Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P334-cd

Increasing the Effectiveness of Development and Operation of Software for Cyber Physical Systems

Jan Prochazka

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic, E-mail: jpr@qma.cz

Petr Novobilsky

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic.

Dana Prochazkova

Czech Technical University in Prague, Technicka 4, 166 00 Praha 6, Czech Republic, Danuse.Prochazkova@fs.cvut.cz

Cyber-Physical Systems (CPS) distributed over a large territory, require secure communication not only among various parts of system, but also with operation center. Building its own communication networks by the system operator is financially demanding, which is why more or less open communication systems are used. This is connected with higher requirements for the security of applications, operated in a CPS. European project COSMOS has been creating a tool that applies DevOps development technologies from the IT field to the field of embedded systems. On the example of requirements on railway operation system, we show that for use this very complex software must be adapted to real requirements on railway operation system. The article shows results of tests parts of complex software created in the COSMOS project for Czech railway operation system.

Key words: Cyber-Physical Systems, risks, security, risk-based design, software, integral safety, railway.

1. Introduction

Today, the number of remote-controlled devices and systems is increasing. The equipment and systems in question are an essential part of critical infrastructures that belong to basic public assets because they ensure the basic functions of the State. Therefore, from the point of view of the needs of human society and human security, it is necessary that the devices in question and their entire sets are safe and efficient. These are interconnected technical networks that are controlled by management systems in which there is increasing automation, that is why we talk about cyber-physical systems.

Cyber-physical systems (*further CPSs*) deployed over a large area require safe communication not only between different parts of the system, but also with the operations center. Building own communication networks by the system operator is financially demanding, so more or less open communication systems are used. This is related to higher requirements for the safety and security of applications running in the CPS. They, like critical infrastructures (such as railways), must meet a high standard in communications security. Responding to new cyber threats is an important part of cybersecurity, and CPS integrators or suppliers must be able to provide software updates in a timely manner. Effective delivery of these services requires effective tools that can identify and eliminate errors in the development phase and during operation that can be used to carry out a cyberattack. The article deals with the conditions at which it is possible to use software developed in Cosmos project (EU 2021) at the management of safe operation of trains.

2. Automation and Its Problems

Automatic control is usually divided into logical, continuous, discrete and fuzzy control. When applying it, probability distributions are most often used: normal, log-normal, Weibull and Gamma. Marek process theory, Kolmogorov equations and others are used. In the theory of automatic control, the importance of a systemic approach to solving

automation tasks is emphasized and practice requires a lot of knowledge in the field of information technology (Leitl 1990). Increasingly, automatic control is realized using cyber networks connected via the Internet. As the Internet is characterized by user anonymity, global availability and the simultaneous use of many different technologies, securing information systems connected to the Internet is rather difficult.

Based on the works (Baruh 2014, Klas 2004, Maixner 1980, QS2015, Zlochova 2012) the rules of automatic control are created for a given technical system on the basis of modeling based on reliability theory. Based on the previously mentioned facts, the reliability of equipment is built only on the basis of data on random processes. Therefore, the safety of the equipment under all conditions, i.e. critical and extreme conditions caused by knowledge gaps or extreme influences, is not guaranteed. This fact gives rise to a number of other sources of risk for technical works, especially those using remote data transmission.

Based on the idea of interconnection of the control and controlled system in (Prochazkova, Srp, Prochazka 2013), it is clear that the basic importance in automatic control are feedbacks, on the basis of which control systems adjust the operation of the entire technical work according to information from the controlled systems. Positive feedbacks support the results of controlled processes, and negative feedbacks weaken them. Control systems have algorithms that give commands and execute some operations. The control system ensures that the specified physical quantities are maintained at predetermined values. In the process of regulation, the control system changes the state of the controlled system by acting on the action variables so that the desired state is achieved.

The control system, according to recent concepts place the highest emphasis on safety. It is necessary to achieve properties such as: safety (level of compliance with specified operating conditions and not creating harmful (unacceptable) impacts on the system itself and its surroundings); functionality (level of performance of the required actions); operability (level of performance of required tasks depending on normal, abnormal and critical conditions); operational durability (level of compliance with specified conditions of operation over time); and inherently built-in disaster resistance (Prochazkova et al. 2019).

A controlled system is usually a complex nonlinear system that: consists of a finite number of elements; each element is uniquely described by a finite number of measurable quantities; The interconnections between the elements are clearly formulated. The dynamic properties of a controlled system can be described using differential equations, the solution of which is a state vector. The state vector allows to determine the state of the system at any point in time using a minimum number of quantities (Prochazkova, Srp, Prochazka 2013).

If it is not possible to completely eliminate the sources of risks, which applies, for example, to natural disasters, the next best choice is protection against impacts associated with the occurrence of the risks, by minimizing the occurrence of the realization of the risks in such a way that the appropriate safety protection measures (safety systems) are directly incorporated both into the design of the equipment and into the operating conditions of the projected equipment, i.e. they ensure safety. Other in the acceptable order of priorities are devices for managing hazards and mitigating their impacts (safety-related systems), which have only protective functions. These are, for example, safety valves that protect against unauthorized overpressure in cases in which the illegal increased pressure in the equipment cannot be completely prevented (Prochazkova et al. 2019).

According to this knowledge, safety systems are designed as passive or active. The most effective safety devices are passive devices that operate on the basis of physical principles (e.g. gravity) and do not need any additional impulse to actuate. An example of a passive safety system is a railway traffic light, the arm of which automatically falls into the "stop" position whenever the control current in the supply cable is interrupted. Active safety devices/systems are less suitable because special initiation pulses are needed to activate them to prevent an accident and/or mitigate their impacts. Their creation involves detecting hazards and recognizing the appropriate safety procedure. An example of an active safety system would be a smoke detector connected to a shower system. Current technical knowledge allows the use of hybrid safety systems that switch off separately when the conditions are not within the scope of the conditions specified for the operation of active systems.

The safety management system (*further SMS*) shall always be equipped with measures to minimize damage in cases where safety measures and safety systems fail or an unidentified hazard occurs. Harm reduction can take the form of warning and warning signals, training, instructions and procedures for behavior in dangerous situations, or isolation of dangerous equipment from populated centers. Measures to prevent accidents, including emergency planning, must be drawn up before the installation is put into service because there might not be enough time for this when an accident occurs (Prochazkova 2017).

3. Artificial Intelligence and Cyber-Physical Systems

Artificial Intelligence (*further AI*) has become a major innovative force and it is one of the pillars of the fourth industrial revolution. Big data is nowadays being integrated in systems requiring to process a vast amount of information from (geographically) distributed data sources, while fulfilling the non-functional properties (real-time, energy-efficiency, communication quality and security) inherited from. Software is everywhere and the productivity of Software Engineers has increased radically with the advent of new specification, design and programming paradigms and languages.

AI, to become fully pervasive, needs resources at the edge of the network. The cloud can provide the processing power needed for big data, but edge computing is close to where data are produced and therefore crucial to their timely, flexible, and fast processing. CPSs comprise heterogeneous software and hardware components interacting with each other. They aim at automating operations in different domains, such as automotive, aerospace, healthcare, or railways. As it happens for any software system, CPSs continuously evolve to cope with new customer requirements and technology changes. However, CPSs require a tailored development and operation (*further DevOps*) process and are more challenging to evolve than conventional software (Helle, Shamai, Strobel 2016, Malavolta et al. 2020, Sirasaj, Horvath, Rusak (2019, Törngren and Sellgren 2018).

CPS software developers mainly rely on basic simulation models (Carlos et al. 2018, Sontges, Althoff 2018) , as well as rigid body (Loquercio et al. 2019, Zapridou et al. 2020) and soft body simulation environments (Gambi, Tri, Fraser 2019, Riccio and Tonelly 2020). The usage of CPS simulation environments enables automated test generation and execution (Gunel, Stocco, Tonella 2021, Nguuyen, Huber, Gambi 2021)]. However, the limited budget allocated for testing activities and the virtually infinite testing space pose challenges for adequately exercising the CPS behavior (Flores et al. 2020, Raiaa et al. 2020, Raja et al. 2018).

Related to DevOps applications in a CPS context, Park et al.(2021) analyzed the use and challenges of the digital twin to enable DevOps approaches for cyber-physical production systems to continuously improve them. Specifically, Park et al. identified challenges related to (i) discrepancies between models and their physical counterparts, (ii) integration between heterogeneous models due to the complexity of CPSs, and (iii) security issues due to the tight coupling between the digital twin and the physical environment. Therefore, instead of only looking at automating the production process, we focus more on the continuous integration and delivery (*further CI/CD*) process for CPS development and evolution.

Work QS (2015) concentrates attention to cybersecurity: cybersecurity risk assessments; security policies and cybersecurity compliance; hardware/software implementation; recovery plans; compliance tool support; workforce training; and configuration requirements analysis. For management of software security risk, it pays:

- assess requirements, i.e. to determine the required level of protection for the system(s) and data,
- select controls, i.e. to identify security practices/policies commensurate with the system's required security,
- implement controls, i.e. to install/employ/configure appropriate technical and/or procedural solutions,
- assess controls, i.e. to identify security shortcomings and develop vulnerability remediation plan,
- conduct risk assessments, i.e. to determine if organization accepts the risks associated with the system's operation
- and manage risk, i.e. to maintain system(s) and software while continuously monitoring security posture.

Due to world dynamic development, it is necessary to ensure: continuous process improvement; information and knowledge management policy development; big data management and control; process automation; and information management and course development. Continuous process improvement must remove inefficient processes, which cause problems (such as missed deadlines, dissatisfied customers, unnecessary costs, employee burnout, and other issues) and ensure: faster decision making; improved productivity that results in higher reliability; effective allocation of resources to reduce costs; efficient operations to provide order and consistency; increased task automation to cut down on tedious work; and improved agility to allow companies to easily pivot in a dynamic business environment (EU 2021).

4. Data on CPS Issues and COSMOS Project

Big industry, small enterprises and academics created team up to develop enhanced DevOps pipelines for the development of cyber-physical systems software. The EU-funded COSMOS project (2021) integrates more sophisticated validation and verification, which comprise a mix of static code analysis correlated with issues and bug reports, automated test-case generation, runtime verification, hardware in the loop testing and feedback from field devices. The project also uses machine learning, model-based testing and search-based test generation.

Much of the increasing complexity of information and communication technology systems is being driven by the more distributed and heterogeneous nature of these systems, with Cyber Physical Systems accounting for an increasing portion of Software Ecosystems. This basic premise underpins the COSMOS proposal which focuses on blending best practices DevOps solutions with the development processes used in the CPS context: this enables the CPS world to deliver software more rapidly and result in more secure and trustworthy systems.

The pipelines created in the COSMOS project integrate more sophisticated validation and verification (V&V) which comprise of a mix of static code analysis correlated with issues and bug reports, automated test case generation, runtime verification, Hardware in the Loop (HiL) testing and feedback from field devices. Approaches based on Machine Learning, model-based testing and search based test generation are employed. Techniques to prioritize and schedule testing to maximize efficacy of the testing process and to minimize security threats is also developing. COSMOS leverages existing prototype technologies developed by the partners supporting enhancing them throughout the project.

Pipelines in COSMOS project make use of software-defined infrastructures to allocate the resources necessary to fulfill industrial testing needs. The developed pipelines make use of cloud platforms as necessary to run complex test processes, dynamically scaling infrastructure resources as necessary focus on optimization mechanisms, which make intelligent use of such infrastructures to minimize overall testing time and cost whilst ensuring tests are performed in a timely manner. COSMOS is able to obtain samples from field deployments to improve test effectiveness (higher test coverage, more detected vulnerabilities, etc.), which reflects real-world environments. This is done not by modifying existing code, but rather by modifying the configuration of the application middleware in which the application runs.

Project COSMOS develops tools to maximize test effectiveness while minimizing the time and cost of running tests. More effective test and verification increase software reliability and cybersecurity as there are less potentially exploitable bugs in production systems. Project achieves better software reliability through a sophisticated combination of improving test effectiveness through automated test generation, machine learning techniques to predict test results, judicious inclusion of Hardware-in-the-Loop testing in testing processes, incorporation of feedback from field deployments in test processes as well as static code analysis.

With respect to security, COSMOS specifically develops solutions for detecting security vulnerabilities in cyber-physical systems through a combination of analysis of the source code and generation of input sequences which may trigger security problems. COSMOS also determines anti-patterns - including security related anti-patterns - via static code analysis as well as inferring the attack surface of a given software base using machine learning techniques.

The project results (Zampetti et al. 2022), which were published show solution of problems comes out from theoretical model of CPS and is

on the high theoretical level, but it does not consider that CPS that are used in practice have some structure and some operation rules, which are stipulated by legislative. Their fast change is not possible from economic and time reasons. Therefore, for practice aims it is necessary to find procedure for their use.

For example, for railway it pays: static analyses are done manually; unit test, internal test and develop test are done automatically; system test and non-function tests is automatic but not by pipeline approach developed in COSMOS project. Organization profile for railways is involved in delivering the software for railways, i.e., Train Control Management System (TCMS). In terms of programming languages being used, the interviewee mentions the need of adapting the programming language to the device on which the software has to be executed.

Organization profile already has a CI/CD pipeline in place for CPS development that, at the moment, is in a continuous improvement state. Based on the application domain, organization profile adopts staged builds following the "green-build rule". In the first stage, the build process is executed on a virtual machine, and in the presence of a green status, all the components are deployed together, enabling the execution on the virtual train. In the presence of a green status, it is possible to move to the next stage that relies on the hardware test track, "where [there is] the whole set of devices and even some more that [are not] in the virtual train." Finally, in the presence of a green status it is possible to run the last stage relying on a real train. All the stages include functional testing, while the deployment is automated.

Organization profile is facing problems when trying to onboard new developers (PRC2) mainly due to the complexity of the railways' domain, as also found by Törngren et al. (2018), who found it difficult to automate the test case specification mainly because the standards might be interpreted differently by different developers, and both might be correct. Context: of organization profile is involved in delivering software for railways, i.e., Train Control Management System (TCMS), and similarly to what is reported for the aerospace domain, due to the safety integrity level of the software under development, developers and testers must be different (i.e., "Testers and Developers are in separate teams in presence of new functionality to be implemented both start together to implement and write test cases.").

5. Railway Safety Methodology

According to the Treaty of Maastricht (EU 1992), safety is the highest quality of the CPS, which is in our case the railway. It is a complex CPS with a high number of different links. According to the project, all components and interconnections have their limits, which are set to certain conditions so that together they meet the specified goal (i.e. to be interoperable). As conditions change as the world evolves, so do the conditions for interoperability. Therefore, railway safety changes depending on further evolving conditions. Safety (integral) includes both reliability and functionality, and in the light of internal and external harmful phenomena, its control systems must be secured by both, physically and cybernetically.

In accordance with OECD requirements (2002) and with the results for technical facilities (Prochazkova et al. 2019), railways must have a railway safety management program based on risk management, from design, through construction to operation (Prochazkova et al 2019), as well as maintenance, renewal, completion and innovation. Therefore, due to the importance of the role of cyber infrastructure associated with an automated management system, the SMS must also monitor cyber security and contain a Cybersecurity of Safety Management System (*further CSMS*) - Figure 1.

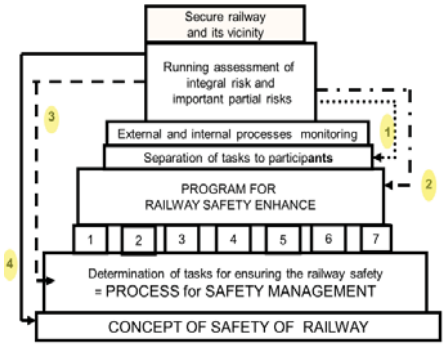

Fig. 1. Railway CSMS model with automated control over time. Processes: 1- conception and management; 2 - administrative procedures; 3 - technical processes; 4 - external cooperation; 5 - emergency readiness; 6 - documentation and investigation of accidents; 7- Cybersecurity. Feedbacks: 1-4 in yellow circles.

The main objective of securing the railway infrastructure during the automatic control is that the instructions for the systems controlling the op-

eration of trains are clear and precise, i.e. not affected by phenomena that distort them. Therefore, signaling systems were previously used on railways, which were closed and patented (Prochazka et al. 2022). With a high degree of automation, it is advisable to use the Internet, which, in turn, brings problems. The main objective of securing the railway infrastructure during the automatic control is that the instructions for the systems controlling the operation of trains are clear and precise, i.e. not affected by phenomena that distort them. Therefore, signaling systems were previously used on railways, which were closed and patented. With a high degree of automation, it is advisable to use the Internet, which, in turn, brings problems.

Cybersecurity is not just a design issue, as the limits and conditions of every system and every device change over time. This means that the CPS cybersecurity problem for CPS manufacturers does not end with user acceptance of the system. For security reasons, the cybersecurity status of each CPS should be monitored during operation until the system is decommissioned. Based on the monitoring results, risk-based maintenance should be performed during the operation of the CPS. Risk-based maintenance requirements depend not only on the structure of the CPS, but also very seriously on the conditions in which they operate.

6. Adaptation of COSMOS Results to Railways in the Czech Republic

At adaptation of COSMOS project results we respect that rail is an essential part of the critical infrastructure of every country and Europe, and therefore an emphasis on integral safety, which includes both reliability and safety, is essential. Based on research (OECD 2002, Prochazka, Prochazkova 2022, Prochazkova et al. 2019), it is necessary to ensure integral safety throughout its lifetime due to the dynamic development of the world and the railway system itself, i.e. mainly in design, operation, maintenance and modernization. Given the variability of the world, overall safety can only be ensured by ongoing qualified risk management, as shown in Figure 1.

In designing, it is very important how the designer divides the real railway risks mastering (Prochazkova 2021, Prochazkova, Prochazka 2022, Zio 2016), see bow-tie diagram in Figure 2: in design by preventive measures, or only at response. In the second case, the designer must in design prepare qualified measures for response. The technique for compilation of railway system risk-based design is described in (Prochazka, Prochazkova 2022). Risk-based operation principles are described in (Prochazkova, Prochazka 2021). As all parts of the railway system become ageing and obsolete, maintenance is very important in practice.

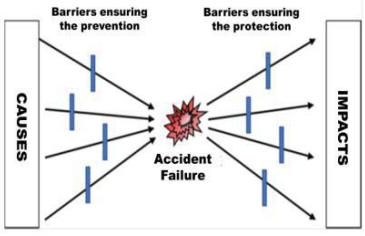

Fig. 2. Separation of countermeasures between design and response (Zio 2016).

A risk-based maintenance strategy is based on two main phases: risk assessment; and maintenance planning based on the risk (IAEA 2002, Jardine, Tsang 2013, Prochazkova et al. 2019). For each identified risk, data needs to be collected. This includes information about the risk, its general consequences and the general methods used to mitigate and predict the risk; risk-based maintenance framework is shown in Figure 3. At the risk evaluation stage, both the probability of the risk and the consequence of the risk are quantified in the context of the facility under consideration. The risk-based maintenance framework is applied to each system in a facility. The likely failure modes of the system are first determined. Then, a typical risk-based maintenance framework is applied to each risk (Jardine, Tsang 2013, Kiran, Prajeeth Kumar, Sreejith, Muraliharan 2016, Krishnasamy, Khan, Haddara 2005, Montgomery, Serratella 2002, Prochazkova et al. 2019).

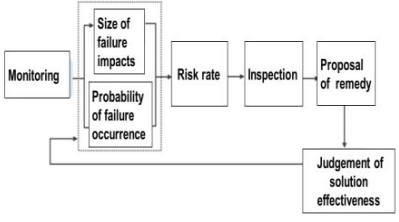

Fig. 3. Risk-based maintenance framework.

For adaptation of COSMOS project results for needs of Czech Railway Management System we use simulator (Q-media 2020). We have been tested individual parts of software developed in COSMOS project on the simulator. During the test we follow the main aim, namely integral safety of railway operation as Czech legislation required.

In this moment results of our tests (Q-media 2023) are the following:

- Some parts of software are very complicated and they do not clearly include present-day instructions that respect demands of Czech legislation on integral safety, and therefore, we do not recommend them into real practise.
- At parts of software dealing with the cyber security we found the instructions that are better than present ones. We inserted them into CSMS on simulator and tested them for design conditions and possible beyond design conditions. Some well-tried we recommended into practice to the Czech Railway Management System. Their use needs time and expenses because it is necessary to change the operating instructions and to train responsible critical railway personnel.

7. Conclusion

Results of COSMOS project are very sophisticated. Our experience based on testing the COSMOS project results on simulator shows that since the railway system is based on integral (overall) safety, before applying the results of the COSMOS project, which primarily emphasizes reliability and security, it is necessary firstly to carry out detailed tests on simulator and accept only those codes that do not compromise overall safety.

Acknowledgement

This work is part of COSMOS project under grant agreement No. 957254, funded by the European Union's Horizon 2020 research and innovation programme.

References

Baruth (2014). *Applied Dynamics*. New York: CRC Press 2014.

Abdessalem, R. B., Panichella, A., Nejati, S., Briand, L. C., Stifter, T. (2018). Testing autonomous cars for feature interaction failures using many-objective search. In: *IEEE/ACM International Conference on Automated Software Engineering.*. IEEE, pp. 143-154.

EU (1992). *Maastricht Treaty*. C 191, 29.7.pp.1–112.

EU (2013). *FOCUS Project Study – FOCUS*. www.focusproject.eu/documents /14976/-5d763378-1198-4dc9-86ff-c4695972 f8a

EU (2021). *COSMOS. DevOps for Complex Cyber-physical Systems*. ID: 957254, EU H2020.

FEMA (1996), *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washington: FEMA.

Flores-García, E,. Kim, G-E., Yang, J., Wiktorsson, M., Do Noh, S, (2020). Analyzing the Characteristics of Digital Twin and Discrete Event Simulation in Cyber Physical Systems. In: *Advances in Production Management Systems. Towards Smart and Digital Manufacturing (IFIP Advances in Information and Communication Technology*), 592, pp. 238–244.

Gambi, A., Huynh, T., Fraser, G. (2019). Generating effective test cases for self-driving cars from police reports. In: *Proceedings of the ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pp. 257-267.

González, C. A., Varmazyar, M., Nejati, S., Briand, C., Isasi. Y. (2018). Enabling Model Testing of Cyber-Physical Systems. In *Proceedings of the 21th ACM/IEEE International Conference on Model Driven EngineeringLanguages and Systems,* pp.176-86.

Helle, P., Schamai, W., Strobel, C. (2016). Testing of Autonomous Systems - Challenges and Current State-of-the-Art. *INCOSE International Symposium*, pp. 571–584.

IAEA (2002). *Maintenance, Surveillance and In-service Inspection in Nuclear Power Plant*. Vienna: IAEA, 95 p.

Jahangirova, G., Stocco, A., Tonella, P. (2021). Quality metrics and oracles for autonomous vehicles testing. In: *14th IEEE Conference on Software Testing, Verification and Validation (ICST).* IEEE, pp. 194-204.

Jardine, A. K. S., Tsang, A. H. C. (2013). *Maintenance, Replacement, and Reliability: Theory and Applications.* London: CRC Press

Kiran, S., Prajeeth Kumar, K. P., Sreejith, B., Muraliharan, M. (2016). Reliability Evaluation and Risk Based Maintenance in a Process Plant. *Procedia Technology.* 24, pp. 576-583. www.sciencedirect.com

Klas, A. (2004). Krok za krokem k výnosné automatizaci montážních linek. *MM průmyslové spektrum*, 2004, p. 28.

Krishnasamy, L., Khan, F., Haddara, M. (2005). Development of a Risk-based Maintenance (RBM) Strategy for a Power-generating plant. *Journal of*

Loss Prevention in the Process Industries. 18, 2, pp. 69-81.

LeitL, R. (1990). *Spolehlivost elektrotechnických systémů*. Praha: SNTL1990.

Loquercio, A., Kaufmann, E., Ranftl, R., Dosovitskiy, A., Koltun, V., Scaramuzza, D. (2019). Deep drone racing: From simulation to reality with domain randomization. *IEEE Transactions on Robotics.* 36, 1, pp. 1-14.

Maixner, L. (1980). *Navrhování automatických výrobních systémů*. Praha: NTL 1980.

Malavolta, I., Lewis, G., Schmerl, B., Lago, P., Garlan, D. (2020). How Do You Architect Your Robots? State of the Practice and Guidelines for ROS-Based Systems. In: *Proceedings of the ACM/IEEE 42nd International.* New York, pp. 31-40.

Montgomery, R. L., Serratella, C. (2002). Risk-Based Maintenance: New Vision for Asset Integrity Management. In: *ASME 2002 Pressure Vessels and Piping Conference.* ISBN 0-7918-4655-5. Vancouver: ASME, pp. 151-165.

Nguyen,Y., Huber, S., Gambi, A. (2021). SALVO: Automated Generation of Diversified Tests for Self-driving Cars from Existing Maps. In *2021 IEEE International Conference on Artificial Intelligence Testing (AITest*). IEEE, pp. 128-135.

OECD (2002).. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for Developing SPI Programmes Related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191 p

Park, H., Easwaran, A., Andalam, S. (2021). Challenges in Digital Twin Development for Cyber-Physical Production Systems. In: *Cyber Physical Systems. Model-Based Design*. Springer International Publishing, Cham, pp. 28-48.

Prochazka, J., Novobilsky, P., Prochazkova, D., Valousek, S. (2022). Cybersecurity Design for Railway Products. In: *Understanding and Managing Risk and Reliability for a Sustainable Future.* ISBN 978-981-18-5183-4. Singapore: Research Publishing 2022, pp. 304-311. doi:10.3850/978-981-18-5183-4_R09-01-099-cd

Prochazka, J., Prochazkova, D. (2022). *Risk Management of Traffic Management Systems.* Praha: ČVUT,129 p. doi:10.14311/BK.97880010 69950

Prochazkova (2017). *Principles of Management of Risks of Complex Technological Facilities.* doi: 10.14311/BK.9788001061824.

Prochazkova, D., Prochazka, J. (2021). Generation of Risk-Based Design of Socio-Cyber-Physical Systems. *International Journal of Economics and Management Systems;* 6, pp. 261– 272. http:// www.iaras.org/iaras/journals/ij ems

Prochazkova, D., Srp, J., Prochazka, J. (2013): Analysis of Cyber Networks in a System Concept. In:*Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics. Recent Advances in Systems, Control, Signal Processing and Informatics*. ISBN 978-1-61804-204-0, Rhodes Island 2013, pp. 102-109.

Prochazkova, D., Prochazka, J., Lukavsky, J., Beran, V., Sindlerova, V. (2019). *Management of Risks of Processes Connecting with Manufacturing the Technical Facility.* Doi: 10.14311%2FBK.978 80 01066096.

Q-media (2020). *Simulator for Testing the Railway Management Instructions.* Praha: Q-media.

Q-media (2023).Results of Tests of COSMOS Software. *Archives.* Praha: Q-media.

QS (2015). *System Reliability Toolkit-V. New Approaches and Practical Applications*. Utica: Quanterion Solutions Inc. https://www.quanterion .com/KnowledgeBase/Relia bilityToolkit.shtml.

Riccio. V. , Tonella. P. (2020). Model-based Exploration of the Frontier of Behaviours for Deep Learning SystemTesting. In P*roceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering.* (ESEC/FSE '20). Association for Computing Machinery.

Sontges, S., Althoff., M. (1918). Computing the Drivable Area of Autonomous Road Vehicles in Dynamic Road Scenes. *IEEE Trans. Intell. Transp. Syst*. 19, 6, pp. 1855-1866.

Tepjit, S., Horvath, I.Rusak, Z. (2019). The state of framework development for implementing reasoning mechanisms in smart cyber-physical systems: A literature review. *Journal of Computational Design and Engineering* . 6,4, pp. 527-541.

Törngren, M., Sellgren, U. (2018). *Complexity Challenges in Development of Cyber-Physical Systems.* Cham: Springer.

Vikhram, R.,Rajvikram Y., Elavarasan, M., Manoharan, M., Mihet-Popa, L. (2020). Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access 8151019–151064*

Zampetti, F., Tamburri, D., Panichella, A., Panichella, S., Di Penta, M., Gerardo, C. (2022). Continuous Integration and Delivery practices for Cyber-Physical systems: An interviewbased study. Doi: 10.1016/j.jss.2022.111425,10.21256/zhaw-25591

Zapridou, E., Bartocci, E., Katsaros, P. (2020). Runtime Verification of Autonomous Driving Systems in CARLA. In: *Runtime Verification.* Cham: Springer International Publishing.

Zio, E. (2016). Some Challenges and Opportunities in Reliability Engineering. *IEEE Transactions on Reliability.* 65, 4, pp. 769-1782.

Zlochová, M. Optimalizace výrobních buněk. *Úspěch - Produktivita a inovace v souvislostech*, 2012 (2012).