Enhancing Model-Based Engineering of Product Lines by Adding Functional Safety

Stephan Baumgart[1] and Joakim Fröberg[2], Sasikumar Punnekkat[2],[3]

[1] Dept. Change Management and Process Development,
Volvo Construction Equipment, Eskilstuna, Sweden
stephan.baumgart@volvo.com
[2] School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
joakim.froberg@mdh.se
[3] BIT-Pilani KK Birla Goa Campus, India
sasi@goa.bits-pilani.ac.in

Abstract. Today's industrial product lines in the automotive and construction equipment domain face the challenge to show functional safety standard compliance and argue for the absence of failures for all derived product variants. The product line approaches are not sufficient to support practitioners to trace safety-related characteristics through development. We aim to provide aid in creating a safety case for a certain configuration in a product line such that overall less effort is necessary for each configuration. In this paper we 1) discuss the impact of functional safety on product line development, 2) describe a model-based approach to capture safety-related characteristics during concept phase for product lines and 3) discuss the usefulness of our proposal.

Keywords: Product Line Engineering, Functional Safety, Model-based, Systems Engineering, ISO 26262

1 Introduction

Reuse of already developed components and system parts is commonplace in industry today and the main goal is to reduce cost and achieve faster time to market. The industrial product lines we observe in our studies are characterized by an engineer's mindset and a clone-and-own strategy instead of a managed and organized reuse in software product line engineering (SPLE) concepts. Accordingly, the practices around product line engineering have flaws in industry today, i.e. the state of the art practices are not implemented. At the same time the products developed in the automotive and construction equipment domain need to fulfill functional safety standards. The functional safety standards like ISO 262626 [1] define requirements on the development process to avoid systematic and random failures. Evidence on how potential hazards have been taken into consideration throughout the development of the product need to be collected and provided in a safety case. Functional safety compliance is achieved by

applying rigor in the process of developing the system. Copying from other products or previous product generations would involve that nothing has changed in the safety argumentation. This is not always the case and instead may lead to unexplored hazards or violations of safety goals. The flexibility in creating variants can in some cases increase the effort for assuring compliance. Instead of just assuring that a component cannot fail dangerously, we now face a situation where we must assure that no variant can fail dangerously, in any of the possible configurations. Many functional safety standards assume a V-model-based development process without support for product line development. While the state of the art methods for product line engineering do not encompass methods and models for achieving functional safety compliance.

There is not just one solution on how to set up a product line, instead different product line strategies can be chosen. Jan Bosch describes different product line strategies for software product lines in [2] and proposes a categorization of maturity levels for product lines. Applying this categorization on the systems level implies that each product line category requires a different approach to functional safety. Choosing a product line strategy has an impact on the possible safety concepts on the one hand and their allocation to technical solutions on the other hand. Both the distributed development and the diversity of tool chains hinder the communication about the development in general and in particular about functional safety. Flawed communication is one reason for potential errors and systematic failures [3]. The effort for achieving functional safety standard compliance is higher than the actual development effort for highly safety-critical single product development already. There is a need to provide guidance and methods enabling practitioners to manage functional safety in product lines more efficiently and effectively.

The contribution of this paper is a model-based approach to manage functional safety during concept phase in product line development. It is necessary to start from the systems perspective since functional safety is a property of the system and we therefore focus on the concept phase described in the functional safety standard ISO 26262 Part 3.

The paper is structured as follows. The related work is discussed in 2 and in section 3 we describe our approach and present a case from the construction equipment domain. In section 4 we discuss our approach and conclude the paper in 5.

2 Background and Related Work

In our work we aim document functional safety and provide the base to derive a suitable product line strategy. Typical concepts for documenting functional safety are *Document-based approaches*, *Architecture Description Languages*, *Component-based approaches* and *Model-based approaches*.

Document-based approaches: It is common in practice to specify the work products required by the functional safety standards in separate documents. This is sufficient for small and less complex systems with independent safety-critical

functions. Documents can be misinterpreted and misunderstood, which especially in companies with distributed global development leads to that functional safety related documents may be interpreted differently and different technical solutions are developed. Managing the complexity of product lines and functional safety with a document-based approach is challenging and dependencies may be missed.

Architecture Description Languages The focus of an architecture description language (ADL) is to describe the architecture of the embedded system. EAST-ADL [4] is an ADL, which has been proposed to aid the development of embedded systems in the automotive domain. It is covering the development phases from vehicle level onwards where features are documented and variability of the product line is analyzed and captured. In EAST-ADL2, the extension of EAST-ADL, an error model and a safety case metamodel are added. The authors in [5] define safety contracts and propose a set of rules for EAST-ADL2 to provide automatic proofs if safety goals and safety contracts are violated. Sun et al. [6] describe a concept to transform a Product Line Fault Tree (PLFT) into an AADL (Architecture Analysis and Design Language) model to enable connecting the hazards to elements in the AADL model. This assumes though that the product line system is already modeled in order to map the hazards. Details on how to derive a product line concept under consideration of functional safety are not yet provided.

Component-based Approaches Component-based approaches aim to describe an embedded system in detail focusing on the software components and their interaction. The CHESS project [7] aims to document safety related information in a component model enabling an automated dependability analysis. The authors introduce dependability concepts added to the component model. Product line engineering is not considered in the project and the concept assumes that all information is available when the component model is used. In the recent years concepts for mapping hazards to specific component have been developed. The authors in [8] describe a concept for creating component fault trees (CFT), which aim to map relate parts of the fault tree to the according components of the design. Gomez et al. [9] describe the application of the CFT concept and claim, that efforts for performing a FTA are reduced in the future, when components are reused. A CFT for a component can first be derived after development and therefore benefits of the approach are first evident during reuse of the component.

Model-based Approaches Model-based development approaches are growing importance for developing embedded systems and can be applied for the systems level (SysML) as well as for the detailed technical descriptions (UML). Biggs et al. [10] propose a SysML based approach to capture safety related information in a model. They assume that all relevant information is available and describe how to use the SysML diagrams to create a common documentation. The authors do not describe how to achieve functional safety in product lines though. Liu et al. [11] describe a concept to perform a safety analysis for software product lines and exploring potential hazardous states using UML state chart diagrams and scenario diagrams. An UML-based approach to model software

product lines is proposed by Gomaa [12], which is both focusing on the domain engineering phase, where a common software architecture is derived to support all relevant product variants and the application engineering phase, where the common architecture is applied to derive the product variants. Functional safety is not considered in the model-based approach by Gomaa.

Summary In order to provide information for deciding a product line strategy, we see a potential to apply a model-based approach and in particular extend the PLUS concept describe by Gomaa. The characteristics of the product line can be described from different views which are necessary to capture functional safety related attributes as well. The PLUS model proposed by Gomaa [12] has a potential to be extended to cover both functional safety and product lines as well as being extended to cover the systems engineering dimension. In the following we present and discuss our approach.

3 Approach

3.1 General Idea

In order to be able to take functional safety into consideration while planning the product line, the relevant information need to be available already in early development phases. Functional safety requires a holistic approach being able to capture information throughout all development phases. On the one hand we can build upon model-based product line engineering approaches as for example PLUS [12]. On the other hand, model-based development is already common for software development and therefore it is possible to build upon already established practice. We aim to answer the research question: How can we add functional safety related artifacts to a product line model?

In Figure 1 we present the general concept of our approach. The model itself is an Add-on to the PLUS approach of Gomaa taking functional safety into consideration. The model-based approach we aim to develop shall contain both development artifacts and safety-related artifacts. By the help of not just adding separate diagrams for modeling the safety-critical functions, it is possible to identify and capture dependencies between safety-related and non-safety-related functions. When all information is captured in one model, automatic consistency checks can be made to identify potential violations of safety goals in specific configurations. Change requests shall be analyzed automatically and may result in an impact analysis report extracted from the model. Since the main goal of our work is to derive a safety case for each product variant, the model shall enable the automatic generation of all necessary documents, i.e. the safety case, for a specific product variant. This can be realized by using a product configuration as an input. Predefined internal rules may extract the relevant information from the model and create the required documentation. A model that captures all relevant information will enable future product line instantiations and evolution.

We developed a model-based approach for the concept phase capturing commonality and variability on the one hand and the ISO 26262 related informa-

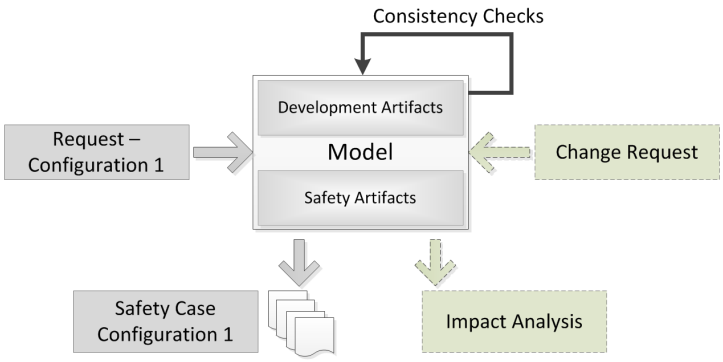

Fig. 1. General concept of our approach

tion on the other hand. We applied our approach using a steer-by-wire example (Comfort Drive Control - CDC) from the construction equipment domain.

Each machine has a mechanical steering wheel, but a steer-by-wire solution can be ordered as an option. We foresee two possible variants for the CDC - a) left-right steering, which imitates the steering wheel functionality using a lever and b) joystick steering, which adds forward/backward movement to the left-right steering. The joystick steering has a higher criticality in comparison to the left/right steering, since the required communication to the engine and gearbox may fail with less possibility to control.

3.2 Approach - Concept Phase

The main challenge we identified is the actual mapping of the V-model-based process described in the ISO26262 to the product line development process. For the concept phase the standard requires that the safety critical features (items) are identified, a hazard analysis is performed in order to identify the criticality of the features and applicable safety concepts shall be defined. The standard furthermore requires that different concepts are analyzed and evaluated to choose the appropriate safety concepts.

Process

During the concept phase the product line strategy is derived that specifies which reusable functions are to be implemented in a platform and which functions are product specific and will be developed in the application engineering phase. Generally, it needs to be decided how the items and concepts are mapped on the common platform or the specific applications. We furthermore aim to capture the variability for items and safety concepts to enable the correct implementation at later design stages. We utilize Use Case diagrams and Feature Diagrams from PLUS for the concept phase and add additional safety related properties. The activity *Product Line Analysis* initializes the concept phase and information about the targeted products, the demanded features and which existing technical

solutions shall be reused are collected and provided for further analysis. The use cases are collected in the *Use Case Diagram* and the required features are derived and documented in the *Feature Diagram*. As a Hazard and Risk Analysis (HARA) [1] we perform a Preliminary Hazard Analysis (PHA) [13] and the information from the diagrams are used for the hazard analysis. A model-based approach to document a PHA has been presented in [14] and has not yet been explored in our work. Today the PHA is documented in a separate table. After performing the PHA, the resulting hazards, Automotive Safety Integrity Level (ASIL), risk reduction strategies and operational constraints are added to the diagrams. This information will be used for later development stages. The results of all analysis are fed back to the *Product Line Analysis* step to review, adapt and improve the product line concept.

Process - Use Case Diagram

The usage of the machines and relation between the machine functionality and the operators or bystanders are captured in the *Use Case Diagram*. Apart from the variability notation proposed in the PLUS model, we introduce a unique title for each scenario and add the stereotypes «hazard», «mitigation strategy» and «operating constraints». In Figure 2 our approach is applied to the steer-by-wire example. The different operating modes need to be defined and in this example we visualize the scenario *pallet handling*. In other scenarios as *idling* or *maintenance* where the CDC is also involved different hazards are related. The «hazard» documents the hazards identified in the PHA and the related ASIL are added as a property. For the optional use case *Left/Right Steering* the hazard *Unintended steering* is connected. There are two variants of this hazard, while for product group 1 the hazard has an ASIL A, for product group 2 an ASIL B is identified. For *Forward/Backward Movement* we connect the hazard *Unintended Forward/Backward Driving* with an ASIL D. From the last

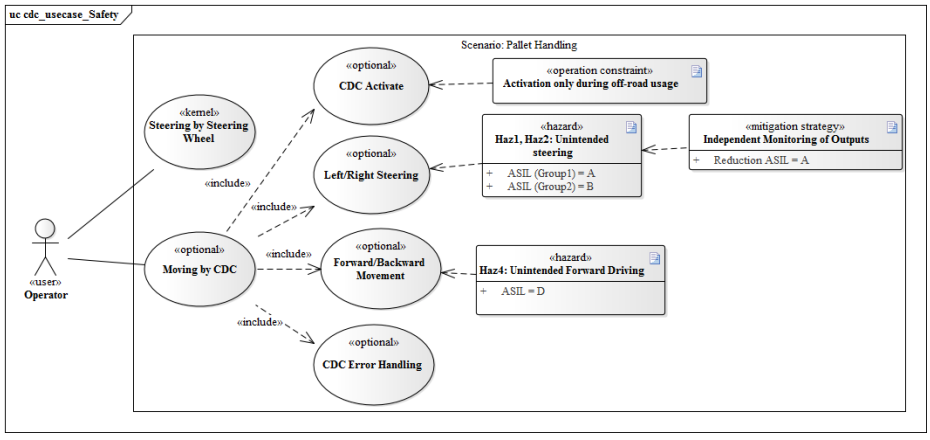

Fig. 2. Use Case Diagram: Functional safety related information added to application scenarios

generation of the product in which only *Left/Right Steering* was implemented, a mitigation strategy can be reused for this use case. A mitigation strategy is a possibility to reduce the criticality of the item. In this case the strategy «Independent Monitoring of Outputs» was used in an earlier generation. The property *Reduction ASIL* is reflecting on how the ASIL could be reduced with the help of the mitigation strategy. The stereotype «operation constraint» can be applied, when knowledge about constraints are available. In this case the activation of the CDC shall only be allowed in off-road usage of the machine to reduce the probability of accidents. By the help of such constraints the hazards related to application during on-road usage can be excluded. The related hazards and mitigation strategies are supporting practitioners to take the safety-related information into consideration when designing the system.

Process - Feature Diagram

The *Feature Diagram* of Gomaa captures different types of variability. We add the stereotypes «hazard» and «safety concept» and different dependencies types. We applied the feature model to the steer-by-wire case in Figure 3. The product

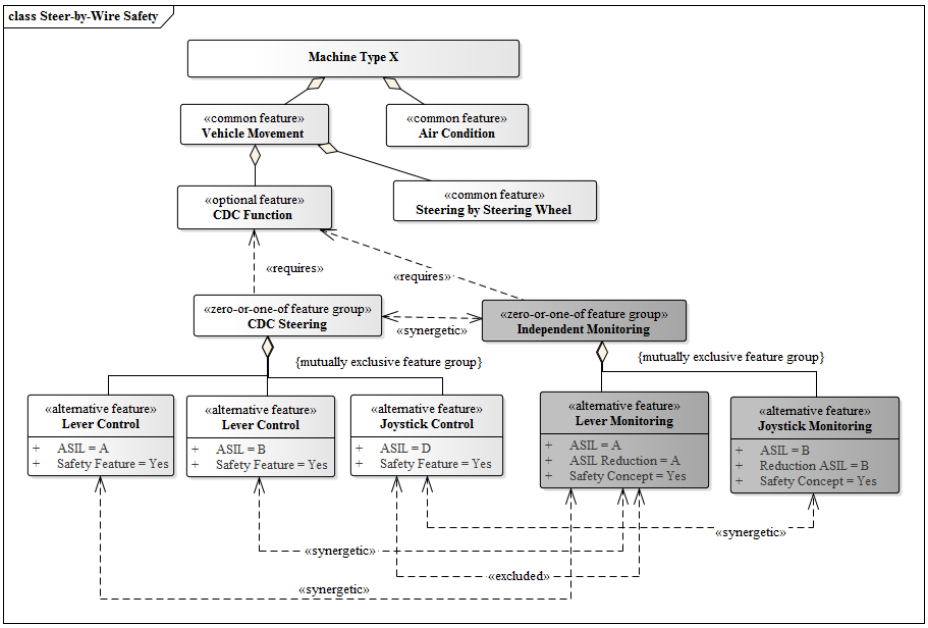

Fig. 3. Feature Diagram: Adding details for chosen safety concept

family ”Machine Type X” is having the «common feature» ”Vehicle Movement”. The feature ”Vehicle Movement” is in each machine represented by the «common feature» ”Steering by Steering Wheel”. It is optional that the ”CDC Function” is used. The feature group ”CDC steering” can be represented by only one fo the subfeatures ”Lever Control” with ASIL A, ”Lever Control” with ASIL B or the

"Joystick Control". The feature "Lever Control" with ASIL A is related to the *Left/Right Steering* use case in the *Use Case Diagram*. There different hazards have been identified for two different product groups. The hazards related to these groups are related to the two different features for "Lever Control". The leaves of the safety critical features are getting the attributes *ASIL* and *Safety-Feature*. So for example the feature "Joystick Control" is a "Safety-Feature" and the ASIL D has been identified in the PHA. The feature group "Independent Monitoring" is grouping the mitigation strategy features "Lever Monitoring" and "Joystick Monitoring". These features are identified by the attribute "Safety Concept" and the possible reduction of the ASIL. Furthermore the mitigation strategy may add new hazards which are represented by the ASIL level. We utilize the dependencies proposed in [15] and more specific «synergetic» to show that features shall be implemented to work in parallel with regular synchronization. In our case the "CDC steering" shall be monitored by the feature "Independend Monitoring". In later stages of the development this dependency can be refined by adding the maximal monitoring intervals. By the help of the «excluded» dependency the configuration constraints are captured. It is not allowed that there is a machine that has a "Joystick Control" which is monitored by the feature "Lever Monitoring".

4 Discussion

The presented approach focuses on the concept phase and to manage functional safety in product lines. We use the PLUS notation and add safety-related stereotypes to the *Use Case Diagram* and *Feature Diagram*. In the following we discuss how our approach helps to overcome some of the challenges.

1) Aid documenting safety concepts in a PL: Documenting safety concepts and taking variability into consideration is important and we document the safety concepts and their variability as well as exploring the dependencies between features and safety concepts. This may aid practitioners in designing the product line.

2) Support in extracting a safety case for each configuration: Part 3 of the ISO 26262 and specifically the requirement 5.4.1 guided us which information is required to be documented for an item. We added the required properties as new stereotypes and added relations. Rules and templates need to be developed to proof the extraction of information, which is part of our future work.

3) Support in choosing a product line concept: When moving towards a product line, a product line concept needs to be chosen. This concept defines which features should be provided by a common platform and which features are product specific. By providing information about variability and functional safety in our approach, the development team can make informed decisions.

4) Support in PL instantiation: By having a model when a new product is planned, rework may be avoided because all details are stored in one model. Furthermore having knowledge about related hazards supports the understand-

ing of product line. An impact analysis of projected changes can be supported by model-internal analyses, which is not yet implemented. This will improve understanding the impact of the change and help identifying the affected parts of the product line.

5) Flawed Communication is a threat to the successful development of safety critical products. A model-based approach helps to create a common view on the one hand and support a better understanding on the other hand, when the specified solutions can be simulated. Since we also combine functional safety, dependencies and variability, relevant information is not hidden anymore as it is the case in a document-based approach.

5 Conclusion

In this work we have investigated how functional safety can be managed during concept phase in industrial product lines. We identified that model-based development concepts have a potential to aid product line engineering and support focusing on functional safety at the same time. We propose a model-based approach for the concept phase defined by the ISO 26262 which is based on the PLUS approach proposed by Gomaa [12]. We use the *Use Case Diagram* and *Feature Diagram* to capture product specific properties and functional safety at the same time. We applied our approach to an industry related steer-by-wire example, visualizing the applicability of our approach. In section 4 we discussed how our approach helps to overcome the challenges of managing functional safety in product lines. In the scope of this paper we did not focus on performing consistency checks in the model. By enhancing the PLUS model with information about hazards, safety mechanisms, safety-related features and dependencies between features such consistency checks become possible and necessary because of the growing complexity of such models.

The research presented by Lee et al. [15] shows the possibilities of performing consistency checks for feature models that include dependencies. Further research is necessary to perform consistency checks with a functional safety focus taking the hazards and safety mechanisms into consideration as well. It is also necessary to map to other development stages from the standard to the product line process and explore the impact of product line strategies more in detail.

It is furthermore possible to extend the model-based approach by a state chart diagram where machine states, potential hazards and safe states documented. This can be useful for later development stages when machine states are refined.

Acknowledgments

The research leading to these results has received funding from the ARTEMIS Joint Undertaking under grant agreements no269265 and no295373, Vinnova and the KKS-funded ITS- EASY Post Graduate School for Embedded Software and Systems.

References

1. ISO: ISO 26262 Road vehicles – Functional safety (2011)
2. Bosch, J.: Maturity and evolution in software product lines: Approaches, artefacts and organization. Software Product Lines (2002)
3. Lutz, R.R.: Analyzing software requirements errors in safety-critical, embedded systems. In: Requirements Engineering, 1993., Proceedings of IEEE International Symposium on, IEEE (1993) 126–133
4. Chen, D., Johansson, R., Lönn, H., Papadopoulos, Y., Sandberg, A., Törner, F., Törngren, M.: Modelling support for design of safety-critical automotive embedded systems. In: Computer Safety, Reliability, and Security. Springer (2008) 72–85
5. Oertel, M., Schulze, M., Peikenkamp, T.: Reusing a functional safety concept in variable system architectures. In: 7th International Workshop on Model-Based Architecting and Construction of Embedded Systems. (2014)
6. Sun, H., Hauptman, M., Lutz, R.: Integrating product-line fault tree analysis into aadl models. In: High Assurance Systems Engineering Symposium, 2007. HASE '07. 10th IEEE. (Nov 2007) 15–22
7. Montecchi, L., Lollini, P., Bondavalli, A.: Dependability concerns in model-driven engineering. In: Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2011 14th IEEE International Symposium on. (March 2011) 254–263
8. Kaiser, B., Liggesmeyer, P., Mäckel, O.: A new component concept for fault trees. In: Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software - Volume 33. SCS '03, Darlinghurst, Australia, Australia, Australian Computer Society, Inc. (2003) 37–46
9. Gómez, C., Liggesmeyer, P., Sutor, A.: Variability management of safety and reliability models: An intermediate model towards systematic reuse of component fault trees. In Schoitsch, E., ed.: Computer Safety, Reliability, and Security. Volume 6351 of Lecture Notes in Computer Science., Springer Berlin Heidelberg (2010)
10. Biggs, G., Sakamoto, T., Kotoku, T.: A profile and tool for modelling safety information with design information in sysml. Software & Systems Modeling (2014) 1–32
11. Liu, J., Dehlinger, J., Lutz, R.: Safety analysis of software product lines using state-based modeling. Journal of Systems and Software (2007) 1879–1892
12. Gomaa, H.: Designing software product lines with UML. Addison-Wesley Boston, USA (2004)
13. Ericson, C.: Hazard analysis techniques for system safety. Wiley-Interscience (2005)
14. Marielle, P., Thomas, F., Belmonte, F.: Interoperability between risk assessment and system design for railway safety critical signalling system development. In: 17eme Congres de Maitrise des Risques et de Surete de Fonctionnement, IMDR (2010)
15. Lee, Y., Yang, C., Zhu, C., Zhao, W.: An approach to managing feature dependencies for product releasing in software product lines. In: Reuse of Off-the-Shelf Components. Springer (2006) 127–141