

Quality Engineering Framework for Functional Safety Automotive Projects

Mădălin-Dorin Pop¹^a and Dianora Igna²

¹Computer and Information Technology Department, Politehnica University of Timișoara, Bvd. Vasile Pârvan, Timișoara, Romania

²Faculty of Automation and Computers, Politehnica University of Timișoara, Bvd. Vasile Pârvan, Timișoara, Romania

Keywords: Automotive Software, Dependent Failure Analysis (DFA), Freedom from Interference, Functional Safety, Quality Engineering, Vehicle Sensors.

Abstract: Safety evaluations represent an important aspect in the development of functional safety (FuSa) automotive projects. The present paper aims to propose a quality engineering framework for automotive projects that uses as input the Failure Mode Effects Analysis (FMEA) and Fault Tree Analysis (FTA) and further applies the Dependent Failure Analysis (DFA) method. More focused attention is also directed toward the impact analysis step during the development phase of a project and not only. By combining both these goals and with the help of the APIS IQ-RM interface, in the end, the paper presents a case study on how to improve an existing system. Furthermore, the proposed approach ensures complete traceability within the project by adding links between the APIS model and the representative test cases for each component.


1 INTRODUCTION

Safety is the most important aspect considered in the development of automotive projects. Anticipation of possible system failures and implementation of safety measures will save lives. As stated by Sini et al. (2022), functional safety (FuSa) represents “the ability of a cyber-physical system to react on time and adequately to the external environment”. Its definition and application rules originate from IEC 61508 (International Electrotechnical Commission, 2010), representing the basis for the development of multiple standards adjusted to the needs of software developed for different fields of industry. In this sense, the development of airborne systems must comply with DO-178C (Radio Technical Committee for Aeronautics, 2011), railway systems with EN 50126 (*Iteh Standards*, n.d.), and automotive systems with ISO 26262 (International Organization for Standardization, 2018).

This article focuses on the FuSa assessment of the development of automotive embedded systems. It considers previous research by Igna and Pop (2023) consisting of an impact analysis conducted using a model-based approach in the APIS IQ-RM tool (*Apis*

Iq-Software | Fmea | Drbfm | Functional Safety, n.d.), which has as a case study the functions and failures of a Central Processing Unit (CPU) that exists in an automotive system. Following this approach, the model obtained unifies both qualitative and quantitative analyses related to ISO 26262 compliance. The current research aims to improve the previous approach of the authors (Igna and Pop, 2023) by adding the links between each component and its specific test cases. In this way, complete traceability is ensured between requirements, developed components, and testcases, allowing failure and its impact on other components to be easily identified. Furthermore, the model proposed in this paper uses the existing Fault Tree Analysis (FTA) as input for a Dependent Failure Analysis (DFA).

This paper achieves the mentioned goals through the following five sections, a brief of each section being further given. The second section presents recent research related to the FuSa concept. This discussion follows three directions, such as developing FuSa-related functionalities, innovative processes, and approaches using quality engineering tools for FuSa projects.

 <https://orcid.org/0000-0002-2524-3370>

Section III presents the theoretical background necessary to understand the context and the proposal of the quality engineering framework from this paper. The discussion begins with a description of APIS model and is followed by the definition of the freedom from interference concept, and, in the end, by a discussion on how DFA is developed by using the safety analysis.

The fourth section describes the proposed quality engineering framework that aims to improve the APIS model. It is followed, in the fifth section, by a practical application of the proposed framework on a generic Electronic Control Module (ECM) schema developed in the APIS IQ-RM tool (*Apis Iq-Software | Fmea | Drbfm | Functional Safety*, n.d.).

The last section summarizes the contributions of this research and designates the directions of future research.

2 RELATED WORKS

Recent research on the development of automotive projects concentrates on the application of the FuSa concept for various functionalities or Electronic Control Units (ECUs), such as steering and braking systems (Rana et al., 2014), electric vehicle charging systems (Kivelä et al., 2021), battery management systems (Chen et al., 2021), combustion engine control and calibration (Isermann and Sequenz, 2016), autonomous driving systems (Gilbert et al., 2018; Liu et al., 2022), etc. Safety evaluations are usually performed using model-based approaches (Chaari et al., 2015; Debbech et al., 2019; Isermann and Sequenz, 2016; Martin et al., 2020; Rupanov et al., 2014; Weissnegger et al., 2016), which simplify the identification of the root cause of a system fault. Martin et al. (2020) propose a framework that provides guidance and links the concepts of safety and security from a system engineering perspective. This approach is compliant with ISO 26262 (International Organization for Standardization, 2018) and SAE J3061 (Society of Automotive Engineers, 2016), the last standard being responsible for defining the cybersecurity process.

The production system also plays an important role in FuSa assurance. Customer expectations relate to a short lead time to market but maintain high quality, especially for safety-relevant products. This can be feasible only if the manufacturing process is continuously adapted to the changes coming from the market or the customer, the integration of the latest technologies being crucial in this sense. Vater et al. (2019) provide a systematic review of the use of

prescriptive analytics in intelligent manufacturing systems. Kampker et al. (2019) proposed an improved general methodology for multiple ramp-up in scalable production systems that can be easily adapted to the needs of the production line and the manufactured product while complying with all safety-relevant aspects.

Open innovation practices are also the subject of recent research in the automotive industry. Etabaa et al. (2019) provide an overview of open innovation ecosystems and their connections with academia or other institutions that can generate ideas. Additionally, they provide a discussion of the effectiveness of open innovation practices in the automotive industry.

Quality engineering is very important in FuSa-related projects, with several approaches available in the scientific literature. The preventive approach is the most used because it ensures a reduced probability of possible quality deviations and a real-time application of corrective measures in the case of their appearance. The statistical process control, known as a preventive measure, assists qualitative evaluations. Godina and Matias (2018) improved the identification of non-conformity by replacing the initial Kolmogorov-Smirnov test with a Shapiro-Wilk test. Da Anunciação et al. (2022) applied the focus group technique to discuss the interactions between the main dimensions in FuSa related to the needs of industry 4.0. The authors emphasized the limitations of the technique chosen for their research and defined the paths for its validation in future studies.

Several studies apply Failure Modes, Effects, and Diagnostic Analysis (FMEDA) (Chaari et al., 2015; Igna and Pop, 2023; Kymal and Gruska, 2021; Lu et al., 2018; Tichkiewitch and Riel, 2014) in FuSa evaluations. Usually, these studies integrate FMEDA with Failure Mode and Effects Analysis (FMEA) and FTA (Igna and Pop, 2023; Kymal and Gruska, 2021). Lu et al. (2018) proposed a framework that uses Fault Injection and Data Analysis (FIDA) in the generation of the FMEDA report. The use of DFA (Park et al., 2021; (Young and Walker, 2018) or driver-in-the-loop systems (Liu et al., 2022) is also proposed by researchers in the analyses of compliance with ISO 26262. Tichkiewitch and Riel (2014) proposed a more complex and general framework that allows the integration of FuSa with Automotive Software Process Improvement and Capability Determination (ASPICE) (*Automotive SPICE*, 2015), and lean six sigma.

3 METHODOLOGY

Even if in the automotive industry, there are many tools capable of implementing safety analyses (e.g., Vector PREE Vision, Ansys medini analyze, ENCO SOX and LDRA tool (Embitel-admin, 2021)), APIS IQ-RM promises to bring to market one of the best tools in this area (Apis Iq-Software | Fmea | Drbfm | Functional Safety, n.d.). Another reason for choosing this tool in this research is the recognition of the major automotive worldwide companies that trusted in using the tool (i.e., these companies are listed in the “Our Customer” section in the APIS website (Apis Iq-Software | Fmea | Drbfm | Functional Safety, n.d.)).

3.1 APIS Model

As stated in the introduction, the goal of this paper is to improve the approach followed by Igna and (2023) in their developed APIS model. This model presents the block diagram of Electronic Throttle Control (ETC) that was used embedded on a Toyota Lexus during a hazardous event (Igna and Pop, 2023; NHTSA, 2011). By using the APIS IQ-RM (Apis Iq-Software | Fmea | Drbfm | Functional Safety, n.d.) interface, it is possible to develop the model in arborescent form (Fig. 1). In this way, different levels were described: the first level represents the engine, the second one is for actuators, the ECU is on the third level, and the last one presents the components of each module. The model focuses more on the ECM, which has a generic structure that is used even today in the automotive industry.

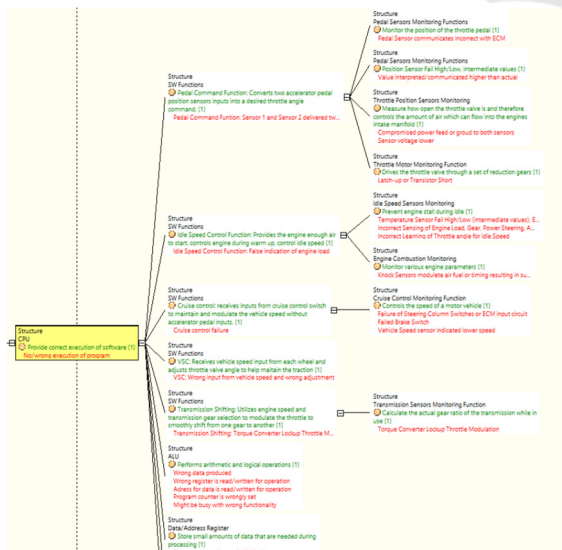


Figure 1: Function connection for main CPU (Igna and Pop, 2023).

The main purpose of the model is to determine for each subsystem or component its feature and failure mode. One of the key features used by automotive engineers while working in APIS is the connection of each component function/failure mode with the top-level component/subsystem. This stage is important because, by having these connections, it also completes the first phase of the following safety analysis: FMEA, FMEDA, and FTA.

Another important point that should not be missed is the introduction of a safety mechanism that acts as protection against various faults. At the top of each system, there are one or more safety goals that must be protected against violations. However, there are situations where the malfunction of one component could corrupt the next component up to the top level, which results in a violation of the safety goal. Fortunately, there is a feature that helps engineers to establish which malfunction could lead to a cascading failure, and this will be discussed in the next section.

3.2 Freedom from Interference and the Role of DFA

ISO 26262 (International Organization for Standardization, 2018) defines the freedom from interference as “absence of cascading failures between two or more elements that could lead to the violation of a safety requirement”.

As mentioned previously, because nowadays vehicles are equipped with multiple ECUs that use a communication channel, the malfunction of one component could easily be transferred to another one. The ISO 26262 (International Organization for Standardization, 2018) standard requires vehicle components to have zero dependences, as well as interference. Those two properties mentioned before are in interest of DFA which focuses on finding the dependent failures.

According to (International Organization for Standardization, 2018), DFA aims at identifying failures that may hamper the required independence or freedom from interference between given elements (hardware/ software/ firmware) which may ultimately lead to violation of safety requirement or safety goal. During the development of DFA (Fig.2), two types of failures can be noticed:

- Common cause failures (CCF) appear during one faulty event that caused a fault in one component and another fault in a different component. In this case, the components do not have dependence (Schnellbach, 2016).
- Cascaded failures (CF) are represented by a fault event that corrupts one component,

causing a fault, and the same fault interacts with another component, causing another failure. In this case, the components interact (Schnellbach, 2016).

As mentioned previously, DFA have two properties: independence and freedom from interference. By achieving freedom from interference, it can be said that the system has no cascading failures. However, the independence property covers both cascading failure and common cause of failure.

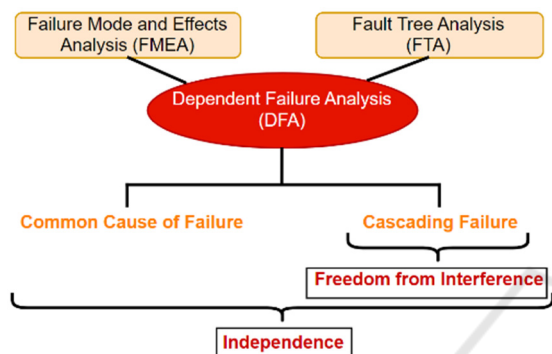


Figure 2: Dependent Fault Analysis (DFA) - methodological overview.

3.3 Develop a DFA Using Safety Analysis

In the first section of this chapter, the APIS model was presented along with the introduction of safety analysis. Another aim of this paper is to develop a DFA using FTA and FMEA as a starting point.

As mentioned in (Igna and Pop, 2023), FMEA is an inductive analysis used to identify potential failures and their effect. In other words, this analysis can highlight all components with similar failures that could eventually cause a dependent failure. On the other hand, the FTA analysis follows a top-down approach based on which undesired hazards are analyzed using Boolean logic. When the FTA is used, the identical faulty event that could trigger the component and produce a cascading failure is highlighted.

With both analyses, it can be assumed that all the inputs needed for DFA are present. After finding all the dependent failures, the DFA ends by performing an improvement of the system, to have the minimum interaction of the components as possible. Furthermore, engineers can also apply additional safety mechanisms to cover the remaining failures, if any.

4 IMPROVEMENT OF APIS MODEL

One of the important topics noticed by safety engineers in the automotive industry is impact analysis between different phases of the project. Several types of event could trigger an impact analysis. For example, the component shortage presented in (Loftus, 2021) caused many problems for hardware engineers. This type of incident puts them in front of one single choice: replacement of components. In these cases, in order to ensure that the components do not interfere in a bad way with the system, an impact analysis made by the safety team is mandatory. One general example which triggers an impact analysis, and which happens very often during the development phase is receiving new requests from the customer.

There are some cases where the impact is very visible, but this is often not the case. In addition to the unification of FMEA, FMEDA, and FTA presented in (Igna and Pop, 2023), this article will try to improve the existing APIS model, to make impact analysis easier to manage, and to establish the actions needed afterward.

Fig. 3 illustrates the proposed quality engineering framework that aims to improve the APIS model. The advantage of using the APIS IQ-RM tool is that it is capable of keeping all the features within one view. Moreover, once the system is placed in the arborescent structure with all the functions and failures, by making the connections the FMEA it is available. Moving forward, FMEDA could be built from FMEA, FTA is done from FMEDA, and DFA is initiated based on FMEA and FTA. However, to make the model more complete, it is also needed to add the tests to be performed for each component to ensure that the component and then the system are working as expected.

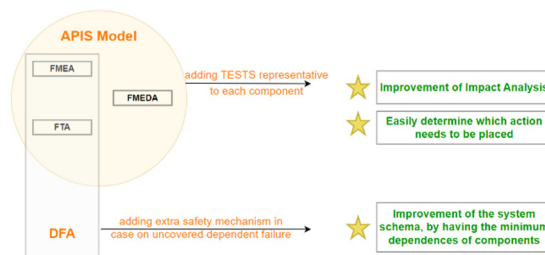


Figure 3: Proposed quality engineering framework.

In this way, if it is established during an impact analysis that the change or new request has an impact

on the system, it is easy to determine which tests need to be re-performed.

5 CASE STUDY

Taking the example of the generic ECM schema (Fig. 4) developed in APIS IQ-RM (Apis Iq-Software | Fmea | Drbfm | Functional Safety, n.d.), one power supply failure will be taken as a case study. With all this said, the main feature of the power supply is to provide power in a controlled way in order for the vehicle to start. One possible malfunction is sending wrong information to the ECM. Undoubtedly, this malfunction leads to a violation of the safety goal. As is well known, inside one vehicle there are a larger number of ECMs that communicate between them. There are two points that can be noticed:

- One faulty event causes multiple failures in different components, which means that the common cause of the failure is established.
- By performing FTA and DFA, the failure will be highlighted, and the action behind will be to add a safety mechanism in front of the failure, in order not to propagate it to the safety goal and violate it.

During the development phase, there are multiple cases in which a failure leads to a violation of the safety goal. Consequently, the team is responsible for

preventing these situations, but this cannot be possible without the appropriate tools. For this reason, this article proposes a mixture of existing tools designed to perform all safety analyzes, the value-added of the proposed approach consisting of the direct identification of the root cause of a safety goal violation. The localization of the failure will easier prevent its propagation to other modules and allows the developers to isolate the defectuous module until the problem is solved.

Following this approach, the engineer can improve the schema by asking the software developers to integrate one additional mechanism.

6 CONCLUSIONS

In this paper, a quality engineering framework for FuSa automotive projects was proposed. This approach improved the APIS model from (Igna and Pop, 2023) by ensuring complete traceability inside the impact analysis by linking the corresponding test cases to each component. In this way, it is easy to identify the requirement that was not implemented correctly. Furthermore, the integration of DFA in the proposed framework ensures the existence of minimum dependences between the components and, consequently, achieves the freedom of interference.

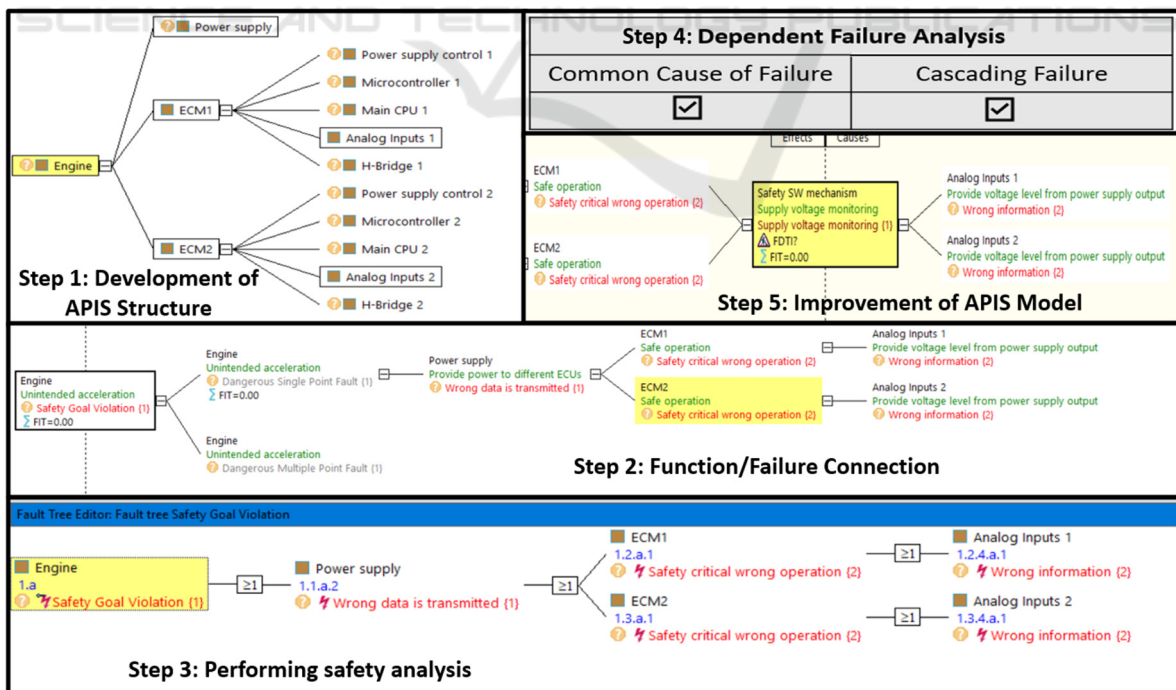


Figure 4: Dependent Fault Analysis (DFA) - methodological overview.

The proposed framework simplifies the identification of the root cause in the event of a system fault, as demonstrated by the case study described in this research.

Future research can focus on the automation of DFA based on the results of FMEA and FTA.

ACKNOWLEDGEMENTS

This paper was financially supported by the Project “Network of excellence in applied research and innovation for doctoral and postdoctoral programs” / InoHubDoc, project co funded by the European Social Fund financing agreement no. POCU/993/6/13/153437.

REFERENCES

- Apis iq-software | fmea | drbfm | functional safety.* (n.d.). APIS Informationstechnologien GmbH. Retrieved April 4, 2023, from <https://www.apis-iq.com/Automotive SPICE>.
- Automotive SPICE. (2015). Retrieved April 4, 2023, from https://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf
- Chari, M., Ecker, W., Novello, C., Tabacaru, B.-A., and Kruse, T. (2015). A model-based and simulation-assisted FMEDA approach for safety-relevant E/E systems. *Proceedings of the 52nd Annual Design Automation Conference*, 1–6. <https://doi.org/10.1145/2744769.2747908>
- Chen, M., Xie, G., Ming, Z., Liu, G., and Li, W. (2021). Functional safety research of battery management system based on risk graph methods. *IOP Conference Series: Earth and Environmental Science*, 645(1), 012058. <https://doi.org/10.1088/1755-1315/645/1/012058>
- Da Anunciação, P. F., De Lemos Dinis, V. M., Peñalver, A. J. B., and Esteves, F. J. M. (2022). Functional Safety as a critical success factor to industry 4.0. *Procedia Computer Science*, 204, 45–53. <https://doi.org/10.1016/j.procs.2022.08.006>
- Debbeck, S., Bon, P., and Collart-Dutilleul, S. (2019). Conceptual modelling of the dynamic goal-oriented safety management for safety critical systems: *Proceedings of the 14th International Conference on Software Technologies*, 287–297. <https://doi.org/10.5220/0007932502870297>
- Embitel-admin.* (2021, April 7). Dependent failure analysis in iso 26262—Freedom from interference. *Embitel*. Retrieved May 24, 2023, from <https://www.embitel.com/blog/embedded-blog/how-important-is-dependent-failure-analysis-in-iso-26262>
- Ettabaa, R., Bouami, D., and Elfezazi, S. (2019). Open innovation in the automotive industry. *2019 8th International Conference on Industrial Technology and Management (ICITM)*, 115–121. <https://doi.org/10.1109/ICITM.2019.8710715>
- Gilbert, A., Petrovic, D., Warwick, K., and Serghi, V. (2018). Autonomous vehicle simulation model to assess potential collisions to reduce severity of impacts: *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems*, 243–250. <https://doi.org/10.5220/0006663102430250>
- Godina, R., and Matias, J. C. O. (2018). Improvement of the statistical process control through an enhanced test of normality. *2018 7th International Conference on Industrial Technology and Management (ICITM)*, 17–21. <https://doi.org/10.1109/ICITM.2018.8333912>
- Igná, D., and Pop, M. D. (2023). Impact analysis according to iso 26262 standard using safety analysis integrated in apis iq-rm tool. *ACTA TECHNICA NAPOCENSIS - Series: APPLIED MATHEMATICS, MECHANICS, and ENGINEERING*, 65(3S). <https://atna-mam.utcluj.ro/index.php/Acta/article/view/1954>
- International Electrotechnical Commission. (2010). IEC 61508-1:2010; Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Parts 1. IEC:Geneva, Switzerland.
- International Organization for Standardization (2018). ISO 26262-2018 Road vehicles - Functional safety, 26262.
- Isermann, R., and Sequenz, H. (2016). Model-based development of combustion-engine control and optimal calibration for driving cycles: General procedure and application. *IFAC-PapersOnLine*, 49(11), 633–640. <https://doi.org/10.1016/j.ifacol.2016.08.092>
- Iteh standards.* (n.d.). ITeh Standards. Retrieved April 4, 2023, from <https://standards.iteh.ai/catalog/standards/clc/e5456892-eb2c-437e-8c4b-91c08007f0b4/en-5012-6-1-2017>
- Kampker, A., Kreiskother, K., Lutz, N., Gauckler, V., and Hehl, M. (2019). Re-ramp-up management of scalable production systems in the automotive industry. *2019 8th International Conference on Industrial Technology and Management (ICITM)*, 137–141. <https://doi.org/10.1109/ICITM.2019.8710702>
- Kivelä, T., Abdelawwad, M., Sperling, M., Drabesch, M., Schwarz, M., Böresök, J., and Furmans, K. (2021). Functional safety and electric vehicle charging: Requirements analysis and design for a safe charging infrastructure system: *Proceedings of the 7th International Conference on Vehicle Technology and Intelligent Transport Systems*, 317–324. <https://doi.org/10.5220/0010398303170324>
- Kymal, C., and Gruska, O. G. (2021). Integrating fmeas, fmedas, and fault trees for functional safety. *2021 Annual Reliability and Maintainability Symposium (RAMS)*, 1–6. <https://doi.org/10.1109/RAMS48097.2021.9605786>
- Liu, R., Lu, K., Zhu, Y., and Wu, Z. (2022). An evaluation method of vehicle functional safety controllability based on driver-in-the-loop platform. *Journal of Physics: Conference Series*, 2173(1), 012054. <https://doi.org/10.1088/1742-6596/2173/1/012054>
- Loftus, D. (2021). *The Automotive Semiconductor Shortage—An Accident*

- Waiting to Happen?* Electronic Components Industry Association. Retrieved April 4, 2023, from <https://www.ecianow.org/assets/docs/Stats/IndustryIssues/ECIA%20Statement%20on%20Automotive%20Semiconductor%20Shortage%20FINAL.pdf>
- Lu, K.-L., Chen, Y.-Y., and Huang, L.-R. (2018). Fmeda-based fault injection and data analysis in compliance with iso-26262. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 275–278. <https://doi.org/10.1109/DSN-W.2018.00075>
- Martin, H., Ma, Z., Schmittner, Ch., Winkler, B., Krammer, M., Schneider, D., Amorim, T., Macher, G., and Kreiner, Ch. (2020). Combined automotive safety and security pattern engineering approach. *Reliability Engineering & System Safety*, 198, 106773. <https://doi.org/10.1016/j.res.2019.106773>
- NHTSA. (2011). *Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation*. Retrieved April 4, 2023, from https://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf
- Park, B., Joo, B., and Lee, S. (2021). Application of dependent failure analysis for development of automotive electronics complying with iso26262 standards. *Transaction of the Korean Society of Automotive Engineers*, 29(10), 967–980. <https://doi.org/10.7467/KSAE.2021.29.10.967>
- Radio Technical Committee for Aeronautics (2011). RTCA DO-178C; Software Considerations in Airborne Systems and Equipment Certification. RTCA: Parañaque, Philippines.
- Rana, R., Staron, M., Berger, C., Hansson, J., Nilsson, M., and Törner, F. (2014). Early verification and validation according to iso 26262 by combining fault injection and mutation testing. In J. Cordeiro and M. Van Sinderen (Eds.), *Software Technologies* (Vol. 457, pp. 164–179). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44920-2_11
- Rupanov, V., Buckl, C., Fiege, L., Armbruster, M., Knoll, A., and Spiegelberg, G. (2014). Employing early model-based safety evaluation to iteratively derive E/E architecture design. *Science of Computer Programming*, 90, 161–179. <https://doi.org/10.1016/j.scico.2013.10.005>
- Schnellbach, A. (2016). *Fail-operational automotive systems* [Doctoral thesis, Graz University of Technology]. Retrieved April 4, 2023, from <https://diglib.tugraz.at/download.php?id=5aa2484fb4bcb&location=browse>
- Sini, J., Passarino, A., Bonicelli, S., and Violante, M. (2022). A simulation-based approach to aid development of software-based hardware failure detection and mitigation algorithms of a mobile robot system. *Sensors*, 22(13), 4665. <https://doi.org/10.3390/s22134665>
- Society of Automotive Engineers (2016). SAE J3061 cybersecurity guidebook for cyber-physical vehicle systems.
- Tichkiewitch, S., and Riel, A. (2014). Integration to face modern quality challenges in automotive. *Procedia Engineering*, 97, 1866–1874. <https://doi.org/10.1016/j.proeng.2014.12.340>
- Vater, J., Harscheidt, L., and Knoll, A. (2019). Smart manufacturing with prescriptive analytics. *2019 8th International Conference on Industrial Technology and Management (ICITM)*, 224–228. <https://doi.org/10.1109/ICITM.2019.8710673>
- Weissnegger, R., Pistauer, M., Kreiner, C., Schuß, M., Römer, K., and Steger, C. (2016). Automatic testbench generation for simulation-based verification of safety-critical systems in uml: *Proceedings of the 6th International Joint Conference on Pervasive and Embedded Computing and Communication Systems*, 70–75. <https://doi.org/10.5220/0005997700700075>
- Young, A., and Walker, A. (2018). Qualifying dependent failure analysis within iso26262: Applicability to semiconductors. In X. Larrucea, I. Santamaria, R. V. O'Connor, and R. Messnarz (Eds.), *Systems, Software and Services Process Improvement* (Vol. 896, pp. 331–340). Springer International Publishing. https://doi.org/10.1007/978-3-319-97925-0_27