Significance of Standards Compliance Organizations for the Sustainable Automotive Software and Car Production

Pavle Dakić[1,2]

[1] Institute of Informatics, Information Systems and Software Engineering, Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava, Vazovova 5, 81 243 Bratislava, Slovakia; pavle.dakic@stuba.sk

[2] Faculty of Informatics and Computing, Singidunum University, Danijelova 32, 11 000 Belgrade, Serbia; pavle.dakic.11@singimail.rs

Abstract: With the advancements in the automobile sector and the growing popularity of the Internet of Things (IoT) and Industrial Internet of Things (IIoT), new generations of vehicles are being developed quickly. When it comes to the creation of autonomous systems, time is of the essence because if they do not adhere to standards and do not have the necessary functional software, they could become useless very quickly. This is, therefore, challenging since necessitates considerable testing and a grasp of the prerequisites for potential applications while using appropriate standards with different requirements of various nations. In terms of legislation and standard compliance, bodies this reflects current challenges. This investigation is more focused on the business side of possible future applicability within the laboratory environment for software testing. We discuss an overview of the benefits, drawbacks, and potential future solutions, which can serve as a solid starting point for subsequent researchers in this field. The main contribution is offered in the form of fresh information that has been summarized and calls for addressing external influences as well as prospective answers to the needs of the IIoT and automotive industries.

Keywords: industry standards; automotive and IIoT; autonomic vehicles; standards bodies; CI/CD

1 Introduction

Sustainable production implies financial profitability when applying new technologies and standards, which is not always the case and requires additional research and the stability of the budget for the implementation of research activities. The desire to modernize the system and interconnect various groups of objects within real-time data transfers implies using the Internet of Things (IoT) in

multiple industries where the system of mutually networked items requires the persistence of unique IDs to establish network communication, without the need for a direct human-to-human or human-to-computer connection [1-4]. Through the current advances and achievements of information technologies within the industry, there has been a simplified connection and application of new communication systems through which it is possible to share common data, information, and resources. As a result of, the implementation of various network protocols, the efficiency of several production processes increased, and at the same time, the operating costs decreased.

This has considerably increased the efficiency of several processes while also lowering operational costs. Various industries such as car manufacturing, health care, the financial sector, and logistics have achieved the greatest benefits and have had a significant impact on the development of technologies that we all have the opportunity to use today. One of the most influential and interesting topics for our research is the automotive industry and IoT together with the Industrial Internet of Things (IIoT). The main reasons are reflected in the possibilities of applying the production process prescribed by Industry 4.0 and 5.0. which is the key basis of normal functioning within this industry. Within the scope of our study, we attempt to present an overview of key standards and communication methods enforced by specific standards organizations, which we had the opportunity to cover in our prior research [4-8]. Standardization is very important to obtain a favorable and safe quality of the final product. Because through the application of the standardization process, it is possible to meet various needs such as food production [9], medical care, help in cases of accidents, and many other cases that are based on the application of standards [10, 11].

Rapid development in the field of IoT leads to an increase in the complexity of IoT solutions. Devices contain a mixture of legacy, third-party, and new code, resulting in the fact that the code is more difficult to understand. One solution to better understand the software is code visualization and testing using CI/CD [12, 13]. Better understanding leads to easier maintenance and extension of the code and, therefore, to easier development, which can affect the reduction of traffic accidents [14]. With knowledge of appropriate IoT standards and software visualization techniques, verifying code compliance with dictated standards may also be possible. Standards compliance organizations in the automotive industry include MISRA, ISO 26262, and IATF 16949. In IIoT, organizations include IEC, ISO, IEEE, ETSI, ISA, and others. Key challenges to automotive standards compliance include managing software complexity, ensuring functional safety, and adhering to evolving regulations. For IIoT, challenges include the convergence of IT/OT, security risks, interoperability, and inadequate regulatory frameworks. In automotive, standards compliance challenges affect software development by increasing verification needs and requiring advanced methodologies. In challenges lead to security vulnerabilities, integration issues, and delays in the deployment of new technologies. Automotive solutions include advanced analysis tools, improved processes, and cross-industry collaboration.

For IIoT, solutions involve security frameworks, plug-and-play architectures, and evolving standards and regulations. Common security problems in embedded software from the automotive industry include lack of encryption, authentication issues, insecure data storage, insufficient input validation, and unpatched vulnerabilities. These can lead to threats such as hacking, denial of service attacks, and loss of sensitive data. CI/CD can help mitigate automotive embedded software security problems by enabling continuous security testing like SAST, SCA, fuzz testing, etc. This allows vulnerabilities to be detected early. Key challenges in implementing CI/CD for automotive embedded software security testing include the complexity of test automation, managing test data, integrating tools, traceability, and differences between IT and automotive software.

The work is organized as follows: materials and methods, literature review, automotive industry and network connectivity, industry standards and key challenges, results and discussion, and conclusions.

2 Materials and Methods

The applied methods within this work were implemented in a way to deal with non-quantitative data, without analysing data sets. During the research and selection of individual articles, the relevant connection with the topic mentioned and the field of research was taken into account. The main focus was on understanding the research directions and challenges facing the automotive industry. The research attempts to look back over a 5-year period and the most recent published results that match our research interests and which are in accordance with the defined title of this paper.

2.1 Selection Criteria, Keywords, and Databases

The selection criteria were implemented based on different keywords collected, which were used to search and find relevant scientific literature. Within this investigation, the qualitative research technique was applied. With this type of research, we focused on a critical analytical approach in order to better understand the different meanings of the experiences of individuals or groups. The limits of this research can be reflected in the necessary prior knowledge from several different scientific fields, in order to be able to clearly understand all the concepts presented. The research in this paper is intended for advanced users and researchers who possess certain knowledge in the field of business and information technologies.

The sources of literature and data are based on various databases and search engines where various scientific sources can be found by applying relevant keywords. The initial literature search was based on the most popular databases,

Google Scholar, JSTOR, Scopus, and Web of Science. The mentioned sources allowed us to conduct research in this area by applying different criteria. Some research papers within this work are a continuation of previously published research within doctoral studies and international projects.

3 Literature Review

In this section, we provide an overview of current research in this area by covering current solutions required to ensure adequate quality of service (QoS) in Internet of Things (IoT) systems [15]. The literature review can be briefly presented within following items:

- QoS with digital transformation and IoT technical scenarios for 5G and networks
- IoT/IIoT privacy risks and security vulnerabilities
- Challenges in developing safety-critical systems within agile large-scale industrial settings

Today's industrial automation systems are undergoing a digital transformation that implies a shift towards the IoT, leading to the Industrial Internet of Things (IIoT) paradigm. Existing Industrial Automated Control Systems (IACSs), enriched with a potentially large number of IoT devices, are expected to make systems more efficient, flexible, provide intelligence, and ultimately enable autonomous control.

A brief overview of the technical scenarios for 5G is presented in the article [16], while the authors in this study [17] cover the connection of mobility of things (MoT) and each of the three LPWAN standards: LoRaWAN, DASH7, and NB-IoT. After which we could see that some of the authors [17] dealt with localization in wireless sensor networks (WSNs). Where their main focus was on technical details about the approaches and algorithms of various important localization techniques using different technologies. Notably, study [18] compares congestion control approaches in 6LoWPAN networks, illustrating the significance of technical nuances in localization techniques. The literature [18] emphasizes a comparative review within this study, highlighting various congestion control approaches in 6LoWPAN networks. In industrial settings, operational technology (OT) encompasses hardware and software that supervise physical equipment, processes, and infrastructure. The convergence of information technology (IT) and OT in manufacturing introduces novel security challenges distinct from IT's data-focused scope. The authors [19, 20] present the status quo in IIoT cybersecurity challenges and mitigation mechanisms and strategies, in sync with potential developments of advanced cyberphysical industrial machines. This requires addressing the challenges that arise due to the use of low-power IIoT devices in the modular manufacturing systems of Industry 4.0 and vehicles [21].

IoT, especially industrial IoT (IIoT), has rapidly developed and is receiving a lot of attention in academic areas and industry, but IoT privacy risks and security vulnerabilities are emerging from a lack of fundamental security technology. The blockchain technique, due to its decentralization and information disclosure, was proposed as a decentralized and distributed approach to guarantee security requirements and motivate the development of IoT/IIoT [22]. IIoT has rapidly developed and is receiving a lot of attention, but IoT/IIoT privacy risks and security vulnerabilities are emerging from a lack of fundamental security technology. In the article [23], the authors first introduce the critical IoT/IIoT infrastructure in industry 4.0, and then [23] briefly presents the blockchain and edge computing paradigms. After that, they show how the convergence of these two paradigms can enable secure and scalable critical infrastructures. Due to the ever-increasing number of IoT/IIoT that are connected to the Internet, the high volume of generated and collected data, with high security and scalability, is becoming a hot concern for critical infrastructures in Industry 4.0. The authors [24, 25] analyze the anatomy of the intersection of ecosystem security of the IoT ecosystem security and blockchain technology in the context of Industry 4.0.

The manufacturing sector has had various difficulties in implementing IIoT, mainly due to characteristics that offer an in-depth review of Industry 4.0 [26]. The primary motivation behind this is to introduce the latest advancements related to the production industry, as well as to address the existing limitations. The authors of this study [27] present an analysis of the most relevant security strategies in Industry 4.0, focusing primarily on DiD. In this article [28], we can see a comprehensive overview of the state-of-the-art network automation technologies, standardizations, and the corresponding impact on IIoT of Industry 4.0. Network automation has been bred by the deployment of 5G based IIoT in Industry 4.0, and further approaching pervasive AI and human-robot interaction with collaboration toward 6G based Industry 5.0.

Unfortunately, these standards were not designed to accommodate technologies such as Machine learning (ML) or the type of functionality provided by an Autonomous Decentralized System (ADS) and have created a conflict between the need to innovate and the need to improve safety. This means that we need to take steps to address this conflict by doing a detailed assessment and adaption of ISO 26262 for ML, specifically in the context of supervised learning. MISRA C is a coding standard that defines a subset of the C language, originally targeted at the automotive sector, but now adopted in all industries that develop C software in safety and / or security-critical contexts [29].

The authors in [30] introduce MISRA C, its role in the development of critical software, especially in embedded systems, its relevance to industry safety standards, as well as the challenges of working with a general-purpose programming language standard that is written in natural language with a slow evolution over the last 40+ years. The complexity and size of Autonomous Driving (AD) software are comparable to those of software implementing other

(standard) functionalities in the car. To make things worse, a large fraction of AD software is not specifically designed for the automotive (or any other critical) domain but for the mainstream market. The results of the study [31] present the experience in applying ISO 26262 – the applicable functional safety standard for road vehicles – software safety guidelines to industrial AD software, in particular, Apollo, a heterogeneous autonomous driving framework widely used in industry.

Attempt to understand [32] the challenges that exist when developing safety-critical systems within agile large-scale industrial settings, in particular in the automotive domain. Some propose an approach [33] to manage the diversity of safety goals and to support the safety certification of software components. Component-based approaches and software product lines have been adopted by industry to manage the diversity of configurations in safety-critical software. Safety certification requires compliance with standards. ISO 26262 standard uses the concept of automotive safety integrity level (ASIL) to assign safety requirements to components of a system under design. Compliance with standards is demonstrated through the achievement of those ASILs which can be very expensive when requirements are high. Although achieving variant-intensive component safety certification without being unnecessarily stringent or expensive is desirable for the economy, it poses challenges to safety engineering. The requirements set for the next-generation powertrain systems (e.g., performance and emissions) are becoming increasingly stringent with ever-shortening time-to-markets at reduced costs. To remain competitive, automotive companies are progressively relying on model-driven development and virtual testing. Virtual test benches, such as hardware-in-the-loop simulators, are powerful tools to reduce the amount of physical testing and speed up the engine software calibration process. Some describe [34] a novel verification process to create a fast-running model for a heavy-duty diesel engine using FRM-d Builder in the GT-SUITE simulation software.

In recent decades, the automobile industry has seen substantial transformations, moving from manual to fully automated vehicles. Advances in artificial intelligence (AI) now enable automobile businesses to use black-box AI models. These models allow vehicles to sense their environment and make autonomous driving decisions, frequently with minimum human participation. The study's authors [35] cover a comprehensive survey of the existing body around explainable autonomous driving. Here, the investigations [36] show the conventional and recent developments of the relevant state of the art for IIoT technologies, frameworks and solutions to facilitate interoperability between different IIoT components. In the era of Industry 4.0, the IoT performs the driving position analogous to the initial industrial metamorphosis. IoT affords the potential to couple machine-to-machine intercommunication and real-time information gathering within the industry domain. Therefore, the enactment of IoT in the industry magnifies effective optimization, authority, and data-driven judgment.

4 Automotive Industry and Network Connectivity

The automotive industry is one of the most evolved industries in the recent past. Even thirty years ago, no one could have predicted the possibilities that today's cars have. The use of IoT in the automotive industry is bringing the automotive sector to the brink of another revolution by moving from human-driven vehicles to fully self-driving vehicles [37]. In 2022, fully autonomous vehicles are not only future concepts, but vehicles still require human interception are still prevalent. The rapid development of the automotive industry and the rapidly growing number of interconnected devices have resulted in the fact that the automotive industry is one of the fastest growing sectors for the development of IoT [5].

With developments in the automotive sector, IoT/IIoT, 5G, Industry 4.0/5.0, etc. in recent times, the new concept of the Internet of Vehicles (IoV) has emerged. All this involves using some form of IoT to connect to the Internet. Various vehicles are connected to all entities on the roads and this can influence the decision making process in the vehicle Machine Learning model. The IoV is expected to eventually evolve into the Internet of Autonomous Vehicles [38]. The main reasons for the development of an autonomous vehicle network are increased traffic safety, less pollution, and better travel efficiency [39]. The applications of IoT in vehicles can be divided into three main categories [40]: safety, information technology, and efficiency. Remote vehicle management, smart navigation, tailored in-car experiences, predictive maintenance, entertainment connectivity, and hands-free controls are examples of convenience features found in IoT applications for vehicles. These features expedite daily duties, optimize travel routes, personalize driving settings, predict maintenance needs, and provide the user with consistent services.

Each of the mentioned systems has its role in efficient vehicle management and requires a certain degree of standardization depending on the country where the final product, such as an autonomous vehicle, will be sold.

The information in connected cars offers drivers many options for information, such as streaming music, maps, vehicle status through the dashboard, and many more [40, 41]. Part of the efficiency consists mainly of traffic control. With the use of IoT, governments get information on traffic volumes at intersections and can adjust traffic light settings accordingly. Other uses could be parking navigation, cooperative driving, or route navigation [40, 41]. When we talk about the use of the Internet of Things that is being developed for the safety of road users, we are talking about functions such as ominous collision detection, lane departure detection, or driver monitoring [41, 42].

4.1 Operational Technology

Managing software complexity as vehicles incorporate more advanced features such as ADAS and autonomous driving. This requires huge growth in software scale and complexity. Ensuring functional safety and compliance with evolving regulations as software takes over more vehicle functions. Safety risks are increasing, and standards of quality are being adhered to in complex global supply chains. The technology itself and the application of operational technology (OT) implies (Figure 1) the stability of wireless communication (wireless networks), cloud solutions, APIs, and edge devices. The choice of the best strategies and solutions for each company depends on several different parameters that include its location, size, and digital maturity in the market. The second important factor refers to the successful application of IT/OT convergence by emphasizing business goals with which the business is above the technology itself. The main reasons can be found in the desire of companies to isolate themselves from a highly layered technical architecture and to align their goals more closely with the goals of management or the board of directors.

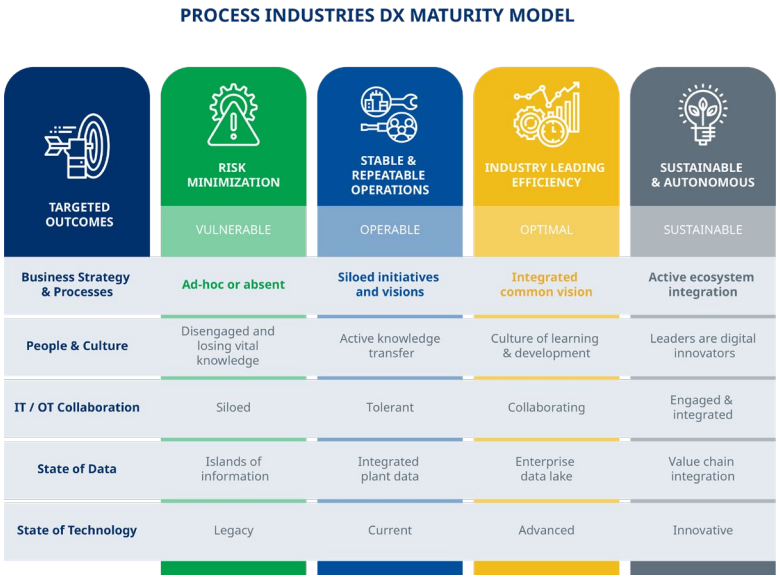

Figure 1
Business DX Maturity Model. Source: [43]

That is why every organization considers and perceives different standardization needs and rules prescribed by different bodies for compliance with standards. One of the approaches we had the opportunity to get acquainted with during the research was that companies create development maps of development over a certain period of time. Through this approach, it is possible to determine the ideal

approach to creating additional digital value with the possibility of initiating the desired changes at the desired moment. One of the ways that can be applied directly refers to the application of the business DX Maturity Model (Figure 1), which is one of the models that significantly changes the position and serenity of the company on the market [43].

By applying IT/OT convergence within corporate functions, it is easier for companies to plan and model a digitally connected enterprise with a certain degree of automation that can be used by every employee. With the application of automation, the ideas and suggestions of the employees are marked, which additionally increases awareness of the current situation and the importance of the information that is exchanged within the work environment. The availability of information is a key factor in making business decisions and directing the company in the right direction. On the other hand, it represents a certain kind of challenge and evolutionary process that they are not always ready to carry out to the end [43]. Smart production in the automotive industry and others that use process production through the application of IT/OT convergence can enable the use of digital technologies and different communication protocols in order to achieve a higher degree of the final product. In this case, it would be one car or a part that is installed inside, where the requirements and production conditions for each product can be seen at any time on the digital control panel and the management dashboard [44]. Most of this transformation is concentrated on production and integrated solutions that enable certain degrees of factory automation through remote control and monitoring. Automotive companies want to get a turnkey system with which they can implement smart production with modular IT solutions to connect physical components within the production line.

In the event that the entire process is successfully applied and done in the right way, the convergence itself can enable integrated access to data within the entire company in real time. The most important insight is maintained in the possibility of a holistic review of the company's functioning, on the basis of which the leaders and the entire organizational structure have transparency. Although the other side of the coin may refer to the unexpected vulnerability of the system due to the increased degree of digitization [45, 46], at the same time, by applying relevant standards, it may significantly increase efficiency and quality, which is maintained by quality control. The main reasons and the desire of the application organization are to obtain the possibility of improving all existing processes and reducing downtime due to the failure of some of the production machines or robots. Based on this, sustainable production can be planned and created over a long period of time.

All this together is the key that drastically changes today's business and can potentially enable the creation of new business models that are based on subscription and focus on results. This ultimately means that, if a certain company has free space in its factory that is empty and not being used, another company can rent a certain production capacity and thus save in the very process of starting

the production process by itself. Most production processes are regulated by some of the standards depending on the area and category of application. One of the most commonly used is regulated by the application of ISA95 (Figure 2), Enterprise Control System Integration Model [47]. Basically, for the needs of improvement and integration of information technologies and the strategy itself called IT/OT convergence strategy, it is necessary to have the appropriate IoT and IIoT infrastructure. Convergence in IT/OT requires the integration of distinct operational approaches and expectations that can reduce the attack surfaces [47, 48]. In this way, it is easier to assess where an interruption or attack occurred within the system.

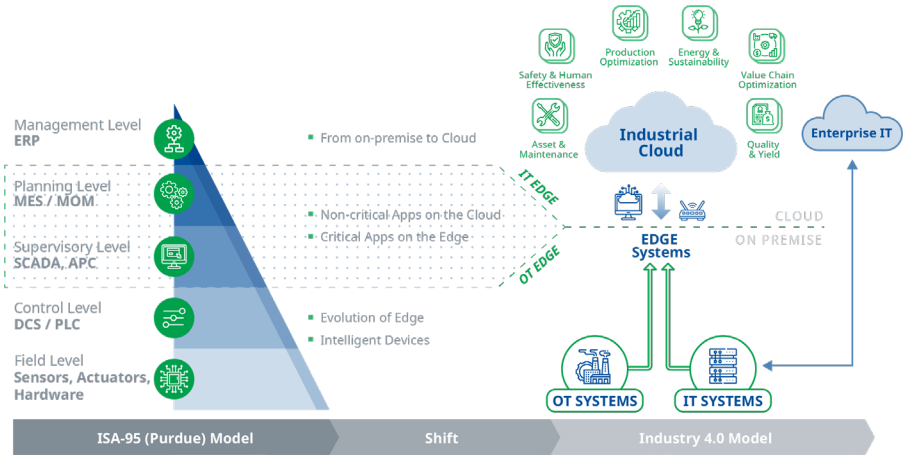

Figure 2
ISA-95 Model and Industry. Source: [43]

Managing increased security risks as connectivity and complexity grow is increasing attack surfaces. For achieving seamless interoperability between diverse systems and components, some of Plug-and-play capabilities are lacking which are inadequate using regulatory frameworks and evolving standards, making the automotive companies can hardly keep up the pace with rapid changes.

4.2 Industry Standards and Key Challenges

In the following subsections, we plan to summarize the standards of IoT/IIoT in the automotive industry. We divided the standards used into network standards and IoT regulations. In the network standards section, we will summarize the protocols and technologies used in automotive IoT. In the section on IoT regulations, we will write about companies or organizations that standardize the use of IoT and mention several standards that are used. Standardization in IoT is

very important for connected cars that collect huge amounts of data from the environment, the driver, and the car itself using many IoT devices. It is important that all IoT devices use the same standards to achieve seamless interoperability. There are many organizations that are creating standards that can be used for all parts of the IoT chain, from start to finish. These standards regulate device manufacturers, IoT service providers, application developers, and retailers as well. The goal of standardization is to create universally accepted specifications and protocols used [4, 49, 50].

Within our research, we focused on the following organizations and divided them into the following categories (Figure 3): network standardization, IoT standardization, and vehicle standardization. On the basis of the mentioned categories, we will explain in a little more detail what each of the mentioned organizations deals with and what are their systems for managing the standardization process.

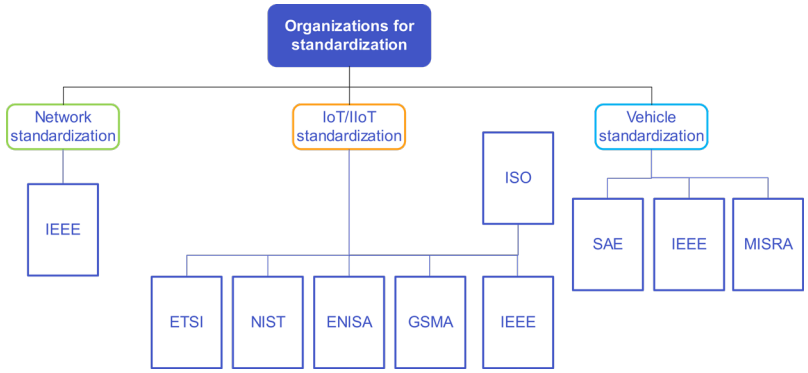

Figure 3
Overview of standards organizations. Source: author's contribution

Within this industry there are some of the following organizations and standards that are important to mention [6]:

MISRA provides guidelines for developing safety-critical electronic systems and software in automotive. It is managed by a steering committee of the major OEMs and suppliers.

- ISO 26262 is an international functional safety standard adapted from IEC 61508 for automotive. It covers requirements throughout the product life cycle.
- IATF 16949 is an ISO technical specification focused on quality management in automotive supply chains. It aims to prevent defects and reduce variation.
- IEC develops international standards for electrical, electronic, and related technologies such as smart manufacturing.

- ISO develops standards for information security, IoT, smart manufacturing, and other areas related to IIoT.
- IEEE involves technologists from academia, industry, and government in developing standards for IoT and related technologies.
- The European Telecommunications Standards Institute (ETSI) produces standards for information and communication technologies that include machine-to-machine communications. The European Telecommunications Standards Institute is a non-profit organization that creates standards in the sector of information and communication technologies. Their standard ETSI EN 303 645 discusses security for constrained devices that are part of the IoT. In the document, they proposed rules such as that no universal default password should be used, which means that all passwords should be either uniquely generated or defined by the user, or they proposed that manufacturers must keep updating the security of devices in a timely manner, and so on.
- ISA develops standards for automation and control systems used in IIoT environments.
- National Institute of Standards and Technology (NIST) - The National Institute of Standards and Technology is an organization under the United States Department of Commerce. In the NIST 8259 series, they provide guidelines for manufacturers and other parties of the chain that we described on how to design, test and sell IoT devices. In Executive Order (E.O.) 14028 NIST described baseline security for consumer IoT devices.
- European Union Agency for Cybersecurity (ENISA) - The European Union Cybersecurity Agency published a document naming baseline security recommendation for IoT in 2017. They presented a series of recommendations, such as it is important to raise awareness of the need for IoT cybersecurity, or they clarified liability among IoT stakeholders and other recommendations.
- GSM Association (GSMA) - the GSMA is an organization that represents the interests of mobile network operators. They published their own security guidelines for IoT in the IoT Security Guidelines Overview document, in which one of the examples used was an automotive tracking system. In this example, they described how to use their guidelines effectively in the field of automotive IoT.
- Institute of Electrical and Electronics Engineers (IEEE) - The Institute of Electrical and Electronics Engineers (IEEE) is an organization active in standardization technology. They have published many documents on network standardization and are active in the IoT sector as well. IEEE P2413-2019 specifies the architectural framework for IoT. IEEE 1451-99 standardized the interoperability of IoT devices and systems. IEEE P2040 standardizes fully automated vehicles. International Organization for

Standardization (ISO) - ISO is an independent, nongovernmental international standardization organization. ISO/TC22 develops standards for all components and systems for Road Vehicles.

- Society of Automotive Engineers (SAE) - SAE created the standard J3016, which defines the autonomous stages of vehicles. We have already defined these stages in the stage-by-stage section of vehicle autonomy.

5 Results and Discussion

Based on the research conducted, we can summarize and present the following observations in the form of advantages and disadvantages. On the basis of the above, certain possible solutions can be proposed which need to be investigated in more detail in the future. The main challenges within these interconnected industries face different aspects of standardization that are not always fully implemented and explained. The main discussion remains on the financial aspect of standardization and a process better described by the bodies that prescribe and define them.

The impact of challenges and potential solutions for the automotive and IIoT industries might be stated as challenges in managing standards compliance as software complexity increases. Some of the important views can be summarized in the following:

Advantages and Impact of Challenges - Automotive Industry

- Increasing verification needs to ensure safety and reliability. Advanced analysis tools are required.
- Necessity of improved processes like continuous integration and rapid debugging.
- Greater need for cross-industry collaboration on standards development. Disadvantages and Challenges - Automotive Industry
- Security vulnerabilities arising from gaps in standards application and alignment.
- Integration and interoperability issues between components and systems.
- Delays in the deployment of new technologies due to regulatory burdens.

Potential Solutions

- Adopt more advanced analysis tools like exhaustive static analysis to verify code using CI/CD.
- Implement improved processes and toolchains to enable agile development with modern project tracking tools.

- Increase collaboration between OEMs and suppliers on standards evolution in IIoT Industry
- Develop security frameworks like IISF that span IT and OT.
- Creating plug-and-play architectures to ease regulatory burdens.
- Developing standards and regulations to keep pace with technology innovation.
- Rental of spare capacities to other producers of the automotive industry

The findings of this study should motivate future research into simulation and computer-aided engineering (CAE) tools. This would enable us to investigate breakthroughs in multiphysics simulations, optimization approaches, and integration with upcoming technology that is connected to sustainable automotive software and car production. In addition, software tools that we should consider in the future would be Simcenter STAR-CCM+, Simcenter 3D, Ansys Fluent, and Keysight ADS which could be investigated further. The scalability of these software tools for large-scale simulations may be an interesting topic for future research.

The first phase of future study should focus on vulnerabilities, delays, and integration concerns. The second section should address solutions such as enhanced processes, frameworks, collaboration, and higher standards. Addressing these issues may be the key to boosting software innovation and standardization. In addition, research may have focused on developing specialized simulation software for specific applications, such as biomedical engineering or renewable energy technologies. We believe that understanding the effects of simulation software on engineering innovation, productivity, and sustainability is critical for future research.

Conclusions

In the industry, we were able to see the connection and important interconnection of IT and operational technology that is offering the novel use of digital technology to accelerate business strategy. Enabling an easy transformation of the automotive industry and the production process. We can see that there are still many challenges that must be addressed and solved in the future of the automotive industry. In the future, programmers will have to become better acquainted with the direct application of standards when creating the logic of the machine model and the devices with which they communicate. This means that successful companies must address the current problems by incorporating industry-required sustainable production methods.

The convergence of IT and operational technologies has accelerated the industry's digital transformation, which is most visible in automotive and manufacturing processes. Despite advances, significant obstacles remain, requiring a more thorough integration of standards into machine logic and communication

protocols. Since, the code for IoT devices is usually a mixture of legacy, third-party, and new code. The most difficult task remains to understand standards and software that should apply certain definitions prescribed by various bodies and organizations, as time is of the essence in rapidly developing industries such as automotive. Some of the challenges and knowledge from this work that we will need to cover in the future. Further research should be continued and look at the information that covers the processes of standardization and direct application.

The most significant of our primary findings is shown in the fact that all interconnected production processes are dictated by standard compliance bodies and laws, which carry the most weight. All this together affects the Business DX Maturity Model and the further development possibilities of the company and its products.

Acknowledgement

The work reported here was supported by the Slovak national project Increasing Slovakia's Resilience Against Hybrid Threats by Strengthening Public Administration Capacities (Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy) (ITMS code: 314011CDW7), co-funded by the European Regional Development Fund (ERDF), the Operational Programme Integrated Infrastructure for the project: Research in the SANET network and possibilities of its further use and development (ITMS code: 313011W988), Advancing University Capacity and Competence in Research, Development and Innovation (ACCORD) (ITMS code 313021X329), co-funded by the ERDF, rurALLURE project - European Union's Horizon 2020 Research and Innovation program under grant agreement number: 101004887 H2020-SC6-TRANSFORMATIONS-2018-2019-2020/H2020-SC6-TRANSFORMATIONS-2020, by the Slovak Research and Development Agency under the contract No. APVV-15-0508, Erasmus+ ICM 2023 No. 2023-1-SK01-KA171-HED-000148295 and Model-based explication support for personalized education (Podpora personalizovaného vzdelávania explikovaná modelom) - KEGA (014STU-4/2024)

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] P. Dakić, L. Filipović, and M. Starčević, "Application of fundamental analysis in investment decision making: example of a domestic business entity," in ITEMA 2019. Association of Economists and Managers of the Balkans - Udekom Balkan, 2019

[2] P. Dakić and V. Todorović, "Isplativost i energetska efikasnost autonomnih vozila u eu," FBIM Transactions, vol. Vol. 9, No 2, 10 2021 [Online] Available: https://www.meste.org/ojs/index.php/fbim/article/view/1198

[3] A. S. Gillis, "What is the internet of things (IoT)?" IoT Agenda, Mar. 2022 [Online] Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[4] P. Dakić and M. Živković, "An overview of the challenges for developing software within the field of autonomous vehicles," in 7th Conference on the Engineering of Computer Based Systems, ser. ECBS 2021. New York, NY, USA: Association for Computing Machinery, 2021 [Online] Available: https://doi.org/10.1145/3459960.3459972

[5] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, "Evolution of iot-enabled connectivity and applications in automotive industry: A review," Vehicular Communications, Vol. 27, p. 100285, 2021

[6] P. Dakić, V. Todorović, and P. Biljana, "Investment reasons for using standards compliance in autonomous vehicles," ESD Conference, Belgrade 75th International Scientific Conference on Economic and Social Development Development, ESD Conference Belgrade, 02-03 December, 2021 MB University, Teodora Drajzera 27, 11000 Belgrade, Serbia, 2021 [Online] Available: https://www.shorturl.at/diMRS

[7] P. Dakić, V. Todorović, and V. Vranić, "Financial justification for using ci/cd and code analysis for software quality improvement in the automotive industry," in 2022 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC) 2022, pp. 149-154

[8] P. Dakić, V. Todorović, and V. Vranić, "Financial sustainability of automotive software compliance and industry quality standards," in Proceedings of Eighth International Congress on Information and Communication Technology. Springer Nature Singapore, 2023, pp. 477-487

[9] M. Ćurčić, V. Todorović, P. Dakić, K. Ristić, M. Bogavac, M. Špiler, and M. Rosić, "Economic potential of agro-food production in the republic of serbia," Ekonomika poljoprivrede / Economics of agriculture, Vol. 68, No. 3, pp. 687-700, 2021

[10] M. Kročka, P. Dakić, and V. Vranić, "Extending parking occupancy detection model for night lighting and snowy weather conditions," in 2022 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC) 2022, pp. 203-208

[11] M. Krocka, P. Dakic, and V. Vranic, "Automatic license plate recognition using OpenCV," in 2022 12th International Conference on Advanced Computer Information Technologies (ACIT) IEEE, Sept. 2022

[12] P. Dakić, J. Savić, and V. Todorović, "Software quality control management using black-box testing on an existing webshop trinitishop," FBIM Transactions, Vol. Vol. 9 No 1, May 2021 [Online] Available: https://www.meste.org/ojs/index.php/fbim/article/view/1137

[13] N. Hroncova and P. Dakić, "Research study on the use of CI/CD among slovak students," in 2022 12th International Conference on Advanced Computer Information Technologies (ACIT) IEEE, Sept. 2022

[14] L. Porkolab and I. Lakatos, "A simulation system for testing side crashes, in non-traditional seating positions, for self-driving cars," Acta Polytechnica Hungarica, Vol. 20, No. 7, pp. 63-82, 2023

[15] G. Tanganelli, C. Vallati, and E. Mingozzi, "Ensuring quality of service in the internet of things," in New Advances in the Internet of Things. Springer International Publishing, jun 2017, pp. 139-163

[16] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prevotet, "Internet of mobile things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and supported mobility," IEEE Communications Surveys & tutorials, Vol. 21, No. 2, pp. 1561-1581, 2019

[17] F. Khelifi, A. Bradai, A. Benslimane, P. Rawat, and M. Atri, "A survey of localization systems in internet of things," Mobile Networks and Applications, Vol. 24, No. 3, pp. 761-785, Aug 2018

[18] H. A. A. Al-Kashoash, H. Kharrufa, Y. Al-Nidawi, and A. H. Kemp, "Congestion control in wireless sensor and 6lowpan networks: toward the internet of things," Wireless Networks, Vol. 25, No. 8, pp. 4493-4522, May 2018

[19] B. Leander, A. Čaušević, and H. Hansson, "Applicability of the IEC 62443 standard in industry 4.0 / IIoT," in Proceedings of the 14th International Conference on Availability, Reliability and Security. ACM, Aug 2019

[20] O. Alsaadoun, "A cybersecurity prospective on industry 4.0: Enabler role of identity and access management," in Day 3 Thu, March 28, 2019. IPTC, March 2019

[21] S. Mantravadi, R. Schnyder, C. Moller, and T. D. Brunoe, "Securing IT/OT links for low power IIoT devices: Design considerations for industry 4.0," IEEE Access, Vol. 8, pp. 200 305-200 321, 2020

[22] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," Internet of Things, Vol. 10, p. 100081, jun 2020

[23] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," IEEE Internet of Things Journal, Vol. 8, No. 4, pp. 2300-2317, Febr 2021

[24] P. Borovska and M. Gugutkov, "The intersection of IoT ecosystem security and blockchain technology in the context of industry 4.0," in THERMOPHYSICAL BASIS OF ENERGY TECHNOLOGIES (TBET 2020) AIP Publishing, 2021

[25] D. Kang, M. Prabhu, R. R. Ahmed, Z. Zhang, and A. K. Sahu, "Digital-IIoTs spheres approach toward public development: an exploiting fuzzy-grey mathematical modeling of IIoTs spheres," Grey Systems: Theory and Application, Vol. 12, No. 2, pp. 389-416, June 2021

[26] M. Alabadi, A. Habbal, and X. Wei, "Industrial internet of things: Requirements, architecture, challenges, and future research directions," IEEE Access, Vol. 10, pp. 66 374-66 400, 2022

[27] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, "Securing iiot using defence-in-depth: Towards an end-to-end secure industry 4.0," 2022

[28] H. R. Chi, C. K. Wu, N.-F. Huang, K.-F. Tsang, and A. Radwan, "A survey of network automation for industrial internet-of-things toward industry 5.0," IEEE Transactions on Industrial Informatics, Vol. 19, No. 2, pp. 2065-2077, Febr 2023

[29] R. Salay and K. Czarnecki, "Using machine learning safely in automotive software: An assessment and adaption of software process requirements in iso 26262," 2018

[30] R. Bagnara, A. Bagnara, and P. M. Hill, "The misra c coding standard and its role in the development and analysis of safety and security-critical embedded software," 2018

[31] H. Tabani, L. Kosmidis, J. Abella, F. J. Cazorla, and G. Bernat, "Assessing the adherence of an industrial autonomous driving framework to ISO 26262 software guidelines," in Proceedings of the 56th Annual Design Automation Conference 2019. ACM, June 2019

[32] J.-P. Steghöfer, E. Knauss, J. Horkoff, and R. Wohlrab, "Challenges of scaled agile for safety-critical systems," 2019

[33] L. Bressan, A. L. de Oliveira, F. Campos, Y. Papadopoulos, and D. Parker, "An integrated approach to support the process-based certification of variant-intensive systems," in Model-Based Safety and Assessment. Springer International Publishing, 2020, pp. 179-193

[34] J. Andric, D. Schimmel, and J. Heide, "Calibration procedure for measurement-based fast running model for hardware-in-the-loop powertrain systems," in SAE Technical Paper Series. SAE International, Apr 2020

[35] D. Omeiza, H. Webb, M. Jirotka, and L. Kunze, "Explanations in autonomous driving: A survey," 2021

[36] A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, "A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions," ACM Computing Surveys, Vol. 55, No. 1, pp. 1-35, Nov 2021

[37] X. Krasniqi and E. Hajrizi, "Use of iot technology to drive the automotive industry from connected to full autonomous vehicles," IFAC-PapersOnLine, Vol. 49, No. 29, pp. 269-274, 2016

[38] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in 2014 IEEE world forum on internet of things (WF-IoT) IEEE, 2014, pp. 241-246

[39] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, and D. Wang, "Survey on the internet of vehicles: Network architectures and applications," IEEE Communications Standards Magazine, Vol. 4, No. 1, pp. 34-41, 2020

[40] W. Wu, Z. Yang, and K. Li, "Internet of vehicles and applications," in Internet of Things. Elsevier, 2016, pp. 299-317

[41] M. N. Sadiku, M. Tembely, and S. M. Musa, "Internet of vehicles: An introduction," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 8, No. 1, p. 11, 2018

[42] Y. Huo, W. Tu, Z. Sheng, and V. C. Leung, "A survey of in-vehicle communications: Requirements, solutions and opportunities in iot," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) IEEE, 2015, pp. 132-137

[43] Yokogawa, "It/ot convergence: Bringing two worlds together," Yokogawa Electric, 2021 [Online] Available: https://www.yokogawa.com/library/resources/white-papers/itot-convergence-bringing-two-worlds-together/

[44] V. Todorović, P. Dakić, and M. Aleksić, "Company management using managerial dashboards and analytical software," ESD Conference, Belgrade 75th International Scientific Conference on Economic and Social Development Development, ESD Conference Belgrade, 02-03 December, 2021 MB University, Teodora Drajzera 27, 11000 Belgrade, Serbia, 2021 [Online] Available: https://shorturl.at/diMRS

[45] M. Aleksic, P. Dakic, I. Stupavsky, and V. Todorovic, "Time and company management in cases of fake news within the automotive industry," pp. 56-66, May 2023, copyright - Copyright Varazdin Development and Entrepreneurship Agency (VADEA) May 18/May 19, 2023; Last updated - 2023-06-06 [Online] Available: https://shorturl.at/aqvOS

[46] I. Stupavsky, P. Dakic, V. Todorovic, and M. Aleksic, "Historical aspect and impact of fake news on business in various industries," pp. 380-389, May 2023, copyright - Copyright Varazdin Development and Entrepreneurship Agency (VADEA) May 18/May 19, 2023; Last updated - 2023-06-06 [Online] Available: https://shorturl.at/cxCQ6

[47] C. Wangsness, “IT OT Convergence: Transforming the World of Operational Technology,” 2023 [Online] Available: https://www.onlogic.com/company/io-hub/it-ot-convergence-transforming-the-world-of-operational-technology/

[48] B. (NYSE:BRC), “IT/OT Convergence 101: Benefits, Strategy & Tools,” 2023 [Online] Available: https://www.bradyid.com/intelligent-manufacturing/it-ot-convergence-101

[49] B. Lloyd, “IoT Device Security Standards & Code of Practice | Coderus,” Coderus, Oct. 2022 [Online] Available: https://www.coderus.com/iot-device-security-standards-and-code-of-practice-for-iot-security

[50] S. Dahmen-Lhuissier, “ETSI,” Dec. 2022 [Online] Available: https://www.etsi.org/technologies/internet-of-things