NordDesign 2016
August 10 – 12, 2016
Trondheim, Norway

Safety-oriented Modular Function Deployment

Markus Kohl, Michael Roth, Udo Lindemann

Institute of Product Development, Technical University of Munich
Michael.roth@pe.mw.tum.de

Abstract

While markets demand for individual products, the importance of safety also continuously increases. Modularization methods are a common approach, but they mainly focus on technical dependencies or other module drivers. From a safety perspective, this leads to non-optimal module concepts, which further increase the efforts connected to safety. To avoid this, safety aspects should be better considered. Thus, this paper presents the safety-oriented Modular Function Deployment (sMFD), which integrates safety aspects in a modularization method. It aims to develop safety-oriented module concepts. Hence, sMFD contributes to a shift of safety considerations to early stages of design and supports the evaluation of alternative concepts. The paper analyses existing modularization methods and assesses their suitability. MFD is identified as most suitable and adapted to support the safety-oriented modularization. Therefore, safety aspects (e.g. safety integrity levels or classes of safety requirements) are defined as module drivers. The resulting sMFD is applied and evaluated in two industrial case studies.

Keywords: modularization, safety, modular function deployment, product architecture

1 Introduction

Currently, the variance and complexity of products is increasing (Lindemann, Maurer, & Braun, 2008). This trend forces companies to keep their complexity under control and provide a flexible product with high variance. A favoured concept are modular product architectures. To develop these, a variety of modularization methods is established (Daniilidis, Enßlin, Eben, & Lindemann, 2011). They rely on different techniques and have different focuses (Holtta & Salonen, 2003). Examples are Modular Function Deployment (MFD), Domain Structure Matrices (DSMs), Design for Variety (DfV) and Function Heuristics (FH).
A second trend are stricter safety regulations (Leveson, 2012). The conformity with those has to be documented and proven. In combination with increasing complexity, this leads to large efforts, especially for safety analyses and the testing of each variant (Leveson, 2012; Roth, Gehrlicher, & Lindemann, 2015). Thus, to stay competitive, this effect has to be reduced and the efficiency of safety analyses or tests should be improved.

To achieve this, safety experts demand for reusable safety analyses and better documentation. Especially in the context of increasing variance, the need for an adequate preparation and the development of safety-oriented architectures are postulated (Roth et al., 2015).
As modularization methods are commonly applied during the architecture definition, they should help to include safety aspects in the product architecture. However, traditional methods do not provide this systematic support (Bernard & Hasan, 2002), so that a new or improved safety-oriented modularization method is needed. Therefore, the paper follows the research question of how safety aspects can be considered during modularization to achieve a product architecture, which reduces the overall safety efforts.
To answer this research question, the paper in the following first introduces key concepts of safety as well as existing modularization methods. It also highlights existing works which establish a link between modularization and safety aspects. Based on this, the research methodology followed in the paper is explained and the resulting safety-oriented MFD is introduced. The method is applied in two case studies and discussed with experts of the involved companies. The paper then concludes with a summary and an outlook on future work.

2 Background

2.1 Safety in product development

The importance of safety consideration in product development steadily increases. Therefore, many researchers demand for a shift of safety considerations to early phases of design (Leveson, 2012; Roth et al., 2015). However, the current practices mainly focus on review-based safety analyses (Sierla, Tumer, Papakonstantinou, Koskinen, & Jensen, 2012) and a gap in the safety processes is identified (Berres, Schumann, & Spangenberg, 2014). Yet, new and upcoming standards might force that shift to be realized. For example, ISO 26262 introduces a standard for functional safety in road vehicles and IEC 62425 introduces a similar concept to rail vehicles. Hence, new methods to enable that shift and facilitate the safety design are required (Cuenot, Ainhauser, Adler, Otten, & Meurville, 2014).

2.2 Modularization methods

Many different modularization approaches and methods with different focuses were introduced over the last years (Holtta & Salonen, 2003). According to Daniilidis, Hellenbrand, Bauer, and Lindemann (2011) the Design Structure Matrix (DSM), Function Heuristics (FH), Modular Function Deployment (MFD) and Design for Variety (DfV) are the major methods.
The **DSM** of Pimmler and Eppinger (1994) is a method for defining the product architecture as well as for understanding and handling of complexity. It can be applied to products, systems, processes and organisations. The DSM comprises architecture elements (e.g. components or functional elements) and their technical and functional dependencies (interactions). This represents the decomposition of the system into elements and the documentation of occurring interactions. These interactions are further distinguished into the four generic types “spatial”, “energy”, “information” and “material”. Moreover, the strength of the interaction is recorded in interaction scores. Depending on the interactions and associated scores, the elements are clustered into chunks from which modules can be derived (Pimmler & Eppinger, 1994).
The strengths of the DSM are the compact and systematic representation and that it allows to apply clustering algorithms. However, the analysis of the product architecture is component-

based and the DSM can thus, be only used in later phases of the product development, when more information about the component structure is available (Daniilidis, Enßlin et al., 2011).
FH by Stone, Wood, and Crawford (2000) are applicable in early phases of the product development process. They are based on the major flows in the functional structure. To apply them, the product functions are decomposed into sub-functions. The connections between these sub-functions are modelled by material, energy and signal flows. Based on this, modules are identified according to three different heuristics. The first heuristic "dominant flow" identifies non-branching flows. All sub-functions connected to that flow before it is branched or transformed, can be clustered to a module. The second heuristic "flow branching" identifies flows that are associated to parallel function chains and combines these chains to modules. The third heuristic "conversion-transmission" identifies flow conversion and transmission chains and clusters them into modules. These heuristics provide support to identify possible modules, but the final selection is left to the applying engineer (Stone et al., 2000).
The FH are easy to apply and to understand. Yet, they involve subjective decisions and thus, do not provide fully reproducible results. Moreover, the applicability is limited to large and complex systems as no algorithms can be used (Daniilidis, Enßlin et al., 2011).
The **MFD** by Ericsson and Erixon (1999) focuses on product strategic aspects. Even though it is based on functional structures, it mainly considers so-called module drivers. They represent influences from the fields of development and design, variance, manufacturing, quality, purchase and after-sales, which often lead to a need for modules. The MDF offers a methodology, which supports the whole design process of a modular product. The MFD's modularization uses the Module Indication Matrix (MIM). In the MIM, the dependencies between the module drivers and technical solutions are assessed. The obtained scores are then used to form modules. A high total score might indicate a solution which is a module by itself. A low total score marks solutions which might form the product platform. Medium sores are solutions which can be grouped together to a module (Ericsson & Erixon, 1999).
The MFD enables a traceable modularization, which incorporates strategic aspects. Moreover, it offers a similar condensed view comparable to the DSM. Yet, the results strongly depend on the user and are not fully reproducible. And the module drivers are very abstract and might lead to large preparation efforts to assess them adequately (Daniilidis, Enßlin et al., 2011).
The **DfV** methodology by Martin and Ishii (2002) considers both, the product strategy and functional dependencies. The aim is a decoupled product architecture with reduced design efforts for future products. For modularization, DfV relies on the Generational Variety Index (GVI) and Coupling Index (CI). The GVI measures the redesign that will be needed for future designs of a component. The CI represents the coupling between the product components. Based on these indices, the modularization of architecture is conducted and the components can be standardised and modularised supported by further metrics (Martin & Ishii, 2002).
By implementing the indices and metrics, the DfV produces results which are to some extend reproducible. Moreover, it can even be applied to large complex systems. However, the DfV focuses exclusively on the product variance and redesign efforts. It does not consider further relevant influence factors (Daniilidis, Enßlin et al., 2011).
In summary, all described major methods have different strengths and weaknesses. Yet, none of them explicitly supports the incorporation of safety aspects. In the following, selected methods that incorporate safety or quality aspects are presented.
Papadopoulos, McDermid, Sasse, and Heiner (2001) focus on software architecture and integrate a number of safety analysis techniques. For instance, the synthesis of fault trees implemented in a special algorithm. However, modularization is only marginally addressed.
In contrast Aguwa, Monplaisir, and Sylajakumari (2012) introduce a modularization method for medical devices. The aim is to reduce the usual high failure rate in first prototype tests and

thereby decrease the costs. First, the functional and structural decomposition is conducted. Modules are evaluated by applying rules according to prioritized product parameters. The module concept is then obtained through a multi-optimization goal programming model.
The approach by Nepal, Monplaisir, and Singh (2006) also uses goal programming for identifying different modules. Fuzzy logic is applied to reduce costs and maximize the overall product quality, especially at early stages of product development. Agard and Bassetto (2013) follow a similar goal including a single-level module design formulation that considers quality and cost. To identify modules, a simulated annealing procedure is applied.
Yet, all these methods base solely on a mathematical optimization and have to be evaluated manually to incorporate other influence factors. Thus, these methods are not suitable to systematically support the development of safety-oriented product architectures.

2.3 Summary of the state of the art and research need

As stated in section 1, a major problem of integrating safety into products is that the designers do not have a formal, systematic approach (Bernard & Hasan, 2002). From a safety perspective, usually technical aspects are in the centre of existing methods (Ghemraoui, Mathieu, & Tricot, 2009). And from a modularization perspective, there is no method which sufficiently considers safety aspects. Some approaches (e.g. Nepal et al. (2006)) integrate quality requirements into the development process, but intervene at quite late stages (i.e. detailed design). Yet, at these stages, the decisions on the product structure have already been made (Ghemraoui et al., 2009). Moreover, designers tend to just add mechanisms to existing products to meet new requirements (Hatamura, Hattori, & Hatamura, 2006). This might lead to delays and cost increases as problems are solved late (Hollnagel, 2008). Especially for safety aspects, this is critical.
Thus, incorporating safety-aspects during modularization might reduce the increasing efforts to fulfil requirements and integrate safety in the early stages of product development. Hence, there is a need for a method which considers safety aspects during modularization.

3 Research Methodology

To develop a modularization method, which incorporates safety-relevant aspects as demanded in section 2.3, we follow a structured procedure. Even though none of the existing approaches provides sufficient support, the established modularization can provide a base for adjustments.
Therefore, first, the requirements on the support method are derived from the research question and the findings of the state of the art. Then, the existing methods were analysed concerning their strengths and weaknesses. According to this analysis, their requirements fulfilment was assessed in a simple score assessment. As the selected method was not able to fulfil all requirements sufficiently, an adaption was necessary. The challenge was to satisfy the requirements on the method and to consider the safety aspects during modularization.
To evaluate the method, it was applied on two exemplary systems. Based on this, the method's quality was improved and evaluated in a discussion with experts from the involved companies.

3.1 Definition of requirements

The requirements on the modularization method, which incorporates safety aspects, comprise two fields: The inclusion of safety aspects during modularization and general requirements for a successful modularization method. The specific requirements are listed in Figure 1.

Requirement	DSM	FH	MFD	DFV
Allow examination of the system	3	3	3	3
Generation of system understanding (Daniilidis, Hellenbrand et al., 2011)	4	4	4	2
Quantitative evaluation of module drivers (Ericsson & Erixon, 1999)	4	0	4	4
Include functional dependencies (Koppenhagen 2014)	4	4	0	3
Consideration of safety relevance (Bishop and Bloomfield 1998)	1	0	2	2
Suitable number of modules (Ericsson & Erixon, 1999)	1	0	3	1
Build on functional structures (Holtta & Salonen, 2003)	4	4	4	4
Possibility of extensions / adaptations	0	0	4	1
Traceability & comprehensibility (Blees, 2011)	4	4	4	2
Independent formation of modules (Blees, 2011)	4	0	4	0
Sum	**29**	**19**	**32**	**22**

scale:
0 (not fulfilled)
to
4 (completely fulfilled)

Figure 1. Defined Requirements and evaluation of the modularization methods.

3.2 Method Assessment

The existing modularization methods were assessed based on their fulfilment of the defined requirements. To ensure objectivity, the methods, their advantages and limitations were in detail analysed by the authors. The assessment with a simple score rating is presented in Figure 1.

The results show that the strength of the DSM is the condensed representation of functional dependencies, while the incorporation of safety aspects is difficult. Further limitations concern the requirement "suitable number of modules". Promising is the DSM in the fields "traceability" and "adaptability". Thus, the DSM is not fully suitable and extensive adaptions would be required to satisfy the defined requirements.

FH cannot be extended to incorporate safety aspects and the evaluation of modules is only qualitative. Thus, FH does not meet the requirements on a level which allows an adaption.

The MFD considers safety aspects indirectly, but does not integrate functional. The module drives might allow an adaption to incorporate safety aspects. And even though the reproducibility is limited, the formation of modules is clear and understandable. Hence, MFD will need an integration of safety parameters and the inclusion of functional dependencies.

DfV implements a reproducible quantitative evaluation through its indices. These indices do not represent safety aspects, but might be adapted. For example, the GVI could be used to model safety aspects and the CI for functional relations. However, the independent formation of modules is not further supported, which limits the adaption options.

In summary, the MFD reaches the best score and provides potential for adaption. Thus, it is selected to derive a modularization method, which fulfils the defined requirements.

3.3 Method adaption

To fulfil the requirements, the MFD needs to include functional dependencies and specific parameters, to model safety aspects. The following describes necessary adaptations.

To consider the functional dependencies during modularization, the MFD must be extended by an approach that compensates this deficit. Of the discussed methods, the DSM was identified as most appropriate because it uses the functional dependencies as main driver for modularization. Already Koeppen (2008) and Koppenhagen (2014) have published approaches to connect DSM and MFD. This is adopted, but as functional dependencies shall not dominate the safety-oriented modularization, it is only used to provide input used in the MFD.

To include safety aspects in the modularization, the module drivers are adapted so that they integrate safety. Therefore, a parameter is required that represents safety requirements as well as the associated efforts. Yet, to evaluate these safety aspects during modularization a new dimension is needed. The literature review identified relevant guidelines, laws and standards of products. However, a special parameter could not be determined.

Accordingly, this paper forms so-called safety categories used as main driver for modularization. They classify the different standards, guidelines and safety requirements.
Beside the safety categories, the actual impact and importance of functions in respect of the overall functional safety shall be considered. Thus, the module driver safety relevance is introduced. It allows the consideration of for example SIL values or protection classes.

4 Results: safety-oriented MFD (sMFD)

The method adaptions described above result in the safety-oriented MFD. It comprises the steps visualized in Figure 2. In general, the method consists of the following three different tasks:

- Determine the functional dependencies
- Analyse the functional centralities
- Identify safety aspects and conduct modularization

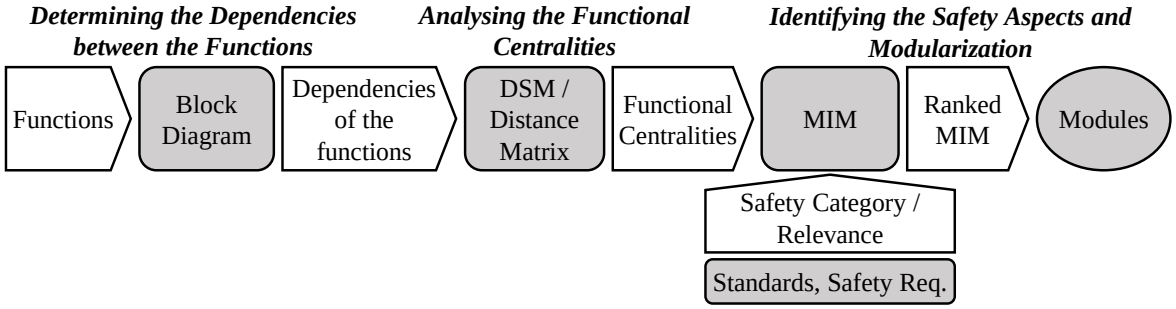

Figure 2. Steps of the safety-oriented Modularization Method.

First, the customer-relevant functions are modelled in a block diagram and their dependencies are identified based on flows. Using this functional structure, the network centralities of functions are computed. Therefore, a DSM and distance matrix are used as well as the number of direct and indirect dependencies. This information is needed during the formation of modules. The modularization also considers the defined safety categories and safety relevance. Thus, these parameters have to be defined. Then, the safety-oriented module drivers are mapped to functions in the MIM and the functions are evaluated. The resulting scores are used to unveil the safety criticality of a function and to group functions with a similar or identical influence of the safety-oriented module drivers. From these groups, modules are derived considering the functional dependencies obtained from the DSM and the optimal number of modules.

4.1 Determine the functional dependencies

The first task determines the functional dependencies within the product. Therefore, the product functions are defined. This can be done according to existing functional models or a Quality Function Deployment (QFD). The aim is to convert the functions into a structure which represents their dependencies. Consequently, the sMFD suggests transferring the functions into a block diagram. Similar to Stone et al. (2000), the structure can result from material and information flows. An abstract example therefore is shown in Figure 3. This step also increases the understanding of the system and supports the identification of critical elements.
In summary, this step prepares the modularization by an analysis of the dependencies between elements and their links. The block diagram is basis of the DSM created in the next task.

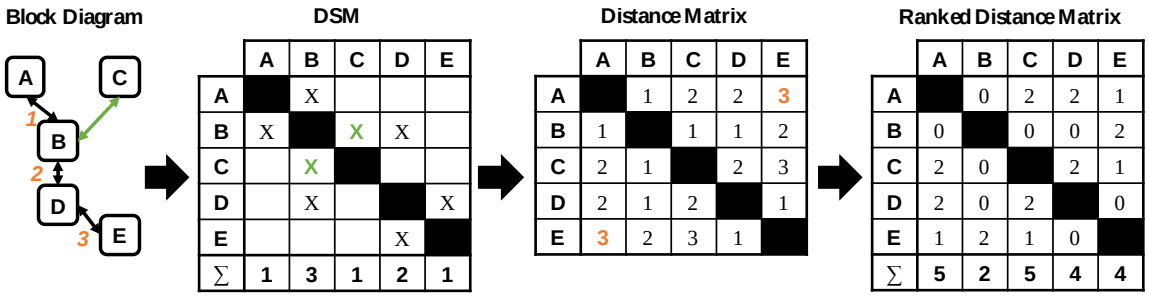

Figure 3. Tasks to determine the functional centralities.

4.2 Analyse the functional centralities

The second task analyses the centralities of functions in the functional structure. Therefore, the block diagram is transferred into a DSM. The sMFD suggests to create a symmetrical DSM by interpreting interactions always as bidirectional. The centrality can then be computed from the number of direct and indirect dependencies. The direct dependencies can be obtained from the active or passive sums of the DSM elements. In Figure 3 the dependency between *B* and *C* is highlighted as an example. *B* has three direct relations and is thus, highly interlinked.
The determination of the indirect relations is conducted and documented distance matrix that identifies the shortest connections between two elements (Lindemann et al., 2008). The example in Figure 3 visualizes *Function A* and *Function E* which have a distance of three. The distance matrix is then transformed into a ranked distance matrix. It computes a weighted passive or active sum of the elements. The shortest distance (usually 2) is considered with the highest score, relations that are more distant are considered less. The example in Figure 3 indicates *A* and *C* with the highest sum of indirect dependencies. Hence, the ranked distance matrix and its weighted sums are an indicator for the global centrality of a function. Combined with the regular DSM (direct dependencies), the functional centrality can be evaluated.

4.3 Identify safety aspects and conduct modularization

The third and last task identifies the relevant safety aspects and conducts the modularization. First, the safety-oriented module drivers are defined. They represent drivers or reasons which might from a safety perspective lead to modules. The sMFD suggests the following types of safety-oriented module drivers: safety relevance, functional centrality and safety category.
These module drivers provide information on the importance of a function in terms of safety. Moreover, the categories describe the quality of the safety aspects of a function, which is a main influence on the composition of modules. In a resulting safety-oriented modularization, a changed specific regulation affects only few module and redesign efforts thus, are reduced.
The module driver *safety relevance* is a general indicator for the importance of a function. For instance, the functions ensuring emergency brake capabilities have a great significance and shall thus be assigned to a high safety relevance. If other indicators like the SIL or the protection class exist, they can be incorporated. However, especially in early stages the assessment of the safety relevance can be challenging. Experience from previous products or expert knowledge can therefore provide support. This evaluation moreover emphasizes the safety impact of functions and can contribute to close the gap between safety and design. Yet, safety relevance is not directly responsible for the composition of the modules, but provides information about the importance of a function concerning safety aspects.
The module driver *system dependency* also is not included in the sMFD as direct module driver. It evaluates functions in terms of their centrality in the system. Derived from the DSM,

this metric can be transferred into the MIM. There, functions with high centrality values indicate functions with many interfaces, which have to be considered during modularization.
The module driver *safety category* represents the safety requirements of the product. They are the main driver for the composition of modules. Similar safety requirements lead to similar solutions, testing procedures or documentation requirements. Thus, from a safety perspective functions with comparable safety requirements should be clustered to modules in order to reduce efforts, complexity and costs connected to safety aspects. As the actual types of safety requirements and their impact vary, the module driver safety category is flexible and has to be adapted to the specific product and situation. Therefore, as described before, for example standards, guidelines and safety requirements are classified into categories.
To prepare the modularization, the impact of a module driver (i.e. safety category) on a function is assessed in the safety-oriented MIM (sMIM). By summing up the scores of a function, the safety-criticality can be estimated. Starting from the most safety-critical function, the elements in the sMIM are clustered. Then, functions with similar influence of the safety category are grouped. Figure 4 illustrates this clustering for a coffee machine. There, similar functions are marked in one colour. The elements with a high safety criticality are considered as module candidates. They can be supplemented by similar functions with a lower safety criticality to define a module. Thereby, aligning with Ericsson and Erixon (1999), the suitable number of modules is approximately the square root of the elements.
In case of uncertain decisions, the functional dependencies from the DSM can provide support: Modules with a smaller number of interfaces should be favoured. It should also be ensured that the safety criticality is not too high within a module to avoid unmanageable complexity.

Module Driver \ Function		grind beans	setting level	provide beans	amount of beans	amount of powder	collect powder	compress powder	heating water	brew up coffee	forward coffee	remove grounds	hand out coffee	light outlet	hand out milk	hand out steam	evaporate water	generate pressure	fasten components	protect risky parts	allwo maintanance	warm cups	absorb liquid	get information	enable standing	protect short-circuit	branch electricity
Safety Relevance	importance	3		1	1	1	1	3	3	3	3	1	9		3	1	1	1	3	1					3	1	3
Functional Centrality	direct dependencies	3	1	1	1	1	1	3	3	3			1	1	1	1	3	3	3	9	3	1	1		3	3	1
	indirect dep.	1	1	1	3	1	1	1	1	3				1	3	3	1	1	1	1	1	9				9	9
Safety Category	electronics	3			1	1		3	3	1				1			3	1				3				3	3
	warming	1						1	3	9	3		3		3	3	9	3				1					
	moisture	1							1	1	1		1		1	1	1		3	3			1		3	3	3
	stability	9		1			1	3			1		1		1	1		1	3	3	3		1		9		
	assembling	3						1	1	1							1	1	3	3	1	1			3		
	leakage of materials								1	3	1		1		3	3	3	1									
	pressure							1		1						1	1	3									
	Sum	24	2	4	6	4	4	16	16	25	9	1	16	3	15	14	23	15	16	20	8	15	3	0	21	19	19
	Module Candidates	X								X																	

Figure 4. Extract of a clustered sMIM.

This step finalizes the safety-oriented modularization. The selection and definition of modules from a safety perspective has to be documented in a comprehensible form. Thus, input which can be compared and balanced with modularizations driven from other aspects can be provided. This allows the identification of contradictions and the evaluation of trade-offs.

5 Case studies and method evaluation

The sMFD method was evaluated within two different industrial examples. First, the approach was applied to a fully automated coffee machine. The aim of this example is to test the general applicability of the method. The second example is a safety-critical brake system. In this way, the method can be evaluated on a system which has to fulfil strict safety requirements.

The fully automated **coffee machine** was decomposed into fifty sub-functions and a functional structure was created. There, material flows of the water, the beans and the milk as well as energy flows were identified. This structure elicited the functions “brew up coffee” and “distribute coffee” as central functions. Moreover, “brew up coffee” and “foam milk” are the elements with the highest level of crosslinking. Regarding indirect dependencies, the functions involved in the energy supply are most critical. According to regulations (i.e. DIN 60335-1) and the resulting safety requirements, the following safety categories have been identified: electronics, warming, moisture, stability, assembly, leakage of materials and pressure.
Based on these safety categories, the assessment of the functions was conducted in the sMIM. Starting point of the module definition were functions with the highest scores like “process control settings”. Other elements with a similar evaluation (e.g. “process electronic signal”) were added to the modules. The application to all module candidates, lead to eight modules.
The resulting modules were discussed with the safety and approval expert of the manufacturing company. His judgement was that the definition of modules from a safety point of view is reasonable. The resulting modules are similar to the current modules. According to the expert, the reason lies in different impacts like make-or-buy decisions and design or assembly aspects. Yet, during development, the company tries to establish a machine core to reduce safety and approval efforts. The core is similar to the most critical modules identified by the sMFD.
In the second study, the sMDF is applied to a **brake system** for rail vehicles. A safety-oriented modularization could help to efficiently confirm to the regulations, which strongly vary and evolve in each country or region. In the case, the brake cylinder pressure control subsystem (BCC) is considered. Its task is to monitor and control the brake cylinder pressure to generate the necessary brake force. Due to high speeds and masses, rail braking systems have to fulfil strict and severe regulations in terms of reliability and safety. Especially the IEC 62425 increases the requirements by adding functional safety.
First, the functional dependencies of the BCC subsystem were determined and modelled in a DSM. It identified the functions “control pressure” and “supply air” as most central. Moreover, five safety categories were identified. This was achieved by incorporating major safety functions or features of the whole braking system.
Applying the sMIM, the functions "store brake energy", "control pre-control pressure" and "amplify pre-control pressure" showed the highest safety relevance. The assessment and module definition in the sMIM established seven modules. This modularization reduced the number of safety aspects which have to be considered within the single modules.
The results differ from the actual functional modularization. The differences were discussed with a very experienced specialist concerned with safety. He emphasized the need of safety-oriented architectures to reduce safety efforts and thinks the sMFD therefore provides a first important support. Even though the considered system was very small, he rates the module concept as reasonable from a safety perspective. Yet, he notes that a more global analysis might be needed to consider all relevant aspects and achieve an optimal modularization.

6 Conclusions

This paper develops and evaluates a method for the safety-oriented modularization. It is derived and adapted from existing modularization methods. The focus of the adaption is the inclusion of safety aspects in the modularization. The resulting sMFD method roughly is based on the Modular Function Deployment and supports both, the integration of safety aspects in modularization and the development of safety-oriented product architectures.

However, the evaluation in two case studies also shows some limitations. First, it has to be mentioned, that safety is not the sole driver for modularization. The resulting modules need to be balanced with modules obtained following other modularization drivers (e.g. assembly, supply chain or functional dependencies). Yet, it still helps to raise awareness for the safety aspects and helps to incorporate them in the final module decision. This contributes to more suitable product architectures and reduced efforts for safety analyses. Therefore, future research has to search for methods which help to balance different module proposals and to quantify advantages or disadvantages in order to improve connected trade-off analyses.
Second, the case studies show differences in the safety categories considered within the sMIM. In both cases, they were defined depending on the experience and knowledge of the involved experts and authors. In order to enable a simple application of the sMFD, further support to identify and define the relevant safety categories needs to be developed. This would enable to find the categories which help to reduce safety efforts more efficient.
Lastly, the second case study shows the importance of the right and suitable system boundary. Only if it is chosen correctly, the global aspects of functional safety can be sufficiently incorporated in the sMFD method. This means, that future work will have to provide support to choose the boundaries correctly and to handle global safety aspects.

Citations and References

Agard, B., & Bassetto, S. (2013). Modular design of product families for quality and cost. *International Journal of Production Research*, *51*(6), 1648–1667.

Aguwa, C. C., Monplaisir, L., & Sylajakumari, P. A. (2012). Rules modification on a Fuzzy-based modular architecture for medical device design and development. *IIE Transactions on Healthcare Systems Engineering*, *2*(1), 50–61.

Bernard, A., & Hasan, R. (2002). Working situation model for safety integration during design phase. *CIRP Annals - Manufacturing Technology*, *51*(1), 119–122.

Berres, A., Schumann, H., & Spangenberg, H. (2014). *European survey on safety methods application in aeronautic systems engineering*. ESREL Conference 2014, Worclaw, Poland.

Bishop, P., & Bloomfield, R. (1998). A Methodology for Safety Case Development. In F. Redmill & T. Anderson (Eds.), *Industrial perspectives of safety-critical systems. Proceedings of the sixth Safety-Critical Systems Symposium, Birmingham, 1998* (pp. 194–203). London, New York: Springer.

Blees, C. (2011). *Eine Methode zur Entwicklung modularer Produktfamilien* (1. Aufl). *Hamburger Schriftenreihe Produktentwicklung und Konstruktionstechnik: Bd. 3*. Hamburg: TuTech.

Cuenot, P., Ainhauser, C., Adler, N., Otten, S., & Meurville, F. (2014). *Applying Model Based Techniques for Early Safety Evaluation of an Automotive Architecture in Compliance with the ISO 26262 Standard*. ERTS 2014 : Embedded Real Time Software and Systems, Toulouse.

Daniilidis, C., Enßlin, V., Eben, K., & Lindemann, U. (2011). A Classification Framework for Product Modularization Methods. In S. Culley (Ed.), *18th International Conference on Engineering Design (ICED'11)* (pp. 400–409). Glasgow: Design Society.

Daniilidis, C., Hellenbrand, D., Bauer, W., & Lindemann, U. (2011). Using structural complexity management for design process driven modularization. In IEEE (Ed.), *2011 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 595–599). Piscataway: IEEE.

Ericsson, A., & Erixon, G. (1999). *Controlling design variants: Modular product platforms*. Dearborn, MI: Society of Manufacturing Engineers.

Ghemraoui, R., Mathieu, L., & Tricot, N. (2009). Design method for systematic safety integration. *CIRP Annals - Manufacturing Technology*, *58*(1), 161–164.

Hatamura, Y., Hattori, K., & Hatamura, T. (2006). The Mind Process of Design Learned from the Revolving Door Accident. *CIRP Annals - Manufacturing Technology*, *55*(1), 155–160.

Hollnagel, E. (2008). Risk+barriers=safety? *Safety Science*, *46*(2), 221–229.

Holtta, K. M. M., & Salonen, M. P. (2003). Comparing Three Different Modularity Methods. In ASME (Ed.), *ASME 2003 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference* (pp. 533–541).

Koeppen, B. (2008). *Modularisierung komplexer Produkte anhand technischer und betriebswirtchaftlicher Komponentenkopplungen*. *Produktentwicklung*. Aachen: Shaker-Verl.

Koppenhagen, F. (2014). Modulare Produktarchitekturen – Komplexitätsmanagement in der frühen Phase der Produktentwicklung. In K.-P. Schoeneberg (Ed.), *Komplexitätsmanagement in Unternehmen. Herausforderungen im Umgang mit Dynamik, Unsicherheit und Komplexität meistern* (pp. 113–162). Wiesbaden: Springer.

Leveson, N. (2012). *Engineering a safer world: Systems thinking applied to safety*. Cambridge: The MIT Press.

Lindemann, U., Maurer, M. S., & Braun, T. (2008). *Structural Complexity Management*. Berlin: Springer.

Martin, M. V., & Ishii, K. (2002). Design for variety: developing standardized and modularized product platform architectures. *Research in Engineering Design*, *13*(4), 213–235.

Nepal, B., Monplaisir, L., & Singh, N. (2006). A methodology for integrating design for quality in modular product design. *Journal of Engineering Design*, *17*(5), 387–409.

Papadopoulos, Y., McDermid, J., Sasse, R., & Heiner, G. (2001). Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure. *Reliability Engineering & System Safety*, *71*(3), 229–247.

Pimmler, T. U., & Eppinger, S. D. (1994). Integration Analysis of Product Decompositions. In ASME (Ed.), *Proceedings of the 1994 ASME Design Theory and Methodology Conference*. ASME.

Roth, M., Gehrlicher, S., & Lindemann, U. (2015). Safety of Individual Products - Perspectives in the Context of Current Practices and Challenges. In C. Weber, S. Husung, G. Cascini, M. Cantamessa, D. Marjanovic, & M. Bordegoni (Eds.): *Vol. 3. Proceedings of the 20th International Conference on Engineering Design (ICED 15), Design Organisation and Management* (pp. 113–122). Glasgow: Design Society.

Sierla, S., Tumer, I. Y., Papakonstantinou, N., Koskinen, K., & Jensen, D. (2012). Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework. *Mechatronics*, *22*(2), 137–151.

Stone, R. B., Wood, K. L., & Crawford, R. H. (2000). A heuristic method for identifying modules for product architectures. *Design Studies*, *21*(1), 5–31.