Present Development of Software for Railway Safety

JAN PROCHAZKA
Q-media s.r.o.
Pocernicka 272/96, 10 800 Praha 10
CZECH REPUBLIC

DANA PROCHAZKOVA
Czech Technical University in Prague
Technicka 4, 166 00 Praha 6
CZECH REPUBLIC

Abstract: - Railway is Cyber-Physical System (CPS), which is distributed over a large territory. It requires secure communication not only among various parts of system, but also with operation center. Building its own communication networks by the railway 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 COSMSOS has been creating a tool that applies DevOps development technologies from the IT field to the field of embedded systems, to which railway system belong. The article shows that this very complex software must be adapted to real requirements, which are put on railway operation system safety.

Key-Words: - Cyber-Physical systems; risks; safety; security; risk-based design, software aim.

Received: July 23, 2023. Revised: April 9, 2023. Accepted: May 14, 2024. Published: June 25, 2024.

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 (*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. Newest type of software tolls for such purpose can be AI. The article deals with the conditions at which it is possible to use software developed in COSMOS project [1] 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 [2]. 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 [2-5] 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 [6], 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.

In the case of a control system according to current concepts, which place the highest emphasis on security (i.e. also security against external threats), the features are emphasized:

- safety (level of compliance with established operating conditions and not creating harmful (unacceptable) impacts on the system itself and its surroundings),
- functionality (level of execution of required actions),
- operability (level of performance of required tasks depending on normal, abnormal and critical conditions),
- operational stability (the level of fulfillment of the established operating conditions over time)
- and inherently built-in disaster resistance.

A controlled system is usually a complex nonlinear system characterized by:

- consists of a finite number of elements,
- each of its elements is clearly described by a finite number of measurable quantities,
- the connection between the elements is clearly formulated.

The dynamic properties of the controlled system can be described using differential equations, the solution of which is the state vector. The state vector makes it possible to determine the state of the system at any moment in time using a minimum number of variables [6].

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 the risks 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 [7].

According to this knowledge [8], 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 [7].

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. Measure for reduction of harms 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 [9].

3 Artificial Intelligence and Cyber-

Physical Systems

Artificial intelligence (AI) has become a significant innovation of last years and is one of the industry 4.0 pillars. In order that AI is able to fully perform its tasks we need collect sets of data about such task. This is the creation of large, complex data sets, which we refer to as "Big data". Structured and unstructured data are therefore integrated into systems that contain a huge amount of information from distributed data sources. Their high-quality processing makes it possible to obtain real-time results for the monitored sections, which consider a wide range of aspects. To solve the tasks, the practice requires specific data processing tools.

Big data is collected data from many diverse sources and applications. Traditional data integration mechanisms such as extraction, transformation and loading are generally not sufficient for this task. Data processing requires new strategies and technologies to analyze large data sets in the terabyte or even petabyte range. For big data, it is necessary to have store facilities, which are used most often in the form of data warehouses (clouds). The data is transferred to the cloud in pre-determined cycles and subsequently analyzed using already prepared algorithms [10].

CPS are complex systems and include heterogeneous software and hardware components that interact with each other. The goal of their management in the sense of control is the automation of operations in various areas, such as the automotive industry, the aerospace industry, healthcare or railways. As with any software system, CPS systems are constantly evolving to cope with new customer requirements and technological changes. CPS software requires adapting the development and operation process (DevOps) to the requirements of practice, and therefore their development is more demanding than the development of conventional software [11-14].

CPS software developers mainly rely on basic simulation models [15, 16], as well as rigid body [17, 18] and soft body simulation environments [19, 20]. The usage of CPS simulation environments enables automated test generation and execution [20, 21]. However, the limited budget allocated for testing activities and the virtually infinite testing space pose challenges for adequately exercising the CPS behavior [21-24].

One of the recent technologies is a digital twin, i.e. a digital image of a real physical element: for example, a model in the product design phase, which we can gradually expand within the life cycle of the product or any system. It connects objects and looks for links, their synergies and conflicts. The real object is connected to the virtual object and individual physical parameters are updated in time in its digital twin. It is the time element that is the fundamental difference between the digital twin and existing modeling approaches. At the digital level, the digital twin system can be experimented with, output verified, behavior simulated, and also applied with artificial intelligence to investigate various phenomena, functions, and qualitative properties. The technology of digital twins can be applied in the entire life process of complex systems, from their design and verification of superior functions through operation, changes, to shut down or replacement by another system [25].

In relation to DevOps applications in the context of CPS, authors of work [26] analyzed the use and challenges of the digital twin to allow DevOps approaches for cyber-physical production systems to continuously improve them. Park et al. [26] specifically identified problems related to:

- discrepancies between models and their physical counterparts,
- integration between heterogeneous models due to the complexity of CPS
- and the security issues caused by the close connection between the digital twin and the physical environment.

Therefore, we need to focus not only on the automation of the production process, but to focus primarily on the continuous integration (CI) and continuous development (CD) of the CPS, i.e. the process referred to as CI/CD .

Work [5] focuses attention on cyber security (more precisely, cyber security of the monitored entity), i.e. on:

- assessment of cyber risks,
- security policy and compliance with regulations in the field of cyber security,
- hardware and software implementation,
- recovery plans,
- compliance support tools,
- employee training
- and analysis of configuration requirements.

To manage software risks from a security point of view [27] it is necessary to:

- assess the requirements, i.e. determine the required level of system and data protection,
- select controls, i.e. identify security procedures/policies corresponding to the required system security,
- implement controls, i.e. install/use/configure appropriate technical and/or procedural solutions,
- evaluate controls, i.e. identify security deficiencies and develop a plan to reduce vulnerabilities,

- carry out a risk assessment, i.e. determine whether the organization accepts the risks associated with the operation of the system
- and manage risks, i.e. maintain the system(s) and software in a desirable state based on continuous monitoring of security conditions.

Due to the dynamic development of the world, according to [27-30] it is necessary to ensure:

- continuous process improvement,
- development of information and knowledge management policy,
- administration and management of big data,
- process automation
- and information management and development of new procedures for the needs of practice.

Continuous process improvement must gradually eliminate inefficient processes that cause problems in the practice (such as missed deadlines, dissatisfied customers, unnecessary costs, employee burnout and other problems) and ensure:

- faster decision making,
- higher productivity, which leads to higher reliability,
- efficient allocation of resources in order to reduce costs,
- efficient operations to ensure order and consistency in the performance of tasks,
- increased automation of tasks to reduce tedious work
- and improve agility that allows companies to easily navigate a dynamic business environment.

4 Data for CPS and COSMOS Project

Large industrial enterprises, small businesses and academics in the European Union have come together to develop improved DevOps practices for cyber-physical systems software development. The European Union funded COSMOS [1] project to integrates more sophisticated validation and verification processes, which includes:

- a combination of static analyzes of standards correlated with problems and error reports,
- automated generation of test cases,
- verification of reliability of measures during operation,
- hardware and feedback testing in operational devices.

The project also uses machine learning, model-based testing, and search-based test generation.

It is a fact that a large part of the increasing complexity of information and communication technology (ICT) systems is due to the highly distributed and highly heterogeneous nature of these systems. Cyber-physical systems have more and more software systems.

Therefore, the core proposals of the COSMOS project focus on connecting the best practices of DevOps solutions with the development processes used in the context of CPS, enabling:

- faster delivery of software for CPS
- and result in safer and more trusted CPS systems.

COSMOS develop enhanced DevOps pipelines focused on CPS software development. These software sets are intended to provide more sophisticated verification and validation of the reliability of the solution and therefore include:

- a combination of static analyzes of standards that correlate with problems and error reports,
- automated generation of test cases,
- verification during device operation,
- hardware testing in the loop (HiL)
- and feedback from operational devices.

In doing so, approaches based on machine learning, model-based testing, and test generation based on finding weak points are used. Test prioritization and test planning techniques are also being developed to maximize the efficiency of test processes and minimize security threats. COSMOS uses existing prototype technologies developed by partners and supports their improvement throughout the project.

The COSMOS project uses software-defined infrastructures to allocate the resources necessary to meet industrial testing needs. Developed practices use cloud platforms on demand to run complex test processes, dynamically scale infrastructure resources, and focus on optimization mechanisms on demand that intelligently use these infrastructures to minimize overall test time and cost while ensuring that tests are executed on time. COSMOS is able to obtain samples from the development area to improve test efficiency (higher test coverage, more vulnerabilities detected, etc.) that reflect the real-world environment. This is not done by modifying existing standards, but rather by modifying the configuration of the software in which the application is running.

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 published results of the project [28] show that the problem solving is based on the theoretical CPS model and is at a high theoretical level, but does not consider that the CPS that are used in practice today already and that they have some structure and certain operating rules that are established by legislation. Their quick change is not possible for operational, economic and time reasons. Therefore, for practical purposes, it is necessary to find a procedure for their use.

The analysis carried out in [28] shows that, for example, for railways it pays to use:

- manual performance of static analyses,
- automatic execution of tests,
- automatic execution of system tests and functionality tests, which are different from the approaches developed in the COSMOS project.

The operation of the railway depends on the software Train Control Management System (TCMS), which is use a certain programming language, which is different from the programming language used in the COSMOS project. Therefore, for applications developed in the COSMOS project, it is first necessary to modify the programming language on which the software is to be run. The railway also already has a CPS continuous integration and development (CI/CD) process in place, which is currently in a state of improvement. Therefore, it has problems when trying to involve newly developed software of the COSMOS project, mainly due to the complexity of the railway domain [14]. Railway standards are based on a certain model and accepted practices, which can be interpreted differently by software designers in the COSMOS project without specific knowledge of railway specifics.

The TCMS control system, similar to the air traffic control system, has specifics from the safety point of view [27]. The management system in question is an integrated management system [27], and we cannot simply insert pieces of general software into that without respecting railway specific standard.

5 Methodology for Ensuring Railway Safety

According to the Treaty of Maastricht [31], safety means the highest quality of each object. It also holds for the CPS, which is in our case the railway. It is a complex CPS with a high number of different links among components. According to the design project, all components and interconnections have their limits [32], 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.

Safety includes both reliability and functionality, and with internal and external malicious phenomena in mind, its control systems must be secured both physically and cybernetically. Therefore, in accordance with the original OECD requirements from 1992 [29] and the results of other works, the railway must have a railway safety management program based on risk management, from design, construction [27] to operation [30], as well as maintenance, renewal, completion and innovation. Due to the importance of the role of the cyber infrastructure associated with the automated management system, the SMS must also monitor cyber security and contain a CSMS (cybersecurity of safety management system) - Figure 1.

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 [33]. 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.

DOI: 10.37394/232022.2024.4.3

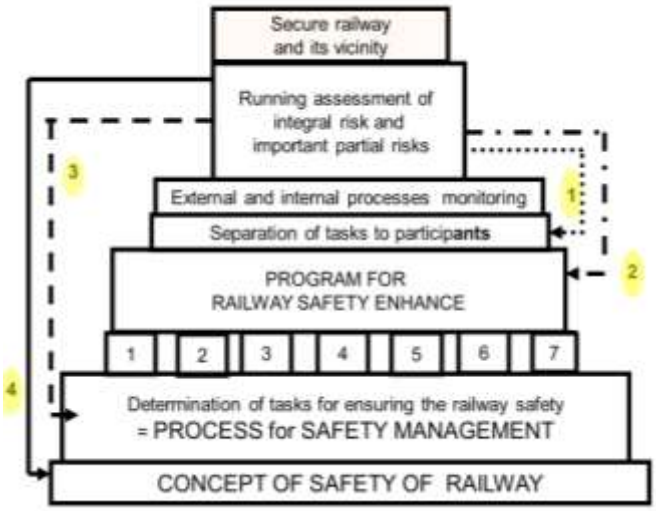

Fig. 1. Railway CSMS model with automated control over time. Processes: 1- conception and management; 2 - administrative procedures; 3 - technical processes; 4 - external cooperation; 5 - emergency readiness; 6 - documentation and investigation of accidents; 7- cybersecurity. Feedbacks: 1-4 in yellow circles- processed according to [32].

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 Assessment of Use of Results of COSMOS Program for Railways

The railway is an essential part of the critical infrastructure of every country and of the whole of Europe, and therefore the emphasis is placed on integral safety, which includes both reliability and functionality. Based on research [30, 32], 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. primarily in the area of design, operation, maintenance and modernization. Due to the variability of the world, overall security can only be ensured by continuous, skilled risk management, as shown in Figure 1.

In design, it is very important how the designer apportions the real risks for the railway [32, 34, and 35], see the bow-tie diagram in Figure 2. In the design, preventive measures are applied to eliminate or reduce the risk, and in operation, the impacts of the risks are reduced by response measures. In the second case, the designer must prepare qualified response measures in the design in order to mitigate the effects of the realized risk.

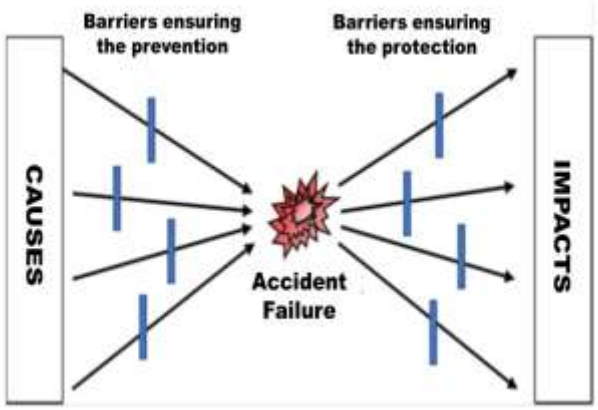

Fig. 2. Separation of countermeasures between design and response [35].

The proposal of processes based on the risks of the railway system is described in work [32]. The principles of risk-based operation are described in [27].

Since train transport ensures permanent service to the area, its interruption due to a revolutionary change in its management means a major intervention in the life of people and the economy of the area. Therefore, revolutionary changes in the railway transport system are only possible in isolated cases in which it is necessary to correct major errors in the operation of trains (feedback 3 in Figure 1), which is unlikely in developed countries after almost 200 years of train operation, or after a major catastrophe that totally destroys everything in the area (feedback 4 in Figure 1). Therefore, for railways, risk mitigation measures for existing infrastructure that are carried out during the operation, i.e. as part of railway maintenance, are realistically possible. As all parts of the railway system age and become obsolete, maintenance is very important in practice.

A risk-based maintenance strategy consists two main phases: risk assessment; and risk-based maintenance planning [30, 36, and 37]. Data must be collected for each identified risk. This includes information about the risk, its impacts and consequences, and the methods that can be used to mitigate and anticipate the risk. A risk-based maintenance framework is shown in Figure 3. In the risk assessment phase, both the probability of the risk and its consequences are quantified in relation to the object under consideration.

A risk-based maintenance framework is applied to every system in the facility. The system can be, for example, a high-pressure vessel or a brake or cooling system. This system will have neighboring systems that are connected to it and interact with each other. First, the probable ways of system failure are determined. A typical risk-based maintenance framework is then applied to each risk [30, 36-40].

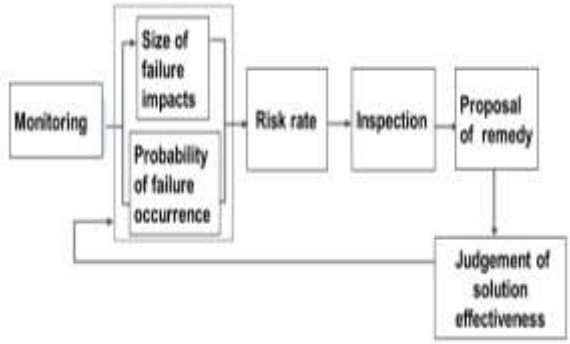

Fig. 3. Risk-based maintenance framework

One of the application areas of "artificial intelligence" is the development, verification and validation phases of system design with respect to risks. These are the stages of development according to the V-cycle [41], during which system functions are tested and possible vulnerabilities are searched for. A variety of methods are used for this testing. It is always necessary to choose an adequate testing methodology according to nature of the system. The more complex the system, the more types of methods are needed, as different aspects require different methodologies.

Metamorphic testing [42] is a method for testing the network systems and consists of two phases. The system functions are tested during the first phase, and vulnerabilities are searched for during the second phase. It is possible in the second phase to use for automation "artificial intelligence" and the manual input of the first phase as input for this automation.

The first step is to create a typological map of the system, which we call metamorphic relationships. It is about defining the relationships between individual elements and processes of the system. In the case of communication systems, it can be, for example, communication channels and their properties, or items from where to where information should flow.

The second step is functionality testing. It is necessary to insert all types of expected valid inputs into the system and assess the correctness of the outputs. Part of the correctness of the input may be the address in the systems where the information is entered. Or the username and password that condition the processing of such information.

The third step is the modification / metamorphosis of inputs and search. At this stage, we look for input that could cause an unwanted system condition. As it involves repeated entry of inputs, similar to those approved, it is an ideal activity for automation. It is important that the "artificial intelligence" proceeds efficiently during automatized building metamorphic inputs.

We can find the effectiveness of "artificial intelligence" in three domains:

- it knows the essence of approved inputs,
- it is able to search for unknown inputs,
- it recognizes similar inputs and thus not repeat the same test multiple times.

Savings of time and resources with automatized input of testing then depends on the complexity of the system. In the case of the simplest systems with one metamorphic relationship, it is 50%, i.e. half of the original testing is still done manually and half is automated. But the more complex the system, the greater are time and resources savings of metamorphic testing with the help of "artificial intelligence" [43].

7 Conclusion

Since the railway system is based on overall safety, it will always be necessary to first inspect and accept only those parts of software developed in the COSMOS project, which do not threaten the overall security, before applying the results of the COSMOS project, which focuses primarily on reliability and security against cyber risks safety.

Based on the principles of risk engineering, we construct the decision support system for decision-making on risks to be able to judge the efficiency, knowledge requirements, finance, operators and installation time of insertion of the software products created by the COSMOS project in the case of their insertion into present railway system management [32]. Then, we decide which software products we implement into railway system today or future during the reconstruction.

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:

[1] EU.*COSMOS. DevOps for Complex Cyber-physical Systems*. ID: 957254, EU H2020.

[2] MEHTA, B. R., REDDY, Y. J. *Industrial Process Automation Systems. Design and Implementation*. ISBN 978-0128-0109-83. Elsevier 2015, 668 p.

[3] HAGGLUND, T. *Automatic Control. Lecture Notes*. Lund: Lund University 2021, 137 p.

[4] GU SHI; ET AL. (2015). Controllability of structural brain networks. *Nature Communications*. 6 (2015), 6. Doi:10.1038/ncomms9414P

[5] QS. *System Reliability Toolkit-V. New Approaches and Practical Applications*. Utica: Quaternion Solutions Inc. 2015.

[6] PROCHÁZKOVÁ, D., SRP, J., PROCHÁZKA, J. 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.

[7] PROCHAZKOVA. D. *Safety of Complex Technological Facilities.* ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244 p.

[8] PROCHAZKOVA, D., PROCHAZKA, J., LUKAVSKY, J., BERAN, V., SINDLEROVA, V. *Risk Management of Processes Connected with manufacturing of Technical Facility and Its Commissioning.* ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi: 10.14311%2F BK.978 80 01066096.

[9] PROCHAZKOVA, D. *Principles of Management of Risks of Complex Technological Facilities.* Praha: ČVUT 2017, 364 p. Doi: 10.14311 /BK.9788001061824.

[10] MAYER-SCHÖNBERGER, V., CUKIER, K. *Big Data.* ISBN 978-80-251-4119-9. *Brno: Computer Press 2015, 256 p.*

[11] HELLE, P., SCHAMAI, W., STROBEL, C. Testing of Autonomous Systems - Challenges and Current State-of-the-Art. *INCOSE International Symposium Proceedings* 2016, pp. 571–584.

[12] MALAVOLTA, I., LEWIS, G., SCHMERL, B., LAGO, P., GARLAN, D. 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 2020, pp. 31-40.

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

[14] TÖRNGREN, M., SELLGREN, U. *Complexity Challenges in Development of Cyber-Physical Systems.* Cham: Springer 2018.

[15] GONZÁLEZ, C. A., VARMAZYAR, M., NEJATI, S., BRIAND, C., ISASI. Y. Enabling Model Testing of Cyber-Physical Systems. In *Proceedings of the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems 2018*, pp.176-186.

[16] SONTGES, S., ALTHOF, M. Computing the Drivable Area of Autonomous Road Vehicles in Dynamic Road Scenes. *IEEE Trans. Intell. Transp. Syst*. 19 (2018), 6, pp. 1855-1866.

[17] LOQUERCIO, A., KAUFMANN, E., RANFTL, R., DOSOVITSKIY, A., KOLTUN, V., SCARAMUZZA, D. Deep drone racing: From simulation to reality with domain randomization. *IEEE Transactions on Robotics.* 36 (2019), 1, pp. 1-14.

[18] ZAPRIDOU, E., BARTOCCI, E., KATSAROS, P. Runtime Verification of Autonomous Driving Systems in CARLA. In: *Runtime Verification*. Cham: Springer International Publishing 2020.

[19] GAMBI, A., HUYNH, T., FRASER, G. 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 2019*, pp. 257-267.

[20] RICCIO, V., TONELLA. P. 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 2020.

[21] NGUYEN, Y., HUBER, S., GAMBI, A. Automated Generation of Diversified Tests for Self-driving Cars from Existing Maps. In *2021 IEEE International Conference on Artificial Intelligence Testing (AITest*). IEEE 2021, pp. 128-135.

[22] FLORES-GARCÍA, E, KIM, G-E., YANG, J., WIKTORSSON, M., DO NOH, S. 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 (2020), pp. 238–244.

[23] VIKHRAM, R., RAJVIKRAM Y., ELAVARASAN, M., MANOHARAN, M., MIHET-POPA, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation,

and Analysis with Cyber Security Applications. *IEEE Access 8151019–151064;* 2020.

[24] ABDESSALEM, R. B., PANICHELLA, A., NEJATI, S., BRIAND, L. C., STIFTER, T. Testing autonomous cars for feature interaction failures using many-objective search. In: *IEEE/ACM International Conference on Automated Software Engineering*. IEEE 2018, pp. 143-154.

[25] SIEMENS. *Digital Twins/ Software Siemens 2022*. https ://www.plm.automation.siemens.com/global/en/ our- story/glossary/digital-twin/24465

[26] PARK, H., EASWARAN, A., ANDALAM, S. Challenges in Digital Twin Development for Cyber-Physical Production Systems. In: *Cyber Physical Systems. Model-Based Design*. Cham: Springer International Publishing 2021, pp. 28-48.

[27] PROCHAZKOVA, D., PROCHAZKA, J. Generation of Risk-Based Design of Socio-Cyber-Physical Systems. *International Journal of Economics and Management Systems.* 6 (2021), pp. 261– 272. http:// www.iaras.org/ iaras/journals/ij EMS

[28] ZAMPETTI, F., TAMBURRI, D., PANICHELLA, A., PANICHELLA, S., DI PENTA, M., GERARDO, C. Continuous Integration and Delivery practices for Cyber-Physical systems: An interviewbased study - 2022. Doi: 10.1016/j.jss.2022.111425,10.21256/zhaw-25591

[29] OECD. *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.

[30] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRAB KA, L. *Management of Risks Connected with Operation of Technical facility during Its Life Cycle*. ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. Doi 10.14 311%2FBK.9788001066751

[31] EU. *Maastricht Treaty*. Brussels: EU 1992. C 191, 29.7.pp.1–112.

[32] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Management of Risks of Systems for Transport Control*. Praha: ČVUT 2022, 129 p. Doi:10.14 311/BK.97880010 69950

[33] PROCHAZKA, J., NOVOBILSKY, P., PROCHAZKOVA, D., VALOUSEK, S. 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

[34] PROCHAZKOVA, D. Risk-based Design of Technical facilities. In: JUFOS 2021. ISBN 978-80-214-5963-2. Brno: VUT 2021, pp. 40-51.

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

[36] IAEA. *Maintenance Optimization Programme for Nuclear Power Plants*. ISBN 978–92–0–110916–3 Vienna: IAEA 2018. 56 p.

[37] JARDINE, A. K. S., TSANG, A. H. C. *Maintenance, Replacement, and Reliability: Theory and Applications*. London: CRC Press 2014.

[38] KIRAN, S., PRAJEETH KUMAR, K. P., SREEJITH, B., MURALIHARAN, M. Reliability Evaluation and Risk Based Maintenance in a Process Plant. *Procedia Technology*. 24 (2016), pp. 576-583. www.sciencedirect.com

[39] LEONI, L., DE CARLO, F., PALTRINIERI, N., SWKVARBOSSA, F., TOROODY, A. B. A Risk-Based Maintenance: A comprehensive Review of Three Approaches to Track the Impact of consequence Modelling for Predicting Maintenance Actions. *Journal of Loss Prevention in the Process Industries.* 72 (2021), 2, pp. 69-81.

[40] KIRAN, S., KUMAR, K. P. P., SREEJITH, B., MURALIDHARAN, M. Reliability Evaluation and Risk Based Maintenance in PROCESS Plant. *Procedia Technology*. 24 (2016), pp. 576-583

[41] CENELEC. *EN 50126-1 Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).* Brussels 2017.

[42] CHEN, T. Y., KUO, F-C., LIU, H., POON, P-L., TOWEY, D., TSE, T. H., ZHOU, Z.Q. Metamorphic Testing: A Review of Challenges and Opportunities. *ACM Computing Surveys* 51 (2018), 4, pp. 1-27.

[43] AMMANN, P., OFFUTT, J. *Introduction to Software Testing.* ISBN 978-1-316-77312-3. Cambridge: Cambridge University Press 2016, 226 p.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.