TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 65, Issue Special III, November, 2022

IMPACT ANALYSIS ACCORDING TO ISO 26262 STANDARD USING SAFETY ANALYSIS INTEGRATED IN APIS IQ-RM TOOL

Dianora IGNA, Mădălin-Dorin POP

Abstract: *The increasing complexity and autonomy of hardware systems make the verification of the functional safety of the entire system, as well as the individual component, a challenging operation, highlighting the need for a synergy concept between FTA, FMEA, and FMEDA. This article provides a model-based risk analysis according to the ISO 26262 standard. Its aim is to develop, with the help of the APIS IQ-RM Tool, the analysis of an existing system in the vehicle. By using the unified safety analysis model proposed in this article, an improvement in the process of identifying possible defects that may occur in a system developed in the automotive industry has been demonstrated.*
Keywords: *functional safety, FMEA, hazardous events, impact analysis, ISO 26262, model-based analysis, risk analysis*

1. INTRODUCTION

From the 18th century, when the first steam engine was invented, until the 21st century, the automotive industry was in continuous development.

Since the 1970s, the first cars were equipped with an ECU (Electronic Control Unit), which was considered the engine's computer and managed to ensure the best possible engine operation. In our days, cars are equipped with several dozens of ECUs. Industrial automation is an interdisciplinary field between mechanical and electrical engineering, ultimately aiming to find methods that lead to the automation of machines without human participation.

As argued by Prostean et al. [1], today's automotive system engineering is in a continuous increase, the automotive systems becoming an ensemble of ECUs, interconnected through specific automotive communication channels. It is well known that functional safety discipline represents an essential concern in all areas of industry, be it in nuclear plants, aviation industries, medical appliance manufacturers, or the automotive industries [2]. Considering the above, it is highlighted that the complexity of cars has reached a very high level, therefore, the need for functional safety has become inevitable. Moreover, also the need for experts in automotive products auditing arises, the quality topic representing a must in functional safety-related projects [3].

The high quality of a functional safety-related project can be achieved by following the ISO 26262 standard [4]. To simplify its application, many researchers proposed various approaches adapted to the current specific needs of the automotive industry, such as automated driving systems [5-6] or electric vehicles [7-8].

The most important step in the development of automotive systems consists of the requirement definition process and its functional safety classification using the ASIL (Automotive Safety Integrity Level) attribute [9-10]. Gharib et al. [11] proposed a model-based approach that considers both technical and social aspects in the modeling and analysis of ASIL requirements. This allows the requirements engineers "*to define clear design specifications concerning the driver's behavior and its interactions and dependencies with other components of the item (i.e., The product)*" [11]. UML (Unified Modeling Language) profiles for safety specifications are usually used in the design step of these components [11-12].

Lu and Chen [13] proposed a model-based framework for the analysis of safety-critical systems based on the following three phases that will generate the FMEDA (Failure Mode, Effect, and Diagnostic Analysis) report as output:

- Safety-critical weak-point analysis;
- Safety-oriented system hardware architecture exploration;
- Safety-mechanism effectiveness assessment.

The architecture of a system, regardless of its nature, is composed of the system itself, subsystems, and components. Based on this premise, the decomposition is done on three levels. Taking a bottom-up approach, each component is given a requirement or a set of requirements.

For a system to work accurately, it must meet all the functional requirements assigned to it. Most of the time, this is quite difficult to verify by system safety engineers, as systems are extremely complex, and an overview is often lacking. The ISO 26262 standard supports the use of formal methodologies for various verification activities throughout the lifecycle of safety-related embedded systems for road vehicles to achieve the highest levels of safety integrity [14]. System safety engineering faces additional challenges as vehicle systems become more complicated. This statement is supported by our daily lives, in which we are constantly exposed to electrical and/or electronic (E/E) systems, the failures of which could have catastrophic safety effects.

The well-known component shortage topic is not closed these days. The announcement that some semiconductor manufacturing plants are closing has caused all kinds of disturbances in several industries, and the automotive industry has not escaped [15]. This is problematic for HW (hardware) engineers who must come up with redesign ideas or even component changes. This can also trigger an impact on the safe operation of the whole system. To demonstrate that component replacement does not impact safety, system safety engineers must perform an impact analysis on the change. First, they need to determine the differences between the two components, then the effectiveness of the new one. To prove the two mentioned above, FMEA (Failure Mode and Effect Analysis) and FTA (Fault Tree Analysis) even FMEDA, analyzes must be present [16].

This paper aims to bring to light the need to develop a model based on both quantitative and qualitative analysis; moreover, a correlation with the requirements will complete this view.

2. ISO 26262 STANDARD AND SAFETY LIFECYCLE

ISO 26262 must be applied to safety-related systems that have one or more E/E systems and that are installed in series production passenger cars with a maximum gross weight of up to 3.50 t. In the automotive industry, everyone must follow the ISO 26262 standard that is created for the safety regulations of the electronic systems of an autonomous vehicle [17]. "*The ISO 26262 standard measures the safety system, performance or probability of failure within electronic components in a vehicle with autonomous features*" [17].

The ISO 26262 standard first appeared in 2011 intending to provide a clear picture of possible hardware (HW) or software (SW) faults and enforce a standard that provides functional safety for automotive E/E systems. This standard is derived from IEC 61508 which is responsible for "*functional safety of electrical /electronic/programmable electronic safety-related systems*" [18]. The first version of ISO 26262 consists of 10 parts, and the second version, which was published in 2018, contains two additional chapters: "*Guidelines on the application of ISO 26262 to semiconductors*" and "*Adaptation of ISO 26262 for motorcycles*".

The safety lifecycle (Figure 1) illustrates the fundamental safety activities during the concept phase, product development, production, operation, service, and decommissioning. According to the ISO 26262 standard, the key safety management tasks are to plan, coordinate, and track the activities related to functional safety. The first part mentioned above takes place as the very first step of each beginning of a project, but it does not mean that after this is done, there is no opportunity to improve. It is recommended to redefine as much as is needed during the product development phases until the final approval for the item to be released [4].

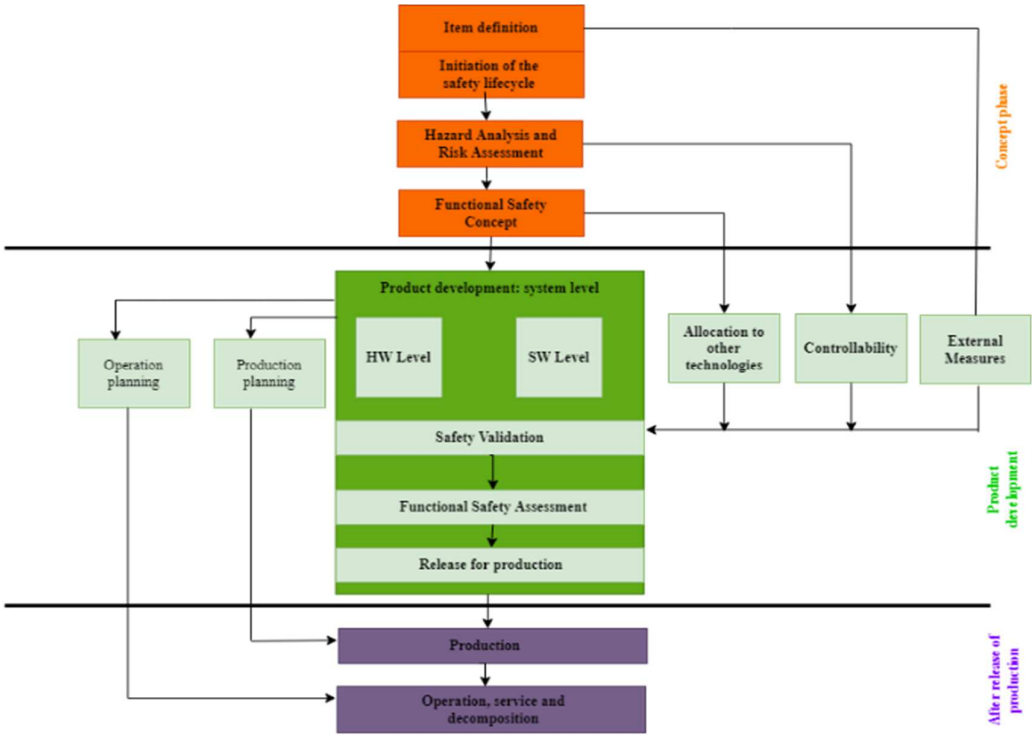

Fig. 1. ISO 26262 Safety Lifecycle.

Severity	S0	S1	S2	S3
	No injury	Light and moderate injury	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries
Exposure	E0	E1	E2	E3	E4
	Incredible	Very low probability	Low probability	Medium probability	High probability
Controllability	C0	C1	C2	C3
	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Fig. 2. Ratings for severity, exposure and controllability [4].

For each safety system, at least one safety goal is assigned, determined based on Hazard Analysis and Risk Assessment (HARA), which is part of the Concept Phase. According to ISO 26262, HARA represents a "*method to identify and categorize hazardous events of items and to specify safety goals and ASIL related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk*" [4].

In other words, the goal of HARA is to identify and assess the risks associated with malfunctions that could lead to E/E system hazards.

Table 1

ASIL determination ISO 26262 [4].

Severity Class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

To correctly perform the HARA, two steps need to be followed:

Step 1: Estimation of the probability of exposure, controllability, and severity of hazardous events concerning the item. Fig. 2 shows the ratings for each item.

After establishing these three characteristics, based on their estimation, the ASIL rating will be given as presented in Table 1.

Four ASIL ratings are defined: ASIL A, ASIL B, ASIL C, and ASIL D, where ASIL A is the lowest safety integrity level and ASIL D is the highest one. In addition to the four ASIL ratings, the class QM (quality management) denotes no requirement to comply with ISO 26262.

Step 2: The HARA output will represent the determination of the safety goals for the item.

The safety goals will be placed at the top level of safety requirements, so at the vehicle level. After this, the safety goals will receive the ASIL rating established in the HARA [4].

3. HAZARDOUS EVENTS

In the history of catastrophic events in the automotive industry, there is one that certainly stands out when it comes to impact on functional safety. On August 28, 2009, Mark Saylor, a police officer, was driving a Lexus ES350 Sedan on the highway together with his family. At one point, he lost control of the vehicle, reaching over 100 mph, and the brakes stopped responding. However, the car crashed into the intersection and the four people in the car died instantly. After many years of spending in the court, the final decision came to light: one of the source codes was faulty and this could provoke a violation of the safety goal.

The National Highway Transportation Safety Administration (NHTSA) reported on the event, citing the incorrect position of the floor mats as the reason for blocking the accelerator pedal, causing the engine to reach maximum speed. This assumption did not hold for long because, due to multiple complaints to Toyota about unintended acceleration, an action was initiated in 2007 whereby all complainants and others were recalled to the garage to have their floor mats changed, and Mark Saylor at the time of the event had a different floor mat in the car that provided more space for the driver's legs.

At that time, it was clear that Toyota and NHTSA had different expectations. On 29 September Toyota is again calling drivers who own one of the eight models, including the Lexus ES, for a floor mat change. NHTSA claimed that the recall was due to an unintended acceleration caused by several factors [19]. On May 25, 2010, a newspaper story announced that "*Toyota's 'Unintended Acceleration' has killed 89*" and the complaints numbered 6,200, things were as serious as it gets, and NHTSA asked NASA for help. The investigation lasted about 10 months, and the result was this: *"Proof for the hypothesis that the ETCS-i caused the large throttle opening UAs as described in submitted VOQs could not be found with the hardware and software testing performed. Because proof that the ETCS-i caused the reported UAs was not found does not mean it could not occur. However, the testing and analysis described in this report did not find that TMC ETCS-i electronics are a likely cause of large throttle openings as described in the VOQs"* [20].

The research carried out by NASA focused a lot on the Electronic Throttle Control System (ETCS), which contains the Electronic Control Module (ECM) that controls the throttle based on the approach from equation (1).

$$air + fuel + spark = engine\ power \quad (1)$$

By pressing the accelerator pedal, the ECM receives some voltage inputs. As today's cars have become more and more automated, pressing the accelerator is just the driver's wish about what is intended to happen.

In 2013 one of the many deadly events was brought before a judge claiming that the problem of unintended acceleration was due to software problems. There were several trials in that time frame, but none had this assumption. This testimony is based on Electronic Throttle Control (ETC), specifically its source code. From the 2009 event to 2013 Toyota claimed that the reasons for unintended acceleration were loose floor mats, a sticky pedal, or driver error. In the 2013 trial, the lawyers present in the trial ended their argument by claiming that the reason for the unintended acceleration was none of the above and that the real reason for the unintended acceleration was caused by ETC [21].

Several integrated systems experts were called in to give their opinion. Michael Barr and the other experts inspected the ETC source code, and after the inspection, they demonstrated that even the flip of a single bit can result in loss of car control. This process concluded that the Toyota ETC source code is faulty and that some bugs can cause unintended acceleration [21].

With the NASA report available online, this article focuses on the ETC block diagram presented in the report, creating a hierarchical model, starting from the system to the components, including functions and failures, performing both quantitative and qualitative analysis to finally observe the real cause of unintended acceleration and how much it impacts the system.

When such an accident, like the one presented above, happens, it is obvious to engineers that an error has infiltrated the system, regardless of its nature: SW or HW, and as a result, one of the safety goals of the system has been violated. To avoid this, the ISO 26262 safety standard emphasizes the absolute necessity of performing safety analyzes. Their importance will be presented in the next section.

4. SAFETY ANALYSIS

This chapter will give details of safety analysis techniques that help to identify and evaluate faults and failures. To develop a safe system, it is necessary to know its safety critical faults and failures and to be able to control them. There are several safety analysis techniques, but in the automotive industry, there are three most common techniques, which will be discussed and put into practice in this thesis as well: FMEA, FMEDA, and FTA [22].

Table 2

Qualitative and quantitative analysis [15].

	FMEA	**FMEDA**	**FTA**
Analysis direction	Inductive	Inductive	Deductive
Qualitative / Quantitative	Qualitative	Quantitative	Qualitative and Quantitative

Safety analysis techniques can be classified in two ways: quantitative/qualitative analysis or inductive/deductive analysis. Table 2 contains a description of the safety analyzes according to the classification.

As additional information, ISO 26262 recommends that deductive analysis should be performed starting with ASIL B, while inductive analysis is recommended regardless of the ASIL level.

Quantitative analyzes determine failure rates and probabilities, whereas qualitative analyzes verify the risk associated with failure modes using only qualitative criteria.

4.1. Failure Mode and Effects Analysis

FMEA is an inductive failure analysis used to identify and evaluate potential failures and their effects, find actions to eliminate or reduce the chance of failure occurring, and document the process.

The goal of this analysis is to:

- Improve quality, safety & reliability of the analyzed item;
- Reduce the risk of high additional implementation costs or of non-conformance costs;
- Aids in the development of robust designs;
- Prioritize tasks;
- Improve customer satisfaction.

4.2. Failure Modes, Effects, and Diagnostic Analysis

FMEDA analysis is a table-based method of hardware analysis. This analysis is used to identify the failure modes, failure rates, and diagnostic capabilities of a hardware component. The characteristics of an FMEDA are described below:

- The outcome of the FMEDA analysis is the HW architectural metrics used for the assessment of the effectiveness of the safety architecture;
- During the FMEDA assumptions are made concerning the existence and effectiveness of safety mechanisms;
- The FMEDA may be supported by means of fault injection.

4.3. Fault Tree Analysis

FTA is a top-down deductive failure analysis in which the undesired hazard is analyzed using Boolean logic along with a series of low-level events. The main objectives of the analysis are to:

- Understand the logic behind the tree structure;
- Prioritizing the risk;
- Monitor and control the safety performance of the system;
- Optimize resources.

If the aim of the paper is to present an impact analysis on a change in the system, regardless of its nature, the focus will be more on qualitative analysis, highlighting the links between the functions of components and their defects, and finally illustrating the defects that can have a direct impact on the safety goal.

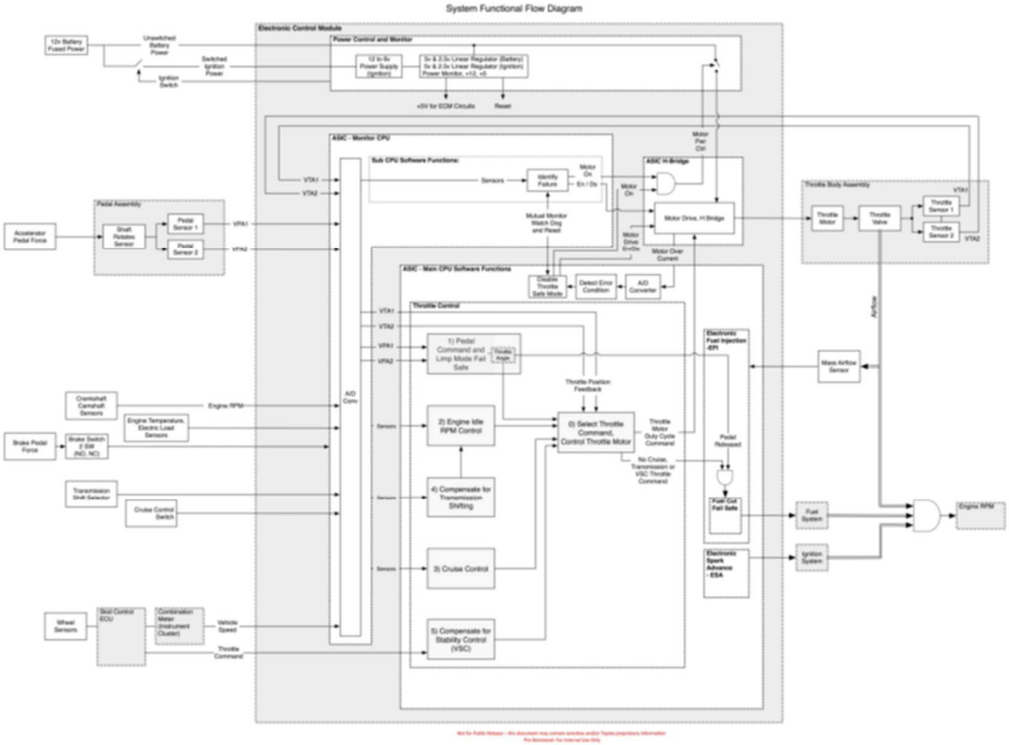

Fig. 3. Overall system function block diagram [17].

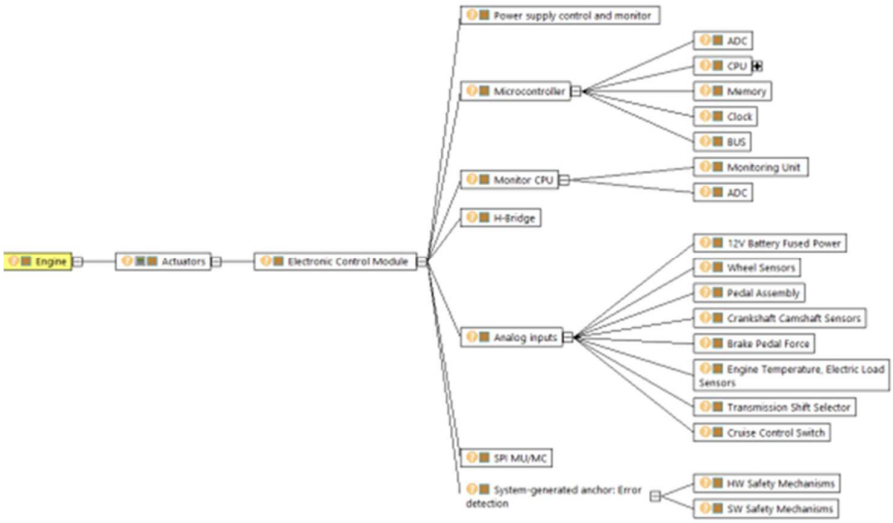

Fig. 4. General structure tree of the system block diagram.

Obtaining such an overview will also demonstrate the need for such an analysis in the automotive industry.

5. DEVELOPMENT

Fig. 3 shows the ETCS-i block diagram. On the left side are the ECM inputs and on the right side are the outputs, respectively, Fuel System, Ignition System, and Throttle Body Assembly. The ECM contains four major sections: Power Control and Monitor, ASIC Monitor-CPU, ASIC Main-CPU Software Functions, and ASIC H-Bridge. Power control and Monitor are located at the top of the diagram and are responsible for the power supply of the ECM. The Main CPU is in the center bottom and controls the operation of various electrical devices (relays, motors, solenoids, and indicator lights) [21]. The analog signals that are used by the main CPU are accessed internally by the analog/digital (A/D) port of the Main CPU [21]. Main CPU software functions according to the NASA UA report [21] are the pedal command function, the idle speed control function, idle speed control, cruise control, transmission shift, VSC (Vehicle Stability Control), and throttle control. Having this very complex and well-described system diagram, the next step would be to develop the block diagram, as presented in Figure 4 in the APIS IQ-RM interface to perform the analysis.

APIS IQ Software is a software implemented for FMEA, Risk Analysis, Functional Safety, and Requirement Management [23], and this is the reason why this tool fits very well in creating the proposed model for this article. The software is optimally adjusted to the world of Windows and is a future-proof basis for integration into workflow and document management systems [23].

The model is developed in an arborescent form. The first level is the engine part, and the second refers to the actuators (Injections System, Fuel System, and Throttle Body). Going further, one can see the Electronic Control Module subsystem and the interfaces for inputs and outputs (from the ECM). The next level refers to the four primary modules: Power Supply, Microcontroller (Main CPU), Monitor CPU, and H-Bridge. The last level presents the components of each module. In addition to the four electronic control modules, there is another block called "Safety Mechanisms" that will serve as protection mechanisms against various faults and SPI (Serial Port Interface) for communication between Microcontroller and Monitor CPU.

A system built for a vehicle is made up of software and hardware components. Hardware components have a failure mode, which can lead to safety violations. To prevent this from happening, automotive engineers have introduced safety mechanisms that aim to detect component failures and prevent them from propagating to a higher level.

For a system, subsystem, or component to be part of a model such as the one shown above, it must have an assigned function. Otherwise, the component should not be part of the structure. Figure 5 presents an example of functions and failure modes from the main CPU.

After giving each component a similar set of functions and failures, the next step will be to link all the component functions and failures in a so-called Function/Failure Net (see Fig.6). In this way, an FMEA analysis will be performed. Having this analysis, the engineers will be able to see the connections of all the subsystems and elements from the top level to the very low level (component level).

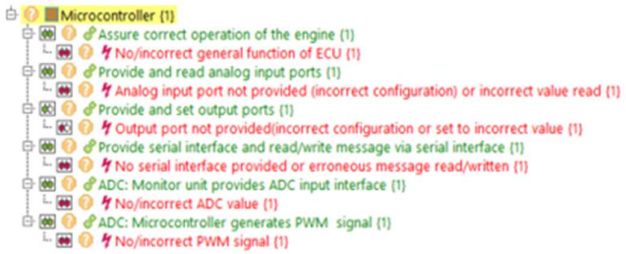

Fig. 5. Example of functions/failures for Main CPU.

Fig. 6. Function Net for Main CPU.

The fault tree analysis is performed from the Failure Net interface. This analysis consists of only those defects that directly impact the safety goal. It is done using logic gates, and the links are made in the following way: if a single component of a module fails and at the same time the safety mechanism covering all components of the module fails, then a safety goal violation occurs. This analysis involves the mathematical theory described by Ross [24].

The next thing to do after establishing the faults with a direct impact on the safety goals is to assign to each safety mechanism a diagnostic coverage. With this diagnostic coverage assigned, the architectural metrics can be calculated, and their result will the reliability of the system.

6. DISCUSSIONS

It is obvious that engineers in automotive companies are dealing with systems much more complex and detailed than the one presented. For this reason, having such an overview of the system represents a huge benefit, especially since the APIS IQ-RM tool is able to bring together all three analyzes in a single view, thus achieving a synergy concept.

At the beginning of this research, we presented some of the benefits that such a unification of safety analyzes would bring. One of them is the current situation, which requires some HW design changes. When a component in a system has failed or is no longer on the market, it must be replaced by another one.

Having such a view, as presented in the previous chapter, it will be easy for engineers to perform a system impact analysis to assess the safety impact it would bring to the system. In such an analysis, it is checked whether the component in question has any safety-relevant input or output and whether its failure directly affects the safety goal.

The reason why a qualitative analysis is not sufficient is that it uses a subjective judgment on the analysis of a system based on non-quantifiable information, in addition to quantitative analysis based on mathematics, statistical models, and measurements. To discuss the risk of endangering one or more human lives, the analysis must be both quantitative and qualitative.

7. CONCLUSIONS AND FUTURE DEVELOPMENT

The purpose of this paper was to improve the automotive functional safety perimeter by raising awareness of the need for both quantitative and qualitative analysis.

The well-known component shortage situation represents an additional reason why a holistic view of the system must be present for each automotive project. If there is a component in a system that is no longer manufactured, a replacement component must be found. Before making the final decision, a system impact analysis needs to be carried out. Having such an overview of the system will make it much easier for automotive safety engineers to assess the impact and moreover, to decide whether the new component can fulfil the features and functions of the old one.

With all these reasons presented above, having an ISO 26262 qualified tool, such as APIS IQ-RM, represents a necessity in the automotive industry to build unified qualitative and quantitative analysis.

This paper took the example of a generic ECU, but in the automotive field, it is known that the systems are more complex than what was presented in this work. Therefore, the structure, as well as the functions and failures, can be upgraded, bringing in this way continuity to the present project. Moreover, another idea would be to link the requirements from the customer to the components and to provide traceability from the requirements to the set of tests that need to be performed to assess that requirement.

Future works should also focus on the development of both quantitative and qualitative analyzes in a more conscious way. In this regard, the current APIS models can be improved to incorporate both qualitative and quantitative characteristics for the development of such analysis. The development of new tools for this purpose can also be considered.

In future studies will be considered the previous developments related to the automated business process management using Machine Learning or Artificial Intelligence presented by [25, 26]. The research context will be extended considering the university – industry collaborations consulting contracts framework, because of the mutual advantages identified [27].

8. REFERENCES

[1] Prostean, G., Hutanu, A., Vasar, C., Volker, S., *A development model for radio-navigation software projects*, Acta Technica Napocensis - Series: Applied Mathematics, Mechanics, and Engineering, 64(1-S1), Feb. 2021.

[2] Rogovchenko-Buffoni, L., Tundis, A., Hossain, M. Z., Nyberg, M., Fritzson, P., *An integrated toolchain for model based functional safety analysis*, Journal of Computational Science, 5(3), pp. 408–414, May 2014.

[3] Gaşpar, M. L., Firescu, V., *New Skills and Qualifications Required by the Current Approaches in the Software Development Industry*, Acta Technica Napocensis - Series: Applied Mathematics, Mechanics, and Engineering, 61(3), 2018.

[4] *ISO 26262-2018 Road vehicles - Functional safety*, 26262, 2018.

[5] Q., Kongjian, Z., Tong, G., Kuiyuan, Z., Hongwei, W., Yu, and C., Haoxin, *The Method of Functional Safety Validation Test of AEBS Based on Fault Injection*, 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, pp. 377–381, Sep. 2020.

[6] Khatun, M., Wagner, F., Jung, R., Glass, M., *An Approach of a Safety Management System for Highly Automated Driving System*, 5th International Conference on System Reliability and Safety (ICSRS), Palermo, Italy, pp. 222–229, Nov. 2021.

[7] Bo, L., Yue, F., *Research on functional safety of electric steering system for passenger vehicle*, International Conference on Control Science and Electric Power Systems (CSEPS), Shanghai, China, pp. 303–306, May 2021.

[8] Yi, F., Zhang, W., Zhou, W., *Functional Safety Design for Torque Control of a Pure Electric Vehicle*, 9th International Symposium on Next Generation Electronics (ISNE), Changsha, China, pp. 1–4, Jul. 2021.

[9] Kochanthara, S., Rood, N., Saberi, A. K., Cleophas, L., Dajsuren, Y., van den Brand, M., *A functional safety assessment method for cooperative automotive*

architecture, Journal of Systems and Software, 179, p. 110991, Sep. 2021.
[10] Noun, H., Urban-Seelmann, C., Abdelfattah, M., Rajesh, G., Mozgova, I., Lachmayer, R., *Quantification of Preconditions for Processing Safety Relevant Vehicle Systems*, 2021 5th International Conference on System Reliability and Safety (ICSRS), Palermo, Italy, pp. 265–269, Nov. 2021.
[11] Gharib, M., Ceccarelli, A., Lollini, P., Bondavalli, A., *A cyber–physical–social approach for engineering Functional Safety Requirements for automotive systems*, Journal of Systems and Software, 189, p. 111310, Jul. 2022.
[12] Giachetti, G., Marin, B., de la Vara, J. L., *Automatic Generation of UML Profiles for Representing Safety Standards*, 2020 39th International Conference of the Chilean Computer Science Society (SCCC), Coquimbo, Chile, pp. 1–8, Nov. 2020.
[13] Lu, K.-L., Chen, Y.-Y., *Model-based design, analysis and assessment framework for safety-critical systems*, 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S), Taipei, Taiwan, pp. 25–26, Jun. 2021.
[14] Makartetskiy, D., et al., *(User-friendly) formal requirements verification in the context of ISO26262*, Engineering Science and Technology, an International Journal, 23(3), pp. 494–506, Jun. 2020.
[15] Loftus, D., *The Automotive Semiconductor Shortage - An Accident Waiting to Happen?*, https://www.ecianow.org/assets/docs/Stats/IndustryIssues/ECIA%20Statement%20on%20Automotive%20Semiconductor%20Shortage%20FINAL.pdf
[16] Kymal, C., Gruska, O. G., *Integrating FMEAs, FMEDAs, and Fault Trees for Functional Safety*, 2021 Annual Reliability and Maintainability Symposium (RAMS), Orlando, USA, pp. 1–6, May 2021.
[17] Verkamp, M., *ISO 26262 Facts and Tips Presented by Industry Experts – (What is functional safety in automotive industry)*, https://www.lhpes.com/blog/what-is-functional-safety-in-the-automotive-industry
[18] *Car safety: History and requirements of ISO 26262*, https://www.lhpes.com/blog/ what-is-functional-safety-in-the-automotive-industry
[19] Finch, J., *Toyota Sudden Acceleration: A Case Study of the National Highway Traffic Safety Administration - Recalls for Change*, Loyola Consumer Law Review, 22(4), pp. 472-496, Jan. 2010.
[20] Austen-Smith, D., Diermeier, D., Zemel, E., *Unintended Acceleration: Toyota's Recall Crisis*, LICKEL, pp. 1–16, Jan. 2017.
[21] *Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation*, https://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf
[22] Schnellbach, A., *Fail-operational automotive systems*, Doctoral thesis, https://diglib.tugraz.at/download.php?id=5aa2484fb4bcb&location=browse
[23] APIS Informationstechnologien GmbH., *APIS IQ-Software, FMEA, DRBFM Functional Safety*, https://www.apis-iq.com/
[24] Ross, S. M., *Introduction to probability models*, 10th ed. Amsterdam; Boston: Academic Press, 2010.
[25] Paschek, D., Luminosu, C. T., Draghici, A., *Automated business process management – in times of digital transformation using Machine Learning or Artificial Intelligence*, MATEC web of conferences, 121, 04007, EDP Sciences, 2017.
[26] Paschek, D., Rennung, F., Trusculescu, A., Draghici, A., *Corporate development with agile business process modeling as a key success factor*. Procedia Computer Science, 100, 1168-1175, 2016
[273] Draghici, A., Baban, C. F., Ivascu, L. V., Sarca, I. (2015). *Key success factors for university–industry collaboration in open innovation*, Proceedings of the ICERI2015, ISBN: 978-84-608-2657-6, 7357-7365, IATED, 2015.

Analiza de impact în conformitate cu standardul ISO 26262 folosind analizele de siguranță integrate în programul APIS IQ-RM

RezumatȘ Odată cu creșterea complexității și a autonomiei sistemelor hardware, verificarea siguranței funcționale a întreg sistemului, dar și a componentelor individuale, a devenit o operație destul de dificilă, evidențiind nevoia unui concept de sinergie între analizele FTA, FMEA și FMEDA. Acest articol prezintă o analiză de risc asupra unui model în conformitate cu standardul ISO 26262. Scopul acestuia este de a dezvolta, cu ajutorul programului APIS IQ-RM, analiza unui sistem prezent într-un autoturism. Prin utilizarea modelului de analiză de siguranță unificat propus în acest articol, s-a demonstrat o îmbunătățire a procesului de identificare a posibilelor defecte ce pot să apară într-un sistem dezvoltat în industria automotive.

Dianora IGNA, M. Sc. Student, Politehnica University of Timisoara, Faculty of Automation and Computers, dianora.igna@student.upt.ro, 2 Vasile Pirvan Bdl, 300223 Timisoara Romania.
Mădălin-Dorin POP, Ph.D., Teaching Assistant, Politehnica University of Timisoara, Computer and Information Technology Department, madalin.pop@upt.ro, 2 Vasile Pirvan Bdl, 300223 Timisoara Romania.