SYSTEMATIC APPROACH FURTHERING CONFIRMATION MEASURES OF SAFETY CRITICAL AUTOMOTIVE SYSTEMS

WALID GANNOUNI[1], MAMADOU LAMINE DOUMBIA[1] & ADEL BADRI[2]
[1]Department of Electrical and Computer Engineering
[2]Department of Industrial Engineering, Université du Québec à Trois-Rivières, Canada

ABSTRACT

Different system elements are developed independently from diverse suppliers and teams before being integrated together into safety critical automotive systems such as steering or braking systems by a manufacturer. It must be guaranteed that, despite this independent development, the achievement of the safety requirements for the overall system can be demonstrated. The necessary agreements and the integration of the necessary safety information for the overall system generate higher extra costs. In order to reduce development time and cost, systematic reuse can be a solution to engineering the required artifacts. Reassessment represents an additional source of cost. Even small modifications of a system or exchanging a component after it has been certified necessitates a reassessment. The effort required for reassessment, in many cases reaches the original effort of certification for the complete system or even exceeds it. To minimize the effort and cost of a reassessment, this paper introduces a theoretical foundation of a model-based engineering approach to reuse a safety case and change only the modified parts. This paper presents a reusability framework to support the distributed development environment together with the different composition scenarios with respect to ISO26262. A further benefit of this approach is that for development of variants in product-line, the Safety assessment process can now be easily expressed and managed.

Keywords: modularization, functional safety, product-line and composition.

1 INTRODUCTION

With the trend of expanding technological complexity and mechatronic implementation, engineers and academic researchers have been faced with increasing risks of safety relevant functionalities [1], [2]. To manage the system complexity, a standard concerning functional safety in the automotive industry ISO 26262 (International Organization for Standardization 26262 Road vehicles – Functional safety) was applied to new safety critical automotive systems since 2011 [3].

As per ISO 26262 the safety related that incorporate at least one electrical or potentially electronic (E/E) systems and that are installed in series production passenger cars should have a safety case [4]. However, even small modifications of a system after it has been certified might modify the system's definition itself and the functional safety assessment of the system is not valid anymore and needs to be performed all over again.

Frequently, modularization [5] is one the most successful ideas for handling complexity in the development of systems in the automotive domain [6]. However, the automotive industry has seen the need of a new approach that integrate the benefits of modularization and reassessment.

Experiences from the field have shown that reuse strategies like "Clone and Own", leading to very inefficient reuse of artifacts and doesn't support the product variant [7]. Although, in most of the approaches in the literature, [8], [9], it was not possible to clearly identify which safety-related assets can be reused modular [10]. The goal and contribution of this work, is to discuss challenges and develop a model-based reuse approach with respect to variable

WIT Transactions on The Built Environment, Vol 174, © 2018 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE170221

safety analyses, regulations, and reuse of certifications, which need further research and elaboration.

This paper is structured as follows: Section 2 present the actual challenges related to reuse of safety work products and design during the safety life cycle. This section examines which possibility exists already on the market, particularly in the area of safety engineering and how this service can be done cheaper abroad, but with the same quality. Section 3 proposes a compositional framework for the integration of safety analysis techniques that supports a modularized and distributed development environment and explained which combination is suitable for the desired analysis. Finally, section 4 presents a discussion with respect to previous studies, followed by the conclusions.

2 SYSTEMATIC EVALUATION OF REUSE

In this section, we describe the actual challenges related to reuse of safety work products and design during the safety life cycle. They will be used to evaluate and approve the mode-base safety engineering approach in the section discussion and related work.

Fig.1 depicts an abstraction of the efficient reuse of safety critical system in which the main blocks of challenge can be identified. In order to properly support the efficient reuse of safety components and the related safety work products, modularity, consistence between safety and development artefacts, safety assessment process, proper tool support is required. The model-based safety engineering solution approach should clarify which work products can reused, modified, or new developed to help estimate the effort needed for reusing components.

To minimize the effort and cost in the application projects, it is essential that the reuse of safety work products can be achieved. Modification of safety critical automotive system parts (Engine control unit, Sensor, Hardware, Software and Motor) due to the customer requirements can cause changes from baselines projects. Incremental assessment foresees

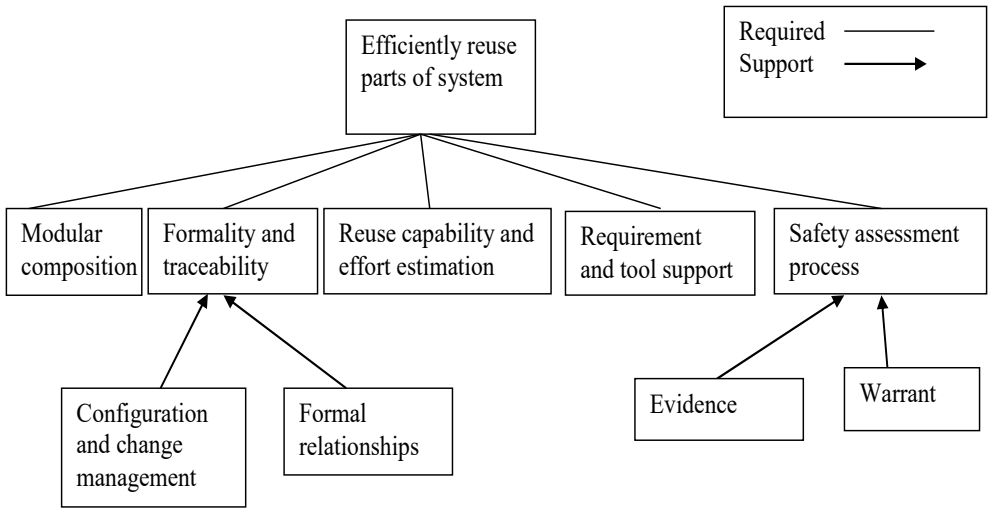

Figure 1: Challenges by reuse of safety related component.

Figure 2: Challenges by reuse of safety related component.

that single parts of a system could be modified or extended without requiring a reassessment of the complete system per ISO 26262. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes. System safety is achieved through several safety measures, which are implemented in a variety of technologies (e.g., mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process.

Fig. 2 depict the question related to reuse challenge for all aspects of the system design and the related work products. The important work product from the safety life cycle in the automotive industries is structured as shown in the Fig. 3 [11].

The developed strategies for reuse shall support the reuse of safety components and work products based on ISO 26262 safety development cycle. To be consistent with the "reuse" philosophy as outlined above and to maximize the reusability of the safety plan content across the full range of current and future system applications. This allows the automotive industry to easily separate development tasks, keep responsibilities confined to their own developed module/component, protect their intellectual property, and increase the reuse potential.

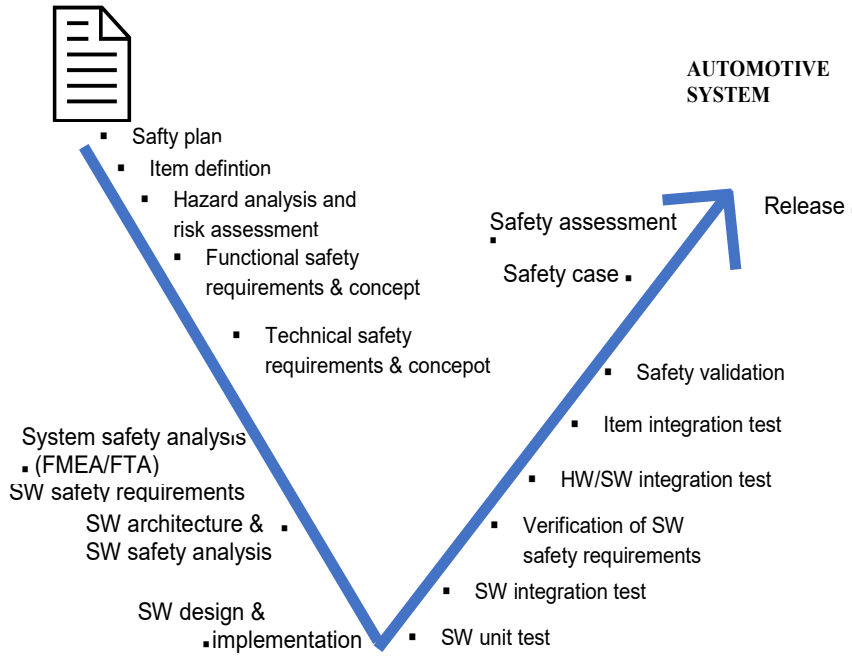

Figure 3: Safety work products in V-Modell.

3 SAFETY REUSE FRAMEWORK

This section portrays an outline of the safety reuse framework and the hypothetical foundation underlying the compositional algorithms. It provides a basic introduction to how to use the framework, its capabilities, and its limitations.

3.1 Implementation in automotive field

The created strategies are based on the key notion of reuse and modular. Modular safety designs increase the chance that the automotive system being suitable for reuse. Reusability and modularity is not a similar thing [12]. Reusability is thought to be the notion of using something that was already created before in another context or in another time. An object being modular means that it comprises of various structures with all around characterized interfaces between them. The relation between reusability and modularity is not outright. If an object is modular, it does not necessarily mean that it can be reused. One imperative perspective is further, that reuse and modularity can be seen in different scope. On a technical level, whole systems, technical components or sub-components can be physically used in different products or they can be composed in different ways to provide a different functionality.

The certification of an embedded system is cost and time-consuming. Modular safety cases form the basic technology to significantly reduce the costs for the certification [13]. The development of systems becomes more and more modular with integrated architectures like AUTOSAR for the automotive industries. To minimize the effort and cost of a recertification, it is essential that the safety case can also be limited to the modified parts. Such incremental certification foresees that single parts of a system could be modified or extended without requiring a recertification of the complete system.

3.2 Modular safety to reduce the costs

The integration or composition of safety analysis techniques is still a challenging task in the automotive field. Different analysis techniques are available and some of them are more suitable for quantitative or qualitative analysis and support modularization in certain level by V-Model. Some techniques are better for describing aspects of system parts (e.g., latent failure, single point failure and functional dependencies) and supporting hierarchical designs than others.

The combination approach should be able to support the product variant and the combination of varied safety analysis methods, e.g. deductive Functional Failure Analysis (FTA) and inductive Failure mode and effects analysis (FMEA)s, on different abstraction layers of V-Model. Furthermore, the method shall allow the composition of safety analysis results from different architecture levels and from different safety analysis techniques.

Regarding the currently used safety analysis techniques it becomes apparent that FMEA, FTA and its extensions safety analysis are classified by the participants as particularly often used. No matter which composition scenarios are used, it should be possible to perform quantitative or qualitative analyses. This means that a composition qualitative result with quantitative result leads to common results (Fig. 4).

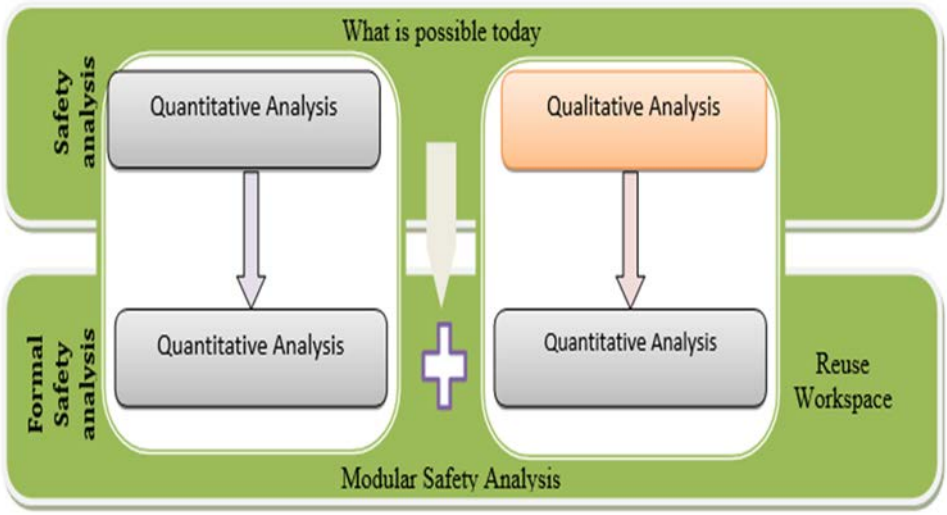

Figure 4: Transition to quantitative analysis.

3.3 Composition scenarios capability

We are motivated to facilitate the assessment process based on reuse framework. In large and complex systems, the manageable components are usually developed by independent parties, which determine how these components should interact and match with each other during the design phase. This is known as distributed development. To evaluate the used method, we evaluate different scenario according to safety critical automotive systems. The analysis is performed in model-based composition scenarios.

With regards to an appropriated improvement, the synthesis framework depicts in Fig. 5 could be utilized as a part of two primary circumstances. In the main situation, a few organizations need to mutually build up a safety-critical system. In the option situation, here various division groups might be in charge of the advancement of the modules. Having defined the overall functional requirement of the system each organization can build up its appointed module and utilize its favored technique for the safety analysis. The modules are connected with interface-based composition context includes safety requirement and Automotive Safety Integrity Level (ASIL). As we state before, we break down the safety analysis into different sub-analyses, where each one is applied to one component. Afterwards, we perform the dominance check in order to assure that the safety aspect follows the successful decomposition of components, in order to assure that the top-component is realized by the sub-components.

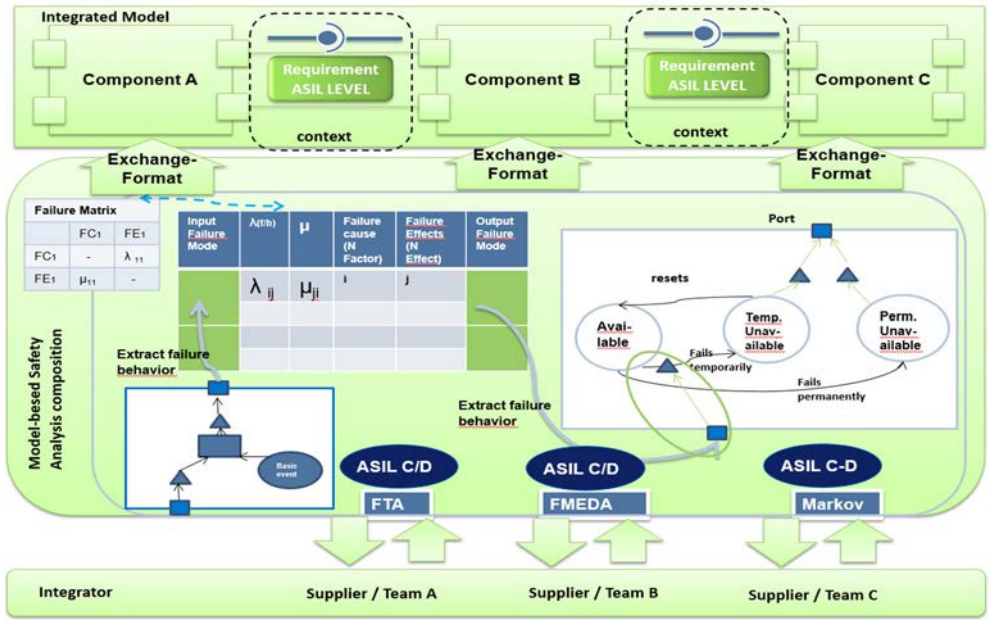

Figure 5: Safety reuse framework vision.

This kind of combination based on an array association, can be used throughout the safety development life cycle where the information from component with FTA be used in higher abstraction level (e.g., Subsystem). The analysis framework apply model-driven techniques to create a link between bottom-up and top-down safety analysis methods. The safety evaluation environment contains a refined data exchange tools used for FMEDA: Failure Modes, Effects, and Diagnostic Analysis (e.g., Excel spreadsheets) and FTA: Fault Tree Analysis (e.g., Isograph's Reliability WorkbenchTM). The scenario represents the case in which FTA provides output failure mode that is used as input failure mode by the FMEA. The FTA is allocated to component A and FMEA to component B. The safety analysis with FTA can offer the Minimal Cut sets and Failure In Time (FIT rate λ) for each output failure mode. An FMEA can make use of the input failure modes (qualitative aspect) and their associated probability (quantitative perspective) provided by the FTA. The Safety FMEDA is refined with failure matrix (FIT rate λ ij and reparable rate μji) to derivate Safety measures and to verify the safety goal quantitatively. The safety Target values will have provided to Markov chain.

Markov analysis is enclosed as a part of the safety reuse framework. One of the advantages of the Markov analysis technique is the possibility to consider a reparability rate between non-operational and operational system states, along with a failure rate λ. This is however not so relevant for the safety analysis in the automotive industry, as the systems are typically not reparable: i.e. a failed Electronic control unit (ECU) of brake system is simply replaced. Nevertheless it is possible to take benefit of this advantage for the consideration of testability measures. In conclusion, Markov analysis can be more versatile and precise than Fault trees, but at cost of higher modeling and computation complexity. In this sense, a balance between complexity and size of the model need to be found in order to gain from the use of Markov models.

3.4 Integration of composition framework in Product-Line Safety Assessment Process

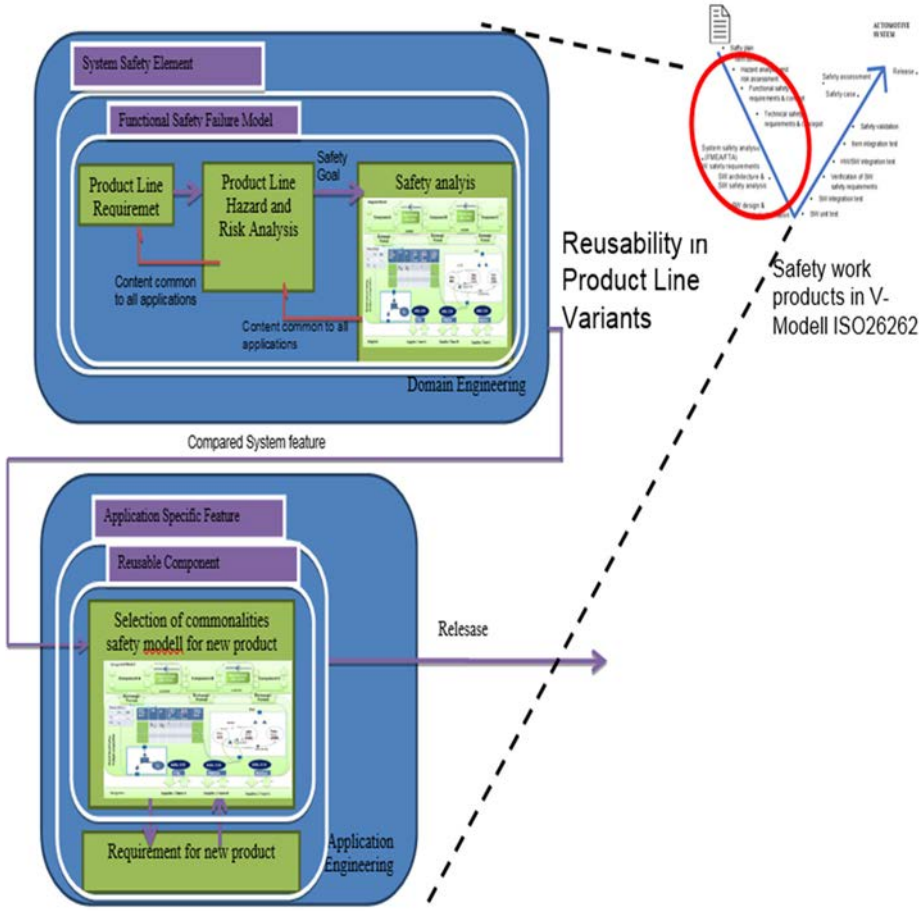

Figure 6: Approach for composition of safety analysis in Product-Line Safety Assessment Process.

The safety composition framework is implemented in the safety model for new product variants to support the reusability. The models depicted in Fig. 6 is useful in safety-critical systems engineering as a way for determine the safety analysis elements an architectural way. The variation in a product line comprises a configurable domain engineering architecture and a set of reusable system description assets in the application product. Usually this variation is supported in that particularly artifacts such as requirements, system design and analysis models in early product development process specify and then reused as long as they are attached to the context. Same function in variant system can be realized with different elements like sensor and actuators.

4 DISCUSSION AND RELATED WORK

In this section, we identify and discuss the specific needs of the automotive industry that still require interdisciplinary research activities.

Challenge: Beside the presented model-based safety engineering approach, the motivation behind a modular safety case reflects two more challenges in the field of automotive safety. Nowadays, for each new safety-critical automotive system or new safety requirement for existing product, a large manual work is expected to achieve a suitable set of safety mechanism and argumentation. The safety analyses of a system, which currently is not structured as the system itself, must relate to the system structure in an appropriate way. Then we can apply the modularity of our products even to the aspect of safety.

Industry: The automotive industry tries to solve the challenge related to distributed dependable system development with standardization (e.g., AUTOSAR) and integrated modelling view (e.g., SysML, EAST-ADL, AADL, Rhapsody and PREEVision) but still need manual work requiring expert knowledge. Formal foundation standard to achieve high quality with reduced cost, e.g., by reusing existing components is not available in the automotive industry.

Academia: The academics propose a comprehensive overview for distributed system development and integration at early stages in development life cycle. Specific safety modelling approach, e.g., Failure Propagation and Transition Notation (FPTN) in [14] and the Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS) in [15], does not support the modelling of complex states, which be required for specific modes of automotive system. However, it faces some practical issues, e.g., existed not modulated product, the academicals solution is not practical. Formalism that combines advantages of safety composition models is introduced by [16]–[18]. MetaFPA [19], an internal framework for Metamodeling-based Failure Propagation Analysis system shows an effort reduction of up to 70% compared to manual approaches. However, MetaFPA does not support the variant product, the modularization, reusability and product line management and need manually refinement by input and output deviation.

CONCLUSION AND FUTURE WORK

We have perceived that safety elements cannot be viewed as a completely modular and reusable, as an open issue, and therefore we pay increasing attention to the integration of safety-related work products along the development process. In particular, safety analysis techniques have gained a lot of interest because they are a means for validating designs and support the certification process.

Our contribution is to identify the specific needs of the automotive industry and the academic solution. In future work, we will discuss the influence of cyber-security in technical and architectural aspect of safety critical autonomous driving system based on ISO 26262 and SAE International Standard J3016 [20]. Follow up queries corresponding to “How the created safety requirements are coupled to the system itself?”, “How do the results amendment if the input parameters change?” and “What is that the most value effective ways in which to boost dependableness?” require a sensitivity analysis of the reliability.

REFERENCES

[1] Lin, Y.H., Li, Y.F. & Zio, E., “A reliability assessment framework for systems with degradation dependency by combining binary decision diagrams and Monte Carlo Simulation,” *in IEEE Transactions on Systems, Man, and Cybernetics: Systems*, **46**(11), pp. 1556–1564, 2016.

[2] Ramezani, Z., Latif-Shabgahi, G.R., Khajeie, P. & Aslansefat, K., "Hierarchical steady-state availability evaluation of dynamic fault trees through equal Markov model," *24th Iranian Conference on Electrical Engineering (ICEE),* Shiraz, pp. 1848–1854, 2016.
[3] International Organization for Standardization ISO/IS 26262 – Road Vehicles – Functional Safety. *Technical Committee 22 (ISO/TC 22),* Geneva, Switzerland, 2011.
[4] Gomes, A., Mota, A., Sampaio, A., Ferri, F. & Watanabe, E., Constructive model-based analysis for safety assessment: *International Journal on Software Tools for Technology Transfer,* **14**(6), p. 673, 2012.
[5] Habli I.M., "Model-Based Assurance of Safety-Critical Product Lines", September 2009
[6] Boudali, H., Crouzen, P. & Stoelinga, M., "Dynamic Fault Tree Analysis Using Input/Output Interactive Markov Chains," *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07),* Edinburgh, pp. 708–717, 2007.
[7] Biehl, M., DeJiu, C. & Törngren, M., Integrating safety analysis into the model-based development toolchain of automotive embedded systems. *In Proceedings of the ACM SIGPLAN/SIGBED 2010 conference on Languages, compilers, and tools for embedded systems (LCTES '10).* ACM, New York, USA, pp. 125–132, 2010.
[8] Schulze, M., Mauersberger J. & Beuche, D., Functional safety and variability: can it be brought together? *In Proceedings of the 17th International Software Product Line Conference*, pp. 236–243, 2013.
[9] Burton, S. & Habermann, A., Automotive Systems Engineering und Functional Safety: The Way Forward. *In ERTS 2012, Toulouse, France, 2012.*
[10] Schwinn, J., Adler, R. & Kemmann, S., Combining Safety Engineering and Product Line Engineering. In Software Engineering 2013 Workshop, Aachen, Germany, 2013.
[11] Kaessmeyer, M., Moncada, D.S.V. & Schurius, M., "Evaluation of a Systematic Approach in Variant Management for Safety-Critical Systems Development,"
[12] *2015 IEEE 13th International Conference on Embedded and Ubiquitous Computing*, Porto, 2015, pp. 35–43.
[13] Mader, R., Obendrauf, R., Prinz, P & Grießnig, G., "Experience Report: A Safety Engineering Tool Supporting Error Model Creation and Visualization," 2014 *IEEE 25th International Symposium on Software Reliability Engineering*, Naples, pp. 255–266, 2014.
[14] Bate, I. & Kelly, T., "Architectural Considerations in the Certification of Modular Systems," *in Proceedings of the 21 st International Conference on Computer Safety*, Reliability and Security (SAFECOMP'02), Springer, pp. 303–324, 2002.
[15] Lisagor, O., McDermid, J.A. & Pumfrey, D.J., Towards a Practicable Process for Automated Safety Analysis. *In: 24th International System Safety Conference*, pp. 596–607, 2006.
[16] Papadopoulos, Y. & McDermid, J., Hierarchically performed hazard origin and propagation studies, in *Proceedings of the 18th International Conference on Computer Safety, Reliability and Security,* LNCS 1608, pp. 139–152, 1999.
[17] Naseh, H. & Mirshams, M., "A Bayesian networks approach to reliability analysis of a space vehicle separation sub-system," 2013 *6th International Conference on Recent Advances in Space Technologies (RAST),* Istanbul, pp. 807–810, 2013.
[18] Han, X. & Zhang, J., "A combined analysis method of FMEA and FTA for improving the safety analysis quality of safety-critical software," 2013 *IEEE International Conference on Granular Computing (GrC),* Beijing, 2013, pp. 353–356.

[19] Mauri, G., Integrating safety analysis techniques, supporting identification of common cause failures; *Thesis submitted for the degree of Doctor of Philosophy*, The University of York, Department of Computer Science, Sep. 2000.
[20] Chaari, M., Ecker, W., Kruse, T., Novello C. & Tabacaru, B.A., "Transformation of Failure Propagation Models into Fault Trees for Safety Evaluation Purposes," 2016, *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, Toulouse, pp. 226–229, 2016.
[21] SAE International Technical Standard, *WARRENDALE*, Pa., 2 Oct. 2014.