Smart Automation for Enhancing Cybersecurity

Ângelo Neves
Expert, 20192365@academia.uatlantica.pt

Virgínia Araújo
Professor, varaujo@uatlantica.pt

Department of Information Systems, Atlântica University Institute, 2730-208 Barcarena, Lisbon, Portugal

Abstract

In an intelligent automation ecosystem, namely in the context of Robotic Process Automation, there is a need to review the development and operation processes and practices. One must combine competences from these two areas for any organization's security. It is with security that quality, efficiency, and profitability become possible.

The elaboration of guidelines and best practices for the application of a DevSecOps culture is absolutely essential for Agile software development at any organization. In the digitalization era, teams increasingly need a collaborative method to involve several competencies and capabilities, from analysis to the implementation and evolution of a software product. Information security must be an integral part throughout the entire product's lifecycle, as without it, fundamental aspects of confidentiality, integrity, and availability put information and software security at risk of serious implications for the organization's business activities.

Without losing focus on customer needs, it is necessary to model software development practices, following more agile methodologies. In this way, teams can model the software throughout its lifecycle, focusing on adding value for the customer and ensuring they have greater certainty that requirements, plans, and results are 100% aligned with their needs.

This paper presents an analysis of and proposal for the continuous improvement of an intelligent automation platform at a large-scale multinational organization. In parallel, aspects that generate resistance to the implementation of a DevSecOps methodology within the scope of RPA code development are considered.

Keywords: robotic process automation (RPA); business process management; DevSecOps; intelligent automation

Citation: Neves A., Araújo V. (2023) Smart Automation for Enhancing Cybersecurity. *Foresight and STI Governance*, 17(1), 89–97. DOI: 10.17323/2500-2597.2023.1.89.97

Introduction

At any company or organization, there are numerous low-risk administrative tasks that are mandatory for the proper functioning of business processes. However, many of these tasks are repetitive and, in addition to being time-consuming, are obsolete, outdated, and could be performed more efficiently. Thus, an increasing number of companies are seeking to minimize their impact upon the productivity and efficiency of each employee.

Meetings, administrative tasks, e-mails, and answering phone calls consume a lot of employees' time in an organization and are sometimes are a source of distraction during the execution of certain repetitive tasks. As a result, performance and focus are inevitably reduced substantially, reflecting upon employee productivity and their contribution to the most important tasks for the organization.

According to research published in a Harvard Business School article, some breaks can be welcome for those who have been working hard, but the fact remains that humans are easily bored by repetitive tasks. The study found that when assigning a repetitive task to an employee for much longer than necessary, the person prefers to prolong this tedious task rather than finish it as quickly as possible (Brodsky, Amabile, 2018).

RPA, or Robotic Process Automation, is a technology that uses robots to do tasks previously performed by humans. These are not just any tasks, but rather repetitive activities that do not require critical thinking. Leading global giants such as Bosch, Siemens, Caterpillar, and others are constantly coming up with innovative ideas to optimize their processes. The main areas of automation are the inventory of products, the movement of goods around production facilities and warehouses with logistics optimization, safety monitoring, document management, and many more (Lu et al., 2020). By implementing these new technologies, manufacturers have more opportunities to speed up the production cycle, minimize human error, and improve productivity and product quality (Quazi et al., 2022).

However, the higher the degree of automation, the higher the cybersecurity risks and threats to the functioning of organizations. Proactive, customer-focused security opens the opportunity to anticipate, rather than react, to data breaches or cyberattacks. DevSecOps (acronym for development, security, and operations), when implemented correctly from the beginning of the software lifecycle, allows you to reduce the costs associated with fixing security flaws by incorporating security into every step of the software development process. This approach can also be applied in the context of Robotic Process Automation (RPA).

Information security should be intrinsic in all Robotic Process Automation platforms, as well as in all planning, design, construction, testing, implementation, and evolution activities, focusing on data security, privacy, and authentication. One must enfore role-based access control to restrict access to the application based on the functions of each user.

Better control and management of activities within the scope of RPA, through the application of DevSecOps practices and with the automation of code review, is a significant asset for the quality of software releases, significantly reducing the number of incidents in production.

Robotic Process Automation

Robotic Process Automation or RPA is a software technology that streamlines the construction, implementation, and management of software robots that emulate human actions interacting with other software and digital systems. These robots perform a set of tasks following a process without any human intervention. All these technologies reduce the manual workforce, allowing organizations to automate business operations in an agile and cost-effective manner.

RPA can use Application Programming Interface integrations as well as other automation technologies including Artificial Intelligence, Machine Learning models, and cognitive services such as Chatbots, Natural Language Processing, and Optical Character Recognition.

Through this technology, repetitive tasks can be automated, allowing employees to focus on more specialized and critical work. Furthermore, it can be seen in organizations as a potential method to streamline business operations, reducing personnel costs and reducing human error. This consistency can lead to fewer errors in key processes and, ultimately, increased revenue and improved customer service, which leads to greater customer satisfaction.

RPA presents itself as an efficient and productive solution for many tasks. For example, processing invoices is among the most time-consuming tasks. Invoices arrive through various channels and are then combined with purchase orders, and often need to be approved by different people for payment. In this way, it is possible to create rules to automatically send invoices to the right entity for approval, thus creating an improvement in the payment approval workflow. It is also possible to automate the purchase order review process using a checklist for further review before submitting for payment.

RPA implementations are popular in the banking and manufacturing sectors, it is also notable for its implementation in insurance, healthcare, high technology, and utilities such as telecommunications and energy in terms of accounts payable, accounts receivable, and general ledger processing. Whereas card activation, fraud claim discovery, claims processing, new business preparation, reporting automation, and system reconciliation process have high potential in banking and financial services, insurance, and healthcare sectors (Madakam et al., 2019).

DevOps vs DevSecOps

Modern development practices rely on Agile methodology, which prioritizes continuous improvement versus the Waterfall sequential approach. If development teams work in silos mode without considering operations and security, the product developed may have operational problems or security vulnerabilities that may be financially or operationally inefficient[1].

DevOps (acronym for development and operations) has gained notoriety in recent years for combining key operating principles with development cycles, recognizing that these two processes must co-exist during the product lifecycle. Siloed post-development operations can make it easier to identify and address potential issues, but this approach slows software delivery. Implementing operations in parallel with software development processes allows organizations to reduce implementation time and increase overall efficiency (Lwakatare et al., 2019; Azad, Hyrynsalmi, 2021). DevOps is used in many large companies from the fields of electronics, online commerce, and delivery services (e.g., Starbucks, Etsy, Apple, Airbnb, Ashley Madison, etc.) and government agencies (US Federal Reserve, NASA, etc.) (Plant et al., 2022; Rzig et al., 2022).[2]

DevSecOps is an evolution of the DevOps approach, extending its capabilities by focusing on proactive cybersecurity assurance. DevSecOps is the efficient integration of testing and security protection throughout the software development and deployment lifecycle. Therefore, it will be necessary to think about the security of the application and the infrastructure from the beginning. In this multi-layered security approach, the focus is not just on establishing a layer of protection around applications and data, but on the entire context of implementation and integration, operation and maintenance, and use by end consumers.

Just like DevOps, DevSecOps is a mindset that needs to be shared by all team members who participate in the development and implementation of software. The adoption of an information security and cybersecurity culture along with other requirements, allows for sharing responsibility for any specific technology or technique, developing security methodologies that allow for greater control and speed in the management of vulnerabilities and security risks.

The goal of DevSecOps is to release software with higher quality, quickly and safely, thus following the same logic as DevOps. If security is implemented only at the end of the development pipeline, organizations using DevOps can become less efficient, as by not adopting built-in security, the likelihood of duplicate revisions and unnecessary recompilations increases, resulting in a longer delivery time, or even creating less secure code (Rajpakse et al., 2022).

DevSecOps is the movement working on the development and integration of modernized security methods that can keep up with DevOps. DevSecOps is a tactical three-pronged approach that connects three different areas: development, information security, and operations (Myrbakken, Colomo-Palacios, 2017). The goal is to seamlessly integrate security into the Continuous Integration & Continuous Delivery/Continuous Deployment. The CI/CD pipeline is a series of automated steps that must be performed to deliver a new version of the software. We can consider it a complete set of activities performed to improve the efficiency and effectiveness of software delivery throughout the software development lifecycle via automation.

DevSecOps has been successfully implemented by very different companies - Microsoft, Verizon, and the Pokemon Company - to ensure that their development and security teams work together smoothly (Swinhoe, Nadeau, 2019). For example, Verizon created a dashboard to monitor the occurrence of vulnerabilities in its business applications at all stages of the lifecycle (when it occurred and by whose fault). A comprehensive picture of vulnerabilities gives developers near real-time signals of the risks they may pose to the business, allowing them to find ways to improve their skills. The Pokemon Company, using DevSecOps, created a security framework to prevent leaks of the personal data of online game users, which improved the overall corporate security culture.

Finally, Microsoft created a tiered system of communication and experience sharing between different development teams. At the entry level, all employees are trained in standards of business conduct, including security. The next level allows for more in-depth security issues for all employees. The third level is for Microsoft engineers only. This is closed-door training that introduces them to what threat actors do and helps them understand the landscape

[1] https://threatpost.com/apps-built-better-devsecops-security-silver-bullet/167793/, accessed 22.01.2023.

[2] See also: https://digital.ai/catalyst-blog/9-companies-you-wouldnt-expect-to-be-using-devops/, accessed 22.01.2023.

of global risk. Developers and engineers learn the reasons behind Microsoft's security practices, the methods and tactics used by hackers, and the engineering tools available. The goal is to help them build a network of peers and resources that can be used to secure any project. The overall conclusion is that the better security professionals and developers understand what the other team is doing, the more responsive and cooperative they will be in the development process. This will lead to fewer vulnerabilities in the final product and faster fixes.

As new types of cyberattacks increase, securing development and CI/CD environments becomes increasingly important. An effective focus on security at the early stage of the development cycle, continuing throughout the product lifecycle, ensures that developers write more secure code, adopt security best practices, and respond quickly to vulnerabilities.

Case Study – DevSecOps Integrated into the RPA Platform

For business processes, the term RPA often refers to setting up software to do work previously done by people, such as transferring data from various input sources, such as email and spreadsheets, to systems of record, such as Enterprise Resource Planning (ERP), and Customer Relationship Management (CRM) (Lacity et al., 2015).

Deloitte defends that the design of the process is more relevant for the Return on Investment than the technology used. A published use case refers to the experience of a bank in the implementation of RPA technology, in which the bank redesigned its claims process, introducing 85 robots to run 13 processes, handling 1.5 million claims per year. The bank added capacity equivalent to 230 full-time employees at approximately 30% of the cost of recruiting more employees (Schatsky et al., 2016).

Regarding the present case study, Siemens Global Business Services focuses on digital solutions for business process optimization and, increasingly, value-add digital services. In 2017, Siemens decided to implement its first global RPA platform to serve the various internal services. The chosen RPA technology was from Blue Prism, as it is one of the most reputable market leaders. One of the key aspects was the fact that it was one of the pioneering and most mature brands on the RPA technology market. Assessing the state of the current RPA market, Gartner (Gartner, 2022) has identified 15 of the most notable RPA providers that offer complete enterprise solutions that can support an intelligent automation ecosystem or enterprise-wide RPA utility, where it features Blue Prism as a leader. Blue Prism's solutions are designed for large companies. It provides strong support for back-office automation and therefore it has become more suitable for industrial manufacturing companies and healthcare companies (Khan, 2020).

Compared to what the competition offered at the time, Blue Prism stood out for its centralized management, providing for the easy deployment of autonomous robots (fully automated runtime resources), but also meeting Siemens' mandatory financial and security policies so that it would be possible to implement this technology in the context of services within ICFR. Blue Prism fulfilled the main requirement for a Siemens technology partner in compliance with all these rules. Internal control over financial reporting (ICFR) is a process consisting of control policies and procedures to assess financial reporting risk and provide reasonable assurance that an enterprise prepares reliable financial statements. This prevails in the Sarbanes-Oxley Act (SOX), which requires companies to disclose their financial practices.

In this research, the RPA platform is analyzed in terms of its efficiency regarding the integration of the DevOps methodology with the security requirements of the organization. Siemens AG, in the context of digital services, has developed a shared service that includes support for internal Business Process Management. A centrally managed Blue Prism RPA platform automates repetitive, routine, and rules-based processes based on structured data entry. The RPA platform also integrates with other technologies to drive end-to-end automation. This platform is designed considering development, test, and production environments. All environments follow a logical and physical segregations, and at the level of the production environment, there is also the physical segregation of data.

Blue Prism software runs a predefined algorithm on the Runtime Client, i.e., a software robot, which allows the software to authenticate itself to the target applications in an encrypted form and interact with the GUI (Graphical User Interface) of the target applications such as running read/write data into user interface fields, interacting with elements like buttons or sliders, and so on, just like a human user would. An automated process is capable of operating multiple target applications. To operate a target application, the robot needs a user account and appropriate permissions within the target system, therefore, the robot is subject to the segregation of duties, respecting the principle based on shared responsibilities of a key process that disperse the critical functions of this process by more than one person or department. In this case, the same authentication in a system, for example SAP, could not register a purchase order and approve it.

Automated process diagrams are business workflows, which act like software programs. These diagrams use basic programming concepts and create operational process flows as flowcharts. They are basically graphical representations of workflows to create, analyze, modify, and scale the capacity of the business. Every RPA developer has access to the Blue Prism application development environment. For this, environment segregations were created so that it is possible to maintain the Segregation of Duties in accordance with what is required for the security of the entire RPA platform. It is in this environment that processes and objects are created, which are then tested in the test environment and only after the User Acceptance Test has been successfully performed is the automation distributed to production, all this integration is executed and managed by the Release Manager, by CI/CD or on an ad-hoc basis.

In the RPA service created exclusively for the Siemens organization, this approach aims to provide services for the development and management of the operation of RPA automations, for different business units of the organization. It appears that the demand for automated internal services is growing and technological integration is heterogeneous. It can be said that each automation task performed by RPA implies a specific level of development, which makes each software robot unique, both in terms of access to applications and in the diagram of the developed process.

The development of RPA automations based on the software factory approach can bring benefits when compared to conventional software development approaches. Among these benefits, consistency in delivery stands out, as it is possible to share the same resources and similar logic, although it is necessary to share knowledge such as training, documentation, and frameworks. However, using this approach to consistently apply previously acquired knowledge while developing multiple RPA automations can be an inefficient and error-prone process. Another benefit is the quality, due to the integration of reusable code it is possible to save time and resources in the development of automation, allowing one to dedicate more time to working on the unique functionalities of each automation. The expectation is that the probability of design flaws and code errors will be reduced, but without consistency in delivery excellence, it will be difficult to reduce the effort to deliver with quality. Finally, productivity, efficiency, consistency, and quality are discussed and allow for the delivery of each project in the shortest possible time with greater capacity to deliver new projects using the same resources.

Even after release for production, continuous monitoring is carried out. Whenever there is an irrecoverable failure in the robot's operation, the control room manager must alert the developer and the process owner to the fact that the robot is unable to perform the programmed task. Evidence of the operation is collected and the error is checked in detail. The incident can originate from different root causes. It could be something related to the software running on the virtual machine, communication/network issues, or automation issues. The latter might be identifiable if something in the application to be automated changed, or even whether the business process itself changed, but these changes were not reflected in the RPA process. In case of failure at the workflow level of the RPA process (process diagram), developer intervention will be required to resolve the issue.

In cases where it is necessary to correct an automation that is already in production, most of the time the developer will need to access the application to be automated in production to understand the differences in relation to what was developed in the quality environment. To fill this gap, a Blue Prism environment for emergency changes was created.

In the emergency Blue Prism environment, it is possible for the developer to use the production systems to minimize any differences found between the quality environments and the production environments. Therefore, in an automation for handling invoices or purchase orders in SAP, sometimes the quality assurance (QA) environments do not have the same quality in terms of data volume or its heterogeneity, which makes automation training difficult with dummy data.

Development in this emergency environment is part of Siemens' plan for its Business Continuity Management, thus enabling faster recovery from a failure, restarting the service as quickly as possible so that the business does not suffer a major impact due to downtime caused by the incident or disaster.

In the continuous integration and delivery process, an automation approach is adopted, integrating the RPA concept in pipeline management. The RPA automation itself generates the concept of a CI/CD pipeline, allowing all the delivery management of new automations to be carried out in an automated way.

It is important that there are no inconsistencies in the tests performed on the UAT for new automations and major change requests. Documentation should show what type or level of tests were performed to facilitate the assessment of code integrity and resiliency. This procedure is not yet fully automated and it is at this stage that the quality control and acceptance of the authorization terms for passing the code to production is determined. The higher the number of incidents or bugs, the higher the reoccurrence of debugging in the emergency environment, which leads to a higher number of Emergency Change Requests, which in turn increase the CI/CD delivery pipeline. In certain cases, such as minor changes, validations, or tests, steps are skipped and the move to production is straightforward.

Intelligent Automation

RPA solution technologies, especially Blue Prism, allows people other than software developers to automate certain business processes quickly and cheaply. It is aimed at processes that are highly rule-oriented and whose requirements are very tactical or short-lived, aimed at justifying development in IT organizations that follows a service-oriented architecture (SOA), as well as those that encompass a set of tools of business process management (Slaby, 2012).

The Intelligent Automation Platform constitutes an RPA tool that has the capability of the workforce driven by software robots.[3] The software is developed in the Microsoft.Net Framework and supports several platforms such as IBM Mainframe, Windows, Windows Presentation Foundation (WPF), as well as Java or the web. The tool offers visual design in a top-down approach, view from the most general level to the most specific level, and with drag-and-drop functionality, allowing even non-technical users to automate a process by dragging components through a user-friendly interface.

Such characteristics ensure compliance with established security policies (configurable) and provide robust features as this system protects data through encryption and obfuscation. Algorithms ensure secure connectivity, storage, and access to data.

In terms of access control, this allows management to restrict functions by group of users, such as authorizing specific user access to groups of robots, processes, and objects. Blue Prism software supports Payment Card Industry Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act (SOX) in order to provide the necessary security and governance.[4]

Such programs enable scalability with centralized management. This tool is designed to work intelligently without the need for manual interaction in all executions that occur in the automated process. To this end, the software provides a scheduling management module (Control Room), which allows for the automatic execution of an automated process according to a specific time. Thus, all processes can be automated as needed and can be monitored centrally. An enhanced monitoring tool provides detailed real-time feedback on robot status and health for a complete view of the entire digital workforce.

Blue Prism software is also known to be one of the main choices for large-scale implementation. In April 2015, Telefónica O2, owned by Telefónica Group, deployed more than 160 Blue Prism "software robots" that process between 400,000 and 500,000 transactions per month, generating a three-year return on investment of between 650% and 800% (Lacity et al., 2015).

Analysis of the Continuous Improvement Process

Siemens GBS strives for excellence in its digital services and is looking for continuous improvement processes that allow it to adapt its services to the most demanding quality controls.

Quality assurance has the potential to reduce errors or failures in the delivery of a provided service. In the case of RPA, the methods used aim to accommodate any development in the quality assurance of the target applications – systems that will be manipulated by RPA automation – which are not the best environment to develop processes with more resilience to errors. Therefore, it is necessary to create other mechanisms that can help create processes with the best quality. Increasing security automation in the development cycle reduces the risk of errors and the danger of misadministration, which could inadvertently lead to attacks or outages in the RPA service.

A code review aims to improve the quality of the final product, in this case, we will cover the RPA code. It is a systematic approach to reviewing other developers' code for bugs and many other quality metrics. Additionally, a code review verifies that all requirements have been implemented correctly. This process must be planned and executed at an early stage of development, timing is paramount as the review must be anticipated as soon as possible because a late and unplanned code review is more likely to be forced when robots are already running in production, which creates complications.

Security should be the focus throughout the development lifecycle. It is essential to regulate RPA security issues with a set of specialized controls. Creating threat models during the design phase, educating developers on secure programming practices, and

[3] https://www.blueprism.com/products/intelligent-rpa-automation/, accessed 22.01.2023.

[4] https://www.blueprism.com/resources/white-papers/how-blue-prism-sets-the-standard-for-secure-rpa/, accessed 22.01.2023.

conducting frequent code reviews with the relevant security teams will help increase overall code quality and reduce the number of issues reported during a secure code review.

An unplanned approach to continuous improvement creates the potential for business continuity risks, more specifically, this is the case when a large volume of objects is based on an old version of a given application. There is no RPA automation that is not affected by time, every week new technologies appear on the market and Siemens monitors the necessary updates so that its infrastructure remains secure to avoid the existence of software that is no longer supported and at the end of its life cycle. Due to these changes and innovations, it is necessary to perceive development in RPA as something changes.

As part of a robotic process automation governance framework, regular risk reviews and audits of RPA processing activities are required. Employees under the responsibility of the RPA service must be clear about their security responsibilities, which include managing access to the robotic process automation environment, logging, and monitoring operations, and so on. There should be defined duties for conducting regular RPA information security compliance assessments and a checklist of security requirements for existing robotic process automation technologies. The respective cataloging of Confidentiality, Integrity, and Availability (CIA) levels of each RPA process must be considered in order to speed up the identification of risks in consequent audits of Internal Control over Financial Reporting (ICFR). CIA describes three crucial components of data and information protection which can be used as guides for establishing the security policies at an organization. If security on the RPA platform fails, the operations logs will need to be examined and reviewed by IT and security teams. Robotic process automation logs must be stored on a separate system in order to protect their security and forensic integrity.

The process of developing new RPA automations, in the first instance, needs to involve more criteria regarding the security and quality of the code. A secure code is higher quality code. Automated code review tools are essential for standardizing and scaling RPA code development efforts. It is necessary to review the RPA script or code as early as possible, so that the time spent on development is not in vain and to minimize the chances of repreatedly rewriting the code.

Conclusions and Future Work

RPA has already seen significant uptake in practice to support an intelligent automation ecosystem or enterprise-wide RPA utility. Contrasting with this practical adoption is the relative lack of attention to RPA in the academic literature (Syed et al., 2020; Ivancic et al., 2019). With the purpose of contributing to initiatives to achieve significant advances in the field, this study was conducted. It was based on the large-scale implementation of an RPA service, at Siemens GBS, which in its portfolio of RPA use cases, has hundreds of processes and objects for intelligent automation. The essential criteria for the theoretical foundations and practical understanding of the DevOps model in the areas of intelligent automation were approached, thus allowing for the implementation of DevSecOps in the RPA service of Siemens GBS. For this concept to work, it was essential to implement an Agile methodology by all teams inherent to the service, maintaining a culture of cooperation and involvement in aspects of continuous improvement and security throughout the entire life cycle of the product/RPA code.

It is necessary to provide tools that allow developers and operations to benefit from the aspect of efficiency and quality in the development of an RPA code and thus reduce bug fixing after delivery in production to considerably reduce downtime in the service of RPA robots. This goal will only be possible if both teams work on a collaborative model. By switching from a separate delivery model to the operations model, benefits are gained in terms of maintaining RPA cases after production delivery. The advantages can be significant when it comes to a large-scale implementation, which requires constant adaptations or changes to the already developed code.

An automatic code review solution mirrors the existence of flaws in the RPA code that need to be corrected. The use and integration of this solution in the Siemens GBS RPA service will be able to promote quality and thus improve resource management. It will be a major investment for the stabilization of the RPA platform, allowing for the development of safer, more stable and resilient automated processes that require less effort.

It is important to review the test controls by architects or senior developers, as the ease of debugging in production increasingly creates a risk at the security level. During a code change, fundamental security aspects must be taken into account, not only by looking at the developed code, but also at the entire process inherent in the development of a change in RPA use. This could involve the need to deliver a code for production without the correct testing process, or the non-involvement of the customer which poses a potential risk of the need for debugging in the post-production stage. Test environments should simulate all potential functionalities as much as possible and if it is not possible to apply all functional requirements, the development team should involve the operations team in the first instance as well.

The stability of an RPA platform in production is only achieved if there are fundamental requirements that are not ignored, as such exceptions increase risks and make cybersecurity attacks targeting RPA platforms more likely.

Most companies prefer to develop RPA software robots over multiple iterations using an Agile development methodology as this delivers faster value to customers. However, RPA implementations can include a mix of heterogeneous applications, components, and technologies running on multiple operating systems. As automation becomes an integral part of digital transformation, organizations are increasingly embracing robotic process automation as it is easy to implement and uses software bots that reduce operational costs and improve efficiency. The actual costs of an RPA implementation largely depend upon the scalable power of the platform, as well as the quality provided during robotic process development. The lower its quality, the higher the maintenance costs. The inoperability of a software robot entails maintenance costs for a platform without the desired profitability.

References

Azad N., Hyrynsalmi S. (2021) What Are Critical Success Factors of DevOps Projects? A Systematic Literature Review. In: *Software Business. ICSOB 2021 Proceedings* (eds. X. Wang, A. Martini, A. Nguyen-Duc, V. Stray), Heidelberg, Dordrecht, London, New York: Springer. https://doi.org/10.1007/978-3-030-91983-2_17

Brodsky A., Amabile T.M. (2018) The downside of downtime: The prevalence and work pacing consequences of idle time at work. *Journal of Applied Psychology*, 103(5), 496–512. https://doi.org/10.1037/apl0000294.

Ivančić L., Suša-Vugec D., Bosilj-Vukšić V. (2019) Robotic Process Automation: Systematic Literature Review. In: *Business Process Management: Blockchain and Central and Eastern Europe Forum, Vienna, Austria, September 1–6, 2019, Proceedings* (eds. C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar-Štemberger, A. Kő, M. Staples), Heidelberg, Dordrecht, London, New York: Springer, pp. 280–295..

Khan S. (2020). Comparative Analysis of RPA Tools-Uipath, Automation Anywhere and Blueprism. *International Journal of Computer Science and Mobile Applications*, 8, 1–6. https://doi.org/10.47760/ijcsma.2020.v08i11.001

Koskinen A. (2019) *DevSecOps: Building security into the core of DevOps,* Jyväskylä: University of Jyväskylä. https://jyx.jyu.fi/handle/123456789/67345, accessed 17.10.2022.

Lacity M., Willcocks L., Craig A. (2015) Robotic Process Automation at Telefónica O2 (The Outsourcing Unit Working Paper 15/02), London: The London School of Economics and Political Science, accessed 21.01.2023.

Lu Y., Xu X., Wang L. (2020) Smart manufacturing process and system automation – A critical review of the standards and envisioned scenarios. *Journal of Manufacturing Systems,* 56, 312–325. https://doi.org/10.1016/j.jmsy.2020.06.010

Lwakatare L.E., Kilamo T., Karvonen T., Sauvola T., Heikkilä V., Itkonen J., Kuvaja P., Mikkonen T., Oivo M., Lassenius C. (2019) DevOps in practice: A multiple case study of five companies. *Information and Software Technology,* 114, 217–230. https://doi.org/10.1016/j.infsof.2019.06.010

Madakam S., Holmukhe R.M., Jaiswal D.K. (2019) The Future Digital Work Force: Robotic Process Automation (RPA). *Journal of Information Systems and Technology Management*, 16(1), 1. https://doi.org/10.4301/S1807-1775201916001

Myrbakken H., Colomo-Palacios R. (2017) DevSecOps: A Multivocal Literature Review. In: *Software Process Improvement and Capability Determination* (eds. A. Mas, A. Mesquida, R.V. O'Connor, T. Rout, A. Dorling), Heidelberg, Dordrecht, London, New York: Springer, pp. 17–29.

Plant O.H., Van Hillegersberg J., Aldea A. (2022) Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment. *International Journal of Accounting Information Systems,* 45, 100560. https://doi.org/10.1016/j.accinf.2022.100560

Qazi A.M., Mahmood S.H., Bahl A.H.S., Mohd J., Gopal K. (2022) The impact of smart materials, digital twins (DTs) and Internet of things (IoT) in an industry 4.0 integrated automation industry. *Materials Today: Proceedings,* 62(1), 18-25. https://doi.org/10.1016/j.matpr.2022.01.387

Rajapakse R.N., Zahedi M., Babar A.M., Shenc H. (2022) Challenges and solutions when adopting DevSecOps: A systematic review. Information and Software Technology, 141, 106700. https://doi.org/10.1016/j.infsof.2021.106700

Rzig D.E., Hassan F., Kessentini M. (2022) An empirical study on ML DevOps adoption trends, efforts, and benefits analysis. *Information and Software Technology*, 152, 107037. https://doi.org/10.1016/j.infsof.2022.107037

Schatsky D., Muraskin C., Iyengar K. (2016) *Robotic process automation*: *A path to the cognitive enterprise*, London: Deloitte.

Slaby J.R. (2012) *Cheap, easy-to-develop software robots will eventually supplant many offshore FTEs,* Cambridge (UK): HfS Research, Ltd.

Smolander K., Akbar M.A., Mahmood S., Alsanad A. (2022) Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology,* 147, 106894. https://doi.org/10.1016/j.infsof.2022.106894

Swinhoe D., Nadeau M. (2019) 3 DevSecOps success stories. CSO Online, 26.09.2019. https://www.csoonline.com/article/3439737/3-devsecops-success-stories.html, accessed 17.11.2022.

Syed R., Suriadi S., Adams M., Bandara W., Leemans S.J., Ouyang C., Ter Hofstede A.H., Van de Weerd I., Wynn M.T., Reijers H. A. (2020). Robotic Process Automation: Contemporary Themes and Challenges. *Computers in Industry,* 115, 103162. https://doi.org/10.1016/j.compind.2019.103162