	low costs intermediate level of current knowledge short leveling time low security risk
Disadvantages	high costs low level of current knowledge high level of knowledge is required low leveling time high security risk	lower degree of automation high level of knowledge is required

The analysis showed that although Web services as a strategy had several disadvantages, the company was ready to make investments to eliminate them due to the advantages that this strategy offers. In the end, it was rejected because there is a high-security risk that is very difficult to remove or mitigate the consequences of a

potential cyber attack, because the Web service technology is based on the publicly available Internet and as such is subject to numerous vulnerabilities. Cyber attackers are very good at analyzing these vulnerabilities using dedicated software packages and then using known network mechanisms that allow them to carry out cyber security attacks. In addition, in the recent past, RGA has been the target of serious cyber-attacks that caused service unavailability [21]. Therefore, in the case of taking data from RGA, the decision was made that migration is a better strategy primarily due to the high cyber security risk.

Data migration into the legacy system

Migration as one of the important strategies has its place when we want to migrate data from the legacy system to the database of the new system. Also, although it is not often in practice as in the case mentioned above, we can perform the migration in the opposite direction, i.e. to migrate the data to the database of the legacy system. This may be justified in a situation where we want to keep an existing legacy system in use while improving business operations with minimal software reengineering. As the new data is up-to-date, it can enable the company to make certain business processes more efficient.

In cooperation with RGA, PUC BWS has taken up-to-date data together with spatial data and with a completely new data model that includes a new and more complete address system. The competent department for the geographic information system migrated the data to the database SQL Server 2019 of the ESRI ArchGIS system.

To improve the business processes of invoicing and sales, as well as the business processes of reporting and repairing faults in the water and sewage network, along with updating data on customers and suppliers, the programming team was given the task of migrating data from SQL Server 2019 to Progress OpenEdge 10.2B database and then perform minimal software re-engineering in legacy system applications to use the new address model and up-to-date data. For this purpose, the following activity plan was defined:

1. fetching data from the SQL Server database, transformation and loading into the Progress database of the legacy system;
2. creation of program procedures for automatic mapping of the existing street code book with the new one;
3. creation of a software solution for manual mapping of the existing street code book with the new one in case it is not possible to carry out automatic mapping
4. implementation of software reengineering in order to modify the existing applications of the legacy system and connect them with new data.

In the first phase, it started with an ETL process that retrieves data from a data source in SQL Server, transforms it appropriately and loads it into a destination, ie. tables in the Progress database. In order for the mentioned phase to be realized, it was necessary to choose a suitable tool for carrying out the ETL process. There were two options: OpenEdge DataServer for Microsoft SQL Server and Microsoft SQL Server Integration Services (hereafter SSIS). OpenEdge DataServer for Microsoft SQL Server

is a solution of PSC Corporation, and it enables access to the SQL Server database by writing queries in the Progress 4GL programming language. By executing the program code in the procedures of the Progress 4GL programming language, the entire ETL process is implemented. Microsoft SQL Server Integration Services is a software package that enables ETL operations to be carried out through the Visual Studio integrated development environment by creating appropriate diagrams and running them.

To select an adequate tool for the implementation of the first phase of the project, a comparison of these tools was made according to 3 criteria: mode of operation, speed of operation and representation of errors created in the ETL process in the tool itself. The results are presented in Table 1.

Table 2: ETL tool comparation

Criterion	**OpenEdge DataServer for Microsoft SQL Server**	**Microsoft SQL Server Integration Services (SSIS)**
mode of operation	typing the code (programmatically)	drawing a diagram (mostly visual)
speed of operation	lower	higher
representation of errors	unclear	clear

In the first tool, the code is typed as for any Progress 4GL application, where for each table it is necessary to create a separate part of the code or a separate procedure, while in the second tool, it is possible to do this by modelling the interaction between the source and the destination, whereby the data flow between can go through a certain number of transformations. In this way, the SSIS tool proved to be much more productive for development compared to the manual coding that is applied in the DataServer for Microsoft SQL Server tool, especially in a situation where it is necessary to carry out the ETL process on a large number of tables. In terms of speed, the comparison was made on 120,000 rows from one table, and SSIS processed the entire data set almost twice the time. The third criterion is the representation of errors, wherein a certain number of cases it has been shown that SSIS provides a much clearer representation of the errors in the ETL process, which allows the development team to correct them in a shorter time. The largest number of errors was related to the use of inadequate data types, where in SSIS even before starting the entire processing, which can take several hours, it was immediately seen that the type conversion was not correct, which is not the case with OpenEdge DataServer and the software manufacturer didn't make an extra effort to display clearer messages in those situations.

The project is currently at the end of the third phase and after that, it will move on to the implementation of the last one. It is expected that fresh and up-to-date data will contribute to an increase in income, through more accurate delivery of bills and other business documents to up-to-date addresses of consumers, while on the other hand, the timely elimination of failures, leakages and problems in the distribution network of water and sewage will make consumers have even greater trust in the company's services, and therefore will pay for them more regularly. In this way, much better

communication with customers is achieved, which puts them in focus [22]. This contributes to the creation of greater trust, thereby achieving stability in the billing of an important first-rate entity that constitutes a critical infrastructure.

Conclusion

When implementing integration and choosing an integration strategy, it is important to conduct an analysis and compare all aspects. The aspect of security is also very important because it directly depends on the extent to which a certain business will be able to continue its work due to the increase of spaces suitable for carrying out cyber attacks by malicious users. Data migration can also be used in the opposite direction from the usual when we want to improve the business operations of a company that has a legacy system with minimal software reengineering. This is justified in a situation where it is not possible to make significant modernization efforts, due to limited resources or due to high risks when the system cannot be withdrawn from use, while there is an opportunity to improve the core business using up-to-date data from other systems. In the example of PUC BWS, a strategy for improving the legacy system was defined, and the migration to the database of the legacy system was one of the phases. With the completion of the entire project, it is expected that the strategy will give results, primarily in the processes of invoicing and maintenance of the distribution network.

References

[1] S. L. Vesić, "Towards smart city: Modernization of Legacy Systems of the City Waterworks on the Example of PUC Belgrade Waterworks and Sewerage," in *IRASA - Fourth International Scientific Conference - SCIENCE, EDUCATION, TECHNOLOGY AND INNOVATION - SETI IV*, 2022, 439–448.
[2] S. L. Vesić, "Uticaj razvoja IT tehnologija na prevazilaženje problema nasleđenih sisitema," *Kult. polisa*, vol. XVII, no. 42, 667–678, 2020.
[3] I. Sommerville, "Legacy systems," *Software Engineering*. https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Web/LegacySys/index.html (accessed May 12, 2020).
[4] W. S. Adolph, "Cash cow in the tar pit: reengineering a legacy system," *IEEE Softw.*, vol. 13, no. 3, 1996, doi: 10.1109/52.493019.
[5] L. Aversano and M. Tortorella, "An assessment strategy for identifying legacy system evolution requirements in ebusiness context," *J. Softw. Maint. Evol.*, vol. 16, no. 4–5, pp. 255–276, 2004, doi: 10.1002/smr.296.
[6] K. Vestues and R. Knut, "Making Digital Infrastructures More Generative Through Platformization and Platform- driven Software Development: An Explorative Case Study," in *Tenth Scandinavian Conference on Information Systems (SCIS2019)*, 2019, 1–15, [Online]. Available: https://aisel.aisnet.org/scis2019/4.
[7] K. H. Bennett, "Legacy systems: coping with success," *IEEE Softw.*, vol. 12, no. 1, 1995, doi: 10.1109/52.363157.

[8] R. Nassif and D. Mitchusson, "Issues and approaches for migration/cohabitation between legacy and new systems," in *SIGMOD '93: Proceedings of the 1993 ACM SIGMOD international conference on Management of data*, 1993, 471–474, doi: 10.1145/170035.170145.
[9] W. Nowakowski, M. Śmiałek, A. Ambroziewicz, N. Jarzębowski, and T. Straszak, "Recovery and Migration of Application Logic From Legacy Systems," *Comput. Sci.*, vol. 13, no. 4, 2012, doi: 10.7494/csci.2012.13.4.53.
[10] A. Alderson and H. Shah, "Technical Opinion: Viewpoints on legacy systems," *Commun. ACM*, vol. 42, no. 3, 115–116, 1999, doi: 10.1145/295685.295722.
[11] D. Bojić and D. Velašević, "Softversko reinženjerstvo - pregled stanja," in *Infoteh*, 1999.
[12] R. Khadka, B. V. Batlajery, A. M. Saeidi, S. Jansen, and J. Hage, "How do professionals perceive legacy systems and software modernization?" in *ICSE 2014: Proceedings of the 36th International Conference on Software Engineering*, 2014, 36–47, doi: 10.1145/2568225.2568318.
[13] W. M. Ulrich and P. H. Newcomb, *Information Systems Transformation: Architecture-Driven Modernization Case Studies*. Morgan Kaufmann OMG Press Titles, 2010.
[14] United States Government Accountability Office, "GAO-19-471 - INFORMATION TECHNOLOGY - Agencies Need to Develop Modernization Plans for Critical Legacy Systems," 2019. Available: https://www.gao.gov/assets/700/699616.pdf.
[15] D. Cassel, "COBOL Is Everywhere. Who Will Maintain It?" https://thenewstack.io/cobol-everywhere-will-maintain/ (accessed May 30, 2020).
[16] L. Papić, "Theory of 'Black Swan' Events: Risk of Human Blindness According to Randomness," in *ICDQM-2016, 19th International Conference Dependability and Quality Management*, 2016.
[17] S. L. Vesić and M. Bjelajac, "CYBER SECURITY OF A CRITICAL INFRASTRUCTURE," *Pravo - Teor. I Praksa*, vol. 40, no. 2, 77–88, 2023, doi: 10.5937/ptp2302077V.
[18] T. Alladi, V. Chamola, and S. Zeadally, "Industrial Control Systems: Cyberattack Trends and Countermeasures," *Comput. Commun.* vol. 155, 1–8, 2020, doi: 10.1016/j.comcom.2020.03.007.
[19] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physicalenvironment," *Electr. Power Syst. Res.*, vol. 149, 156–168, 2017, doi: 10.1016/j.epsr.2017.04.023.
[20] N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed. Random House Trade Paperbacks, 2010.
[21] A. Bojović, "Hakerski napad na katastar," *Politika*, 2022. https://politika.rs/sr/clanak/509880/Hakerski-napad-na-katastar (accessed Jul. 01, 2024).
[22] G. Radivojević, G. Šormaz, B. Lazić, and B. Tasić, "CRM Strategy - Description and Effects," in *ICDQM-2010, 13th International Conference Dependability and Quality Management*, 2010.