Towards Efficient Functional Safety Certification of Construction Machinery Using 
a Component-Based Approach

Stephan Baumgart, Joakim Fröberg
E&E System Architecture Department
Volvo Construction Equipment
Eskilstuna, Sweden
stephan.baumgart, joakim.froberg@volvo.com

Sasikumar Punnekkat
School of Innovation, Design and Engineering
Mälardalen University Sweden
Västerås, Sweden
sasikumar.punnekkat@mdh.se

Abstract—Electronic systems in the automotive domain implement safety critical functionality in vehicles and the safety certification process according to a functional safety standard is time consuming and a big part of the expenses of a development project. We describe the functional safety certification of electronic automotive systems by presenting a use case from the construction equipment industry. In this context, we highlight some of the major challenges we foresee, while using a product line approach to achieve efficient functional safety certification of vehicle variants. We further elaborate on the impact of functional safety certification when applying the component-based approach on developing safety critical product variants and discuss the implications by cost modeling and analysis.

Keywords—functional safety, component based development, safety certification, cost modeling;

I. INTRODUCTION

Each new generation of cars or construction machinery that is rolled out onto the market is characterized by an increasing amount of functionality being realized by software. Software is the key-enabler for new technologies and hence the main innovation driver in the automotive domain. Both the number of Electronic Control Units (ECU) and the complexity of the applied interacting software functionality in the Electrical/Electronic (E/E) Systems are increasing. Being cost-conscious as well, due to strict time-to-market requirements, the automotive industry has been more and more looking at component-based development and product line engineering [5][10].

However the highly dynamic operational environment of these vehicles, where many different types of users are involved, causes even small failures in their E/E systems to probably result in accidents with fatal consequences.

In order to avoid those failures, functional safety standards like IEC 61508 [7] have been developed and introduced in different domains. Recently the ISO 26262 [8], a functional safety standard for the automotive domain, has been released. Functional safety is defined as the “absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems” [8].

At the beginning of a new development process, when the planned usage of the target system is agreed upon, the possible hazards of the new system need to be identified and documented in a hazard list. For each hazard a Safety Integrity Level (SIL) [7] or Automotive Safety Integrity Level (ASIL) [8] can be defined, which is based on the levels of probability, controllability and severity [8] of a hazard. Due to the fact that hazards are connected to the vehicle’s operational environment and since the construction equipment machinery is used in many different environments, a thorough analysis of possible hazards is necessary. Adequate product development evidence must be given to the certifying authority/assessor to confirm that the specified safety goals are met. For example, by providing a safety argument why usage of certain software modules could avoid a particular hazard. Both process and design need to confirm to the rules stated in the functional safety standard. The certification process according to a functional safety standard is rather time consuming and a big part of the expenses of any safety-critical product development project.

The evidence that all requirements on avoiding the identified hazards have been handled in the development process is collected in the safety case [4]. A safety case is an “argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development.” [8].

However the existing functional safety standards [7][8] are following a top down approach and hence the concept for reuse is only addressed superficially. The only concept for reusing software and/or hardware in the new functional safety standard for the automotive domain ISO 26262 is the qualification of the software and/or hardware that is planned to be reused. In part 10 of ISO 26262 [9], which is yet to be published, the concept of a Safety Element out of Context (SEooC) is being introduced, but not described in detail. We believe that a bottom-up-approach focusing both on the reuse of the components as well as their safety evidences could result in an efficient safety certification of products in the vehicular domain.

A model for developing core assets in relation to management and product development, all, which are processes in a development effort, is presented by Clements and Northrop in [6]. This model enables analysis of system and costs and provide guidance for identifying and analyzing which components could be considered core or important enough to be developed in a reusable form. However, this model does not include the notion of functional safety certification. In Figure 1, we present the Software Product Line Engineering (SPLE) concept in [6] together with the
context of functional safety certification of the developed product. 

Since functional safety certification is a big part of the project expenses and the functional safety standards assume a holistic view and stipulate a new functional safety procedure for each new product, the benefits of using the SPLE concept as proposed in [6] are significantly reduced due to the missing dimension for functional safety. 

In this paper we elaborate on how a procedure for assets certification could be realized together with its impact on the cost model. We also describe a platform software, which includes components that are reused by different vehicle variants. In section II, we present this use case. In Section III we identify some of the major challenges of using SPLE in the context of functional safety certification of vehicle variants. In Section IV, we analyze the technical aspects of the problem and present some pointers to a solution. 

II. USE CASE 

In this paper we are focusing on the development and certification requirements in the construction equipment industry with more than 150 product variants, operating in different environments having diverse safety concerns. However this work is equally applicable to the functional safety certification of vehicles in general. 

Figure 1. SPLE in the context of Functional Safety Certification

Figure 2 shows two V-process models representing projects aimed at developing construction equipment machines, called “vehicle A” and “vehicle B”. The electronic system in both will include reusable subsystems. Through analyzing the commonalities of the requirements for the software to be developed for vehicle A and vehicle B, one can identify the set of software components that can be reused in both vehicles. These components can even belong to different abstraction layers depicted in Figure 3. In the following we will focus on the platform software components. Figure 2 shows that the platform software, PS, will be developed separately from the vehicle projects A and B and a synthesis of the requirements of vehicle A, $R^P_{A}$, and of vehicle B, $R^P_{B}$, is performed at the beginning. The platform software project will deliver the platform software and each vehicle project will integrate it at its appropriate integration points $I^P_{A}$ and $I^P_{B}$. It is common [2] to subdivide the software running on an ECU into different layers which at the same time classify the software components that can be reused (see Fig. 3). The hardware abstraction layer is dependent on the electronic hardware used and provides an interface to the available electronic hardware components. In the platform software layer, software components like Controller Area Network (CAN) communication protocols, general diagnostics, real time operating system (RTOS) and other services are provided. The software components in the application layer are using the provided services and enable the vehicle functionality. Two different kinds of reusable software components are developed during the core assets development phase – the application software components and the platform software components. Both are characterized by different lifecycles. While platform software components are reused to a large extent across multiple products, the application software components undergo many changes to cater to newer functionalities. Keeping track of component variants and versions together with their dependencies itself requires a major effort. 

The ECU in Figure 3 with the developed functionality will be used in the E/E systems of both vehicles A and B where the application software and platform software are configured in order to fit the respective context. But as described in Section I, evidence must be provided that all the safety goals for vehicle A and vehicle B are fulfilled and hazards are avoided.

Figure 2. Platform software development and relation to vehicle projects

Figure 3. Platform Software in its context on an ECU
The safety argumentation has to be traced through the complete development process and has impact on the identification of reusable software components of the different abstraction levels on the ECU.

III. CHALLENGES

We now present some major challenges foreseen, while using a product line approach to achieve efficient functional safety certification of vehicle variants. These challenges can broadly be classified as organizational challenges, standardization challenges and technical challenges (TC), where solving the technical challenges is necessary for solving the organizational and standardization challenges.

C1. Organizational / Management Challenges: In the automotive context, the systems are often complex and functionality is distributed on different Electronic control units (ECU). Furthermore the development effort is spread over several development organizations and suppliers. There is a challenge to define and follow up how safety requirements are specified and communicated and how the delivered parts are integrated.

Specifically there are a number of technical challenges that are related and derived from the above challenges:

C1-TC1. Variability management: The variability management as described in [6] needs to be extended to take the effort for functional safety certification into account in order to identify the most efficient handling of software components.

C1-TC2. There is a challenge in achieving an efficient functional safety certification where time consuming tasks do not have to be repeated for very similar subsystems. The cost model presented in [11] needs to be updated by the functional safety dimension. In the context of developing safety critical products by using the family-based software development approach presented in [11], the investment is necessary for replacing the traditional software development process by SPL, needs to be identified. The cost for developing each new family member needs to be identified. With the help of both these values, estimation for a new pay off point can be made.

C1-TC3. Certification in an evolutionary development context: The model of development for a company that begins its core assets development as well as certification from scratch will be different from the model that is applicable to a company which already has multiple product variants in production and wants to identify certifiable components and platforms.

C1-TC4. Functional Safety Scoping: Similar to the scoping procedures in [6] such a method for functional safety certification could give answers as to what is beneficial.

C1-TC5. Certification Effort Estimation: A clear identification of the costs for safety certification with respect to individual software components could be hard in reality due to a) the current state of practice of integrated methods for safety certification at system level and b) the lack of appropriate methodology for recording such costs.

Apart from the organizational challenges, challenges concerning the functional safety standards also exist.

C2. Lack of support in safety standards for modular composition: The functional safety standards do not readily support such a notion of certifying specific assets, but instead assume a holistic view and stipulate a new functional safety procedure for each new product, even if it is based on many already used components.

C2-TC1 Component-based functional safety certification: We believe that a reusable functional safety certification of software components and the identification of their safety arguments, would improve the efficiency of the overall development process of safety critical products due to an enhanced reuse of components.

C2-TC2 Tools for development and certification: As the functional safety standards require a qualification of the tools used to perform the activities in the software development, the tools used for “core assets development” and “product development” need to be certified or qualified according to the functional safety standard as well. Appropriate methods and tools to handle functional safety certification and safety argumentation also need to be identified.

IV. ANALYSIS OF THE PROBLEM

In this section, we elaborate on how a solution to the technical challenge C1-TC1 “Variability Management” could be achieved. For identifying the dimensions of this challenge in greater detail, we are using a notation of software components similar to the one used in [3].

We are developing a set of components \( C = \{C_1, \ldots, C_i, \} \), \( i \in \mathbb{N} \). A component \( C_j \) can have a number of versions \( j \), \( j \in \mathbb{N} \), and variants \( k, k \in \mathbb{N} \), which are all stored in the repository \( REP = \{C_{11}, \ldots, C_{ijk}, \ldots\} \).

If we want to build a new system whose target environment is characterized by several hazards, certain functional safety goals \( G = \{G_1, \ldots, G_m\} \), \( m \in \mathbb{N} \), must be fulfilled. We want to identify those components that fulfill the system requirements \( R = \{R_1, \ldots, R_n\} \), \( n \in \mathbb{N} \), and the safety goals \( G \) of the system.

We also assume that we can identify the functional safety certification effort \( E(C_{ijk}) \) for the component \( C_{ijk} \) in the repository. Through analyzing the components and their functional safety effort, there are 3 different types of components:

Type 1: A reuse is completely possible, because the component had been used and certified in an exactly similar configuration and environment. In this context, the safety certification effort \( E(C_{ijk}) = 0 \).

Type 2: A complete reuse is not possible and the component must be changed in order to fit it in the new context. For such components, the safety certification effort is typically less than the original certification effort, i.e., \( 0 < E_{new}(C_{ijk}) \leq E(C_{ijk}) \).

Type 3: A reuse of the component \( C_{ijk} \) is not at all possible. The functional safety effort of the new component \( C_{ijk} \) is typically at least as high as the original functional safety certification effort for the original component \( C_{ijk} \).

Further analysis of the functional safety characteristics of software components is needed. We believe that a better
understanding and classification of software components and their impact on the effort for functional safety certification of the complete system, will improve the overall development effort.

In Figure 4 we compare the cost model presented in [11] with a cost model for developing safety critical products. Line A in Figure 4 represents the cost $\text{Cost}_T$ for developing the $N$ products in the traditional way, as proposed by [11]. If we assume a cost for functional safety certification of each product $\text{Cost}_{\text{Cert}}$, the total cost for developing $N$ products in the traditional way and for functional safety certification would be $\text{Cost}_{\text{Total}} = N(\text{Cost}_T + \text{Cost}_{\text{Cert}})$ and is shown as line D. As described in [11] line B shows the cost assuming an investment $\text{IF}$ that is necessary to introduce SPLE in an organization and the cost for developing a new member of a family $\text{Cost}_{\text{F}}$, which results in a total cost $\text{Cost}_{\text{Total}} = \text{IF} + N \cdot \text{Cost}_{\text{F}}$. Assuming that $\text{Cost}_{\text{F}} < \text{Cost}_T$ the pay off point $P_{AB}$ is reached. It is most likely that an investment $\text{IF}$ for applying the SPLE concept for developing functional safety certified products will be higher than the investment $\text{IF}$: $\text{IF}_C = \text{IF} + \delta$, $\delta > 0$. As we described above, the functional safety standards follow a top-down approach and we can very well assume that the cost for functional safety certification of each product is not significantly reduced by using the SPLE concept alone. Accordingly the total cost for developing $N$ safety critical products using the SPLE approach is $\text{Cost}_{\text{Total}} = \text{IF}_C + \delta + N(\text{Cost}_{\text{F}} + \text{Cost}_{\text{Cert}})$ which is shown as line C in Figure 4. It will be important to show, when the investment $\text{IF}_C$ is amortized and the pay off point $P_{CD}$ is reached. Line E is showing our expected cost curve when solving the technical challenge C2-TC1 (component-based safety certification) which is making the reuse of safety argumentation of components possible. The initial investment $\text{IF}_{\text{F,CB}}$ for applying the SPLE approach in combination with component-based functional safety certification is probably much higher than $\text{IF}$ or $\text{IF}_C$. Through making reuse of functional safety certified components possible, the new safety certification cost for each product $\text{Cost}_{\text{Cert,CB}}$ will be lower than the above described $\text{Cost}_{\text{Cert}}$. The total cost for using this approach will be $\text{Cost}_{\text{Total}} = \text{IF}_{\text{F,CB}} + N(\text{Cost}_{\text{F}} + \text{Cost}_{\text{Cert,CB}})$. A better pay off point $P_{DE}$ can now be reached.

V. CONCLUSIONS

We have indicated that functional safety certification plays an important role in the automotive and construction equipment domain and that applying the SPLE concept could increase efficiency, but would introduce some major challenges. We presented a use case from the construction equipment industry domain. We highlighted challenges, refined those challenges into technical challenges and presented our preliminary analysis directions towards a viable solution.

We have established a research team and are participating in the EU-Artemis funded SafeCer project [1] with several industrial and academic partners, which are focusing on a component-based approach for safety certification of embedded systems. By showing the impact of functional safety certification on the overall development cost in Figure 4, we indicated that further research on improving the SPLE concept for developing safety critical products is necessary.

ACKNOWLEDGMENT

We are grateful for the financial support received from the ARTEMIS Joint Undertaking under grant agreement n° 269265, Vinnova and the KKS-funded ITS-EASY Post Graduate School for Embedded Software and Systems.

REFERENCES