TECHNISCHE UNIVERSITÄT MÜNCHEN
Fakultät für Maschinenwesen
Lehrstuhl für Produktentwicklung

Efficient Safety Method Kit for User-driven Customization

Michael Roth

Vollständiger Abdruck der von der Fakultät für Maschinenwesen der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender:	Prof. Dr.-Ing. Johannes Fottner
Prüfende der Dissertation:	1. Prof. Dr.-Ing. Udo Lindemann
	2. Prof. P. John Clarkson, Ph.D.
	3. Prof. Dr.-Ing. Birgit Vogel-Heuser

Die Dissertation wurde am 14.11.2016 bei der Technischen Universität München eingereicht und durch die Fakultät für Maschinenwesen am 31.05.2017 angenommen.

for all those who left too early

FOREWORD OF THE EDITOR

Problem

Successful products meet the needs of their customers and users. Since the industrial mass production introduced uniform mass products, the actual customer needs moved to the central focus of product development activities. Mass customization, which for example is widely applied in the European automobile industry, was one important step in this direction. Nevertheless, the industry and research strive to further increase the levels of customer integration and customization. Applications of Open Innovation show that an integration of users in the product development process can be highly beneficial and can for example improve the elicitation of user requirements. This is used in new concepts like user-driven customization to better fulfill the individual user needs. On the other side, increased customization implies increased variety and complexity; a challenge many companies are struggling with. The increasing number and strictness of safety requirements adds further complexity. The existing methods from the fields of mass customization and safety analysis provide various methods and tools. However, they are primarily tailored to closed product development processes. Consequently, their applicability in open product development and their compliance with intensive user integration, which user-driven customization realizes, are limited. Approaches, are missing, which combine the established methods with new forms of user integration to enable the industry to successfully realize new forms of individual products with user-driven customization.

Objectives

The objective of this thesis is to integrate safety analysis and customization to enable an efficient realization of user-driven customization. It therefore addresses the interface between the fields of user integration, mass customization, and safety analysis. The aim is to research and provide a framework and set of methods, which support product developers in managing the connected complexity, for both, the preparation of a product for user-driven customization as well as the efficient safety analysis of the resulting individual products.

Results

The major result of this thesis is the so-called efficient safety method kit for user-driven customization. It provides a framework and a set of methods and tools, which both aim to improve the efficiency of the safety analysis of user-driven customization products. During its development, the thesis researches the field of user-driven customization and identifies the implications of user-driven customization on the development process together with connected challenges. This thesis adopts the challenges connected to safety analysis and the state of science in the fields of safety analysis and customizations to develop the common framework behind the methods of the efficient safety method kit. It represents a meta-model with an exemplary implementation, which unite the relevant entities and relations of the two fields in a model-based format. Within this framework, the thesis adapts existing and develops new methods to provide a set of twelve support methods, which tackle the identified specific challenges and tasks along the development process of user-driven customization products. The methods are developed as independent but compliant methods and they can be applied and adapted based on the specific situation. Suggestions for alternative methods, which might be better suited in some situations supplement the methods of the efficient safety method kit. The validation in three evaluation cases shows that the efficient safety method kit contributes to enabling user-driven customization by successfully improving the efficiency of the safety analysis in this setting. Especially the required experience and familiarization for developers are reduced. Yet, high quality and up-to date models are the prerequisite for a successful application of the methods.

Conclusions for Industrial Applications

For industrial application, especially the individual methods of the efficient safety method kit and their broad applicability is a valuable contribution. As the methods are independent, they can be applied in different contexts and situations. This supports the cautious introduction within existing structures and organizations. In addition, the framework and methods are easy to adapt, which supports their transfer to related fields and applications in the industrial context. Many of the methods are suitable to create awareness for safety aspects within many areas of product development. This will support and foster the development of safe and successful products. Moreover, the methods explicate safety knowledge and by that facilitate the documentation and management of this expert knowledge. This reduces the risks connected to implicit knowledge and simplifies the integration and familiarization of less experienced engineers. Besides improving the efficiency of safety analysis, this effect can be beneficial for other fields like requirements engineering or complexity management as well. Hence, the efficient safety method kit not only enables improved user integration and customization, it also can improve the integration and change management within companies.

Conclusions for Scientific Researchers

From a research perspective, this thesis introduces and researches the concept of user-driven customization. This concept has the potential to improve mass customization and user integration hand in hand. The conducted survey shows the implications of this concept on the development process and the need for an improved integration of development processes. Moreover, the framework and the methods underline the benefits of model-based analyses and their automation by rule-based algorithms. The methods, especially the pattern-based model verification strongly contribute to an improvement model quality. This insights can be used to improve the models applied in research as well as they are a starting point for further automatic verification methods an integration with model-checking approaches.

Garching, November 2017

Prof. Dr.-Ing. Udo Lindemann

Lehrstuhl für Produktentwicklung
Technische Universität München

ACKNOWLEDGEMENTS

This work would not have been possible without the valuable support of various persons, their thoughts, time, trust, and encouragement. My thank goes to all those, who in the following cannot be mentioned specifically.

The first and foremost thank goes to my supervisor Prof. Udo Lindemann. He not only supported my research. Rather, he created an environment rich of opportunities and freedom at the Institute of Product Development. I met brilliant researchers and great persons and had the privilege to gather many unique and valuable experiences.

One of these persons is Prof. Paul John Clarkson, to whom I am obliged for taking the role as second examiner. His feedback and guidance helped to shape this thesis and strongly contributed to the quality of the results. Also, I want to thank Prof. Birgit Vogel-Heuser for engaging as third examiner and Prof. Fottner for accepting the chair of the examination board.

The evolution of this thesis was not a straight journey. On this path, it was good to have a mentor to rely on. Hence, I have to express my deepest gratitude to Thomas Kipp. He provided constructive criticism when I was too confident and encouragement when I was too skeptical.

The constructive environment at the institute was also shaped by my colleagues. I especially thank Daniel Kasperek and the InnoCyFer-team for the great moments in our projects. My office partners Constantin and Julian who created an inspiring atmosphere. Further thanks goes to the members of our "Diss-Group" Nepomuk, Sebastian, Christopher, and the two Daniels. I also thank Robert Weiss, Katja Zajcek, Edit Marquard, and Michael Riedl for their support in administration and the small everyday problems.

I also have to express my gratitude to colleagues from industry. I especially want to point out Josef Ponn, Heiko Gremel, Andreas Aigner, and Therese Brantsved. I thank the team of Soley who provided fast support during the implementation. In addition, I owe my gratitude to all students who contributed by working under my supervision. It would be too much to name them all, but I want to point out Felix Gantenbein, Melanie Hensel, Lisa Mayr, and Matthias Naubert.

Besides work, there is always another side in life: I have to thank all my friends, for their trust, their encouragement and their unrestricted support. Here, the "Kieferngarten-Stammtisch" deserves a special mentioning. Furthermore, I thank the proofreaders together with Landon Reitz and the TUM language center, who coached my English.

Last but not least, my deepest gratitude goes to my family. Kristin showed enormous patience withstanding my ups and downs during writing and helped me to find mental balance. My parents provided me unlimited and extraordinary support. They taught me the importance of education, the passion for engineering, and made it possible to catch opportunities, which allowed me to grow as a person as well as to collect so many valuable and unique experiences.

Garching, November 2017 Michael Roth

PRIOR PUBLICATIONS

The following publications are part of the work presented in this thesis (chronological order):

Roth, M., Kasperek, D., & Lindemann, U. (2013). Functional Analysis and Modeling of Complex, Evolutionary Grown, Mechatronic Products. In IEEE (Ed.), 2013 IEEE International Conference on Industrial Engineering and Engineering Management (pp. 346–350). Piscataway: IEEE. doi:10.1109/IEEM.2013.6962431

Becerril, L., Kasperek, D., Roth, M., & Lindemann, U. (2014). Visualization of Interdisciplinary Functional Relations in Complex Systems. In D. Marjanović, M. Storga, N. Pavković, & N. Bojcetić (Eds.), Proceedings of the DESIGN 2014 13th International Design Conference (pp. 1239–1248). Glasgow: Design Society.

Holle, M., Roth, M., Gürtler, M. R., & Lindemann, U. (2014). From Customer Innovations to Manufactured Products: A Project Outlook. International Journal of Mechanical, Aerospace, Industrial and Mechatronics Engineering, 8(4), 1078–1082.

Michailidou, I., Roth, M., & Lindemann, U. (2014). From Learning to Experiencing Principles of Engineering Design at the TUM. In E. Bohemia, A. Eger, W. Eggink, A. Kovačević, B. Parkinson, & W. Wits (Eds.), Design education & human technology relations. Proceedings of the 16th International Conference on Engineering and Product Design Education (pp. 354–359). Glasgow: Design Society.

Roth, M., Kasperek, D., & Lindemann, U. (2014). Identifying the Adequate Level of Abstraction Within Structural Modeling. In IEEE (Ed.), 2014 IEEE International Systems Conference (SysCon 2014) Proceedings (pp. 301–308). Piscataway: IEEE. doi:10.1109/SysCon.2014.6819273

Roth, M., Kasperek, D., & Lindemann, U. (2014). Verifying the Abstraction Level of Structural Models. Procedia Computer Science, 28, 497–504. doi:10.1016/j.procs.2014.03.061

Roth, M., Scholz, S., Gövert, K., Kasperek, D., Lozano, C., Mund, H., & Lindemann, U. (2014). Standardisierungskonzept für Kleinserien im Maschinen- und Anlagenbau. In M. S. Maurer & S.-O. Schulze (Eds.), Tag des Systems Engineering (pp. 361–370). München: Carl Hanser.

Bauer, W., Elezi, F., Roth, M., & Maurer, M. S. (2015). Determination of the required product platform flexibility from a change perspective. In IEEE (Ed.), 9th Annual IEEE International Systems Conference (SysCon 2015) (pp. 20–26). Piscataway: IEEE. doi:10.1109/SYSCON.2015.7116723

Kasperek, D., Roth, M., Lozano, C., & Lindemann, U. (2015). Ein Leitfaden zur marktorientierten top-down Modularisierung im Maschinen- und Anlagenbau. In S.-O. Schulze & C. Muggeo (Eds.), Tag des Systems Engineering (pp. 377–386). München: Carl Hanser.

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. Marjanović, & 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.

Roth, M., Gürtler, M. R., & Lindemann, U. (2015). Identifying and Utilizing Technological Synergies—A Methodological Framework. In A. Chakrabarti (Ed.), ICoRD'15 – Research into Design Across Boundaries Volume 1: Theory, Research Methodology, Aesthetics, Human factors and Education (Vol. 2, pp. 291–302). Springer India.

Roth, M., Harmeling, J., Michailidou, I., & Lindemann, U. (2015). The "Ideal" User Innovation Toolkit - Benchmarking and Concept Development. In C. Weber, S. Husung, G. Cascini, M. Cantamessa, D. Marjanović, & M. Bordegoni (Eds.): Vol. 9. Proceedings of the 20th International Conference on Engineering Design (ICED 15), User-centred design, design of socio-technical systems (pp. 249–260). Glasgow: Design Society.

Roth, M., Kronfeldner, L., Kasperek, D., & Lindemann, U. (2015). A Framework to Assess the Cost Impact of Organization and Processes in Complex Systems. In S.-O. Schulze & C. Muggeo (Eds.), Tag des Systems Engineering (pp. 217–226). München: Carl Hanser.

Roth, M., Nerb, A., Kasperek, D., & Lindemann, U. (2015). A tool to bridge the gap from functional dependencies to configuration rules translating knowledge on functional restrictions from systems engineers to a configurator for sales and decision makers. In IEEE (Ed.), 9th Annual IEEE International Systems Conference (SysCon 2015) (pp. 158–163). Piscataway: IEEE. doi:10.1109/SYSCON.2015.7116745

Roth, M., Wolf, M., & Lindemann, U. (2015). Integrated Matrix-based Fault Tree Generation and Evaluation. Procedia Computer Science, 44, 599–608. doi:10.1016/j.procs.2015.03.027 Roth, M., Wolf, M., & Lindemann, U. (2015). Integrated Matrix-based Fault Tree Generation and Evaluation. Procedia Computer Science, 44, 599–608. doi:10.1016/j.procs.2015.03.027

Holle, M., Straub, I., Roth, M., & Lindemann, U. (2016). Customer individual product development: Methodology for product architecture modification. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 744–749). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490627

Kohl, M., Roth, M., & Lindemann, U. (2016). Safety-oriented Modular Function Deployment. In C. Boks, J. Sigurjonsson, M. Steinert, C. Vis, & A. Wulvik (Eds.), Proceedings of NordDesign 2016 (Vol. 2, pp. 103–113). Bristol: Design Society.

Maisenbacher, S., Behncke, F. G. H., Roth, M., & Fleckenstein, F. (2016). Integrated Value Engineering – Increasing the value of a forklift subsystem. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 916–921). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490654

Müller, M., Roth, M., & Lindemann, U. (2016). The Hazard Analysis Profile: Linking Safety Analysis and SysML. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 123–129). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490532

Roth, M., Beetzen, C. von, & Lindemann, U. (2016). Matrix-based Multi-hierarchy Fault Tree Generation and Evaluation. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 140–146). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490535

Roth, M., & Gantenbein, F. (2016). Model-based Hazard and Propagation Assessment of Product Changes. In American Society of Mechanical Engineers (ASME) (Ed.), 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Charlotte: American Society of Mechanical Engineers.

Roth, M., Mayr, L., & Lindemann, U. (2016). A Knowledge Framework for Safety Analysis of User-Induced Changes. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 1553–1562). Glasgow: Design Society.

Roth, M., Münzberg, C., & Lindemann, U. (2016). A Method to Explicate Safety Functions. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 463–472). Glasgow: Design Society.

Roth, M., Ulrich, C. M., Holle, M., & Lindemann, U. (2016). The Impact of User-driven Customization on the Development Process. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 1357–1366). Glasgow: Design Society.

List of Student Projects

The following 14 student projects were created in the context of this dissertation project. The author of this work in his role as supervisor defined the tasks and scope of these student projects and gave continuous input to the students. In frequent meetings, the methodology, objectives and results were discussed and coordinated. These projects in chronological order are:

Gehrlicher, S. (2014). Risiko- und Gefährdungsanalyse von individuellen Produkten (Bachelor Thesis). Technical University of Munich, München.

Harmeling, J. (2014). Konzeption von Open Innovation Toolkits für Nutzerinnovation und -Co-Kreation (Bachelor Thesis). Technical University of Munich, München.

Wolf, M. (2014). Integration von Fehleranalyse- und Qualitätsmanagement Methoden in die Strukturmodellierung (Bachelor Thesis). Technical University of Munich, München.

Beetzen, C. von. (2015). Refinement of an Approach to Automatically Generate Fault Trees (Semester Thesis). Technical University of Munich, München.

Isemann, M. (2015). Optimierung der FMEA für individualisierbare Produkte durch Model-Based Systems Engineering (Semester Thesis). Technical University of Munich, München.

Kohl, M. (2015). Berücksichtigung sicherheitsrelevanter Aspekte in der Modularisierung (Bachelor Thesis). Technical University of Munich, München.

Müller, M. (2015). Sicherheitsanalyse von Architekturkonzepten durch Verbindung von SysML und Fehleranalysemethoden (Master Thesis). Technical University of Munich, München.

Rapp, M. A. (2015). Entwicklung einer Methodik zur Identifikation, Validierung und durchgängigen Dokumentation von Sicherheitsanforderungen (Semester Thesis). Technical University of Munich, München.

Ulrich, C. M. (2015). Auswirkungen der kundenbezogenen Produktindividualisierung auf den Entwicklungsprozess technischer Produkte (Master Thesis). Technical University of Munich, München.

Bermond, L. (2016). Validierung und Optimierung des Anforderungsmanagementprozesses bei BMW-Motorrad (Master Thesis). Technical University of Munich, München.

Cakir, I. (2016). Visualization and Assessment of Elements in Fault Trees (Semester Thesis). Technical University of Munich, München.

Gantenbein, F. (2016). Modellbasierte Auswertungsmethodik zur Gefahrenabsicherung bei Produktindividualisierungen (Semester Thesis). Technical University of Munich, München.

Kowalski, S. (2016). Effektchecklisten für die Produktindividualisierung (Semester Thesis). Technical University of Munich, München.

Schürmann, J. (2016). Pattern-Based Validation of Product Models (Master Thesis). Technical University of Munich, München.

CONTENTS

LIST OF ABBREVIATIONS

ACT	activity diagram
BDD	block definition diagram
BoM	bill of material
BSH	BSH Hausgeräte GmbH
C&CM	Contact Channel Model
CAD	computer-aided design
C-FAR	Change Favorable Representation
CPM	Change Prediction Method
D	detection (during the FMEA)
DfV	Design for Variety
DfX	Design for X
DMM	Domain Mapping Matrix
DRM	Design Research Methodology
DS	Descriptive Study
DSM	Design Structure Matrix
ECM	engineering change management
ESMK	Efficient Safety Method Kit for User-driven Customization
ETA	Event Tree Analysis
EU	European Union
FBS	Function Behavior Structure
FH	Function Heuristics
FMECA	Failure Mode, Effects and Criticality Analysis
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
FFIP	Functional Failure Identification and Propagation Framework
HDMDM	hierarchical decomposition MDM
HiP-HOPS	Hierarchically Performed Hazard Origin and Propagation Studies
HoQ	House of Quality

IBD	internal block diagram
MATChEMIB	mechanical, acoustic, thermal, chemical, electric and magnetic, intermolecular, and biological fields
MBHPA	model-based hazard and propagation assessment
MCS	minimal cut set
MDM	Multiple-domain Matrix
MFD	Modular Function Deployment
MHFTA	multi-hierarchy fault tree generation and evaluation
MIM	module indication matrix
O	occurrence (during the FMEA)
OEM	original equipment manufacturer
OI	Open Innovation
PS	Prescriptive Study
QFD	Quality Function Deployment
R&D	Research and Development
RC	Research Clarification
REQ	requirements diagram
REQ1	requirement no. 1 (defined in this thesis)
RPN	risk priority number (during the FMEA)
RVTM	requirements verification and traceability matrix
S	severity (during the FMEA)
SIL	safety integrity level
sMFD	safety-oriented Modular Function Deployment
STEP	STandard for the Exchange of Product model data
SysML	Systems Modeling Language
TRIZ	theory of inventive problem solving
UC	use case diagram
UDC	User-driven Customization
VBA	Visual Basic for Applications
XML	Extensible Markup Language

1. Introduction

"Any customer can have a car painted any color that he wants so long as it is black."

(Henry Ford, entrepreneur 1909)

"Ask your customers to be part of the solution, and don't view them as part of the problem."

(Alan Weiss, author and consultant 2016)

1.1 Initial Situation

More than a century separates the two quotes above. Even though they express completely different attitudes, both authors have been and still are prominent and successful individuals of their time. Thus, the markets and the society changed drastically.

Globalization and digitalization in the current situation strongly influence the markets. These influences lead to a more global and more severe competition (Baumberger, 2007, p. 32; Hildebrand, 1997, p. 18; Piller, 2006, pp. 51–53). To remain competitive in this environment, manufacturers are forced to aspire to fully satisfying the customer needs (Piller, 2006, p. 52).

However, these needs also change due to developments and trends in society and technology. During the last decades, the surplus of goods has been leading to a spirit of post-materialism and self-actualization. Thus, the values of many customers are shifted and they expect **products fully satisfying their individual needs** (Inglehart, Basanez, & Moreno, 2010, pp. 34–36; Piller, 2006, p. 44; Schenk, Müller, & Wirth, 2014, p. 15).

Manufacturers have reacted to these demands during the last decades with the concept of mass customization. They provide a large bandwidth of variants connected with configuration options to achieve a perceived customization through the customers by simultaneously realizing an efficiency close to mass production (Piller & Stotko, 2003, p. 21).

These configuration options are predefined in early phases of the development process in the tension between customer needs and internal or external restrictions (Baumberger, 2007, p. 2007; Piller, Moeslein, & Stotko, 2004, p. 443). Hence, it is necessary to elicit and define the individual customer requirements first. This task is challenging due to the large number of different customers and the partial implicit character of the individual customer needs (Franke & Hippel, 2003, pp. 1199–1200; Hippel, 2001, p. 247). The efforts and costs connected to these challenges are accordingly described as the so-called "sticky information transfer costs" (Hippel & Katz, 2002, p. 824).

To successfully define product variants and configuration options in the early phases of development, the identified customer needs and derived requirements have to be balanced with **existing restrictions**. As described above, these restrictions may result from various internal sources, like quality, manufacturing, and logistical restrictions, as well as from external sources, like legislative, economic, and environmental restrictions (Lindemann, 2005, p. 357; Piller et al., 2004, p. 438).

An essential aspect of these restrictions is to **ensure product safety**. The analysis and assurance of safety are crucial and prerequisite for the approval and the market launch of products. In addition to the previously described developments in markets and society, safety regulations are getting stricter and more rigorous (Mhenni, Choley, & Nguyen, 2014, p. 378; Roth, Gehrlicher, & Lindemann, 2015, p. 121; Stirgwolt, 2013, p. 1).

However, not only the stricter regulations, but also the increasing complexity of products and processes challenges safety analysis and assurance. Examples of this are increasing requirements, a greater amount of involved parties, globalization as well as technological evolution. Moreover, impacts of customization like increasing product diversity and decreasing badge sizes induce further product complexity (Danilovic & Browning, 2007, p. 2007; Lindemann, Maurer, & Braun, 2008, pp. 4–5).

The stricter safety restrictions together with complexity induce additional challenges to safety analysis and assurance. However, researchers criticize that despite these developments, the methods of safety analysis did not evolve (Leveson, 2012, p. xvii). Hence, large manual efforts are required to analyze and ensure the product's safety (Majdara & Wakabayashi, 2009, p. 1076; Maurer & Kesper, 2011, pp. 180–181). These developments as a consequence impose further restrictions to the efficient realization of customized products (Jiang, Liang, Ding, & Wang, 2007, p. 1156).

Thus, on the one hand the complexity and restrictions emerging from product development, especially product safety, result in challenges and restrictions for efficient customization. On the other hand, new manufacturing technologies **resolve some restrictions in production**. While mass customization strives to achieve competitive customized products through mass production and assembly lines, new manufacturing technologies like flexible manufacturing systems and additive manufacturing technologies provide additional degrees of freedom (Blecker, Abdelkafi, Kaluza, & Kreutler, 2004, p. 900; Gibson, Rosen, & Stucker, 2015, pp. 1–3; Lachmayer, Gembarski, Gottwald, & Lippert, 2015).

Flexible manufacturing systems anticipate product varieties through built-in flexibility. They are able to realize a production of customized products to a certain extent and provide agility (ElMaraghy, 2005, pp. 261–262). While these flexible manufacturing systems rely on traditional manufacturing technologies, additive manufacturing offers new possibilities. Additive manufacturing directly fabricates products layer-wise from a three-dimensional computer-aided design (CAD) model. It thus renders process planning unnecessary by providing flexibility in shape and material (Gibson et al., 2015, p. 2).

In summary, the increasing diversity, flexibility, and aspiration level of the markets characterize the current situation. Increasing restrictions, especially from the field of product safety oppose these trends. While new manufacturing technologies resolve restrictions from production perspective, the **safety analysis** in product development due to increasing complexity and stricter regulations becomes a **bottleneck for efficient and successful customization**.

1.2 Problem Description

Methods of Open Innovation (OI) are one solution to react on the diversity of individual customer needs and to reduce the previously described sticky information transaction costs (Franke & Hippel, 2003, p. 1200; Hippel & Katz, 2002, p. 823). Their basic idea is to divide the product development into smaller tasks and use external knowledge to solve them (Hippel & Katz, 2002, p. 823). OI includes methods like user innovation and user co-creation, which directly involve users or customers in the concept and detailed development of products or allow them to create the products for themselves (Franke & Hippel, 2003, p. 1200).

A new type of customization emerges, if this idea is combined with the customization of products: Customers obtain the ability to customize the product on their own according to their individual needs. This thesis defines this concept as **User-driven Customization** (UDC). It extends traditional mass customization, as the customers are not limited to an individual configuration but can customize their individual product within a theoretically indefinite solution space (see definition in Subsection 2.1.4).

While UDC can help to satisfy the current market needs and reduce the sticky information transaction costs, it induces new challenges. This especially applies for the restrictions described in the previous section and the bottleneck resulting from product safety and complexity.

In UDC, the customization through the user takes place in late phases of the development process and it is not possible to fully anticipate its nature and extend. This situation is similar to a late **change to the product**, which is conducted **by a non-expert**. However, the **non-expert involvement** makes it different from a regular engineering change. This results in the following two major challenges, which in traditional product development are tackled by methods of engineering change management (ECM) (Langer, 2016, p. 520,527).

First, changes to a component or a part of a product can influence or change other parts. This phenomenon is referred to as change propagation. With increasing product complexity, the likeliness of such propagation also increases (Eckert, Clarkson, & Zanker, 2004, p. 1). While ECM in the traditional product development strives to identify, predict, and manage these propagations, users, as non-experts, will not be able to anticipate and manage occurring propagations. Especially the impact on the product safety will be out of their scope.

Second, the late point of time of these changes contradicts the common strategy in product development to reduce the amount of late changes. These late changes and their possible propagations usually lead to higher cost and efforts (Ehrlenspiel, Kiewert, Lindemann, & Mörtl, 2014, p. 14; Jarratt, Eckert, Caldwell, & Clarkson, 2011, p. 110).

Despite these challenges implied by UDC, manufacturers still have to **meet the challenges of safety analysis** described in previous section and ensure the product safety to obtain approval and be able to sell the UDC product on the markets. As described, especially the late non-expert changes potentially lead to propagations, which can have a strong impact on product safety and together with complexity increase the efforts for safety analysis (Mhenni et al., 2014, p. 378; Roth et al., 2015, p. 121).

Moreover, the safety analysis is still dominated by manual tasks, which require high experience and expertise (de la Vara, Jose Luis, Borg, Wnuk, & Moonen, 2016, p. 14). If these tasks have to be conducted for each individual product, the concept of UDC is most likely not capable to compete with mass products.

The previous paragraphs lead to the assumptions that an increased level of UDC causes increased safety efforts, and the diversity caused by individual UDC products leads to increasing cumulative safety efforts. The resulting challenge for manufacturers, which plan to realize UDC, is to keep the increased safety efforts below the benefits obtained through UDC.

To offer products for UDC successfully, manufacturers have to **balance** the gained **customer satisfaction** through customization options with the increased **efforts and costs required,** as visualized in Figure 1-1. This especially applies for efforts to ensure product safety and meet restrictions. To achieve this, customization options and their impact through propagations on product safety have to be anticipated and evaluated. This will allow estimating the caused efforts and costs so that manufacturers will be able to identify suitable customization options in advance. In addition, the efforts to react on the individual changes and analyze their safety impact have to be reduced to increase the total efficiency of UDC and to allow competition with other customization concepts.

1.3 Objectives and Thematic Classification

This thesis aims to contribute to a successful realization of UDC products. It aims to solve the above-described challenges resulting from UDC and to enable manufacturers to balance requested and offered customization options and safety efforts in a way that allows for competitive UDC products. As safety analysis and assurance is one of the most important bottlenecks amongst the restrictions limiting customization options (see Section 1.1), this thesis focuses on safety aspects.

Thus, the main objective of this thesis is a **support to realize and balance UDC products with respect to product safety**. This balancing as illustrated in Figure 1-1 involves two aspects to solve the above-identified challenges.

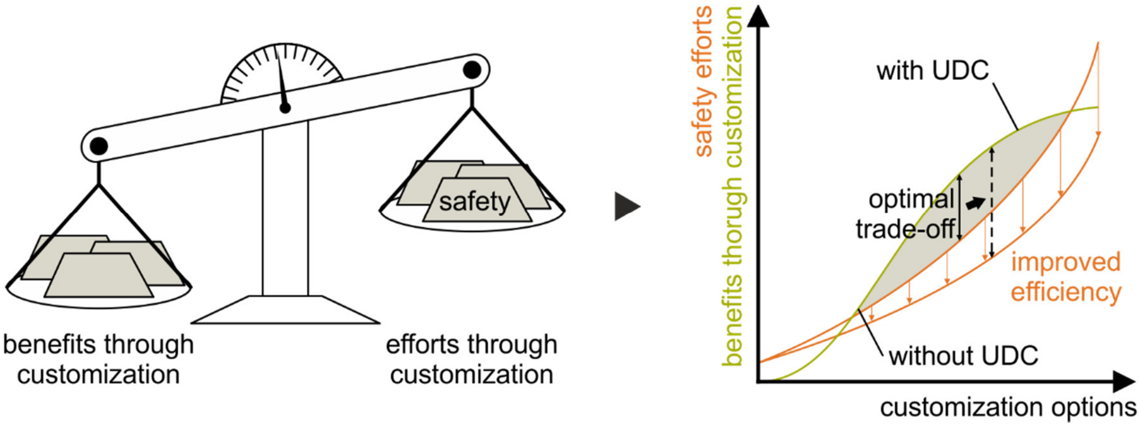


Figure 1-1: The objective of this thesis: balancing customization options and safety efforts and the derived two fields of action

The first aspect is the **evaluation of customization options** with respect to their resulting implications on product safety. This shall allow manufacturers to limit the efforts for safety analysis prior to the customization. In other words, manufacturers shall be enabled to find the optimal trade-off between the dimensions of customization benefits and safety efforts.

The second aspect is the **efficient safety analysis** of the customized products. This shall allow manufacturers to limit the efforts for safety analysis after the customization and shift the optimum. Here, efforts represent every consumption of human resources, time, and costs.

To achieve the above-stated main objective, this thesis defines the following research question:

Which approaches and methods can support the safety analysis of User-driven Customization products in order to reduce the time and resources needed to analyze the safety of each customized product?

The main objective and research question define the overall scope of this thesis. They will be further detailed and translated to requirements on a solution approach in Section 3.4.2 building on the comprehension of the existing situations. In addition, this thesis narrows its focus based on the background of the author and existing related research as follows:

The problem description in Section 1.2 introduces the emerging challenges resulting from a customization through users, who are usually not experts in development and design. A customization through expert designers or expert users might reduce the significance of these challenges. Experts might be able to identify and avoid propagation effects of their changes. Yet, the consideration of non-expert customization represents a worst-case scenario. To address this, this thesis focuses on **technical consumer products** and a **non-expert customization**.

As the users are considered as non-experts, a customization from scratch is not likely. Thus, this thesis assumes that the UDC is conducted starting from a basic product and excludes a greenfield approach. This thesis and its developed support aim at existing products and their **transfer to UDC** or their **redesign into an UDC product**.

As described in Section 1.1 the degrees of freedom of a UDC product underlie various restrictions, of which product safety is an important bottleneck. Thus, this thesis focuses on **restrictions and challenges connected to the field of product safety** only. To meet the wide variety of further restrictions and challenges, further specific solution approaches are necessary. Existing research on an abstract level for example supports the identification of the requested degrees of freedom and evaluates their suitability in a generic manner based on the product structure (Holle & Lindemann, 2014; Holle, Maisenbacher, & Lindemann, 2015). However, the interdependency between the degrees of freedom for UDC (UDC options) and restrictions emerging from product safety is not addressed on a detailed level by existing research.

Moreover, this thesis does **not consider the legal aspects** related to safety and UDC. It focuses on the analysis of safety and preparations for approval but excludes the approval process and product liability. In addition, challenges regarding intellectual property and property rights, resulting from UDC, are not addressed. This includes questions like who is responsible for ensuring that no existing patents are violated, and who owns the property rights of the design of the customized UDC product.

With the main objective and the narrowed focus above, this thesis, as shown in Figure 1-2, aims at the **intersection of the research fields of customization, safety analysis and ECM**. It unites customization, respectively UDC, with the field of safety analysis and the field of ECM. The ECM therein acts as a bridge and enabler to combine and integrate the two other fields more efficiently. In addition to this main contribution at the triple interface, this thesis also contributes to the dual interfaces of these three research fields (see numbers in Figure 1-2).

The thesis integrates customization and safety analysis (1). Thereby, it increases the awareness for safety aspects during the development of customizable products. This not only is limited to UDC. The consideration of safety can also support for example the modularization of mass customization products.

Moreover, the thesis connects the fields of safety analysis and ECM (2). While the majority of ECM methods focuses either on process management or on propagations on structural and functional level, the impact on safety analyses and safety cases is not considered in depth.

At the third dual interface, this thesis contributes to the integration of customization and ECM (3). It enlarges the scope of ECM by analyzing variance and customization options and their propagations instead of engineering changes only. By that, a new perspective of change is integrated into ECM.

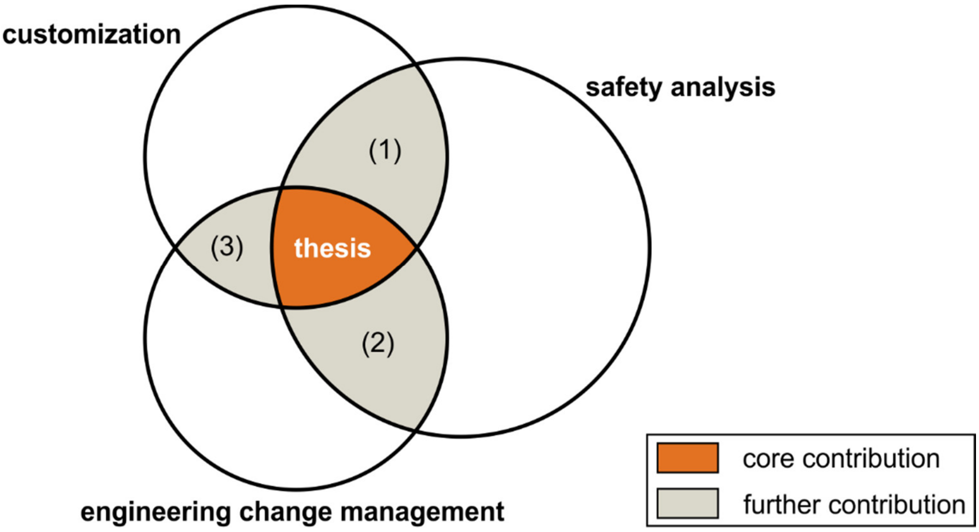
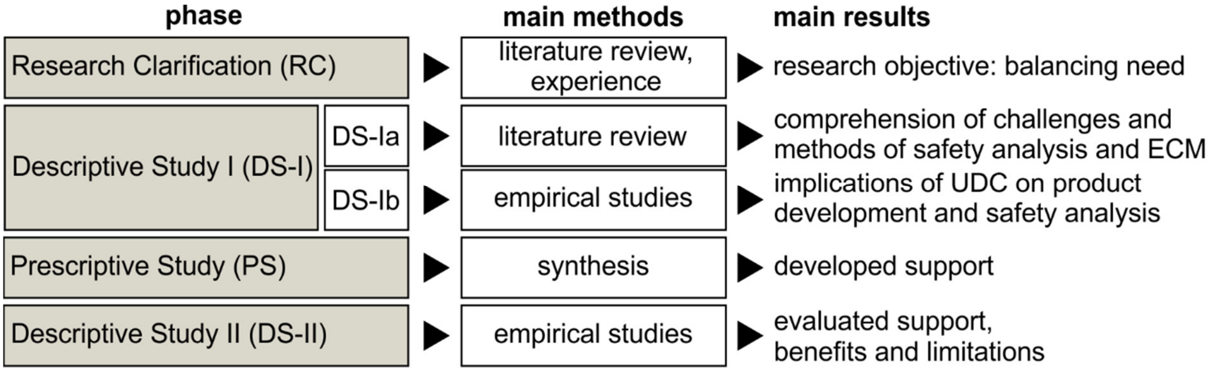


Figure 1-2: Research fields and the core contribution of this thesis

1.4 Research Methods

To achieve the contributions described above and answer the research question defined in Section 1.3, this thesis on a general level adapts the Design Research Methodology (DRM) by Blessing and Chakrabarti (2009). The DRM provides four stages to structure and support research in the field of engineering design. The four stages Research Clarification (RC), Descriptive Study I (DS-I), Prescriptive Study (PS), and Descriptive Study II (DS-II) do not prescribe a linear procedure but allow for iterations and recursions. For each stage a guideline and methodological support is given (Blessing & Chakrabarti, 2009).

The DRM framework is suitable for different research projects. Not all its stages have to be undertaken in the same depth or undertaken at all. Among the seven defined types of design research projects this thesis can be classified as development of support based on a comprehensive study of the existing situation (type 5) (Blessing & Chakrabarti, 2009, p. 62). As drawn in Figure 1-3, this thesis conducts a review-based RC stage followed by a comprehensive DS-I and PS as well as an initial DS-II. For a better differentiation within the DS-I, this thesis divides this stage in two sub-stages of which DS-Ia covers the review-based aspects and DS-Ib conducts detailed studies on the existing situation. The following paragraphs describe the scope and methods for each of these stages.



phase		main methods	main results
Research Clarification (RC)		literature review, experience	research objective: balancing need
Descriptive Study I (DS-I)	DS-Ia	literature review	comprehension of challenges and methods of safety analysis and ECM
	DS-Ib	empirical studies	implications of UDC on product development and safety analysis
Prescriptive Study (PS)		synthesis	developed support
Descriptive Study II (DS-II)		empirical studies	evaluated support, benefits and limitations

Figure 1-3: Research approach of this thesis with main methods and results (adapted from Blessing and Chakrabarti (2009, p. 15))

The **Research Clarification** is based on a literature review and the experience of the author. In detail, the identified trends and developments were used to elicit challenges and problems of the existing situation. The main objective and research question were derived from those. This represents the starting point for the detailed analysis of the existing situation and the concretization of the objectives.

In **Descriptive Study Ia**, an extensive literature review analyzes the state of science. The review systematically searches digital libraries and analyzes the works identified to understand the current situation in the research fields of customization and safety analysis. Moreover, the field of engineering change management is reviewed similarly. The understanding for each of these fields is developed by identifying its established methods and current developments. Based on this, the key challenges of each field are identified.

Building on the understanding of the three fields, **Descriptive Study Ib** researches the existing situation regarding the interface and integration of UDC and safety analysis. A literature review does not identify sufficient information. Hence, as suggested by Blessing and Chakrabarti (2009, p. 62), further analyses are conducted. First, an explorative questionnaire survey is conducted to identify the general implications of UDC on the development process and its activities. As this survey confirms the safety analysis as important and strongly influenced field, a series of focus-interviews is conducted to in detail research the impacts and resulting challenges in this field.

Based on the impact and challenges of UDC identified in DS-Ib, the main objective is concretized into specific requirements on a design support within the comprehensive

Prescriptive Study. Moreover, the PS defines the specific design tasks, where a support is needed. For each of these tasks, a support method is developed. The development follows the procedure suggested by Blessing and Chakrabarti (2009, pp. 146–148). This procedure is described at the beginning of Chapter 4 in detail. All twelve support methods are integrated in the "Efficient Safety Method Kit for User-driven Customization".

This design support is evaluated in an initial **Descriptive Study II** within three industrial case studies. Therein, the single support methods and the method kit are applied and evaluated. These applications are a fully-automatic coffee machine, a kitchen machine and a suspension strut for a motorcycle.

1.5 Structure of the Thesis

This thesis comprises seven chapters, which are roughly aligned with the research methodology described in the previous Section 1.4. Figure 1-4 provides an overview of these seven chapters. There, the Chapters 2 and 3 cover the DS-I. Chapter 4 presents the major parts of the PS and Chapter 5 the evaluation of the support (DS-II). In the final Chapters 6 and 7, the findings are discussed and conclusions are drawn. In the following a detailed overview of the contents is given.

Based on the scope and the objectives defined in this Chapter 1, **Chapter 2** summarizes the **theoretical background** of this thesis. This includes the fields of customization (Section 2.1), engineering change management (Section 2.2) and safety analysis (Section 2.3). Each of these sections contains subsections, which define the basic terms and concepts, introduce the established methods, identify current developments, and derive the challenges in the respective field. Section 2.4 summarizes the challenges of the three fields and deduces the need for a more detailed analysis of their interfaces.

These detailed **interface considerations** are provided in **Chapter 3**. In Section 3.1 the challenges at the interface and existing solutions are identified and compared based on literature. As the results with respect to UDC are not sufficient, a study on the implications of UDC on product development activities is conducted in Section 3.2. This general analysis is complemented in Section 3.3 by interviews, which focus on the implications and challenges in connection with safety analysis. Based on the governed understanding, Section 3.4 summarizes the findings and deduces the detailed problem to solve. Consequently, detailed objectives and requirements on the solution approach for this thesis are derived.

To achieve these objectives and meet the requirements, the **solution approach** is systematically developed in **Chapter 4**. First, the systematic procedure is described. The resulting "Efficient Safety Method Kit for User-driven Customization" (ESMK) is introduced in Section 4.1. In Section 4.2, the ESMK's underlying common knowledge framework is developed. Based on this, Section 4.3 introduces the specific methods of the ESMK. This section is subdivided in further subsections corresponding to the phases of the solution approach. Each subsection provides an overview of the tasks in this phase and the focus of the ESMK. For the specific tasks, the developed support methods are explained. Section 4.4 summarizes this chapter and its aspired contribution.

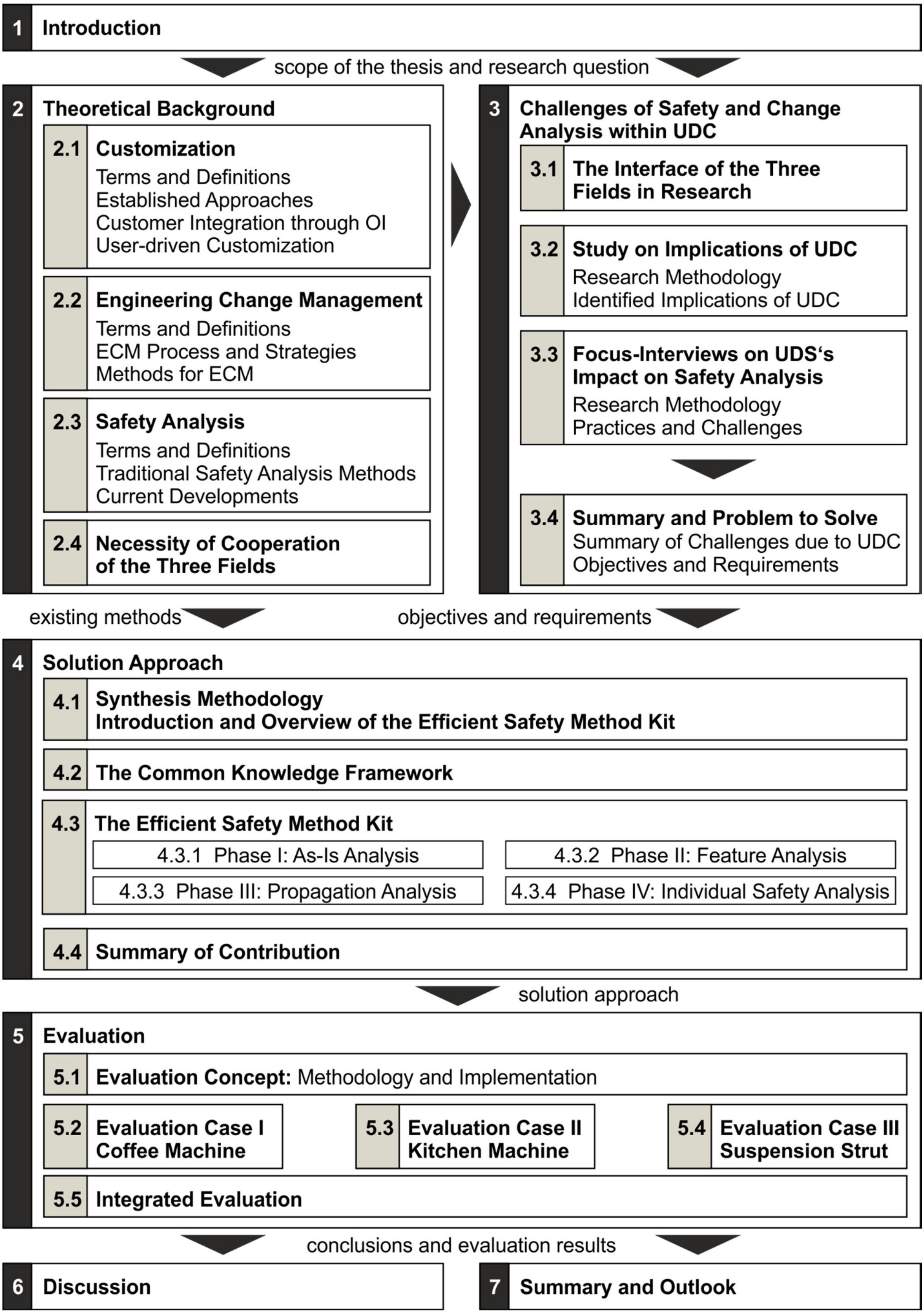

1 Introduction
scope of the thesis and research question
2 Theoretical Background
2.1 Customization
Terms and Definitions
Established Approaches
Customer Integration through OI
User-driven Customization
2.2 Engineering Change Management
Terms and Definitions
ECM Process and Strategies
Methods for ECM
2.3 Safety Analysis
Terms and Definitions
Traditional Safety Analysis Methods
Current Developments
2.4 Necessity of Cooperation of the Three Fields
3 Challenges of Safety and Change Analysis within UDC
3.1 The Interface of the Three Fields in Research
3.2 Study on Implications of UDC
Research Methodology
Identified Implications of UDC
3.3 Focus-Interviews on UDS's Impact on Safety Analysis
Research Methodology
Practices and Challenges
3.4 Summary and Problem to Solve
Summary of Challenges due to UDC
Objectives and Requirements
existing methods
objectives and requirements
4 Solution Approach
4.1 Synthesis Methodology
Introduction and Overview of the Efficient Safety Method Kit
4.2 The Common Knowledge Framework
4.3 The Efficient Safety Method Kit
4.3.1 Phase I: As-Is Analysis
4.3.2 Phase II: Feature Analysis
4.3.3 Phase III: Propagation Analysis
4.3.4 Phase IV: Individual Safety Analysis
4.4 Summary of Contribution
solution approach
5 Evaluation
5.1 Evaluation Concept: Methodology and Implementation
5.2 Evaluation Case I Coffee Machine
5.3 Evaluation Case II Kitchen Machine
5.4 Evaluation Case III Suspension Strut
5.5 Integrated Evaluation
conclusions and evaluation results
6 Discussion
7 Summary and Outlook

Figure 1-4: Structure and contents of the thesis

The “Efficient Safety Method Kit for User-driven Customization” is **evaluated** in C**hapter 5**. Section 5.1 introduces the concept of the evaluation and describes the implementation of a support tool. Section 5.2 evaluates the complete solution approach with the use case of a fully-automatic coffee machine. In addition, the major methods of the solution approach and the reuse potentials are evaluated in a second use case of a kitchen machine in Section 5.3. Moreover, Section 5.4 evaluates the concept of the knowledge framework in the use case of a suspension strut for a motorcycle. Each case consists of subsections, which introduce the case, discuss the application of the solution approach, and draw a resume. The evaluation of all three cases is consolidated in Section 5.5 and an integrated evaluation is derived.

The findings of the evaluation are **discussed** in **Chapter 6**. In Section 6.1 conclusions from the case studies are drawn and the results are discussed in the context of the defined requirements and objectives. Based on this, the limitations of the solution approach are identified and its contributions are summarized in Section 6.2.

The final **Chapter 7** concludes by providing a **summary** of the thesis and its contributions (Section 7.1). It moreover derives the needs for further research (Section 7.2).

2. Theoretical Background

This chapter introduces the theoretical background, which is necessary to follow and achieve the objective defined in Section 1.3. There, the three fields customization, engineering change management and safety analysis are identified as relevant research fields as the objective of the thesis tackles their triple interface. This chapter introduces the fundamentals of customization in Section 2.1, of engineering change management in Section 2.2, and of safety analysis in Section 2.3. Section 2.4 finally summarizes the three fields, identifies their dependencies, and derives their need for mutual interaction.

2.1 Customization

Customization is the main concept enabling individual products. Subsection 2.1.1 clarifies and defines the term of customization. Based on this understanding, Subsection 2.1.2 analyzes the origins of customization and introduces the existing archetypes to realize it. There, customer integration emerges as important aspect of all archetypes. Thus, Subsection 2.1.3 discusses Open Innovation and its customer integration potentials in connection with customization. The User-driven Customization unites both fields and is defined in Subsection 2.1.4. Finally, Subsection 2.1.5 summarizes the section and derives existing challenges.

2.1.1 Key Terms of Customization

In common language, to customize means, "to modify or build according to individual or personal specifications or preference"[1]. In a product context, it can be described as the "[…] intentional design of a product in respect of its usage through an individual" (Mayer, 1993, p. 37). Accordingly, Pine, Peppers, and Rogers (1995, p. 105) define customization as "[…] manufacturing a product or service in response to a particular customer's needs". Piller (2006, p. 115) instead describes customization as a strategy, which aligns the features of the offered products with the individual needs of the customer.

All these definitions emphasize different natures of customization but are consistent in their core. This thesis therefore, focuses on the product and defines **customization** as follows:

Customization is the modification of a product according to individual preferences or requirements and in respect of its usage through an individual.

Accordingly, a customizable product offers options for its modification according to individual preferences and requirements. As result, a customized product is a product, which is modified according to these individual preferences and requirements. Customized products have specific characteristics. Their focus of value creation aims at the individual customer and the amount of customers of each customized product is limited to one and a very few (Mayer, 1993, p. 50).

[1] Source: http://www.dictionary.com/browse/customization, last access: 2016/09/29

The term **mass customization** describes a specific form of customization, which is widely used but not defined consistently. It originates from Pine (1993) who describes mass customization as "[…] developing, producing, marketing, and delivering affordable goods with enough variety and customization that nearly everyone finds exactly what they want" (Pine, 1993, p. 44). In a further work he just defines it shortly as "mass customization means doing it [customization] in a cost-effective way" (Pine et al., 1995, p. 105). Piller and Stotko (2003) precise this cost-effective way by defining mass customization as "[…] the production of goods or services according to individual customer needs with an efficiency of mass production" (Piller & Stotko, 2003, p. 21). However, customization can add additional value to the product (see Baumberger (2007, p. 52) and Lindemann, Reichwald, and Zäh (2006, p. 10)) so that the efficiency of mass production does not have to be fully achieved to remain competitive.

Following this notion, this thesis slightly adapts the interpretation of Piller and Stotko (2003, p. 21) and uses the following definition:

Mass customization is the production of goods or services according to individual customer needs with an efficiency close to mass production.

2.1.2 Established Customization Archetypes

The reasons for an increased customization of products can be found in societal and technological change as well as in changes of the markets and the competition (Baumberger, 2007, p. 28). The following paragraphs briefly describe these influences.

The societal change comprises two aspects. The first aspect is the **demographic change** with an increased number of single households and the changed age structure (Piller, 2001, p. 83). The second aspect is the **increased wealth** (e.g. income, education, health) (Baumberger, 2007, pp. 27–31; Piller, 2006, p. 44). Both changes lead to an increased demand for individual products, as humans in addition to the need for survival also possess a strong need for novelty and variety (Fournier, 1994, p. 59; Piller, 2006, p. 44).

Digitalization mainly drives the technological change. It allows a direct interaction between customers and manufacturers (Piller & Walcher, 2006, p. 309), improved performance of hardware (e.g. storage and processors) at decreased costs (Baumberger, 2007, p. 32; Hildebrand, 1997, p. 17), and more flexible production technologies (Gibson et al., 2015, p. 2; Gräßler, 2004, p. 27; Lindemann et al., 2006, p. 15).

The change in markets is mainly characterized by an increased **globalization**. This leads to an increased variety of products, removed entry barriers and the loss of competitive advantages (Piller, 2006, pp. 51–52). Moreover, the customers are getting more demanding, due to the large bandwidth of offers, and expect their individual needs to be fulfilled for low prices (Baumberger, 2007, p. 31; Hildebrand, 1997, p. 12; Lindemann & Reichwald, 1998, p. 7).

In summary, the current markets and societies supported by high competitiveness and new enabling technologies demand for individual (i.e. customized) products. Customization offers various **advantages** and possibilities to react on this changing environment. It aims to achieve an exact match of customer needs and product characteristics (Piller & Stotko, 2003, p. 166). Figure 2-1 illustrates this aim compared to mass products and variant products.

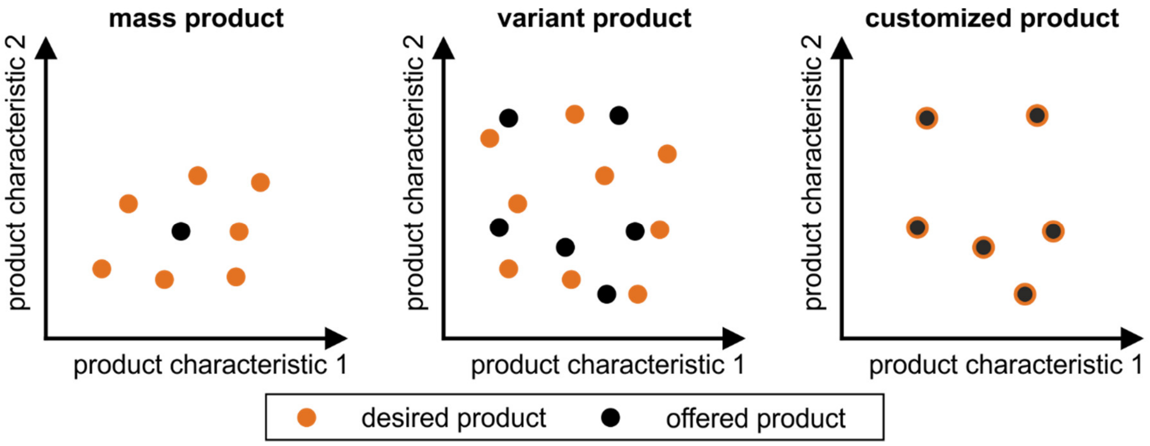


Figure 2-1: Comparison of mass, variant, and customized products (adapted from Baumberger (2007, p. 51) and Schenk et al. (2014, p. 103))

If the product meets or even exceeds the customer expectations, the customer satisfaction will be on a high level. Thus, customization offers the potential to increase customer satisfaction and loyalty (Piller, 2006, p. 119). Especially in saturated markets, these achievements are more important than the acquisition of new customers (Hinterhuber, Bailom, Handlbauer, & Matzler, 1998, pp. 343–344). They result in further advantages, which for example, but not limited to, are, quasi-monopolistic options (Piller, 2006, pp. 116–118) and reduced price sensitivity of the customers (Baumberger, 2007, p. 52; Lindemann et al., 2006, p. 10).

Despite these advantages, customization can also induce **drawbacks** for both, customers and manufacturers. According to Baumberger (2007, pp. 53–55), there is a risk that customers are unable to cope with the large amount of options offered. They in connection with missing experience might not be able to identify suitable product characteristics. For manufacturers, costs and efforts for product structure planning, requirement elicitation and customer interaction will increase, while productivity and utilization of plants and machinery can decrease (Baumberger, 2007, p. 53; Lindemann, 2005, p. 357; Piller et al., 2004, p. 438). These effects lead on both sides to an increased complexity, which has to be efficiently handled (Blecker, Friedrich, Kaluza, Abdelkafi, & Kreutler, 2005, p. 46). This implies that customization can only be successful, if the trade-off between the mentioned challenges and advantages is successfully managed (Piller et al., 2004, p. 443).

To find the optimum of the previously described trade-off, various **customization archetypes** exist. To classify these existing concepts, literature suggests various dimensions. Among those, the degree of customization and the decoupling point of the individual products within the product life cycle are the most common (Gräßler, 2004, p. 20). The degree of customization often is also represented by the degree of customer integration (see e.g. Baumberger, 2007, p. 36; Piller et al., 2004, p. 443). Figure 2-2 draws these dimensions and classifies the archetypes of existing customization concepts.

The relatively new concepts, which achieve the highest degree of customization and customer integration, are **Open Innovation** (OI) or User-driven Customization (for details and definition see Section 2.1.4). OI mainly aims at early phases like product planning and it applies and expands the lead-user approach to develop new products in close relationship to the customers and their needs. However, these products usually aim at a larger groups of customers or are used as a base for further customization (Baumberger, 2007, p. 36; Piller & Stotko, 2003, pp. 84–85).

Instead, a more traditional approach to achieve a high degree of customization and to realize individual products is the **engineer-to-order** concept. Engineer-to-order develops and manufactures an individual product. Large parts of the product are individually developed and adapted in close cooperation with the customer (Baumberger, 2007, pp. 35–36; Piller et al., 2004, p. 443).

In **make-to-order**, the decoupling takes place in the manufacturing phase. Here, products including individual components are individually manufactured. Closely related is the **assemble-to-order** concept. Customized products are realized by the assembly of standardized components and modules, based on the customer's configuration or selection. These concepts are probably the most common and for example applied in the EU car market. There, the customers can apply online configurators to combine their individual product from a set of given modules and components (Baumberger, 2007, p. 35; Piller et al., 2004, p. 443).

Concepts, which decouple after manufacturing are **bundle-to-order** and **match-to-order**. In bundle-to-order, existing products are bundled to a customer-specific product according to his or her specification. Match-to-order instead only selects existing products according to the individual specification. Both concepts decouple in sales or retail processes and do not intervene in the value creation processes (Baumberger, 2007, p. 35; Piller et al., 2004, p. 443).

The latest decoupling takes place in the usage phase. There, following **self-customization**, the customer adapts the product according to his or her needs and capabilities during the usage on his or her own (Baumberger, 2007, p. 35).

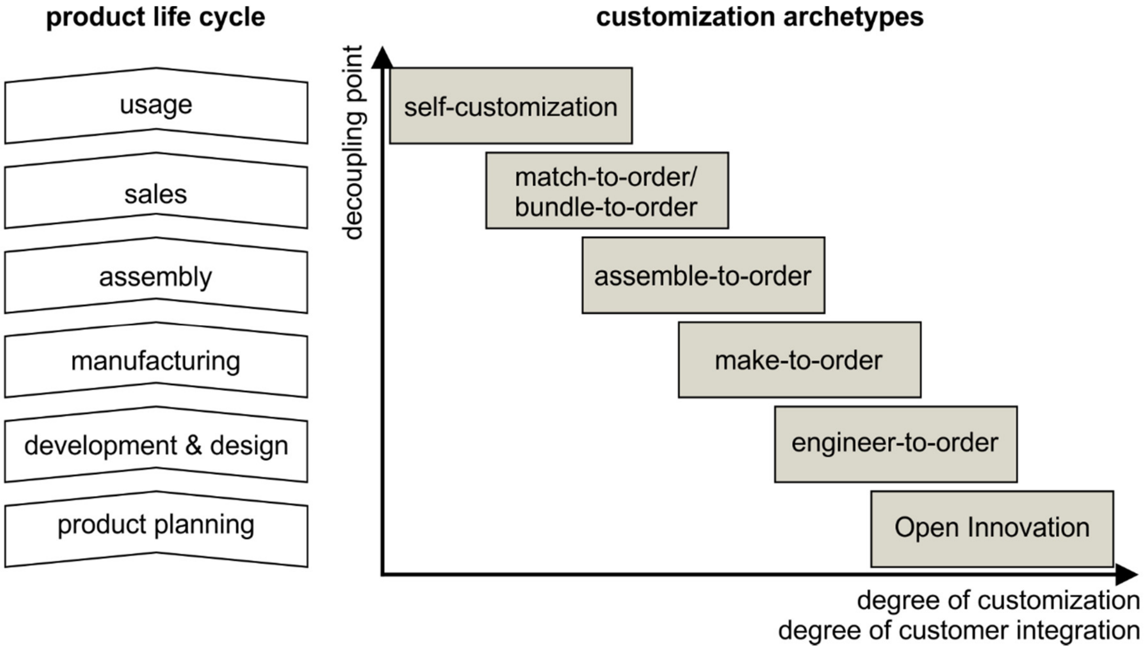


Figure 2-2: Archetypes of customization (adapted from Baumberger (2007, p. 36), Piller et al. (2004, p. 443), and Piller and Stotko (2003, p. 85))

Even though the literature defines these archetypes of customization, a clear and consistent differentiation often is not possible. This also implies that a clear boundary between variant standard products and customized products cannot be drawn. Moreover, this fact aligns with the variance of the definitions of mass customization discussed in Section 2.1.1. Nevertheless, all customization archetypes still comply with the general idea and definition of customized products.

2.1.3 Customer Integration through Open Innovation (OI)

As elaborated in the previous subsection, a close interaction with the customers is characteristic for customization and represents a major difference to variant products (Gräßler, 2004, p. 16). To describe and manage such and related interactions, Chesbrough (2003) introduces the concept of Open Innovation (OI).

OI is a management theory whose basic idea is to **acquire knowledge from inside and outside of the enterprise** to create something new (Chesbrough, Vanhaverbeke, & West, 2014, pp. v–vi). In a more general form it can be described as innovation process between multiple actors, which interact across enterprise boundaries (Reichwald, Piller, & Ihl, 2009, pp. 153–154). This differentiates OI from classical innovation processes, which usually take place within an enterprise (closed innovation) (Reichwald et al., 2009, p. 117).

OI can be further distinguished according to the direction of knowledge flow. Outside-in OI acquires knowledge from outside the enterprise and transfers it into the company. In contrast, inside-out OI transfers knowledge from the enterprise into new markets. Coupled OI describes cooperation projects between multiple partners or competitors (Gassmann & Enkel, 2006, pp. 132–133). This underlines that OI is a suitable support for customization and the realization of its customer integration.

Especially to support outside-in OI, a wide variety of methods exists. Saucken, Gürtler, Schneider, and Lindemann (2015) for example provide an overview of this variety. Examples of those methods are idea contests and idea platforms (see Walcher (2007)) or the lead-user approach (Hippel, 2005, pp. 19–31). Another group of methods are the so-called toolkits for OI. In early phases, according to Saucken et al. (2015, p. 205), user innovation toolkits allow the users to design their "perfect" product (Reichwald et al., 2009, pp. 193–194). In later phases also user co-design toolkits can be used in the context of customization (i.e. configuration) (Gürtler, Saucken, Tesch, Damerau, & Lindemann, 2015, p. 5; Reichwald et al., 2009, p. 195).

In this group of **toolkits for OI**, various types and variants exist. Most of them are complex and offer a large solution space so that they mainly aim at business-to-business relationships (Franke & Piller, 2004, p. 403). One example of this type is the design of individual integrated circuits presented by Hippel and Katz (2002). However, to integrate the (end)user in the innovation process, usually online toolkits are applied. These toolkits offer a smaller solution space (Hippel, 2001, p. 247). One example is a toolkit to design eyeglasses (Hippel, 2001, p. 252). To classify and structure this variety, Reichwald et al. (2009, p. 193) propose to distinguish the following two types:

- toolkits for user innovation, which offer a large solution space and aim to generate innovative product features
- toolkits for user co-design, which provide a predefined solution space and enable the customers to customize their product by selecting desired features

Following this classification, only **toolkits for user innovation** are suitable for a high degree of customization. Based on Hippel and Katz (2002, p. 823), this thesis defines them as follows:

Toolkits for user innovation are a coordinated and integrated set of tools that enable users to develop new product innovations for themselves.

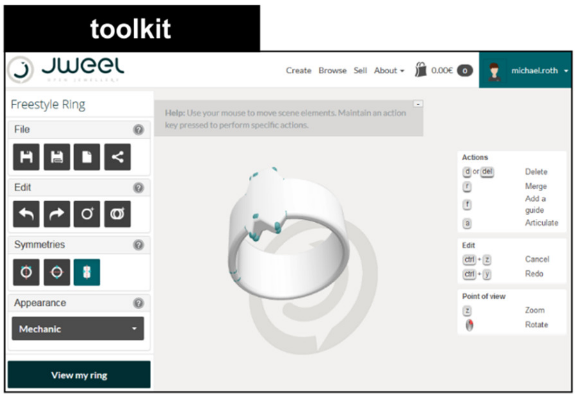
The major **advantages** of these toolkits are reduced efforts for eliciting the individual customer needs (Hippel, 2001, p. 247). This process is usually difficult and time-consuming. Thus, the information on customer needs is described as “sticky” (Hippel, 2001, p. 248). The associated costs to transfer this information into the enterprise (sticky information transfer costs) can usually be reduced through the application of toolkits (Hippel, 2001, p. 248; Hippel & Katz, 2002, p. 824). A further advantage of toolkits for user innovation are “[...] faster, better and cheaper [...]” (Hippel, 2001, p. 248) learning by doing processes. These learning by doing processes constitute of trial-and-error cycles with the three phases of design, build and test/feedback (Thomke & Hippel, 2004, p. 52). Toolkits for user innovation moreover contribute to satisfy individual customer needs and, hence, to increase customer satisfaction (Franke & Hippel, 2003, p. 1200).

In summary, toolkits for user innovation help to minimize risk and cost within product development and customization. However, the development of these toolkits itself is a difficult and challenging task (Hippel, 2001, p. 249).

To enable the previously mentioned advantages, a toolkit for user innovation according to Hippel (2001, pp. 250–254) has to comprise the following **five elements**:

- complete trial-and-error cycles
- appropriate solution space
- user friendliness
- libraries of standard elements or modules
- producibility check and translation for production

Despite the advantages described above, the **applications of toolkits for user innovation**, which include all five elements, are limited. In their review, Goduscheit and Jørgensen (2013) only identified 16 articles discussing toolkits for user innovation. Their classification according to the five elements of toolkits for user innovation described above underlines that none of the examples fully implements all five elements (Goduscheit & Jørgensen, 2013, p. 287). Most examples aim at simple consumer goods like cell phone covers, t-shirts or software. For technical consumer products, the applications remain even more limited. A further research on commercial toolkits for user innovation in Roth, Harmeling, Michailidou, and Lindemann (2015) did not reveal other insights. The maybe most complete toolkits identified there only allow the design of jewelry as exemplarily shown in Figure 2-3.



Help: Use your mouse to move scene elements. Maintain an action key pressed to perform specific actions.

Appearance: Mechanic

Select a material: Silver

Select a finish: Premium

Sterling Silver, Gloss. Hand polished.

Select a ring size: 51mm

Shipping to MUNICH, DE: free

size: 51mm
18.69 x 20.07 x 10.18mm

Figure 2-3: Example of an existing toolkit for user innovation offering the design of jewelry[2]

2.1.4 User-driven Customization (UDC) - A New Approach

The trends and changes identified in Subsection 2.1.2 demand for both, an increasing degree of customization and an increased involvement of the users. Simultaneously the customers strive for increased self-actualization. Figure 2-4 positions those demands within the existing customization archetypes. It clearly shows that existing concepts are not able to satisfy all the demands. Especially, the impact of increased complexity and increasing sticky information transfer costs limit the existing concepts. However, the toolkits for user innovation introduced in Section 2.1.3 can reduce these drawbacks. Thus, a new concept of customization is required. This concept is developed and defined by Holle, Roth, Gürtler, and Lindemann (2014) and Roth, Ulrich, Holle, and Lindemann (2016).

The new concept of **User-driven Customization** (UDC) combines a high degree of customization with an intensive user integration, an adapted concept of self-customization, and the idea of toolkits for user innovation. In UDC, a web-based toolkit (UDC-toolkit) is provided, which allows the users to adapt and customize a provided basic product according to their individual needs. When ordered, this customized product is directly produced according to the individual design realized in the toolkit. As shown in Figure 2-4, UDC resolves the linear nature of existing customization archetypes and opens up new potentials in the characteristic dimensions of customization.

In Figure 2-5, an exemplary workflow of the UDC of a coffee machine is illustrated: The user first designs his or her individual coffee machine in the web-based UDC-toolkit. He or she then submits his or her draft to the connected online community. In this community, he or she can discuss his or her drafts and exchange ideas with other members. Based on the feedback, he or she improves the design and finally submits the order. The toolkit then translates the individual design and directly transfers it to the production planning system. From there, the design is transferred to its production in a highly flexible production system. Finally, the customized coffee machine is shipped to the ordering user.

[2] Source: www.jweel.com, last access: 2016/09/29

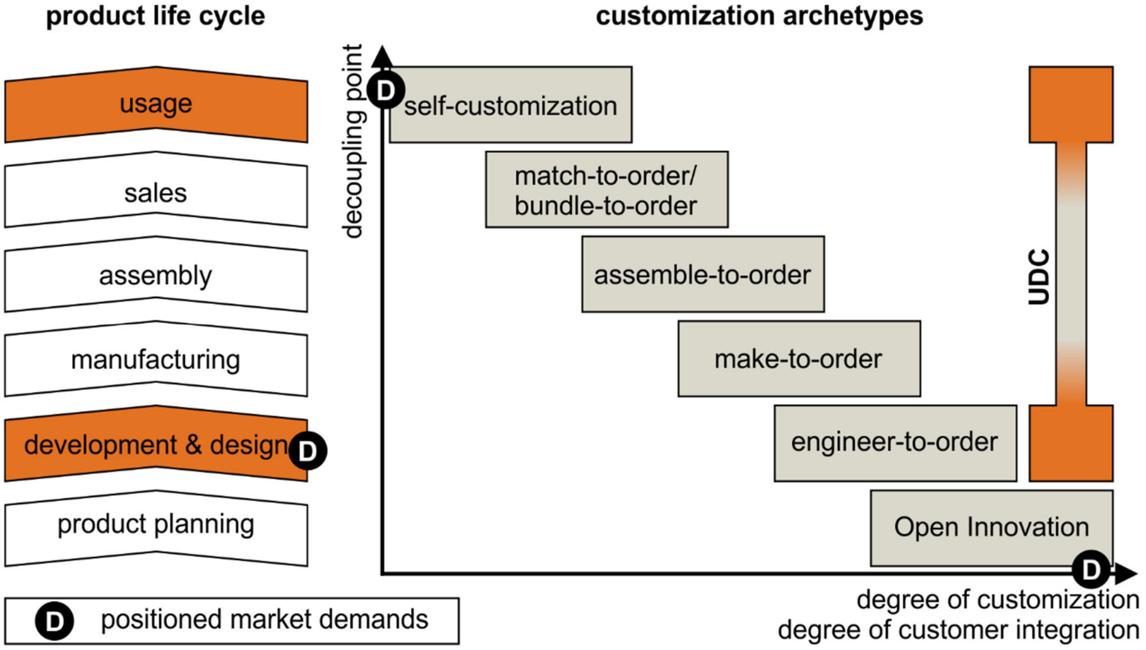


Figure 2-4: The new concept UDC in comparison to the customization archetypes and the current demands (adapted from Baumberger (2007, p. 36), Piller et al. (2004, p. 443), and Piller and Stotko (2003, p. 85))

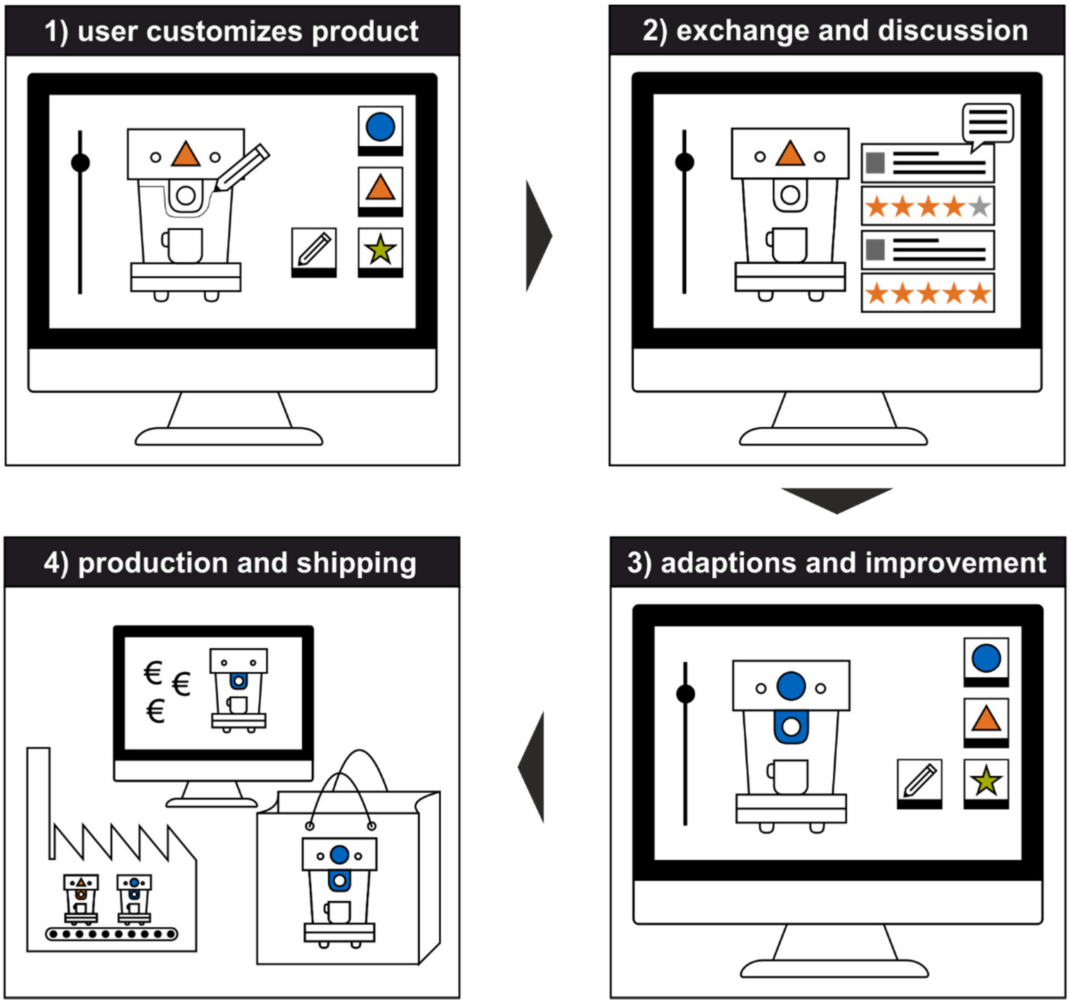

1) user customizes product
2) exchange and discussion
3) adaptions and improvement
4) production and shipping
€
€
€

Figure 2-5: Exemplary workflow of User-driven Customization of a coffee machine (adapted from: HYVE AG)

UDC-toolkits represent a form of toolkits for user innovation and include all their essential elements. They provide a non-predefined and theoretically infinite solution space for the users. This aspect is the fundamental difference to the established mass customization concepts assemble-to-order and make-to-order. Moreover, through the link to production and the automated translation, the users can undergo complete trial-and-error cycles. This direct link from the UDC-toolkit to production also represents the important difference to engineer-to-order concepts where designers of the manufacturer realize the individual or improved design instead of the users.

2.1.5 Summary and Challenges of Customization

The previous subsections show that there is an increasing demand for individual products and increasing customization. Currently applied concepts of mass customization like assemble-to-order and engineer-to-order are not able to satisfy these needs, especially in the field of technical consumer products. Moreover, there is a demand for increased customer integration, which can be achieved by methods of OI. Exemplary methods are toolkits for user innovation.

UDC reacts on these developments and combines aspects of customization and OI. It allows the customization through the user within a web-based UDC-toolkit, which directly translates and transfers the custom design to production.

However, full applications of UDC are not yet realized for technical consumer products. Existing research mainly focuses on toolkits for user innovation. In the small number of publications (see Goduscheit and Jørgensen (2013)), only partial aspects are implemented and most publications focus on the discussion of advantages of single applications. The question how these toolkits can be designed and integrated in the product development process, especially for UDC products, are not yet answered by research.

2.2 Engineering Change Management (ECM)

Customization as described in the previous sections implies alterations made to a product. In the product development context occurring alterations are usually considered as engineering changes. This section in Subsection 2.2.1 defines engineering change and related key terms. Based on this, Subsection 2.2.2 introduces the main processes and strategies of engineering change management. Moreover, specific support methods for ECM are introduced and discussed in Subsection 2.2.3. Subsection 2.2.4 summarizes this section and based on the presented methods highlights existing challenges in this field.

2.2.1 Key Terms of Engineering Change Management

Change is a common phenomenon in the daily business of product development. The term change usually is used with regard to a business or organizational context (Jarratt et al., 2011, p. 105). In the product development context, the term engineering change is used instead. In the following, this subsection defines the term along with the related concepts of change propagation and engineering change management (ECM).

Engineering change was discussed widely in literature during the last decades. Jarratt et al. (2011) provide an extensive review of these contributions. However, they assert that the used terms and definitions are not fully consistent (Jarratt et al., 2011, p. 105). For example Inness (1994) uses the term "product change" and Ollinger and Stahovich (2004) use "design change" to describe this phenomenon (Jarratt et al., 2011, p. 105). The same applies for the definitions of these terms. Jarratt, Clarkson, and Eckert (2005, pp. 266–268) attempt to consolidate the varying definitions and based on Terwiesch and Loch (1999, p. 160) define an engineering change as "[...] an alteration made to parts, drawings or software that have already been released during the design process" (Jarratt et al., 2005, p. 268). Even they go further to investigate the variable magnitude of an engineering change, this thesis relies on this core definition of an engineering change. Nevertheless, this thesis extends the scope to product data as for example documentation and models. It considers these artifacts as released, as soon as subsequent work relies on them. Thus, this thesis defines an engineering change as follows:

An engineering change is an alteration made to parts, models or other product data that have already been released during the design process.

Engineering changes can be differentiated according to their origin in changes arising from mistakes in the development process or from innovation (Lindemann & Reichwald, 1998, pp. 28–29). However, the principles of user co-creation and UDC add another perspective. Even though resulting changes arise from a need for innovation, users implement the alternations directly to the model of the product. These users are external to the company but the changes affect the product and internal processes prior to production.

Hence, the origin of the change and the implementation of the change slightly differ from an engineering change, while other general aspects remain. To describe this specific type of change, this thesis defines the term of **user-induced change**:

A user-induced change is an alternation made to parts or models that have been designed in the internal design process and are offered for UCD, which is conducted by an external user.

Engineering changes occur frequently during the design process (Jarratt et al., 2011, p. 121). They can have effects, which spread to other parts of the product, its properties or processes and to other business areas (Jarratt et al., 2005, p. 276; Lindemann & Reichwald, 1998, pp. 193–194). This phenomenon usually is described as change propagation. The existing literature only describes this phenomenon (see Jarratt et al. (2005), Lindemann and Reichwald (1998) and Fricke, Gebhard, Negele, and Igenbergs (2000)) but does merely define the term in a compact from. Thus, this thesis extends the description of Eckert et al. (2004, p. 10) and defines **change propagation** as follows:

Change propagation occurs, if a change to a single part or system impacts the properties of other parts or systems or causes changes at other parts or systems.

The origin of change propagation lies in links, interactions and dependencies of the system elements (Eckert et al., 2004, p. 10; Lindemann & Reichwald, 1998, pp. 193–194). As a consequence, the likeliness of change propagation itself and the likeliness of resulting further change propagation is high in complex closely interlinked products (Eckert et al., 2004, p. 1).

This definition of change propagation shows that engineering changes can lead to various challenges during the product development process. Accordingly, engineering change management (ECM) describes all strategies and activities to organize, conduct, control and prevent the process of engineering change (Jarratt et al., 2005, p. 266; Langer, 2016, p. 524).

2.2.2 Engineering Change Management Process and Strategies

The nature of engineering changes and change propagations defined in the previous Subsection 2.2.1 implies various challenges, which have to be handled. For example, potential consequences of change propagations are major rework cycles in the development process (Maier, Wynn, Biedermann, Lindemann, & Clarkson, 2014, p. 287) and information deficiencies between involved domains and individuals (Fricke et al., 2000, p. 172). Hence, an effective management of change propagation and the connected challenges can provide large benefit (Langer, 2016, p. 513).

Engineering changes in enterprises are usually embedded in a change process. Change processes can vary for companies and departments, but the requirements on these processes are standardized (i.e. ISO 9001). To consolidate the general practices, Jarratt et al. (2005, pp. 270–272) describe a generic **engineering change process**. It consists of the six steps visualized in Figure 2-6.

To initiate this process, a change has to be triggered, which usually leads to an engineering change request. Based on the request, potential solutions are identified. These solutions are evaluated for their risk and impact. Based on this assessment, a solution is selected and approved. Following the implementation of the solution, a review of the engineering change and its process terminates the generic engineering change process. This process moreover includes possible iterations and breakpoints, if for example the identified solutions are not satisfactory (Jarratt et al., 2005, pp. 270–272). After approval, additionally to the review, existing norms and standards demand a full documentation of the changes in order to ensure complete traceability (Langer, 2016, p. 514).

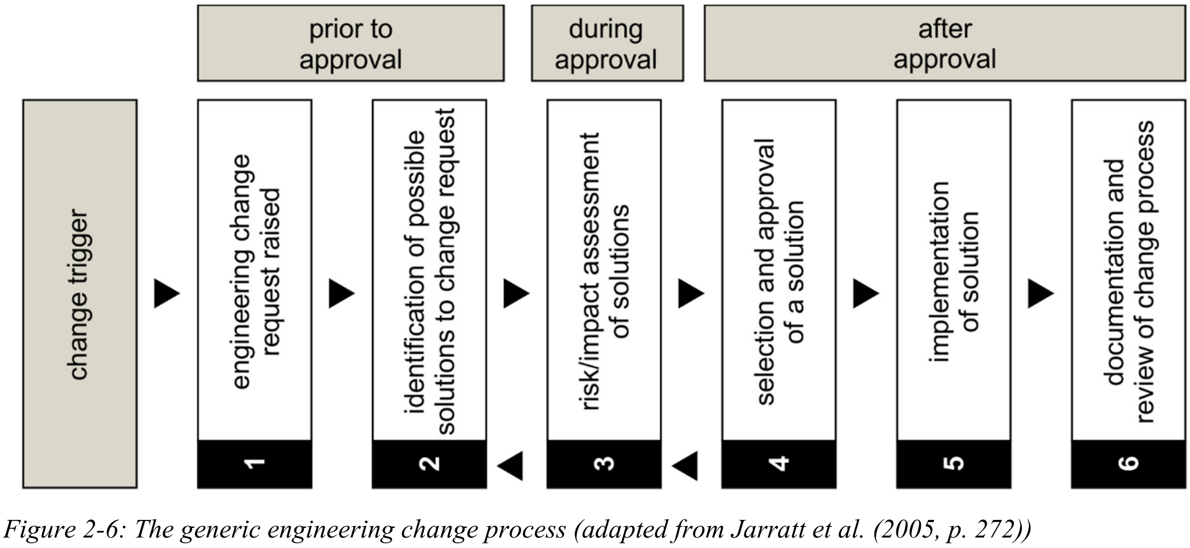

prior to approval
during approval
after approval
change trigger
engineering change request raised
1
identification of possible solutions to change request
2
risk/impact assessment of solutions
3
selection and approval of a solution
4
implementation of solution
5
documentation and review of change process
6

Figure 2-6: The generic engineering change process (adapted from Jarratt et al. (2005, p. 272))

The generic engineering process described in the previous paragraph establishes the organizational setup to handle and process engineering changes within ECM. To minimize their negative impact on cost, time and quality, it is necessary to improve the management of changes (Fricke et al., 2000, p. 172). To achieve this, various authors suggest **strategies to better cope with changes** (Jarratt et al., 2005, p. 279). A comprehensive list can be found in Fricke et al. (2000, pp. 173–176) who identify the following five strategies:

- prevention
- frontloading
- effectiveness
- efficiency
- learning

The strategy of **prevention** aims to reduce the number of changes that emerge during the development of a product. This can mainly be achieved by the limitation of errors in the design process, which however is challenging (Fricke et al., 2000, p. 173; Jarratt et al., 2011, p. 120; Lindemann & Reichwald, 1998, p. 112).

The strategy of **frontloading** aims to detect emerging changes earlier and to implement them at earlier development stages. This can for example be achieved through the involvement of suppliers or improved product flexibility (Fricke et al., 2000, pp. 173–174; Jarratt et al., 2011, p. 120).

The strategy of **effectiveness** aims to better assess whether changes are necessary and provide a good cost/benefit ratio. To achieve this, effects of changes and their need should be better evaluated (Fricke et al., 2000, pp. 174–175).

The strategy of **efficiency** aims to improve the usage of resources during the implementation. To achieve this, the engineering change process needs to be improved for example by removing bottlenecks (Fricke et al., 2000, pp. 175–176; Jarratt et al., 2011, pp. 120–121).

The strategy of **learning** finally aims to increase the efficiency and effectiveness of the whole ECM. Implemented changes should also be used to "[…] do it better the next time" (Fricke et al., 2000, p. 176). Hence, the reviews conducted in the sixth step of the generic change process and the resulting documentation are important to enable this learning (Fricke et al., 2000, p. 176; Jarratt et al., 2011, p. 121).

To understand, how these strategies can be implemented and how methods can support these strategies, it is necessary to discuss the **relation between engineering changes and the characteristics of the product**. According to Jarratt et al. (2011, p. 113), the complexity of the product, the degree of innovation in the product, and the architecture of the product determine which extent the impact of an engineering change has.

The **complexity** of a product can be understood as the number of components, dependencies and their variance (Lindemann et al., 2008, p. 29). Thus, complex products imply a large number of engineering changes (Jarratt et al., 2011, p. 114). Moreover, as described during the definition of change propagation (see Subsection 2.2.1), complex products usually are highly coupled and, hence, imply a higher probability of propagations (Eckert et al., 2004, p. 1). In addition, these propagations are harder to control in complex products (Fricke et al., 2000,

p. 171). Therefore, when analyzing changes, it is necessary to consider change networks instead of change chains (Eckert et al., 2004, p. 10).

In **innovative** products, there usually is a low degree of information and knowledge of the product and its technologies (Fricke et al., 2000, p. 172). This might lead to a higher probability of engineering changes and resulting change propagations (Jarratt et al., 2011, p. 115). Especially, if multiple new technologies are deployed and integrated in one product, late engineering change can occur (Eckert, Wyatt, & Clarkson, 2009).

The third impact is the **product architecture**. It describes the arrangement of functional elements, their mapping to physical components, and the specification of interfaces between the physical components (Ulrich, 1995, p. 420). Product architectures can be distinguished into modular architectures, where each physical component carries out only one function, and integrated architectures, where physical components carry out multiple functions (Ulrich & Seering, 1990, p. 224). As products usually lie somewhere in the span between both types of architectures (Jarratt et al., 2005, p. 276), Lindemann and Reichwald (1998, p. 149) differentiate engineering changes accordingly into local engineering changes and interface-overlapping changes. This classification of engineering changes correlates with the classification of components in respect of their change behavior. Eckert et al. (2004, p. 13) classify components into constants, absorbers, carriers, and multipliers. For example, absorbers can absorb more changes themselves than they cause and multipliers vice versa (Eckert et al., 2004, p. 13).

2.2.3 Methods for Engineering Change Management

Due to the large number of influences and strategies described in the previous subsection, a large bandwidth of methods, tools, and studies on ECM is published. Extensive reviews can be found in Wright (1997), Jarratt et al. (2011), Ahmad, Wynn, and Clarkson (2011) as well as Helms et al. (2014).

According to Jarratt et al. (2011, p. 115), the existing tools and methods can be differentiated into those, supporting the workflow or documentation of the engineering change process and those, supporting engineers in their decisions at particular points within the engineering change process. In respect of the main objective of this thesis to support the balancing between increased efforts and UDC options, the focus of interest lies on the latter.

Moreover, in the context of UDC, where users induce the changes, especially the strategies of prevention, effectiveness and learning are of minor relevance and efficiency. Thus, this thesis focuses on the strategies of frontloading and efficiency. For those strategies, the evaluation of change propagations plays a major role. Hence, in this thesis, a complementary literature review on the keywords of “change” and “propagation” in relevant databases and journals[3] is conducted. This review identifies 617 publications of which 106 discuss aspects of engineering changes.

[3] Databases: Design Society, IEEE Xplore; Journals: Res. in Eng. Design, Journal of Eng. Design, IEEE Trans. on Eng. Mgmt., Systems Engineering

The following paragraphs describe the identified major ECM methods within the focus defined above. The description is based on the reviews by Jarratt et al. (2011), Helms et al. (2014), and the complementary review, which is partially published in Roth, Mayr, and Lindemann (2016).

The most discussed method is the **Change Prediction Method (CPM)** by Clarkson, Simons, and Eckert (2004). It aims to support the designer in evaluating how an engineering change can propagate through the product. Therefore, the CPM predicts the effect of an engineering change through a simple concept of risk. This risk is calculated as the product of the likelihood of a change propagation and the impact this propagation will have. Therefore, two numerical Design Structure Matrices (DSMs) (Browning, 2001) are populated with the likelihood and risk values of each possible propagation. Then, a route-counting algorithm calculates the combined risk for each potential change propagation. This includes direct as well as indirect risks. By that, all possible propagation paths are determined so that the result can be displayed in form of a propagation tree (Clarkson et al., 2004; Jarratt et al., 2011, p. 118).

Many other works adapt and extend the CPM. For example Giffin et al. (2009) establish a connection between the CPM and a database with industrial data on past change requests. Another example for extension are Koh, Caldwell, and Clarkson (2012), who in their Change Modeling Method unite the CPM with the House of Quality (HoQ) to obtain possible propagations of engineering change options and support their selection. Another extension is provided by Hamraz, Caldwell, and Clarkson (2012), who integrate the functional perspective by combining the CPM and the Function Behavior Structure (FBS) in their FBS linkage model.

The **Functional Analysis of Change Propagation** of Flanagan, Eckert, Eger, Smith, and Clarkson (2003) follows a similar approach. It is based on the assumption that an engineering change always causes a change of form and a change of function simultaneously. Following this assumption, they use DSMs and Domain Mapping Matrices (DMMs) (Danilovic & Browning, 2007) to identify and trace potential propagations (Flanagan et al., 2003).

Similarly, Reddi and Moon (2009) propose the **framework for managing engineering change propagation**. It also aims to identify components in a product, which are affected by an engineering change and to estimate the likelihood of the identified propagations. For each dependency between initiator and target in early stages of design, the type of change is captured together with the likelihood of the change in a database. Then, all possible propagation paths are identified using database query-based algorithms (Reddi & Moon, 2009).

Conrad, Deubel, Köhler, Wanke, and Weber (2007) in their **Change Impact and Risk Analysis** try to identify the impact and risk of changes by evaluating both criteria in a FMEA-like assessment method. They rely on the Characteristics-properties Model/Property-driven Development theory of Weber (2005) to model and describe the product and based on this evaluate and quantify the impact of engineering changes.

Ollinger and Stahovich (2001) and (2004) suggest a simple model-based tool **"RedesignIT"** to evaluate engineering changes triggered by redesign plans. It uses abstract and qualitative models to describe the dependencies and casual influences between product components in terms of physical quantities. Starting from the initiator component and its changed physical quantity, the tool also is able to draw propagation trees (Ollinger & Stahovich, 2001, 2004).

A more detailed view is realized by Cohen, Navathe, and Fulton (2000) in their methodology **Change Favorable Representation** (C-FAR). They aim to capture possible consequences of engineering changes and use data in the STEP format to trace engineering changes related to design. C-FAR decomposes the product in its design elements and stores their interactions together with a predicted quality of the effect in matrices. Based on this, the propagation paths and their quality are computed (Cohen et al., 2000).

Further methods are proposed for example by Rutka et al. (2006) who use Boolean dependencies, strength values and types of changes to identify possible change propagations. Bauer, Chucholowski, Lindemann, and Maurer (2015) use a Multiple-domain Matrix (MDM) to analyze and evaluate the impact of engineering changes via multiple domains. Moreover, Grantham Lough, Stone, and Tumer (2006) rely on data of past failures and behavior to predict change propagations and the connected risk in functional decompositions. Furthermore, Pasqual and Weck (2012) develop a multilayer network model, which extends the analysis of change propagations to the levels of organization and individuals.

2.2.4 Summary and Challenges of Engineering Change Management

The previous subsections show that managing engineering changes is a challenging and complex task. To improve this and achieve the optimal benefits, different strategies are followed and engineering changes are usually handled within an engineering change process. Moreover, the actual characteristics of the product (e.g. complexity and product architecture) strongly influence the potential impact of engineering changes.

As the aspects and influences on engineering change are manifold, researchers develop manifold support methods. An overview on the methods relevant for this thesis is given in the previous Subsection 2.2.3. Each support method emphasizes specific aspects of engineering change and thus, provides specific support at some points in the engineering change process. While some methods like the CPM focus on the risk of propagations, others like the C-FAR offer a representation to visualize potential propagations and support the decision-making.

However, a major limitation of the methods is that the majority of methods requires suitable data of the product, of engineering changes or potential change propagations (Jarratt et al., 2011, p. 119). The acquisition and preparation of this data can be very time-consuming and require experience and expert knowledge for good results (Lindemann et al., 2008, pp. 79–80). Moreover, in a changing environment, the additional challenge is to keep the data or model up-to-date and valid (Jarratt et al., 2011, p. 119).

These limitations show that the strategies for efficient ECM are not easy to implement. Especially further support methods are necessary to enable sufficient frontloading and an efficient assessment of engineering change impacts. These methods have to reduce the efforts for information acquisition and support the updating and maintenance of the model or data. Promising approaches in this direction are the creation of knowledge models (e.g. Ahmad, Wynn, and Clarkson (2013)) and the implementation of the learning strategy through data mining in databases of past engineering changes (e.g. Wickel and Lindemann (2015)).

2.3 Safety Analysis and Assessment

Changes to a product can have an impact on the product safety. The efforts, which have to be undertaken to evaluate these effects are mainly safety analyses. This section defines the basic terms and concepts of safety analysis in Subsection 2.3.1. Based on these definitions, Subsection 2.3.2 introduces the FMEA and FTA, which are the most common methods of safety analysis. Moreover, Subsection 2.3.3 derives current challenges in the field of safety analysis and presents current research to cope with those. Subsection 2.3.4 summarizes the section and identifies remaining unsolved challenges.

2.3.1 Key Terms and Concepts of Safety Analysis

To understand the methods and challenges of safety analysis, it is necessary to define the key terms illustrated in Figure 2-7. In particular, the following paragraphs define the terms safety, hazard, failure and safety function.

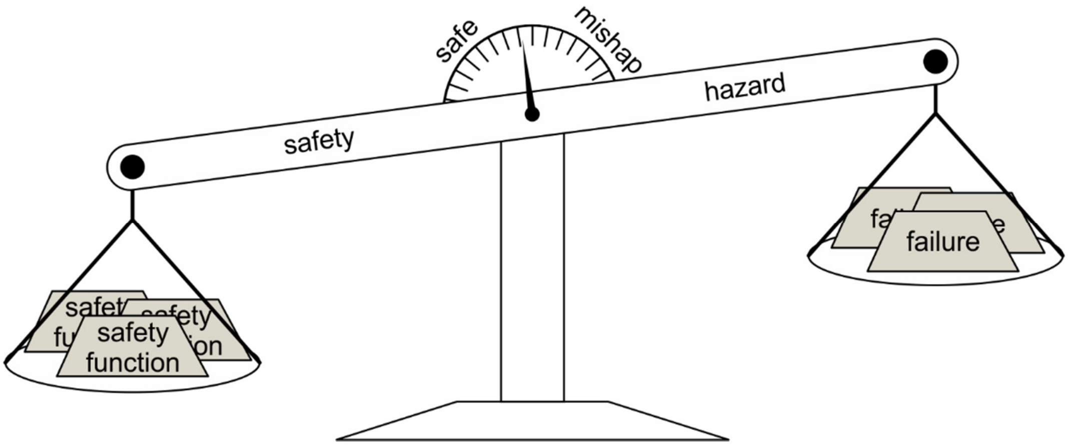


Figure 2-7: The key terms of safety analysis and their interrelation

The interpretations of the term **safety** vary depending on background and context. On the one hand, driven from systems engineering and systems theory, safety is defined as a system state. On the other hand, engineering design and related fields interpret safety as a system property.

The military standard MIL-STD-882E is a major representative of the first group. It is the approved standard for system safety of the United States Department of Defense and serves as central element of their systems engineering. According this standard, safety is the "freedom from conditions that can cause death, injury occupational illness, damage to or loss of equipment or property, or damage to the environment" (MIL-STD-882E, p. 7). This definition, driven from military operations, emphasizes the intactness of the military equipment and the soundness of its occupants or environment. This focus aligns with Leveson (2012), who defines safety as “freedom of accidents (loss events)” (Leveson, 2004, p. 250, 2012, p. 467). In summary, according to these definitions, safety is a system state, which describes the freedom of undesired events (i.e. losses or harm).

Yet, from an application perspective, this state of total freedom cannot be maintained in any case. Thus, Neudörfer (2014) interprets safety as system property instead of a system state.

According to him, “[...] safety is an immaterial system property. It ensures that the risk of hazards during the expected product life cycle and under defined conditions remains in an acceptable range” (Neudörfer, 2014, p. 587, freely translated). In short, this definition is also used by IEC 61508, which in summary defines safety as “freedom of unaccepted risks” (IEC 61508, p. 12). Even though Jensen and Tumer (2013) basically align with the first group, they define safety as system property, which can be measured by the “[…] relative difficulty of those [safety] constraints to be violated” (Jensen & Tumer, 2013, p. 827). They include the acceptable risks of the occurrence of accidents under the defined conditions, represented by safety constraints.

Both definition groups are not contradictory. Yet, as this thesis focuses on UDC products, the interpretation of safety as property, which has to be ensured, is better suitable. Thus, this thesis combines the interpretations of Neudörfer (2014, p. 587) and Jensen and Tumer (2013, p. 827) and defines safety as follows:

Safety is an immaterial system property. It describes the relative difficulty (risk) of hazards to occur during the planned product life cycle and under defined conditions. A system remains safe as long as the risk remains in an acceptable range.

A threat to the above-defined safety are **hazards**. Here, the interpretations from different backgrounds more or less align. All definitions emphasize the binarity of safety and hazard. MIL-STD-882E defines a hazard as “a real or potential condition that could lead to a series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment” (MIL-STD-882E, p. 5). Leveson (2012) interprets the undesired events as an accident and similarly defines hazard as “a system state or set of conditions that, […] will lead to an accident (loss)” (Leveson, 2012, p. 467).

Moreover, Neudörfer (2014) emphasizes the potential origin of the hazard by defining hazard as “[…] potential state […] characterized through latent or virulent material or energetic potential, which, when freed, can harm persons or objects or cause other negative effects […]” (Neudörfer, 2014, p. 579. freely translated). However, according to him, the state when hazard is binary to safety only emerges from the “[…] spatial and temporal co-occurrence of a potential hazard state with persons […]”(Neudörfer, 2014, p. 579. freely translated).

This thesis focuses on the design and safety analysis phase of UDC products. In these phases, it is important to consider the potential nature and source of hazard as well as the interaction of users with the customized product. Thus, this thesis uses the slightly adapted definition of Neudörfer (2014, p. 579) and defines hazard as follows:

A hazard is a potential condition with latent or virulent material or energetic potential that could lead to harm to persons, other objects, and the environment, or cause other undesired effects.

To describe the condition under which a system transits between the safe state and an accident, the terms error, fault and failure are used. However, literature does not define these terms consistently. This thesis sticks to the following definitions:

An **error** is a not tolerable deviation between actual and desired (i.e. theoretically correct) value (Neudörfer, 2014, p. 587). Errors usually occur as a result of a fault (Dubrova, 2013, p. 9). A

fault is a physical defect, incorrect process, or other flaw that occurs in the system (Dubrova, 2013, p. 9). It can also described as “abnormal condition that can cause an element […] to fail” (ISO 26262). The result of a fault can be a failure. A **failure** occurs, if the system is not able to deliver the required performance or behavior (Dubrova, 2013, p. 9; Neudörfer, 2014, p. 578). Finally, a **failure mode** “[…] is a physical description of the manner in which a failure occurs” (Stamatis, 2003, p. 84).

This thesis defines the term **safety function** as counterpart to failures. It mainly builds on the interpretation of Jensen and Tumer (2013, p. 827). They draw an analogy according to which a safety function resembles a “[…] system’s inertia, causing the system to resist moving to the mishap state” (Jensen & Tumer, 2013, p. 827). However, according to their definition, safety functions are not decomposable and occur on a system level. Considering UDC products and user-induced changes, this definition is not sufficient. Hence, this thesis extends and adapts the definition of Jensen and Tumer (2013, p. 827) and defines a safety function as follows:

A safety function either prevents the system’s transition from hazard to mishap or maintains the current (safe) system state. Safety functions can be decomposed and be allocated on every system level. They can manifest in multiple components, with multiple principles, and as passive features or active control structures.

2.3.2 Traditional Methods for Safety Analysis

To analyze and assess safety in the product development process, during the last decades various support methods and tools were developed. This on the one hand includes norms and standards, which provide requirements and constraints aiming to support and assure the development of safe products. Amongst these standards for technical products, EU Dir.2006/42/EC, EU Dir.2001/95/EC, and IEC 61508 are the most general.

On the other hand, a wide variety of methods to support safety analysis and assessment are available. The database of Everdij, Blom, and Kirwan (2006) currently lists over 700 methods related to safety analysis or assessment[4].

Out of this variety, Berres, Schumann, and Spangenberg (2014, p. 7) identify the Failure Mode, Effects and Criticality Analysis (FMECA) as well as the Fault Tree Analysis (FTA) as the two methods most commonly used in the detailed design of aerospace systems. Moreover, according to Neudörfer (2014, pp. 140–142), the Event Tree Analysis (ETA), Failure Mode and Effects Analysis (FMEA) and FTA are the major quantitative methods for the safety assessment of complex plants and machines.

In summary, FMEA, FMECA and ETA as well as FTA are the methods most commonly applied. However, the actual FMEA nowadays usually includes the FMECA (see the suggestions of IEC 60812 and AIAG (2008)). In addition, the ETA and FTA follow the same methodological principle (Neudörfer, 2014, p. 142). Moreover, standards like IEC 61025 suggest to combine the inductive FMEA with deductive FTA and many standards (e.g. ISO 26262) define the combination of both principles as mandatory for product development

[4] Source: http://www.nlr-atsi.nl/services/safety-methods-database, last access: 2016/09/29

(Cuenot, Ainhauser, Adler, Otten, & Meurville, 2014, p. 1). Thus, the following paragraphs introduce the fundamentals of FMEA and FTA as most important methods.

Failure Mode and Effects Analysis (FMEA)

The FMEA is a quantitative[5] analysis method, which aims to identify failures in products and processes (Lindemann, 2009, p. 263). Hence, it is commonly applied in various fields of product development and for various types of products. Its major applications are in quality management and safety analyses (Bertsche, 2004, pp. 106–107; Kamiske & Brauer, 2011, p. 64). As identified by Berres et al. (2014, p. 7), the FMEA plays a major role in the safety process. Thus, even though the FMEA is standardized in IEC 60812, various compendiums (e.g. Bertsche (2004), Werdich (2011), Eberhardt (2015), Carlson (2012), Stamatis (2003)) and software tools (e.g. IQ-FMEA[6] and SCIO-FMEA[7]) exist.

The standard FMEA can be applied in various phases of the product development process and on multiple abstraction levels (Kamiske & Brauer, 2011, p. 64). The most common types are the System FMEA, Design FMEA and Process FMEA (Bertsche, 2004, p. 108; Eberhardt, 2015, p. 155). Common to all types and variants is the inductive nature of the FMEA. Its main objective is to identify and assess the impact of possible failure modes on the considered system (Hering, Triemel, & Blank, 2003, p. 164; Kamiske & Brauer, 2011, p. 65).

The literature does not provide a consistent standard procedure or sequence of steps for the FMEA (Carlson, 2012, p. 108). Depending on context and background, the names and allocations of activities to phases vary slightly. This thesis summarizes the FMEA in the four steps illustrated in Figure 2-8, which are described in the following. This procedure combines the recommendations of Bertsche (2004, p. 125) and Eberhardt (2015, p. 121) and summarizes all activities prior to the failure analysis in the preparation step. All steps of the procedure are usually documented in FMEA-forms (Kamiske & Brauer, 2011, p. 68).

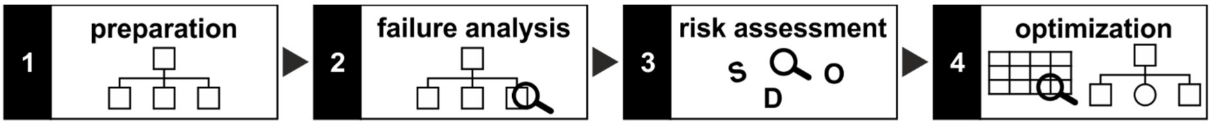


Figure 2-8: Procedure of the FMEA

The first phase **preparation** is essential for a successful FMEA (Carlson, 2012, p. 66). It first defines the aim and scope of the analysis. Based on that, the form and type can be selected (Eberhardt, 2015, p. 89; Werdich, 2011, p. 19). Moreover, for best results, the FMEA requires an interdisciplinary team, consisting of subject-matter experts and members familiar with the methodology (Bertsche, 2004, pp. 109–110; Carlson, 2012, p. 14). Moreover, access to relevant information and software to conduct the FMEA has to be ensured (Carlson, 2012, p. 67).

[5] Deviating from the given reference, some researchers interpret the FMEA as pseudo-quantitative or qualitative (e.g. Blum (2010, p. 25))

[6] Source: https://www.apis-iq.com/software/products, last access: 2016/09/29

[7] Source: http://www.plato.de/scio-fmea-en.html, last access: 2016/09/29

Once this organizational environment is defined, the preparation of the considered system is required. It is necessary to define the systems boundary and the interfaces to the environment. Based on this, the system can be decomposed in its elements (e.g. modules and components). Most authors suggest to arrange these elements hierarchically to obtain a tree-like system structure (Bertsche, 2004, pp. 125–127; Hering et al., 2003, pp. 138–144). Moreover, it is necessary to identify the functions of these system elements and their structure. By that, a functional structure is modeled and this model is connected to the system structure (Bertsche, 2004, pp. 128–130).

Using the previously modeled functional and system structure, the "core of the FMEA" (Eberhardt, 2015, p. 97), the **failure analysis** can be conducted. It identifies potential failure modes for each of the considered functions. The potential origins and effects of these failure modes are identified as well. For these tasks, support like checklists, statistics, creative methods and fault trees can be beneficial (Bertsche, 2004, pp. 130–136; Carlson, 2012, p. 119). During the considerations, it is important to keep a worst-case perspective (Eberhardt, 2015, p. 99).

The following **risk assessment** evaluates and assesses the risks of the identified failure modes. Therefore, three categories are defined (Bertsche, 2004, p. 127):

- The **severity** (S) ranks the severity of the failure mode's effects on a previously agreed scale (Carlson, 2012, pp. 125–126).
- The **occurrence** (O) ranks the likelihood of the failure mode's origins to occur and to cause the considered failure mode (Bertsche, 2004, p. 139; Carlson, 2012, p. 138).
- The **detection** (D) describes the likelihood that currently established control mechanisms (e.g. in production or the product) will be able to detect the failure mode (Bertsche, 2004, pp. 139–140; Carlson, 2012, p. 145).

The ranking scale used for all these categories usually ranges from one to ten (Kamiske & Brauer, 2011, p. 66). The risk priority number (RPN) merges these single rankings. It is defined as the product of the three category rankings (Bertsche, 2004, p. 141):

$$RPN = S \times O \times D$$

The risk priority number can help to prioritize the failure modes for optimization activities (Kamiske & Brauer, 2011, p. 66; Stamatis, 2003, p. 181). Usually, thresholds are defined to classify the failure modes into risk levels (Bertsche, 2004, p. 141). However, the validity of the risk priority number is limited. Exemplary reasons are that its values underlie subjectivity, its scale is not continuous, and extremely severe events might be neglected due to low occurrence and detection values (Carlson, 2012, pp. 150–151; Werdich, 2011, pp. 45–46). Instead, other methods like the risk matrix are suggested for practical application (Carlson, 2012, pp. 151–152; Werdich, 2011, pp. 47–54).

Based on the prioritization and risk levels of the failure modes, countermeasures to reduce the risk (i.e. RPN value) to an acceptable range are defined in the phase of **optimization** (Bertsche, 2004, pp. 143–146). The filled FMEA-forms including the optimization measures are used as documentation and for future reuse (Kamiske & Brauer, 2011, p. 68).

In summary, the FMEA is a systematic method, which helps to identify possible failure modes and mitigate or reduce their risk (Stamatis, 2003, p. 21). For example, according to Booker

(2012, p. 509), Carter (1986) found out that the application of the FMEA helped to detect 70 % of all failure modes in the design process. The FMEA thus, strongly contributes to an improved product safety.

However, this positive effect of the FMEA is opposed by some limitations. First, a problem of the FMEA is its limited efficiency and ergonomics (Maurer & Kesper, 2011, p. 181). The FMEA conducted in teams consumes high amounts of time of experienced engineers and causes high manual efforts (Höfig, Zeller, & Grunske, 2014, p. 111; Maurer & Kesper, 2011, pp. 180–181). Second, the quality of the outcome strongly depends on the information quality and hence, is influenced by uncertainties (Würtenberger, Kloberdanz, Lotz, & Ahsen, 2014, pp. 417–418). Lastly, as described above, the results are strongly affected by subjectivity.

Fault Tree Analysis (FTA)

The FTA is a quantitative[8] analysis method, which aims to identify dependencies between undesired events (i.e. failures) and their causes as well as to assess the probability of these failures (Lindemann, 2009, p. 262; Vesely, Goldberg, Roberts, & Haasl, 1981, p. IV-1). As for the FMEA, its applications are spread to various fields, but especially to quality management and safety or reliability analyses (Hering et al., 2003, pp. 137–138). The FTA can be used to in depth analyze events identified by prior analyses like FMEA (Flaus, 2013, p. 229). Moreover, it is standardized in different standards (e.g. NUREG-0492 (Vesely et al., 1981), IEC 61025) and various adaptions (e.g. success trees (Vesely et al., 2002) and dynamic fault trees (Dugan, Bavuso, & Boyd, 1992)) as well as software tools (e.g. FaultTree+[9] and CAFTA[10]) exist.

The standard FTA can be applied to various product classes and abstraction levels (Majdara & Wakabayashi, 2009, p. 1076; Vesely et al., 2002, p. 7). Common to all applications is the deductive nature of the FTA. Its main objective is to model and identify the root causes of undesired events and their contribution to the occurrence of the undesired event in a top-down hierarchical manner (Taylor & Ranganathan, 2014, p. 331). The FTA according to Vesely et al. (2002, p. 22) (NUREG-0492) consists of eight steps. However, this thesis combines three steps and adds the system analysis, which following Hering et al. (2003, pp. 138–144) is important for the preparation of an FTA. The resulting procedure of the FTA consists of the seven steps visualized in Figure 2-9.

In the first step, **identify FTA objective**, it is necessary to clearly identify and define the objective of the analysis. This ensures that the results allow to draw the required conclusions (Vesely et al., 2002, p. 22). Based on these objectives, the step **system analysis** examines the considered system and decomposes it into its elements (e.g. subsystems or components). The system usually is modeled in a system structure or block diagram, which includes the system boundary (Hering et al., 2003, p. 145).

[8] The FTA can also be used as qualitative method only (see Hering et al. (2003, p. 157)).

[9] Source: http://www.isograph.com/software/reliability-workbench/fault-tree-analysis, last access: 2016/09/29

[10] Source: http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001015514, last access: 2016/09/29

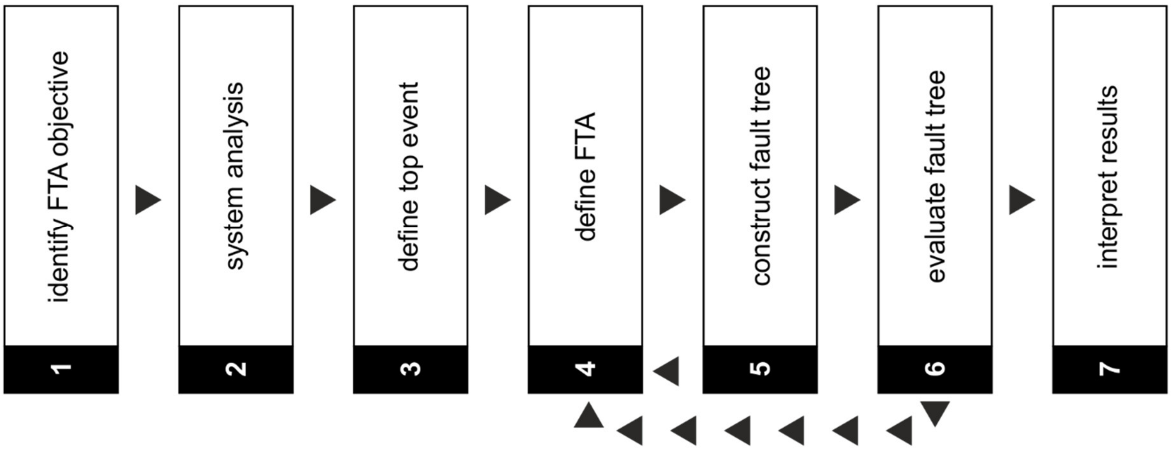


Figure 2-9: Procedure of the FTA (adapted from Vesely et al. (2002, p. 22))

The next step, **define top event**, builds on the objective and the understanding of the system created in the first two steps. It identifies and defines the top event of the FTA, which usually is the failure of the system, "[…] that will be analyzed" (Vesely et al., 2002, pp. 22–23) and whose causes will be identified (Vesely et al., 2002, pp. 22–23).

The following step, **define FTA**, includes the definition of the analysis's scope, its resolution, and its ground rules. The scope defines the boundary conditions and the selection, which faults are included in the analysis. The resolution describes, which level of detail is chosen and the ground rules define nomenclature and selected construction elements of the fault tree (Vesely et al., 2002, pp. 23–24).

Once the FTA is defined, the actual **construction of the fault tree** is conducted (Vesely et al., 2002, p. 23). A fault tree consist of two categories of elements: events and gates. Events represent errors, faults, or failures (Taylor & Ranganathan, 2014, p. 332). They can be classified in top events, intermediate events and basic events. According to this classification, basic events represent the roots of the fault tree and are not further decomposed in the FTA (Taylor & Ranganathan, 2014, p. 332; Vesely et al., 2002, p. 34). Gates connect the events of different hierarchical levels. Usually Boolean logic is used for the gates, for example AND-gates and OR-gates. In the first case, the higher-level fault only occurs, if all input faults occur. In the second case, the occurrence of one input fault is sufficient to cause the higher-level fault (Vesely et al., 2002, p. 34). The result of this step is a fault tree as shown in Figure 2-10.

The sixth step **evaluates the constructed fault tree**. This can be done qualitatively and quantitatively (Vesely et al., 2002, p. 24). The qualitative evaluation determines cut sets. Cut sets are sets of basic events that cause the top event when they are simultaneously active (Flaus, 2013, p. 232; Vesely et al., 2002, p. 3). A special variant of cut sets are the minimal cut sets (MCSs). Cut sets are minimal cut sets, when "[…] it is impossible to retain one of its elements without the entire set being a cut set" (Flaus, 2013, p. 232). The quantitative evaluation instead calculates probabilities. By that, the probability of the top event can be determined and the dominant cut sets are identified (Vesely et al., 2002, p. 24). However, to conduct this calculation, all probabilities of the basic events need to be known (Flaus, 2013, p. 231).

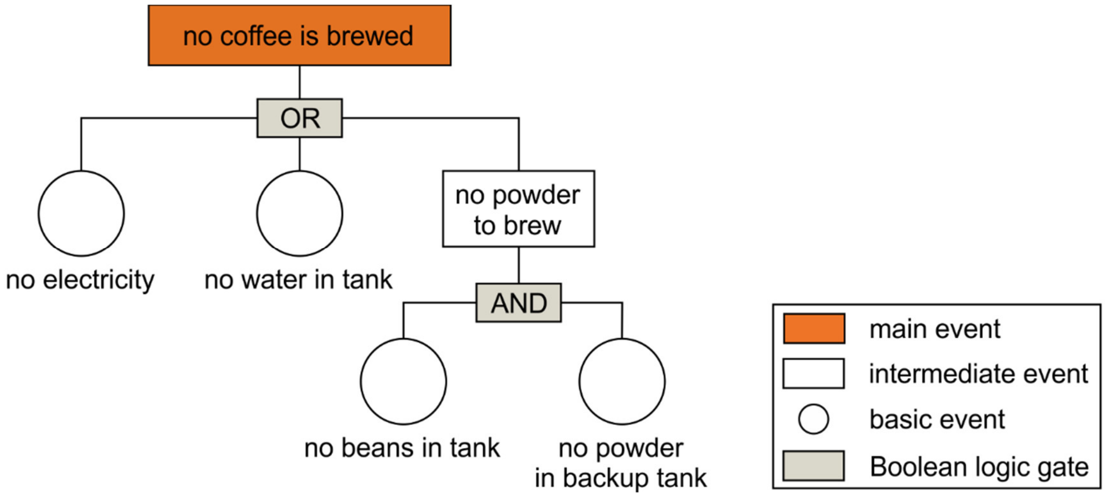


Figure 2-10: Exemplary fault tree of a coffee machine

In the last step **interpret results**, the results of the evaluation are interpreted and visualized adequately. Based on this, conclusions for optimizations can be drawn and the evaluation of top event probabilities can be documented (Vesely et al., 2002, p. 24).

In summary, the FTA helps to evaluate systems reliability by using a graphical notation to determine combinations of faults, which will cause an undesired event (Majdara & Wakabayashi, 2009, p. 1086; Vesely et al., 1981, pp. IV-1). By that, amongst other advantages, the FTA supports the prevention of top events, monitors system performance, and supports the understanding of the system architecture as well as its influence on top events. All these advantages support the system design (Taylor & Ranganathan, 2014, p. 339; Vesely et al., 2002, p. 5). Additionally, the FTA helps to assess the impact of design changes (Stamatis, 2003, p. 46).

However, the FTA is not able to consider fault dependencies and their dynamic nature (Taylor & Ranganathan, 2014, p. 339). Moreover, many researchers point out that the application of the FTA is a time-consuming task, which needs much efforts, experience and is error prone (Majdara & Wakabayashi, 2009, p. 1076; Mhenni, Nguyen, & Choley, 2014, p. 716; Sierla, Tumer, Papakonstantinou, Koskinen, & Jensen, 2012, p. 138).

Further Methods for Safety Analysis

As the reviews of Wang and Ruxton (1997) and Berres et al. (2014) underline, apart from the previously described FMEA and FTA, various other, but less prominent, methods are applied. For example, the Preliminary Hazard Analysis is a suitable method to identify and evaluate hazards in the early phases of design (Roland & Moriarty, 1990, pp. 206–212). Another example is the Hazard and Operability Study, which analyzes planned operations and identifies potential risks (Ericson, 2005, pp. 365–381). However, these and others usually supplement the established methods FMEA and FTA.

2.3.3 Overview of Current Developments in Safety Analysis

At current stage, the limitations of the traditional methods for safety analysis and assessment, described above (see Subsection 2.3.2), lead to various challenges for the safety-related activities in the product development process. In addition, general developments of the markets and technology influence these safety-related activities.

As previously described, the **complexity of products** in the current markets steadily grows and the technology evolves (Leveson, 2012, pp. 3–4). However, the methods of safety analysis like FTA and FMEA made little progress and did not evolve with technology (Leveson, 2004, p. 238, 2012, p. xvii). Moreover, the **regulations** according to which products have to be certified prior to commercialization are getting **more rigorous and strict** (Mhenni et al., 2014, p. 378; Stirgwolt, 2013, p. 1). Most prominent examples are IEC 61508 and ISO 26262. For example IEC 61508 introduces safety integrity levels (SILs). They translate the acceptable risk of safety-relevant failures to discrete levels (Blum, 2010, p. 24; IEC 61508). These developments impose various new challenges, which in the following are described.

The FMEA and FTA same as many other established safety methods are mainly applied in the later stages of design, like the detailed design stage (Berres et al., 2014, p. 7; Cuenot et al., 2014, p. 1; Ghemraoui, Mathieu, & Tricot, 2009, p. 161). The applications mainly are of a review-centered nature (Jensen & Tumer, 2013, p. 825). Moreover, the role of safety often receives not sufficient attention in early stage design methods (Sierla et al., 2012, p. 137). Yet, if failures are discovered at late phases, costly late changes can be the result (Ehrlenspiel et al., 2014, p. 14; Jarratt et al., 2011, p. 110).

An early integration of safety analysis, which represents an early consideration of safety aspects, can help to fulfill safety requirements with relatively low costs and reduce late rework (Biehl, Chen, & Törngren, 2010, p. 125; Krus & Grantham Lough, 2007, p. 1). Moreover, an early evaluation of safety can provide great benefit to designers (Jensen & Tumer, 2013, p. 827). An **early consideration and analysis of safety** would allow designers to design within a safe solution space instead of checking in a review-based manner, if their solution is safe (Jensen & Tumer, 2013, p. 825).

To enable this integration of safety considerations in early phases, safety analysis and early-stage design methods need to be harmonized. However, Berres and Schumann (2014, pp. 143–144) and Biehl et al. (2010, p. 131) identify a **gap between the domains of safety analysis and design**. Moreover, many authors like Cuenot et al. (2014, p. 1), Herfeld, Fürst, and Braun (2007, p. 271) and Blum (2010, p. 26) emphasize that the increasing complexity of products further impacts the safety analysis: The high number of components and interactions complicates the analysis and often different tools are used for engineering design and safety analysis. Thus, to bridge the gap between both domains, their methods, processes and tools should be harmonized and mutual awareness should be fostered.

The increased complexity not only leads to an increased need for harmonization, but also increases the volume of the safety analysis. As described in Section 2.3.2, the traditional methods of safety analysis as major limitations are work-intensive, involve large experience, provide limited ergonomics, and are error-prone. As shown by de la Vara, Jose Luis et al. (2016, p. 14), even in the domain of software engineering still many tasks of the safety analysis remain manual. Hence, their **efficiency** has to be improved or new methods are needed. Efficiency in this context especially comprises time, experience and resources.

In summary, the current developments impose the following **three challenges for safety analysis** and safety considerations within the product development process:

- early integration of safety aspects
- bridging the gap between domains
- improving efficiency of safety analysis methods

Various research tries to tackle these challenges. The following paragraphs list and depict current approaches based on an extensive literature review. The search was conducted in relevant databases and journals[11]. A publication was selected from the huge number of results, when it addresses aspects of the safety analysis in connection to the design of technical products.

The identified publications can be classified into two categories. On the one hand, publications propose design methodologies, which shift safety considerations in the center of the design process. On the other hand, publications propose specific methods, which aim to improve specific tasks or methods of safety analysis. The following paragraphs briefly describe these publications. Moreover, Figure 2-11 summarizes them and evaluates their contribution to the challenges identified above.

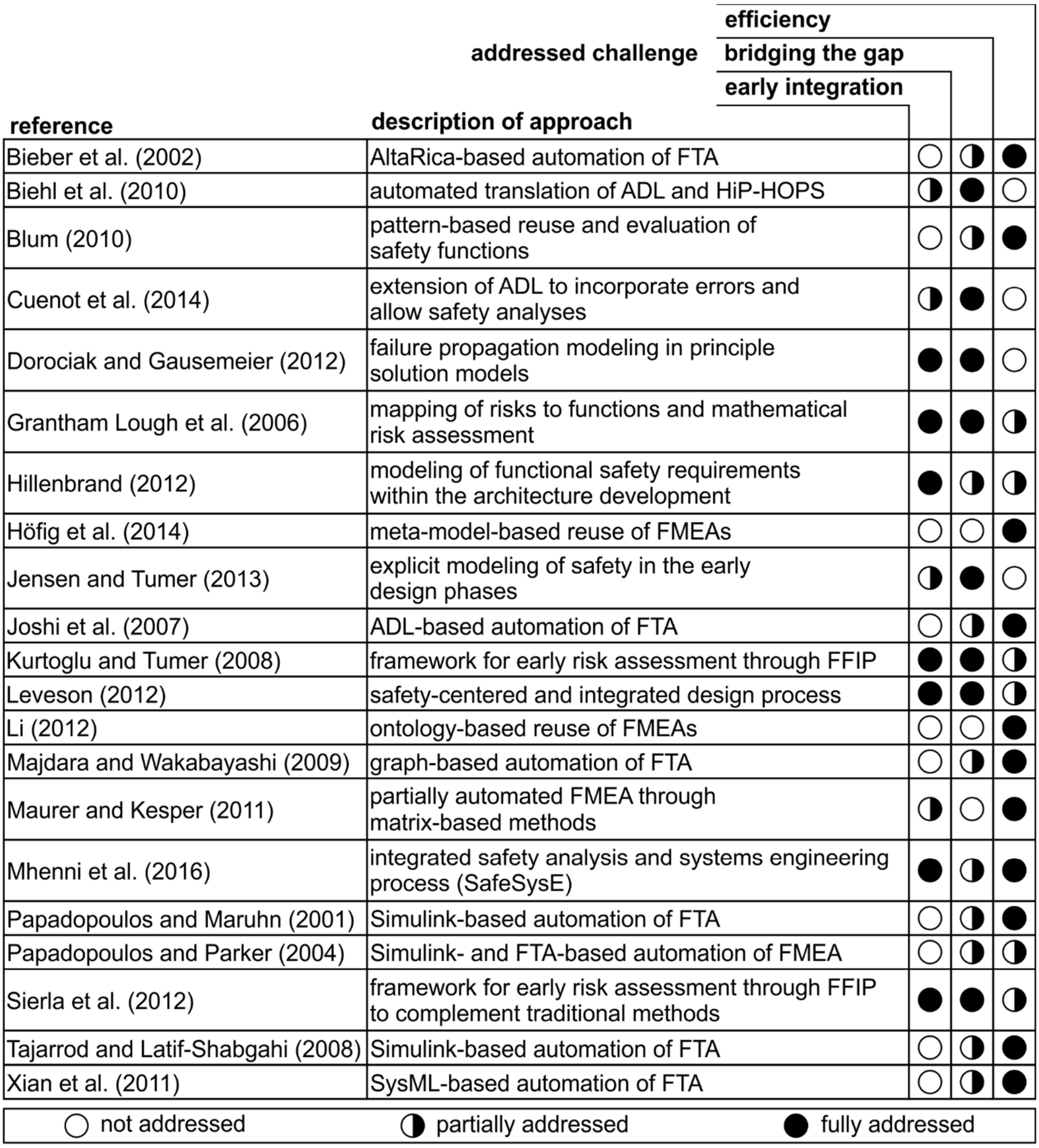
The most basic methodology tackling the hurdles above is the safety-guided design process of Leveson (2012). She uses the System-Theoretic Accident Model introduced in Leveson (2004) and supplements it by a new and **safety-guided design methodology** together with in integrated system and safety engineering process. Its main intention is to use a safe solution space instead of analyzing existing designs on safety flaws.

Jensen and Tumer (2013) follow the same notion and try to achieve an early integration by integrating safety into a model-based design methodology. They also build on the System-Theoretic Accident Model and provide a six-step **safety-centric design process** to include safety functions into model-based functional systems design.

Moreover, Mhenni, Nguyen, and Choley (2016) integrate the safety analysis in a model-based systems engineering approach. They provide a **process integrating safety analyses and systems engineering** in the early phases of design. Using a product model in the Systems Modeling Language (SysML), they propose further methods to automate parts of FMEA and FTA (see Mhenni, Nguyen, Kadima, and Choley (2013), Mhenni et al. (2014) and Mhenni et al. (2014)).

Kurtoglu and Tumer (2008) also aim to integrate safety considerations in an early stage of design. They provide the **Functional Failure Identification and Propagation Framework (FFIP)**. It allows the analysis of functional failures and fault propagation on a very abstract system concept level. Sierla et al. (2012) use this framework additionally in combination with simulations to allow a risk assessment in early stages of design.

[11] Databases: Design Society, IEEE Xplore; Journals: Res. in Eng. Design, Journal of Eng. Design, Systems Engineering, Reliab. Eng. Syst. Safe.



		addressed challenge		
reference	description of approach	early integration	bridging the gap	efficiency
Bieber et al. (2002)	AltaRica-based automation of FTA	○	◑	●
Biehl et al. (2010)	automated translation of ADL and HiP-HOPS	◑	●	○
Blum (2010)	pattern-based reuse and evaluation of safety functions	○	◑	●
Cuenot et al. (2014)	extension of ADL to incorporate errors and allow safety analyses	◑	●	○
Dorociak and Gausemeier (2012)	failure propagation modeling in principle solution models	●	●	○
Grantham Lough et al. (2006)	mapping of risks to functions and mathematical risk assessment	●	●	◑
Hillenbrand (2012)	modeling of functional safety requirements within the architecture development	●	◑	◑
Höfig et al. (2014)	meta-model-based reuse of FMEAs	○	○	●
Jensen and Tumer (2013)	explicit modeling of safety in the early design phases	◑	●	○
Joshi et al. (2007)	ADL-based automation of FTA	○	◑	●
Kurtoglu and Tumer (2008)	framework for early risk assessment through FFIP	●	●	◑
Leveson (2012)	safety-centered and integrated design process	●	●	◑
Li (2012)	ontology-based reuse of FMEAs	○	○	●
Majdara and Wakabayashi (2009)	graph-based automation of FTA	○	◑	●
Maurer and Kesper (2011)	partially automated FMEA through matrix-based methods	◑	○	●
Mhenni et al. (2016)	integrated safety analysis and systems engineering process (SafeSysE)	●	◑	●
Papadopoulos and Maruhn (2001)	Simulink-based automation of FTA	○	◑	●
Papadopoulos and Parker (2004)	Simulink- and FTA-based automation of FMEA	○	◑	◑
Sierla et al. (2012)	framework for early risk assessment through FFIP to complement traditional methods	●	●	◑
Tajarrod and Latif-Shabgahi (2008)	Simulink-based automation of FTA	○	◑	●
Xian et al. (2011)	SysML-based automation of FTA	○	◑	●

○ not addressed ◑ partially addressed ● fully addressed

Figure 2-11: Relevant publications aiming at the identified challenges and their contribution to them

Dorociak and Gausemeier (2012) follow a similar approach and provide an extended **modeling environment to describe failure propagations** on the level of principal solutions. By that, they enable first safety evaluations at a concept stage. And Grantham Lough et al. (2006) propose a method to map functions and risks in order to enable an **early risk assessment** in the conceptual design phase.

Biehl et al. (2010) strive to integrate safety analysis into design by enabling an **automated translation between models** in the Architecture Description Language and the Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS). Cuenot et al. (2014) also rely on the Architecture Description Language to achieve an integration of design and safety analysis. However, instead of translations, they extend the Architecture Description Language to model errors and to analyze the architecture models respectively.

Incorporating a specific regulation, Hillenbrand (2012) provides an approach to **include functional safety** according to ISO 26262 in the concept and modeling of electric/electronic architectures. He applies extraction methods to provide model data for subsequent development activities.

Moreover, Blum (2010) develops a methodology to improve the efficiency of the design process by the **reuse of safety function patterns**. He proposes to reuse these patterns and automatically evaluate them to reduce the efforts involved in design and safety assurance of mechatronic products.

Concerning the traditional methods, many researchers strive to **improve the efficiency of the FMEA**. For example Li (2012) provides a method and tool to reuse failure modes in FMEAs based on ontologies. Moreover, Höfig et al. (2014) aim to reuse FMEAs of components by providing a meta-model for FMEAs. And Maurer and Kesper (2011) apply matrix-based methods to automate the generation of the system and failure structure during the FMEA to ensure completeness and improve efficiency. As already described above, Mhenni et al. (2014) automatically derive pre-filled FMEA-forms from SysML models and Papadopoulos, Parker, and Grante (2004) similarly deduce FMEAs from Simulink models and derived fault trees.

Same as for the FMEA, multiple researchers tackle the **efficiency of the FTA** and its integration with models used during the design process. For example, Mhenni et al. (2014) and Xiang, Yanoo, Maeno, and Tadano (2011) automatically derive fault trees from SysML models. Moreover, Papadopoulos and Maruhn (2001) and Tajarrod and Latif-Shabgahi (2008) automate the generation of fault trees in Simulink. Majdara and Wakabayashi (2009) use directed graphs, Bieber, Castel, and Seguin (2002) rely on Alta Rica, and Joshi, Vestal, and Binns (2007) on the Architecture Description Language to automate the FTA.

In summary, none of the existing publications is fully able to solve all three identified challenges. Most proposed methods are only suitable in specific situations or have a limited area of application.

2.3.4 Summary and Challenges of Safety Analysis

The previous subsections show that the traditional methods FMEA and FTA still play a major role, even though various approaches in literature try to tackle the identified challenges. The published approaches usually focus on one or two of the challenges in the field of safety analysis only and are not able to solve all three challenges together.

The first category of approaches aims at an integrated methodology of safety analysis and design. It mainly addresses the challenges of early integration and a closing of the gap between both domains. The proposed methodologies usually integrate models used in both domains. This is achieved by either translation algorithms or the integration of safety aspects in product models. The second category mainly focuses on an improved efficiency of the safety analysis by full or partial automation. To generate fault trees or FMEA-forms automatically, models are used and processed. Thus, model-based methodologies seem to be suitable to address all challenges.

However, the majority of approaches originates from the design of embedded systems or software. The application to mechatronic products is discussed in single cases but not extensively. Thus, the applied models mainly are specific models used in these domains (e.g. Architecture Description Language, Simulink). Still, SysML is commonly used to tackle the challenges and improve the safety analysis and provides potentials for further improvement.

To solve the identified challenges in the field of technical consumer products, an integration of models will be necessary to enable a transfer or adaption of existing approaches. Only if this is achieved, the challenges can be solved, the benefits of newer methods can be accessed, and an early integration of safety considerations can be realized.

2.4 The Interface and Necessity of Cooperation of the Three Fields

The previous Sections 2.1 to 2.3 introduce the theoretical background of customization, engineering change management and safety analysis as well as their methods and current challenges. This section summarizes them in Figure 2-12 and the following paragraphs. The section moreover, derives the necessity of their cooperation with special focus to UDC.

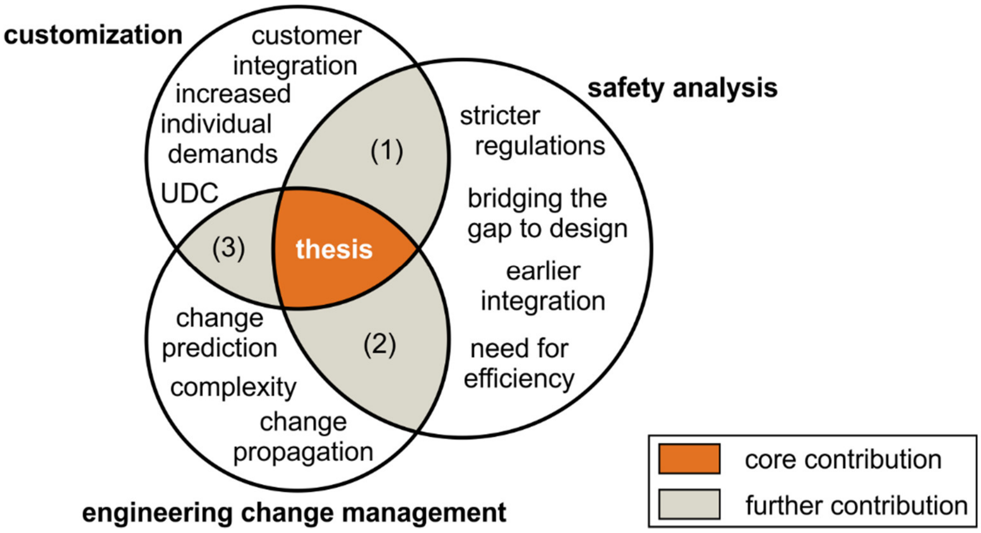


Figure 2-12: Summary of the challenges in the relevant research fields of this thesis

The field of **customization** is characterized by an increasing demand for individual products, which cannot be fully satisfied by existing customization concepts. New methods from the field of Open Innovation allow and demand for a more intense involvement of the users. In connection with technological progress, the concept of UDC is a promising approach to react on these demands.

On the flipside, customization induces **changes** to the product. However, even in the development of mass products, engineering changes are challenging to handle. As products get more complex and engineering changes can propagate to other elements of the products, methods and tools are applied to evaluate and manage changes. The challenge is to predict changes, acquire information on the product as well as past engineering changes, and to keep the used models or databases up-to-date.

Due to these challenges and especially in connection with change propagation, the concept of UDC imposes further challenges. The self-customization leads to various user-induced changes conducted by non-experts. These changes have to be managed despite the tightened conditions, which further intensify the existing challenges.

Not only the management of engineering changes, but also the **analysis and assurance of safety** becomes more and more challenging due to the increasing complexity of products. Stricter safety regulations even further worsen this challenge from a product development perspective. However, still the established methods of FMEA and FTA are mostly applied in the process of safety analysis. Both methods require large efforts. Thus, to handle the challenges, researchers demand an early integration of safety aspects, a closing of the gap between design and safety analysis, and an increased efficiency. Current approaches try to tackle these points of action by the development of model-based analyses and automated workflows.

An increased variance or customization imposes further challenges for validation and quality activities like safety analysis (Jiang et al., 2007, p. 1156; Papakonstantinou, Sierla, & Koskinen, 2011, p. 1). Especially for the challenge of early consideration, UDC represents a potential contradiction. Late customization through non-experts can have a strong impact on safety aspects. Thus, also ECM should consider the impact of changes on safety and safety analyses.

In summary, it can be stated that for a successful realization of customized products, more flexible and efficient products and processes are required. (Lindemann et al., 2006, p. 11). In addition, the previous paragraphs identified the dependencies between the three fields of customization, ECM and safety analysis. Hence, a cooperation between the three fields is essential and methods supporting the design and usage of this interface between the tree fields are necessary.

3. Challenges of Safety and Change Analysis within User-driven Customization

The previous chapter identifies the need for a detailed consideration of the interface of customization, ECM, and safety analysis, with special focus on UDC. This chapter analyzes this interface. In Section 3.1, the state of science concerning the interface is discussed. An explorative questionnaire survey in Section 3.2 researches the general impacts of UDC on the product development process. Building on the identified influences, Section 3.3 conducts focus-interviews to identify industrial practices and UDC's impact on those. Section 3.4 consolidates the findings and uses them to concretize the objective of this thesis and to derive requirements.

3.1 The Interface of the Three Fields in Research

The previous Section 2.4 summarizes the challenges within the three fields of customization, ECM, and safety analysis as well as it outlines the resulting challenges at the interface. Existing research supports these findings in general. For example, Lindemann et al. (2006, p. 11) demand for changes within the product development for customized products compared to conventional mass products. According to Pulm (2004, p. 141) customization adds additional efforts, complexity, and uncertainty to the development activities. From a general perspective, Lindemann et al. (2006, p. 11) identifies a need for product structures and development processes tailored to customization, as well as for flexible production systems.

This underlines the need for a cooperation between the three fields and simultaneously represents important challenges, especially considering the new concept of UDC. In the following, the specific interfaces are discussed in detail, their occurring challenges are derived from literature, and general solution approaches proposed by research are introduced. Figure 3-1 summarizes the major challenges and solution approaches identified at the dual interfaces.

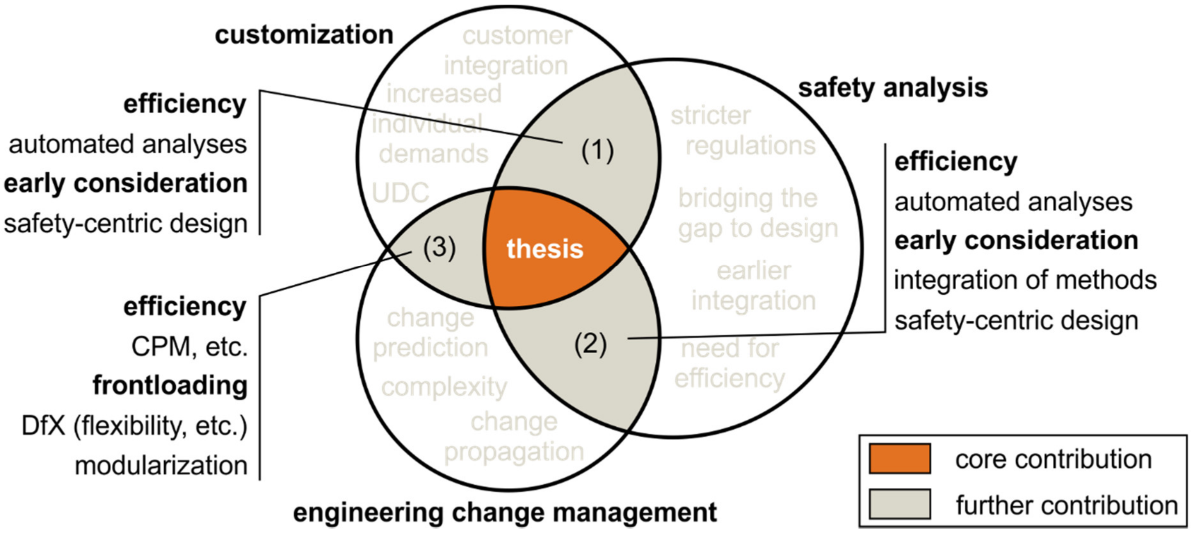


Figure 3-1: Summary of the challenges and approaches at the dual interfaces considered in this thesis

As described in Section 2.4, customization implies challenges for the assurance of quality and safety. Hence, the **interface between customization and safety analysis (1)** is important. Increasing customization leads to a higher variance, which in turn increases the total efforts of safety analysis, approval, and validation (Jiang et al., 2007, p. 1156; Papakonstantinou et al., 2011, p. 1). From a general perspective, the challenges of safety analysis described in Subsection 2.3.3 comply with the impacts of customization. The challenge from both perspectives is, to reduce efforts by **increased efficiency** and an **early integration of safety aspects**.

To solve this compliant challenge at the interface of customization and safety analysis, especially the domain of software development focuses on **automated and formalized methods**. For example, Papakonstantinou et al. (2011) automatically create and validate software instances of a software product line. As another example, Jiang et al. (2007) develop a quality management system for customized products. However, even though these existing works are connected to the interface, none of them aims to explicitly support the interface between safety and customization. Yet, concepts for reuse of analyses (e.g. the metaFMEA by Höfig et al. (2014)) to some extent might also be suitable to solve challenges at this interface.

UDC adds further challenges. The integration of users in the design process intensifies both, the challenge of an early consideration of safety aspects and the challenge of **bridging the gap between safety analysis and design** (see Subsection 2.3.3). The reasons are unforeseen design outcomes and instead of closing the gap between engineers of the domains of design and safety analysis, the bridge has to be built between engineers and users. These specific aspects are not yet discussed in literature.

The second **interface between ECM and safety analysis (2)** to large parts consists of harmonic challenges. As Subsections 2.2.2 for ECM and 2.3.3 for safety analysis deduce, both fields strive for **frontloading and efficiency**. Research in safety analysis aims to consider safety aspects early during the design process. This notion can prevent or shift changes to earlier stages. It complies with the basic ECM strategies. Moreover, research in both fields introduces new methods for an improved efficiency of analyses and strongly relies on model-based approaches.

Despite both fields face compliant challenges, no existing research tries to integrate both fields. While major ECM methods introduced in Subsection 2.2.3 mainly focus on propagations in the domains of components and engineering processes, the bridge to safety analyses and corresponding impacts has not been built. Hence, a support closing the gap and supporting the analysis of the impact of engineering changes on safety is currently missing.

The third **interface between customization and ECM (3)** is important as well. As defined in Subsection 2.1.1, customization represents an alteration of the product. This alteration to some extent can be considered an engineering change. However, customization contradicts many of the basic strategies to cope with engineering changes, described in Subsection 2.2.2. If additionally a customization concept with a late decoupling point is chosen, neither prevention, nor learning might be possible. The resulting challenge at this interface is the **efficient** handling of these changes. Research approaches and methods to improve the efficiency of ECM are already discussed in Subsection 2.2.3.

Moreover, research at the interface between customization and ECM tries to implement **frontloading** strategies (see Subsections 2.2.2 and 2.2.3). Many methodologies strive to anticipate customizations and resulting change requests to reduce the corresponding efforts. Examples are the incorporation of flexibility (Neufville & Scholtes, 2011), using change forecasts to improve modularization (Koh, Förg, Kreimeyer, & Lienkamp, 2015), or Design for X (DfX) guidelines like design for adaptability (Hashemian, 2005) and design for changeability (Fricke & Schulz, 2005).

However, UDC adds another perspective to customization: changes directly applied within a web-based UDC-toolkit through users, who often are non-experts in design (see Subsection 2.1.4). This might even worsen the challenges at the interface described above. Especially, the late and external decoupling point of UDC induces **late user-induced changes**. These changes through non-experts further contradict to the strategies of effectiveness and prevention. Yet, research until now does not tackle this specific interface.

The discussion on the three dual interfaces in previous paragraphs highlights on the one hand the interrelations between all three fields, and on the other hand the limitations of the current state of science. Thus, an **integration of all three fields** is necessary.

However, the existing approaches described above fail to unite the three fields and their challenges. The general methodologies or guidelines like design for adaptability try to integrate flexibility in design to react on configuration needs. The resulting changes occur late in the development process or even in the phase of usage. Consequently, the safety impact of these adaptions will be analyzed review-based once it occurs. To support this, newer approaches of safety analysis try to enable a reuse of analyses. However, as identified above, a direct link to methods of ECM and customization is missing.

In summary, the connection of ECM and safety analysis to the concept of UDC is not discussed in existing literature. The actual impact of UDC on the three fields and on the identified interfaces is not known at this stage. The above-described challenges at the interfaces are derived from the state of science. However, at this point, they include many assumptions.

3.2 Study on Implications of User-driven Customization

The review of literature addressing the interface of UDC, Safety Analysis and ECM in the previous Section 3.1 does neither suggest solutions, nor provide sufficient research to evaluate the implications of UDC on the development process and connected challenges. Section 3.1 proposes general implications of customization and draws to some extent conflicting challenges and approaches for safety analyses, ECM, and customization concepts with a late decoupling point. Thus, the state of science does not provide sufficient knowledge of UDC and its implications. However, to answer the research question of this thesis and develop suitable methods, which support the safety analysis of UDC products, the knowledge of these implications is essential.

To analyze the current situation, Blessing and Chakrabarti (2009, p. 104) suggest to apply real-time data-collection methods (e.g. observations) or retrospective methods (e.g. questionnaires or interviews). However, as explained in Subsection 2.1.5, UDC still has a visionary character and is not yet fully realized in industrial application. Thus, real-time data-collections are not a suitable tool for analysis. Instead, it is necessary to draw conclusions from the experience of professionals of the relevant domains. To achieve this, interviews and questionnaires are most suitable (Blessing & Chakrabarti, 2009, p. 104). Thus, this thesis conducts an explorative questionnaire survey based on experience and expertise of subject-matter experts, to identify the general implications of UDC on the product development process.

The following subsections describe the methodology and the results of the explorative questionnaire survey to determine the possible implications of UDC on the development process. This study was conducted in a student project (Ulrich, 2015) and is partially published in Roth et al. (2016).

3.2.1 Research Methodology of the Questionnaire Study

The existing literature described in previous section allows only assuming some potential impact areas of UCD. It does not directly allow deriving a suitable set of hypotheses on the impacts of UCD on the product development process. Therefore, the research methodology of the explorative questionnaire survey combines a qualitative and quantitative approach. Figure 3-2 summarizes this resulting research methodology. It comprises a qualitative exploration through interviews, the generation of hypotheses, and a quantitative exploration in the questionnaire survey. The following paragraphs describe this methodology in detail.

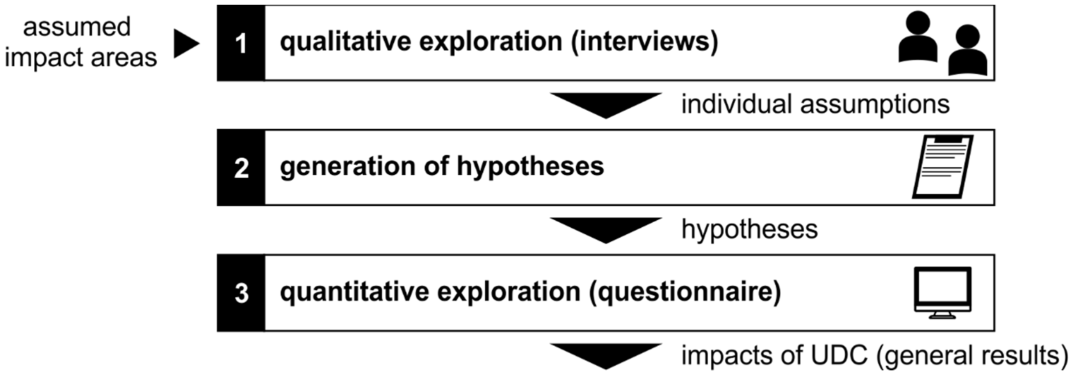

assumed impact areas
1
qualitative exploration (interviews)
individual assumptions
2
generation of hypotheses
hypotheses
3
quantitative exploration (questionnaire)
impacts of UDC (general results)

Figure 3-2: Research methodology to identify the potential impacts of UDC on the product development process

The methodology builds on the clarification of the term UDC and the drawn boundaries to other customization concepts provided in Section 2.1. Moreover, the potential impact areas of UDC identified in Section 3.1 were used as input.

Based on this, initial qualitative **semi-structured interviews** were selected to prepare the generation of hypotheses. This method is specifically suitable to generate and pretest hypotheses (Keuneke, 2005, p. 259; Kurz, Stockhammer, Fuchs, & Meinhard, 2009, p. 464). The central question of these interviews was defined as:

“What are the impacts of UDC on the development process of technical products?”

However, due to the novelty of UDC, the interviewees at the beginning were introduced to the concept of UDC and the V-Model (VDI 2206). The latter was used as reference model and to structure the following interview according to the phases of the traditional development process.

The main part of the interviews was conducted following the central question stated above. This central question was supplemented by a semi-structured guideline (see Appendix 9.1.1). The guideline provides ten question items, which were derived from the knowledge provided in Section 2.1 and 3.1. The items address general aspects as well as the specific impacts on:

- phases of the design process (requirements, task clarification, system design, domain-specific design integration and ensuring properties)
- cross-disciplinary tasks (scheduling and costing, risk and configuration management)

The interviews were conducted with four interviewees selected according to the following criterion: They should have a similar position and possess profound knowledge of all phases of the development process. As a result, all four interviewees were either consultants or project managers in product development. To avoid potential bias the interviewees consisted of young and very experienced professionals. As suggested by Keuneke (2005, p. 255), the interviews were conducted by a student involved in the project in the natural environment of the interviewees (i.e. their company) and approximately took one hour. They were recorded and transcribed afterwards.

The individual assumptions and expectations from the interviews were consolidated to **derive hypotheses on the impact of UDC** on the product development process. If necessary, the hypotheses were subdivided to reduce the complexity of the assessment and achieve a higher precision of the results.

These hypotheses were tested in a **quantitative questionnaire survey**. This method is suitable, as it allows to collect the personal assessment of a large group and potential bias through the interviewer is avoided (Häder, 2015, p. 193). Thus, a web-based questionnaire survey was conducted. Its questionnaire (see Appendix 9.1.3) uses in total 18 questions to obtain general information on the participants and to test the hypotheses.

To make the participants familiar with the concept of UDC, a comic similar to Figure 2-5 on page 18 describes its possible process flow. Moreover, the basics of the V-Model (VDI 2206) were explained to provide a reference model and to structure the questionnaire. The resulting questionnaire consists of the following five sections:

- questions on professional experience and industrial sector
- questions addressing the whole development process and all general phases
- detailed questions regarding the task clarification
- questions on user involvement and other aspects
- employment information and professional background

The questions connected to the hypotheses were measured on a five-level Likert-scale (McIver & Carmines, 1981, pp. 22–37), if applicable. When possible, the answer items were sorted randomly and, if suitable, fields for additional comments were provided.

To ensure the questionnaire quality, a pre-test was conducted with eight participants familiar to the topic and one without specific knowledge in product development. Based on their feedback, the questionnaire was subsequently adapted and improved.

To conduct the main study, the questionnaire was hosted on a web portal[12] for eight weeks starting from 6th of August 2015. Invitations were distributed via email to members of the Chair of Product Development's professional networks as well as in suitable groups of professional and non-professional social networks. The obtained study results were analyzed and evaluated using the software SPSS 22.0. The analysis included a test of significance (2-tailed student's t-test) for the items measured with the Likert-scale. Based on this analysis, the hypotheses were confirmed or rejected to determine the impacts of UDC on the product development process.

3.2.2 Implications of UDC on the Product Development Process

Based on the research methodology described above, this section presents the results of the qualitative interviews and the quantitative questionnaire survey. First, the individual assumptions and expectations of the interviewees are summarized. Then, the hypotheses are derived and their validity discussed based on the results of the questionnaire survey.

The **first interviewee** (transcript see Appendix 9.1.2) is a very experienced consultant. He is quite sceptic on the success of UDC. As prerequisite for success, he especially pointed out the need for a flexible production system. In product development, he expects a need for extensive preparation and modular product structures. From his point of view, also aspects like durability, functionality, and safety have to be considered intensively starting from early stages. For these activities, he expects increasing efforts due to UDC.

The **second interviewee** (transcript see Appendix 9.1.2) also is sceptic on how UDC products can be produced. He emphasized that there is a need to cover all possibilities a priori and to provide borderlines or restrictions. These restrictions have to limit the user to a solution space, which is manageable. From his point of view, this goes hand in hand with an early consideration of quality, safety, and their early assurance. In addition, he expects increased efforts for testing and integration due to UDC. For example, it might not be possible to apply standard testing procedures on customized products.

In their interview (transcript see Appendix 9.1.2), the **third and fourth interviewee** mainly focused on aspects of the development process. They also expect a modular product structure to be an essential prerequisite for UDC and they emphasized the need to cover all possibilities a priori. To achieve this, they demanded clear borderlines and restrictions. They stated: "A coffee machine should not be changed into a juice maker" (freely translated). Moreover, they also expect difficulties during acceptance tests of UDC products. There will be a gap between the user's imagination and the product he actually gets. In addition, they also pointed out the challenge to ensure quality, compatibility, approval, and to handle scheduling or pricing. To overcome these hurdles, the interviewees demanded a strongly integrated development process.

Based on the findings of the interviews the nine hypotheses listed in Figure 3-3 were postulated. The figure additionally briefly explains the origin of the hypotheses.

The web-based questionnaire survey to test the hypotheses had a total number of more than 60 participants. Thereof, 33 participants filled the questionnaire completely. Together with the

[12] https://www.umfrageonline.com

participants who filled major parts of the questionnaire, a sample size of *N = 44* was achieved. Figure 3-4 visualizes the composition of this sample. It shows that the sample has a high heterogeneity regarding both, background and experience. Many industrial sectors are represented in the sample and the experience of the participants in a balanced way comprises young and experienced professionals. Moreover, the majority of participants is either involved in R&D (*n = 35 %*) or project management (*n = 25 %*).

no.	**hypothesis** (With increasing UDC,...)	**explanation**
H1	…the needed interconnection and integration of development process phases also increases.	The interviewees mentioned that strict boundaries between process phases might no longer exist and a strong process integration is needed.
H2	…the required safety efforts, especially in early phases, also increase.	All interviewees emphasized the important role of safety considerations.
H3	…the efforts needed for the task clarification also increase.	Especially for the task clarification, the interviewees expect increasing efforts.
H4	…the need to define restrictions during the task clarification also increases.	Two of the interviewees explicitly mentioned the need to define borders/restrictions to limit the solution space of UDC.
H5	…the relevance of quality (H5.1), safety (H5.2) and compatibility (H5.3) considerations during the task clarification also increases.	All interviewees pointed out that the ensuring of relevant system properties during early phases will be essential.
H6	…the efforts involved in acceptance tests will decrease.	Some interviewees expected increasing efforts due to individuality, others expected fewer efforts due to user involvement.
H7	…the need for continuous involvement of the users in the development process by suitable communication platforms also increases.	All interviewees emphasized the importance of a continuous communication with the user.
H8	…the efforts for scheduling and pricing (H8.1) and the technical and economic risk (H8.2) also increase.	According to the interviewees, the unpredictability of the customization induces challenges and risks.
H9	…the need for complete and consistent documentation of safety analyses also increases.	This aspect was indirectly mentioned by the interviewees but also identified by literature.

Figure 3-3: Overview of the nine hypotheses on the impact of UDC on the development process

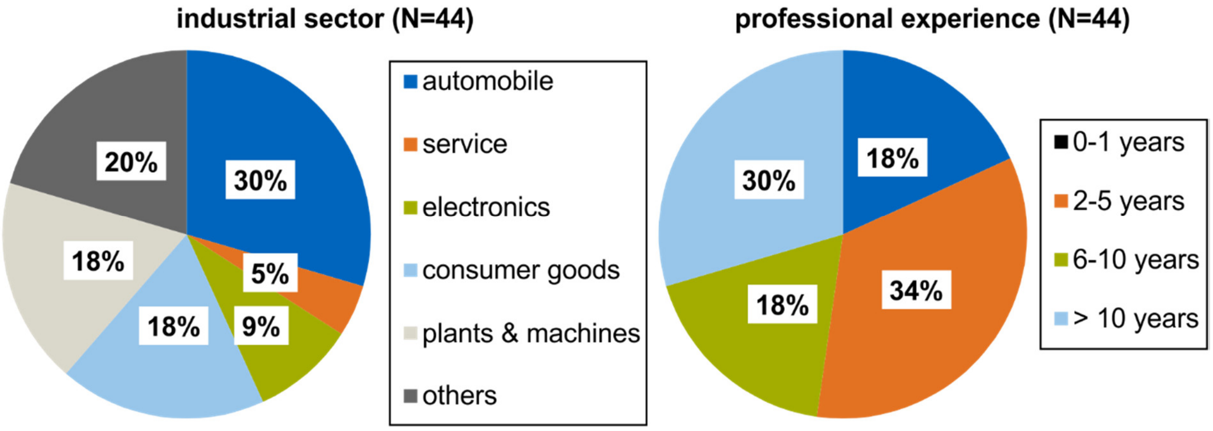


Figure 3-4: Background (industrial sector and professional experience) of the participants of the questionnaire survey

The statistical results of the survey are documented in Appendix 9.1.4, while the following paragraphs summarize the results for each hypothesis.

The first hypothesis H1 addresses the **interconnection and integration of process phases**. 55 % of the participants agree or totally agree that with increasing UDC the needed interconnection and integration of the development process phases increases as well. The values are significantly different (significance: 1.3 %) to the test value (undecided) so that H1 can be accepted.

Hypothesis H2 addresses **safety efforts** and tests how UDC impacts their role in the different phases of the development process with five question items. For the phases of task clarification, system design, system integration, the mean value is significant above the test value. For the validation phase, only a significance level of 11 % is achieved. Thus, with increasing UDC the required safety efforts especially in early phases of the development process also increase, while the impact on the validation phase cannot be significantly determined. This result is consistent with the fact that no significant results are obtained for the question item which states that the efforts will be equal in all phases.

Hypothesis H3 assumes increasing **general efforts** due to UDC **during the task clarification**. Approximately 67 % of the participants expect higher or much higher efforts. Thus, the hypothesis can be accepted on a very high significance level. This implies that with increasing UDC, the efforts during the task clarification phase also increase.

Hypothesis H4 focuses on the need for restrictions. The results show that the need for defined system borders and an extensive product structure planning during task clarification increases (with perfect significance), when UDC is increased. Thus, H4 can be accepted for system borders and product structure planning. Yet, for restrictions, which cover all possibilities no significant results are obtained, so that the hypothesis for comprehensive restrictions has to be rejected. The same applies for the maximization of the degrees of freedom for customization.

Hypothesis H5 examines the **efforts needed to consider and ensure system properties**. Its results for maintainability, quality, functionality, producibility, compatibility, conformity, and safety all are highly significant. Thus, with increasing UDC, the relevance of quality (H5.1), safety (H5.2), and compatibility (H5.3) considerations during task clarification increases as well. This also applies for the other mentioned properties.

Hypothesis H6 addresses the **testing efforts**. The results on a high significance level indicate for component, integration, and system tests increasing efforts due to increasing UDC. This contradicts the original formulation of H6, which expected a decrease. In addition, for acceptance tests no significant results are obtained. Thus, H6 has to be rejected.

Hypothesis H7 states that with increasing UDC, the need for a **continuous involvement of the users** in the development process by suitable communication platforms also increases. The survey clearly confirms this hypothesis. For all tested forms of communication, a result with a very high significance is obtained. Thus, H7 can be accepted.

Hypothesis H8 expects drawbacks for **general development tasks and aspects** due to UDC. The results of the study state that complexity, scheduling, and certification efforts (very high significance) as well as efficiency and pricing (H8.1) (high significance) deteriorate with increasing UDC. For general risks (H8.2), no significant result is obtained. Thus, while H8.1 can be accepted, H8.2 has to be rejected.

Hypothesis H9 addresses the **role of documentation of safety analyses** in UDC. The majority of participants expects an important role for the documentation of safety analysis results. In addition, documentations of basic functions and adaption processes are expected to be important. Only a small group of five participants expects no added importance due to UDC. Hence, the hypothesis can be weakly accepted.

To ensure the internal validity of the hypothesis tests, further analyses were conducted. As the sample consists of experienced and young professionals, a possible correlation of the results with the professional experience was examined. Especially for the rejected H6, its high standard deviation of the answers leads to the speculation that the experience influences the assessment of the participants. However, the correlation analysis leads to now significant results. Participants with less than five years of experience, have the same expectations as the participants with more than five years of experience.

3.2.3 Summary of the Study on Implications of UDC

The study on the implications of UDC reveals the nine hypotheses and connected implications on the product development process summarized in Figure 3-5. In general, UDC implies increased efforts, especially in early phases of the development process and for the assurance of system properties like safety and quality.

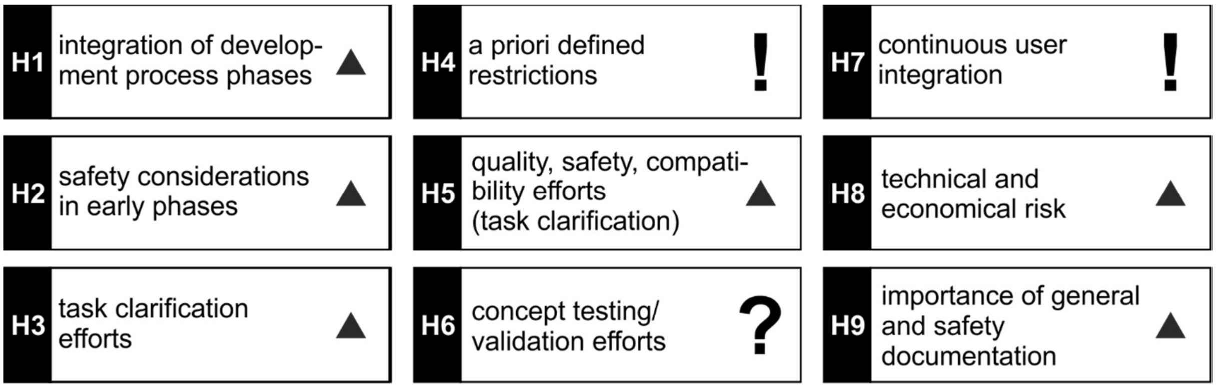

H1 integration of development process phases ▲
H4 a priori defined restrictions !
H7 continuous user integration !
H2 safety considerations in early phases ▲
H5 quality, safety, compatibility efforts (task clarification) ▲
H8 technical and economical risk ▲
H3 task clarification efforts ▲
H6 concept testing/ validation efforts ?
H9 importance of general and safety documentation ▲

Figure 3-5: Implications of UDC on the development process

The study implies that to realize UDC, the **single phases of the development process have to be better integrated and interconnected**. As the user performs a self-customization and intervenes on a design level, the borders between the phases of the design process can blur and the traditional V-model (VDI 2206) might not be suitable any more. This finding complies with the definition and classification of UDC made in Section 2.1.4.

Moreover, a **suitable preparation of the product** figures out to be a key success factor for UDC. This induces increased efforts for the task clarification (H3), which builds the foundation for the future customization. Increased efforts are necessary to ensure safety, quality, and compatibility (H5) of the customized products.

A particularly challenging aspect will be the **assurance of safety**. The survey confirms that UDC will increase the efforts for safety considerations in nearly all early phases of the development process (H2). The reason is that the solution space for customization should be as safe as possible (aligning with Section 2.3.3). However, the survey also states that it is not possible to consider or cover all possible customizations by a priori restrictions (H4). This implies an increasing importance of general and safety documentation (H9). These documents should be prepared for customization during all stages of the development process.

To limit these efforts, the uncertainty induced by UDC should be limited in advance. Therefore, **extensive product structure planning** and suitable system boundaries are necessary (H4). They both should limit the customization to a manageable space and preserve the actual nature of the product. In addition, a **continuous integration of the users** by multiple means of communication (H7) is required for UDC. To achieve this, web-based toolkits or online platforms are suitable solutions.

Even though the continuous integration can provide a full trial-and-error cycle, it might not be the case that UDC decreases **testing efforts** (H6). On the one hand, the early integration of the users might decrease testing efforts concerning the general acceptance. On the other hand, these efforts simultaneously may increase, as the users usually are non-experts and are not necessarily able to design the product according to their expectations on the first attempt. Moreover, the uncertain customization result can make it impossible to prepare standard test procedures for integration, safety, or quality tests.

This uncertainty might also be the reason, why the study cannot prove the assumption that UDC decreases the **technical and economic risk** (H8). The study shows that while UDC offers promising advantages, it implies various uncertainties and increased efforts in multiple areas of the development process. To achieve a risk reduction it is first necessary to handle the increased efforts and the resulting challenges.

3.3 Focus-Interviews on User-driven Customization’s Impact on Safety Analysis

The survey conducted in Section 3.2 identifies early safety considerations, the sufficient preparation, and the documentation from a safety perspective as prerequisite for UDC. Moreover, Sections 2.3.2 and 2.3.3 introduce current methods for safety analysis. However, these methods do neither provide information on their application in industry, nor on the handling of customizations. Yet, as identified in Section 3.1, this knowledge is essential to realize and balance UDC products with respect to product safety and to develop suitable methods to support an efficient safety analysis within the interface of UDC and safety analysis.

Hence, there is a need to analyze how the methods of safety analysis are currently applied in industry and how UDC impacts them. Blessing and Chakrabarti (2009, p. 105) suggest to apply real-time or retrospective data-collection methods for such analyses. To capture the current practices, observations would be most suitable. Yet, as also the impact resulting from UDC is analyzed, same as in Subsection 3.2.1, interviews are better suitable. These qualitative interviews (Keuneke, 2005, p. 259) with subject-matter experts can provide insights on, current applications and upcoming challenges through UDC with special focus to safety.

Consequently, in this thesis focus-interview study was conducted. It aimed to determine how manufacturers of mechanical and mechatronic products consider safety during their development process and how individual or customized products are handled with respect to product safety. The study was conducted in a student project (Gehrlicher, 2014) and is partially published in Roth et al. (2015).

3.3.1 Research Methodology of the Interview Study

To compare the state of science to the current industrial application, this study on the one hand builds on the methods and challenges of safety analysis discussed in Section 2.3. On the other hand, it conducted qualitative focus-interviews to identify industrial practices and challenges. As shown in Figure 3-6, the findings from both sources were in a last step compared to identify the actual practices and challenges with special respect to UDC. The following paragraphs explain this methodology in detail.

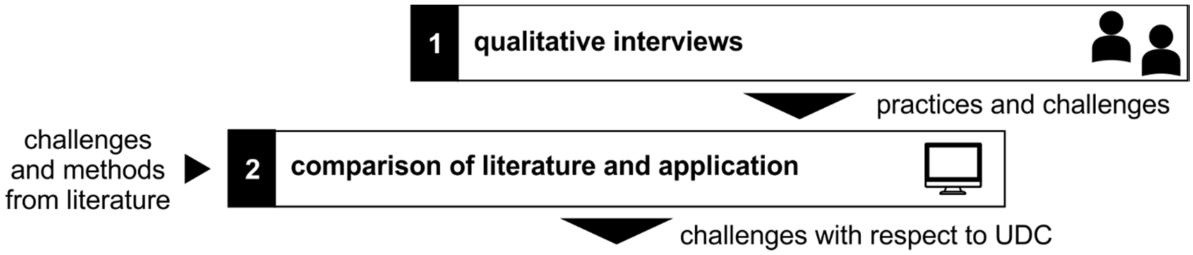

1
qualitative interviews
practices and challenges
challenges and methods from literature
2
comparison of literature and application
challenges with respect to UDC

Figure 3-6: Research methodology to identify the challenges of safety analyses with respect to UDC

The basic input to the planning of the interview study were the methods of safety analysis discussed in Subsection 2.3.2 and the developments and challenges identified in Subsection 2.3.3.

To compare these results with industrial practice, qualitative **semi-structured interviews** were planned. Semi-structured interviews are a suitable method to deepen and test existing knowledge (Kurz et al., 2009, p. 465), which in this case was obtained from the literature analysis in Section 2.3, and the questionnaire survey conducted in Section 3.2.

The interviews were prepared through a semi-structured guideline, which not only focuses on specific methods and challenges. It also aims to understand the product and company, which determine the context of the safety analyses. As the implications of UDC cause increased efforts (see Section 3.2.2), also approaches to improve the efficiency of safety analyses were included in the semi-structured interviews. In summary, the semi-structured guideline comprises questions to the following three objectives:

- understand the product structure, design processes, and product strategy
- capture practices of safety analysis for standardized and individual products or components
- identify practices and challenges to improve the efficiency of safety analysis and approval

To fulfill these objectives, the semi-structured guideline (see Appendix 9.2.1) contains a set of 17 central questions. They were clustered in three thematic blocks shown in Figure 3-7, which align with the objectives defined above.

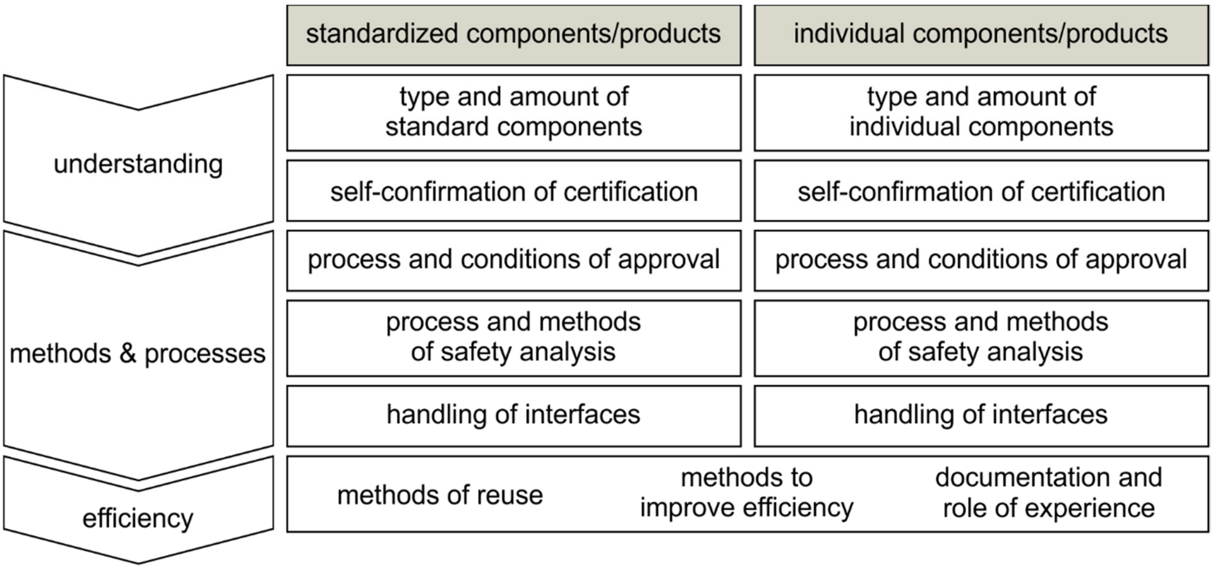

standardized components/products
individual components/products
understanding
type and amount of standard components
type and amount of individual components
self-confirmation of certification
self-confirmation of certification
methods & processes
process and conditions of approval
process and conditions of approval
process and methods of safety analysis
process and methods of safety analysis
handling of interfaces
handling of interfaces
efficiency
methods of reuse
methods to improve efficiency
documentation and role of experience

Figure 3-7: Topics of the 17 central questions of the semi-structured interview guideline

The first block focuses on the general product structure and its standardized components and modules. It aims to capture the ratio of standardized components as well as their characteristics. In addition, processes and methods to handle these components are addressed. The semi-structured guideline moreover discusses strategies to conduct safety analyses for combinations of standardized components.

The second block addresses customized or individual components. For these components, their ratio compared to standardized components together with applied methods and processes is captured as well. Moreover, the block also focuses on how interfaces between standardized and customized components are handled during safety analysis.

Finally, the third block connects both previous blocks. It addresses the aspects of efficiency, documentation, and the reuse of safety analysis data.

For the interviews, three safety analysts from different companies were selected. They more or less cover the whole domain of mechatronic products. The companies of two experts produce customized mechatronic products. Their companies both follow an engineer-to-order strategy. While the first company acts as original equipment manufacturer (OEM) and first tier supplier, the second company is a first tier supplier of safety-critical systems. The third interviewee works for a company in the sector of technical consumer products, which follows a make-to-stock strategy. All three companies are in the size between 4,000 and 50,000 employees.

The interviewees are experts for product safety in their company and are involved in safety analysis and approval activities. Thus, the sample allows capturing the practical application of safety analysis methods in the design of customized as well as mass products.

As suggested by Keuneke (2005, p. 255), the interviews were conducted personally by the student involved in the project in the natural environment of the interviewees (i.e. their company) and took between one and two hours. To avoid reservations of the interviewees, they were not recorded by audio or video. The interviewer was assisted by a minute taker to record the answers.

The notes of all interviews were consolidated to identify communalities and differences. Based on that open challenges, especially under the influence of UDC, were extracted. The same methodology was applied to compare the results with the findings from the state of science.

3.3.2 Practices and Challenges of Safety Analysis in the Context of UDC

Based on the research methodology described above, this section presents the obtained results (minutes see Appendix 0). First, the current practices are discussed. The structure aligns with the three blocks of the semi-structured guideline. Moreover, current challenges are derived and discussed in the context of UDC. Finally, the results are consolidated and compared to the state of science.

Current Practices and Challenges of Safety Analysis in Industrial Application

For **standardized components and modules**, all companies of the interviewees act similar. They try to build new products or variants based on standardized components or modules. In addition, they all strive to increase the ratio of standardized elements in the final product. Even the companies, which follow engineer-to-order strategies, achieve ratios of 60 % up to 80 % of standardized components or modules.

Form a safety perspective, the basic strategy of all companies is to design products according to standards and guidelines from the very beginning. By that, they try to cover known safety risks. To minimize remaining safety risks, all companies apply the traditional methods FMEA and FTA. They often adapt these methods to their specific requirements and some of them rely on special tool support. Moreover, the companies often use these methods more than mandatory. They usually consolidate the results of these methods in a report, based on which either the self-declaration on compliance or external certifications are conducted.

In addition, the companies try to approve their standard components before they integrate them in a product. All standard components successfully passed safety analysis prior to their integration. Yet, the strategies to handle the interfaces and combinations of these standardized modules vary between the companies. While the consumer product company tries to cover multiple combinations of standard components (e.g. product lines) in one analysis and approval, the other companies mainly approve single products only. Nevertheless, all companies try to analyze and approve as much as possible standard components and modules in advance. When these components are integrated in a new product, the interfaces and environmental conditions have to be tested on their compliance with the conditions specified in the original analysis and approval.

For **customized or individual products** or components, the safety analysis in general is the same as for standardized components described above: The consumer product company carries out the safety analysis of a whole product line in one step. Thus, the following paragraphs focus on the engineer-to-order companies.

Custom or individual components usually cannot be analyzed and approved in advance. Thus, the companies analyze the safety of each custom component individually. Therefore, the interviewees noted that the design following standards and guidelines is the most important factor. However, a new product even though it includes a large amount of standardized components usually has to be analyzed and approved as whole again. The interviewees mentioned that only in specific cases, when the degree of customization does not exceed a critical level, a sole analysis and approval of the individual components can be sufficient.

With focus on customization, especially the expert from the company, which produces safety-critical systems, emphasized the importance of an architecture tailored to system safety. The company strives to develop safety-oriented architectures, but according to the interviewee, these efforts still are not sufficient.

The previous paragraphs show that the basic practices and processes of safety analysis in the companies are very similar. The interviewees emphasized the large manual efforts connected to this process. Especially the engineer-to-order companies are struggling due to the immense efforts required for each individual product, while the consumer product company tries to gather individual products within product lines. The interviewees moreover mentioned that the efforts for safety analysis and approval will increase even more, as regulations and laws grow in number and complexity.

All companies try to **increase the efficiency** of their safety analyses. One strategy is the above-mentioned increased usage of standardized components. In addition, the companies try to improve the efficiency of their processes and methods. However, they merely apply newer methods from the state of science (see Subsection 2.3.3) and focus on own improvements and adaptions of FMEA and FTA. One company for example tries to reduce efforts to confirm the compatibility of standardized components in new environments by applying different strategies. Depending on the situation the needed efforts can be reduced. These strategies are:

- rule-based confirmation
- reference-based confirmation
- full safety and risk analysis

Another strategy is the **reuse** of findings and results from previous analyses. According to the interviewee, the consumer product company is able to reuse these previous results efficiently during development projects as the major changes of the product are known starting from the early phases. Yet, he mentioned that the documentation of analyses is often not done sufficiently. As reasons he identified limited time and resources. From his point of view, this implies that even though knowledge and results are reused, it mainly is done based on individual experience and expertise. Analogue, the engineer-to-order companies try to reuse previous results during the safety analysis of individual products. For them, the non-sufficient documentation also is a major challenge and reuse is based on individual experience. Lastly, one of the interviewees criticized the not suitable tool support for documentation and reuse.

In summary, the current practices identified in the interviews above are similar for all three companies. They all face comparable challenges, which can be summarized as follows:

- early consideration of safety aspects in design (safety-oriented design)
- increasing the amount of standardized components or modules
- efficient reuse of safety analyses through documentation and better tool support
- improving documentation of safety analysis results and reducing experience focus

The Influence of UDC on Safety Analysis in Industrial Application

The challenges above emerge from the current situation in the companies. As identified in Section 3.2.2, an increased customization and especially UDC can further influence them.

The early consideration of safety aspects in design according to the interviewees is important in the context of customization as well. However, a late generation of variants, especially for UDC, can diminish potential savings. Possible propagation effects have to be analyzed, which leads to new efforts. For example, one company tries to reduce these efforts by applying their confirmation strategies. Yet, it remains open, if these strategies will stay valid for UDC.

Moreover, depending on the customization options offered, a safety-oriented design process as demanded by the interviewees might not be fully achievable. According to one interviewee, it is important to establish safety-oriented product architectures. These architectures help to separate safety-critical elements from elements subject to customization at an early stage of design.

An increased amount of standardized components or modules might contradict increasing customization. According to the interviewees, again suitable architectures will be needed. They can help to separate customization and standardization areas. However, as stated above, the definition of these architectures also has to involve safety considerations.

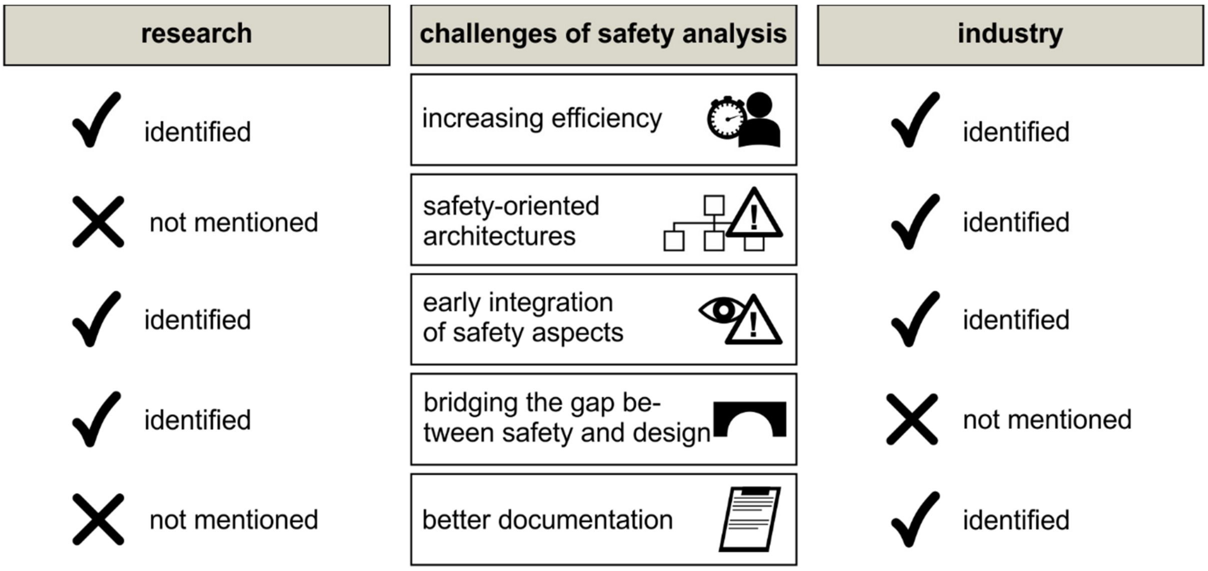
For increasing customization and UDC, according to the interviewees an improved efficiency of safety analyses becomes crucial. The process of safety analysis and approval for each customized product has to be as efficient as possible. According to the interviewees, this will require a consistent strategy of reuse and harmonization of previous safety analysis results. This will allow the preparation of individual changes (e.g. through UDC) from the perspective of safety analysis. One interviewee expects formal analysis methods to be suitable. However, the interviewee of the consumer product company doubted that human evaluation can be replaced.

Instead, he expects increased importance of a consistent documentation. It can reduce the required experience to conduct safety analyses for customized products and thus, further improve efficiency.

Comparison of Research and Industrial Application

The findings of the interviews from a general point of view align with the findings from research (see Section 3.1) and support the conclusions drawn from the questionnaire survey (see Section 3.2). Figure 3-8 compares the challenges identified from both sources. The challenges of early integration and improved efficiency are confirmed. The bridging of the gap between domains in industry is not considered as important as in research. Instead, industry emphasizes the challenges of safety-oriented architectures and improved documentation.

While the interviewees' companies commonly apply the traditional methods of safety analysis, they do not completely follow the current state of science. The development process often is not safety-centric and the safety analysis is more or less conducted review-based. However, the interviewees in accordance with literature demanded an **early consideration of safety aspects** in the design process. Model-based approaches in the state of science provide a potential solution but are not yet applied consequently within the companies.



research	challenges of safety analysis	industry
✓ identified	increasing efficiency	✓ identified
✗ not mentioned	safety-oriented architectures	✓ identified
✓ identified	early integration of safety aspects	✓ identified
✓ identified	bridging the gap between safety and design	✗ not mentioned
✗ not mentioned	better documentation	✓ identified

Figure 3-8: Challenges of safety analysis in research and industrial application

Moreover, all interviewees criticized the experience-based and **inefficient use of safety analysis methods**. They demanded a **better documentation** of the results. Usually, the results are documented in reports only, so that large parts of the connected knowledge remain implicit expert knowledge. Even though model-based methods can provide a solution, the state of science does not explicitly discuss this challenge.

Finally, according to the interviewees, the amount of standardization has to be increased and **safety-oriented architectures** have to be established. While standardization and modular product architectures are widely discussed, the state of science does not connect safety analyses to these methods. Moreover, the standardization is opposed by increased customization. Thus, it is necessary to provide support to balance standardization and customization in the architectures. However, with respect to safety, the state of science does not provide suitable support.

3.3.3 Summary of Current Practices and Challenges of Safety Analysis

The study on current practices and challenges of safety analysis reveals five major challenges. With special focus to UDC, they can be summarized as follows.

The study reveals a demand for an increased **early consideration of safety aspects**. Especially with increased UDC, when late self-customization appears, the early consideration of safety aspects and the preparation of potential changes are required.

While the state of science identifies a need to **bridge the gap** between safety experts and designers, industry does not fully confirm this need. However, for UDC with users an additional player is involved in the development process. For the users, transparency on the defined restrictions might be necessary so that safety knowledge needs to be made more explicit.

Moreover, the study reveals a demand for **increased efficiency of safety analyses**. With increased UDC, this aspect will get essential. To remain competitive with mass products, the safety analysis of the customized products has to be efficiently conducted. This efficiency includes the reduction of manual efforts, of time, and of involved experience.

To achieve increased efficiency especially under UDC, the study demands a **better documentation** of safety knowledge and safety analysis results. A better documentation can improve efficiency by supporting reuse and can reduce the involved experience by making safety knowledge explicit.

Finally, the study reveals the need for **safety-oriented product architectures**. They can be used to optimize the safety analysis efforts induced through new variants or modules and simplify their exchange. For increasing UDC, these safety-oriented architectures gain in importance even more. They can help to keep customization away from areas in the architecture, where changes result in large additional safety analysis efforts.

3.4 Resume of Challenges and the Problem to Solve

Based on the findings of the previous three sections, the actual impact of UDC on the fields of safety analysis and ECM can be understood. This allows concretizing the objectives on a solution approach, which capable to answer the research question of this thesis (see Section 1.3). The following subsection summarizes and consolidates the findings of the three studies in the context of the theoretical background and the objectives of this thesis. Based on this, Subsection 3.4.2 then concretizes the objective and derives a set of six general requirements on the support to be developed.

3.4.1 Summary of Challenges through User-driven Customization

The previous three sections conduct studies on different levels of detail. The first section identifies challenges at the interfaces of ECM, safety analysis, and customization. The second aims to research the general impact of UDC on the development process and these interfaces. Finally, the third in detail analyzes the challenges within safety analysis in connection to UDC. In general, especially the explorative questionnaire survey reveals three major impacts of UDC on the development process.

It first has to be emphasized that the **integration of the product development phases** needs to be improved. This need aligns with the increased complexity and the distributed allocation of UDC within the classification of customization archetypes (see section 2.1.4).

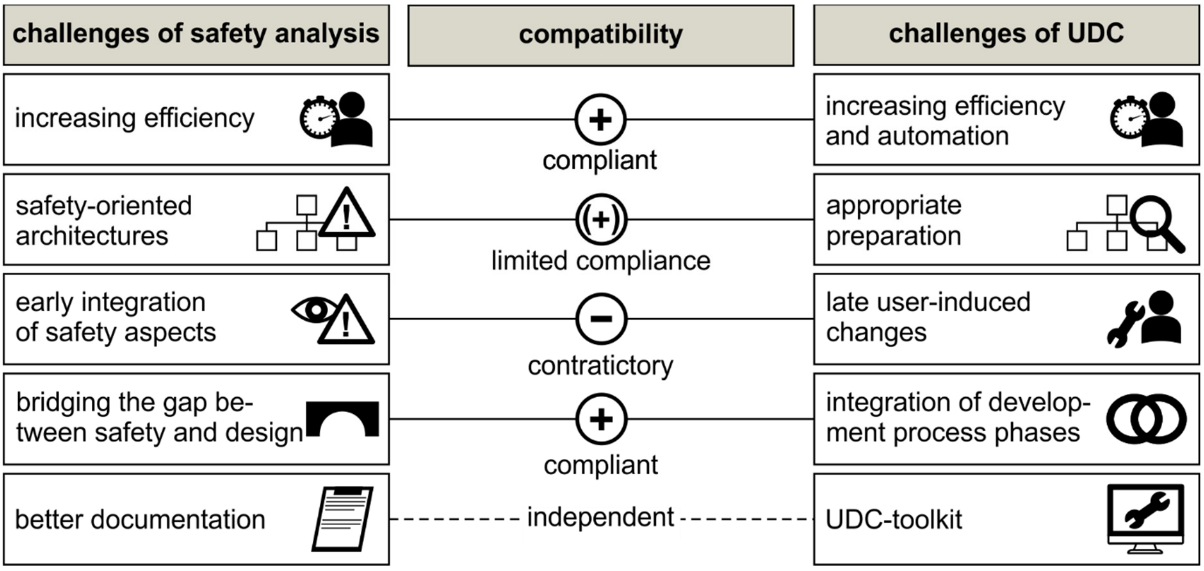
Moreover, a **suitable preparation** according to all studies is essential. This includes an extensive product structure planning, the definition of boundaries, and from a safety perspective the preparation of safety-oriented architectures. This aspect also aligns with the major strategies of ECM.

Furthermore, the **early consideration** of system properties becomes crucial. Aspects like safety, quality and compatibility have to be strongly considered starting from early phases. This can reduce the impact of uncertainties and risks of UDC and connected change propagations. However, UDC especially makes it challenging to realize the demanded safety-centric design processes, as according to the questionnaire survey, not all restrictions can be defined a priori.

Despite these challenges, the studies reveal that all the three fields strive for an **improved efficiency**. While UDC aims to reduce the sticky information transfer costs, safety analysis and ECM aim to reduce the amount of analyses and the connected efforts in time, experience, and resources.

With a special focus on safety analysis, two further challenges are identified. First, **the gap between safety and design** needs to be bridged. Especially the previously described demand for preparation and early integration in the context of UDC increases the need to close this gap. Moreover, in order to cope with the increasing number of variety due to UDC, the **documentation of safety analyses** needs to be improved. Because only a transparent and consistent documentation of the safety analyses allows for an improved efficiency through reuse and reduced experience needed.

In summary, the previously described challenges mainly are imposed by the fields of UDC and safety analysis. ECM acts more or less as mediator between both fields. Thus, Figure 3-9 summarizes the challenges of safety analysis and UDC and evaluates their compliance. Only if these in parts contradictory challenges can be solved, a successful realization of UDC is possible.



challenges of safety analysis	compatibility	challenges of UDC
increasing efficiency	+ compliant	increasing efficiency and automation
safety-oriented architectures	(+) limited compliance	appropriate preparation
early integration of safety aspects	− contratictory	late user-induced changes
bridging the gap between safety and design	+ compliant	integration of development process phases
better documentation	independent	UDC-toolkit

Figure 3-9: Challenges at the interface of safety analysis and UDC and their compatibility

While both fields demand an improved efficiency and automation, they also strive for an appropriate preparation. However, the objectives of the preparation might differ. Moreover, the early consideration of safety aspects and the late user-induced changes through UDC can be contradictory. Based on its definition (see Subsection 2.1.4), UDC requires a connection to an UDC-toolkit. Furthermore, as identified in the explorative questionnaire survey, an improved process integration is required to realize UDC. This complies with a closing of the gap between safety and design. Finally, safety analysis demands an improved documentation of analyses and results to foster reuse.

3.4.2 Objective and Requirements on a Solution Approach

Based on the identified impacts of UDC and the comparison of challenges, the objective and research question of this thesis defined in Section 1.3 can be concretized to the following aim:

The two fields of UDC and safety analysis have to be integrated and a support should be developed to overcome the challenges and enable the efficient balancing and safety analysis of UDC products.

Resulting from this aim and the objective of this thesis, in combination with the challenges discussed in the previous subsection, a set of six general requirements on a solution approach is derived. Figure 3-10 illustrate these requirements and visualizes how they result from the identified challenges. The following paragraphs specify the requirements in detail.

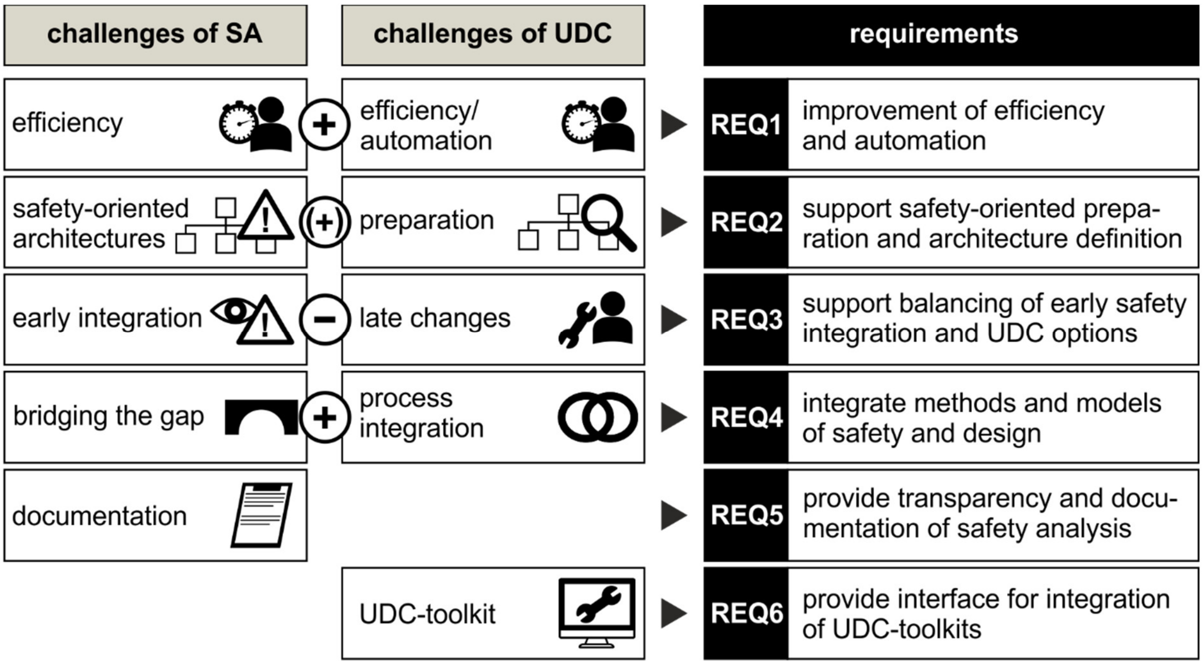

challenges of SA
challenges of UDC
requirements
efficiency
efficiency/ automation
REQ1
improvement of efficiency and automation
safety-oriented architectures
preparation
REQ2
support safety-oriented preparation and architecture definition
early integration
late changes
REQ3
support balancing of early safety integration and UDC options
bridging the gap
process integration
REQ4
integrate methods and models of safety and design
documentation
REQ5
provide transparency and documentation of safety analysis
UDC-toolkit
REQ6
provide interface for integration of UDC-toolkits

Figure 3-10: Requirements on a solution approach resulting from the identified challenges

The **first requirement (REQ1)** addresses the need for an **improved efficiency**. The challenge is to efficiently prepare and process UDC products. This need especially is identified within safety analysis (see Subsection 2.3.3) and ECM (see Subsection 2.2.2). The resulting requirement can be specified as follows:

REQ1: The support shall reduce the required overall manual efforts (in cost, time or experience), which are needed to conduct the safety analysis of an UDC product and all its customized variants.

The requirement is fulfilled, when the manual efforts for a safety analysis are reduced, while the one-time implementation effort of the methodology does not succeed the savings.

The **second requirement (REQ2)** aims at a solution for the challenge of **safety-oriented architectures**. While safety analysis demands a definition of standard elements (see Subsection 3.3.2), it is opposed by a demand for degrees of freedom to realize UDC options. However, the appropriate preparation of UDC products implies further challenges. These other and more general aspects not in of the scope of this thesis (see Section 1.3) and are for example already covered by Holle and Lindemann (2014). The narrowed requirement can be specified as follows:

REQ2: The support shall support the safety-oriented preparation and architecture definition of UDC products. This excludes other and general influences on architecture definition.

The requirement is fulfilled, when the support provides information on safety aspects within the product architecture to evaluate and compare alternative product architectures from a safety perspective and/or supports the improvement of safety-oriented product architectures.

The **third requirement (REQ3)** requests a solution for the contradiction of an **early integration** of safety aspects and late user-induced changes through UDC. As described in Subsection 2.3.3 and Subsection 3.3.2, the early integration usually is achieved by a safety-centric design process or the adherence to standards and guidelines in the design process. In contrast, UDC induces changes of users, who might not be familiar with safety aspects or standards and guidelines. To handle this contradiction, both aspects and their advantages and limitations should be balanced. The resulting requirement can be specified as follows:

REQ3: The support shall support the balancing of early safety integration and degrees of freedom offered for UDC. This includes the conduction of preliminary safety analyses and the elicitation of influences and propagation effects of degrees of freedom offered. Both aspects shall support the evaluation of trade-offs.

This requirement is fulfilled, when the support provides suitable and valid safety analyses to identify and trace the impact and propagation effects of user-induced changes and the degrees of freedom offered for UDC from a safety perspective.

As described in Subsection 2.3.3, the **gap between safety and design** needs to be bridged. Moreover, UDC requests for an improved integration (see Subsection 3.2.2) of development activities. These demands are addressed by the **fourth requirement (REQ4)**. It can be specified as follows:

REQ4: The support shall integrate data, information, models, and methods of the relevant fields in the design process. Based on this, it shall be compatible with existing methods used in these fields and provide a basis for their integrated application.

This requirement is fulfilled, when the solution approach provides a framework, which is compatible with major methods and models used in the fields of safety analysis, ECM, and design and allows the transformation of the data to relevant exchange formats.

The **fifth requirement (REQ5)** is derived from the challenges in safety analysis. In Subsection 3.3.2, the need for a consistent and **transparent documentation** is identified. Only such a documentation can allow the reuse and by that contribute to efficiency. The resulting requirement can be formulated as follows:

REQ5: The support shall provide a consistent documentation of the involved safety and product knowledge and provide input for documentation files during the safety analysis process.

The requirement is fulfilled, when the support documents all information in a consistent and accessible form. It moreover documents the links to relevant safety requirements and allows transparency and traceability according to standards. Additionally, it offers an exchange format, which provides input for standardized documentation files.

The **sixth requirement (REQ6)** originates from the definition of UDC (see Subsection 2.1.4). As UDC involves an **UDC-toolkit** as a central element, a solution approach should be compatible with this notion. The resulting requirement can be formulated as follows:

REQ6: The support shall be in a form, which provides an interface that allows an integration into a toolkit or toolchain, which realizes the UDC products.

This requirement can be fulfilled, when the support is implemented in an environment, which provides exchange formats or interfaces that enable the data exchange with software solutions realizing UDC-toolkits.

4. Solution Approach

This chapter develops a support to answer the research question and fulfill the requirements defined in Subsection 3.4.2. The following paragraphs first refine the research methodology defined in Section 1.4 and in detail describe the procedure of the Prescriptive Study. Following this methodology, Section 4.1 introduces the general concept of the solution approach, which is the "Efficient Safety Method Kit for User-driven Customization" (ESMK). Then, Section 4.2 develops the underlying knowledge framework of the ESMK. Section 4.3 in detail develops and introduces the phases and methods of the ESMK. Lastly, Section 4.4 summarizes the ESMK and its aspired contribution.

To develop the solution approach resulting in the ESMK, this thesis within its Prescriptive Study follows the **systematic process** proposed by Blessing and Chakrabarti (2009, pp. 144–148). As visualized in Figure 4-1, this process consists of the main steps of task clarification, conceptualization, elaboration and support evaluation.

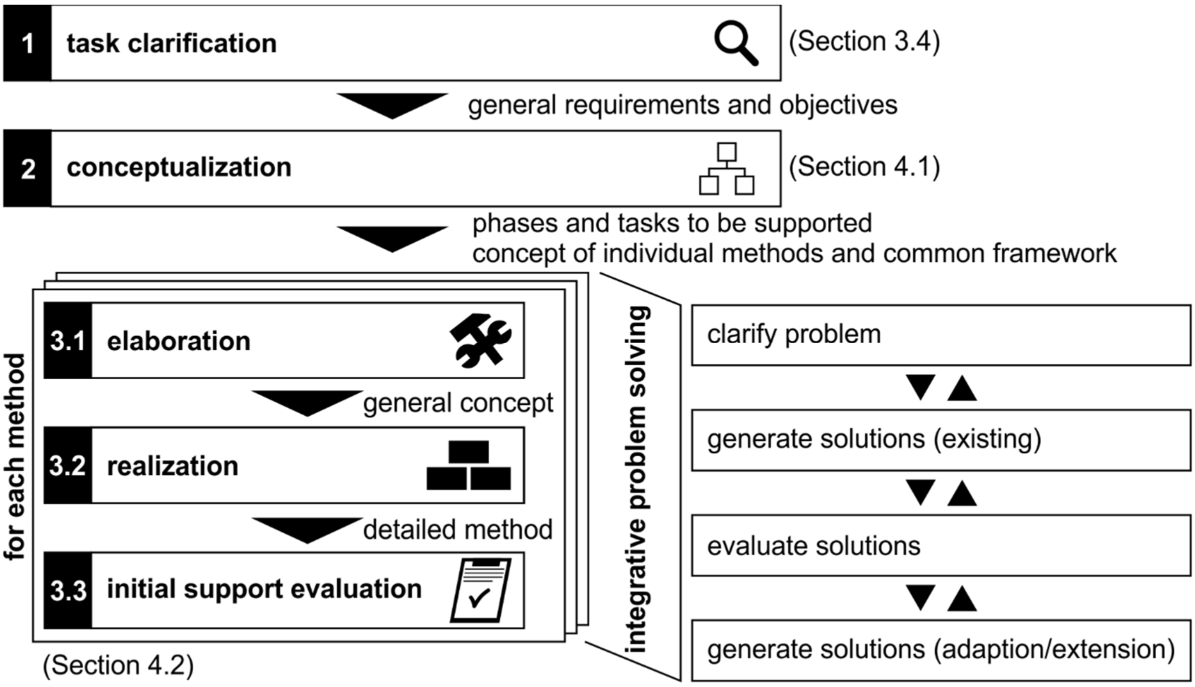

1 task clarification
(Section 3.4)
general requirements and objectives
2 conceptualization
(Section 4.1)
phases and tasks to be supported
concept of individual methods and common framework
for each method
3.1 elaboration
general concept
3.2 realization
detailed method
3.3 initial support evaluation
(Section 4.2)
integrative problem solving
clarify problem
generate solutions (existing)
evaluate solutions
generate solutions (adaption/extension)

Figure 4-1: Methodology of the development of the design support (adapted from Blessing and Chakrabarti (2009, p. 146))

The **task clarification** in Subsection 3.4.2 identifies the general requirements and objectives on a solution for the identified needs and the derived research question. There, these objectives are concretized and broken down based on the findings of Descriptive Study-Ia and -Ib.

Based on these requirements, Section 4.1 in the **conceptualization** step draws a general concept of the proposed solution approach. This includes general conceptual decisions and the definition of tasks, which have to be supported. This results in the general decision for a method kit with individual, but compatible methods and a common framework.

For each of the defined tasks to be supported, the steps of **elaboration, realization and support evaluation** are conducted in an integrative manner. Therefore, the basic problem-solving cycle (Blessing & Chakrabarti, 2009, p. 145) is adapted according to Figure 4-1 and applied for each individual function.

The **problem solving cycle** in its first step clarifies the problem for each individual task. The general requirements identified in the task clarification (Subsection 3.4.2) are detailed for the specific task based on findings of the literature and the Descriptive Studies-Ia and -Ib. If possible, in a first generation of solutions, the existing approaches and methods from literature are identified. These approaches are evaluated on their capabilities to fulfill the specified requirements. If necessary, the most promising solutions are adapted, extended or combined with new approaches in an iteration to generate a suitable solution.

To elaborate and initially evaluate the generated solution within the integrative problem solving, the resulting support is applied to simple theoretical models. If useful, it is additionally applied to the exemplary system of a cordless screwdriver.

4.1 Introduction and Overview of the Efficient Safety Method Kit

This thesis aims to enable the realization and balancing of UDC products from a safety perspective (see Section 1.3). It hence aims to provide support at the interface of customization (i.e. UDC), ECM, and safety analysis. The Efficient Safety Method Kit (ESMK) as solution approach has to enable the balancing between UDC options and their impact on product safety as well as connected analysis efforts. A second field of action is to improve the efficiency of safety analysis. Thus, the ESMK is developed to support both, the preparation of products for UDC from a safety perspective, and the reduction of safety analysis efforts of the customized products. By that, it tackles both fields of action identified in Section 1.3.

According to the definition of customization (see Section 2.1.1), it implies alterations to an existing product. Thus, the ESMK addresses **the two different applications** illustrated in Figure 4-2. Both are based on an existing basic product. The reason is that customization and user involvement are closely connected to experiences, the users made with the product or similar products and these experiences are not available for completely new products. This relates to the assumption that a need for UDC only emerges, when the users can refer to an existing basic product. As consequence, this thesis does not address a greenfield development.

In **application case I**, an existing product is directly transferred into an UDC product. The underlying goal of the development activities is to offer UDC for an existing product. The main task is to reveal options for UDC, evaluate, and select them. Moreover, the user-induced changes through UDC need to be considered in an individual safety analysis.

Application case II extends the first application case and addresses a redesign of an existing product tailored to UDC. Here, the goal of the development is to improve the UDC options and to reduce the drawbacks of UDC. Therefore, product architecture concepts are improved and assessed. For those architectures, again, the UDC options are selected and the safety analysis of customizations needs to be conducted. The major difference to the first application case is that the design is developed in the application case, while the first case exclusively builds on an existing design. After the design is selected, both cases are follow the same process.

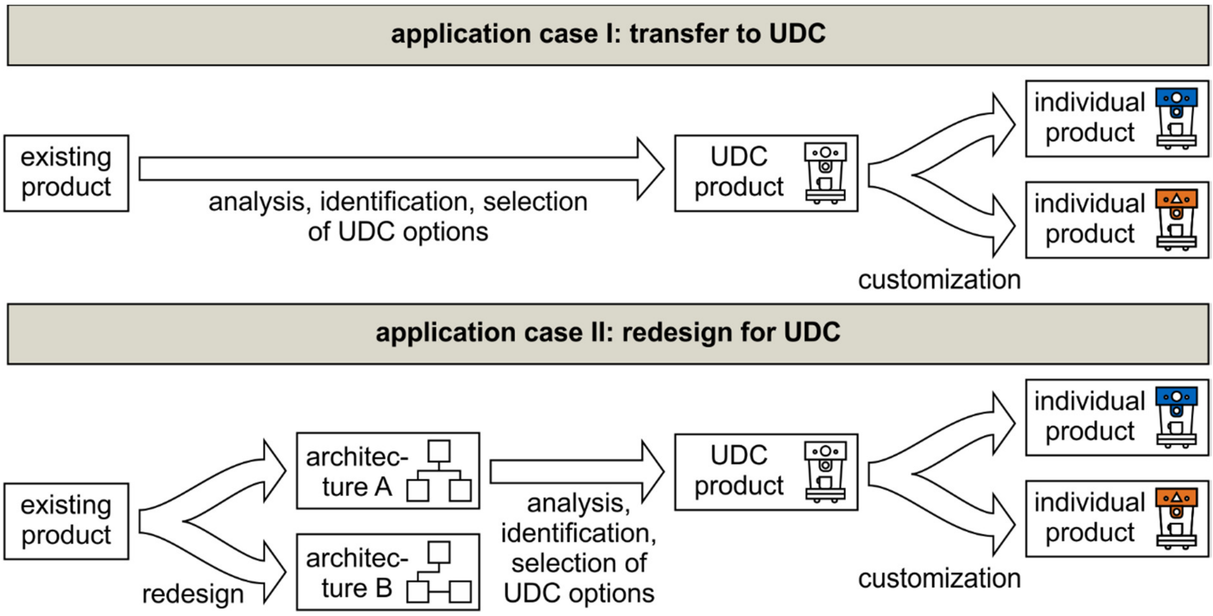


Figure 4-2: Application cases addressed by the ESMK

To provide the aspired support in both application cases, different tasks need to be addressed. Moreover, the analysis of the impact of UDC (see Section 3.2.2) identifies a multitude of challenges through UDC in various areas of the organization and development process. At the same time, other important aspects within the company like complexity or quality management also have to be considered during the development process.

Hence, it is not beneficial to provide a sequential and linear methodology to efficiently prepare and ensure the safety of UDC products. Depending on company, product, and the specific situation, the tasks interact with other tasks and other methods. Thus, the ESMK rather provides **individual support methods** for the specific tasks. These support methods should be independent but compatible to each other as well as to other methods used in the product development process (*REQ4*). The individual methods provide punctual support, when the consideration of the interface of UDC, ECM, and safety analysis is required. Other aspects and restrictions are not addressed by the ESMK but are object of other research (e.g. Holle, Straub, Roth, and Lindemann (2016) and Spallek, Sankowski, and Krause (2016)).

The individual support methods of the ESMK are structured in the **four phases** shown in Figure 4-3. The phases are defined based on an adaption of the generic engineering change process (see Section 2.2.2) combined with the impact and challenges of UDC and the application cases.

The first phase originates from application case I. To transfer an existing product to an UDC product, it is necessary to analyze the existing product and capture all its system elements. Thus, the first phase is the **As-is Analysis**.

The Subsections 2.3.3 and 3.4.1 identify a gap between safety and design. To fulfill the derived requirement (*REQ4*), it is necessary to integrate knowledge from both fields, even though the first phase already models the system. Hence, the second phase **Feature Analysis** aims to capture and explicate the safety knowledge of the existing product (application case I) or to model safety aspects within the redesign concept explicitly (application case II).

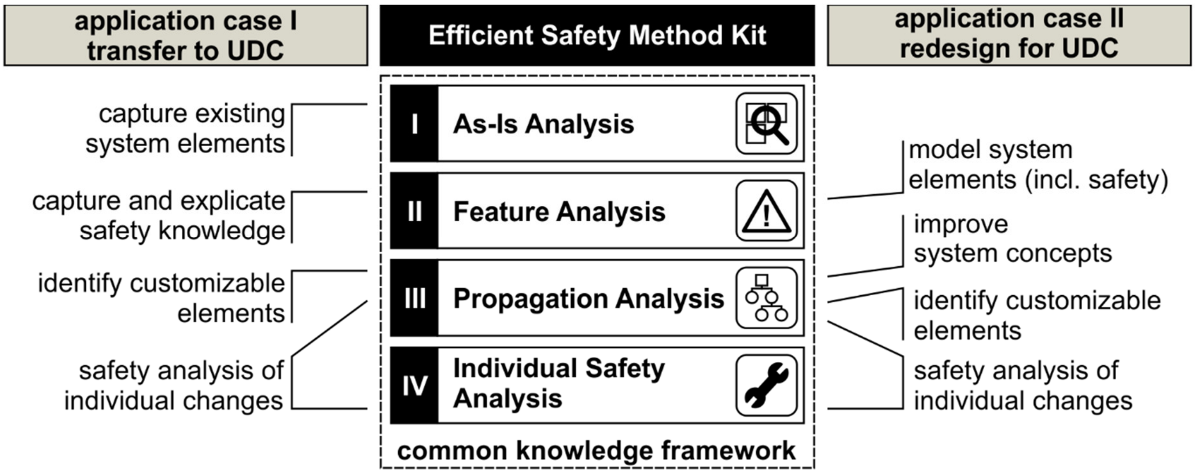

application case I
transfer to UDC
Efficient Safety Method Kit
application case II
redesign for UDC
capture existing system elements
capture and explicate safety knowledge
identify customizable elements
safety analysis of individual changes
I As-Is Analysis
II Feature Analysis
III Propagation Analysis
IV Individual Safety Analysis
common knowledge framework
model system elements (incl. safety)
improve system concepts
identify customizable elements
safety analysis of individual changes

Figure 4-3: The four phases and specific tasks addressed by the ESMK

Phase three aims to identify customizable elements within the product. Aligning with the ECM strategy of prevention (see Subsection 2.2.2), this phase identifies elements whose changes should be avoided. This is achieved by analyzing the impact of potential user-induced changes. The phase, correlates with the assessment step of the generic engineering change process. To assess these changes, their effects need to be determined. The task is to evaluate potential change propagations and identify how they can affect the product safety. Thus, phase three is the **Propagation Analysis**.

The approval in generic engineering change process resembles the definition of customization options. The next step in this process is the implementation of the change. In UDC, the users conduct this step. The task of the manufacturer is then to evaluate the user-induced changes and document the maintained safety. Thus, the fourth and last phase addressed by the ESMK is the **Individual Safety Analysis**.

The previous paragraphs define the application cases and the four phases addressed by the ESMK. The requirements defined in Subsection 3.4.2 in connection with these boundary conditions entail a set of general properties of the ESMK.

The independent nature of the ESMK's support methods combined with *REQ4* and *REQ5*, which demand an integration of methods and an improved transparency, make it essential to have a common and compliant base for all methods. The ESMK has to provide a **common knowledge framework**, which captures the knowledge needed to apply the individual models and methods as well as to ensure their integration.

At the same time, *REQ1* demands improved efficiency and automation. Thus, the common knowledge framework of the ESMK has to be stored in a form, which allows for an automation of workflows.

Moreover, as described before, other aspects also have to be considered in the development of UDC products and a compatibility to other methods is necessary. Therefore, the ESMK in addition to its specific methods also provides suggestions and compatibility for alternative methods to be used. In accordance with the identified challenges and the objective of this thesis, the ESMK primarily addresses the explication of safety aspects, the analysis of change propagations, and the integration of the major safety analysis methods FTA and FMEA.

Based on this conceptualization, the **basic characteristics** of the ESMK can be summarized as follows:

- common knowledge framework as basis
- format suitable for workflow automation
- addressing two application cases and specific tasks assigned to four phases
- independent but compliant support methods
- providing flexibility and method alternatives
- focus on explication of safety, propagations, and integration of FTA and FMEA

4.2 The Common Knowledge Framework

The ESMK as introduced in the previous section is based on a common knowledge framework. This framework represents the integrative element to connect the individual methods and enables the integration of, and connection to other methods or approaches. It unites the relevant domains involved in safety analysis and ECM.

The relevant domains to be integrated were systematically identified and selected based on existing research and approaches. This identification is partially published in Roth et al. (2016) and is described in the following. First, the relevant domains from an ECM perspective were identified and selected. Then, the relevant domains from a safety analysis perspective were identified and selected as well. In the last step, the domains from both fields were merged to the knowledge framework.

The identification of the **relevant domains from an ECM perspective** builds on the literature review described in Section 2.2.3. The identified 106 publications discussing engineering changes were analyzed again to identify their scope.

According to the challenges at the interface between ECM and customization (see Section 3.1), the propagation of changes is the central element. This focus does not allow to directly rely on the existing reviews by Jarratt et al. (2011) and Helms et al. (2014). The user-induced changes within UDC shift the product to the center of the analysis. In addition, the validity of existing development processes in UDC might be limited (see Subsection 3.2.2). Thus, publications addressing propagations to processes and organizational units are of minor importance. The publications' **relevance for the definition of the knowledge framework** was assessed using the following three categories:

- high relevance: The publication addresses aspects of change propagation within a technical product and its elements.
- medium relevance: The publication addresses aspects of change propagation within other domains, but establishes a connection to elements of the technical product.
- no relevance: The publication does not address change propagation within technical products.

Based on this classification, in total 41 high and 12 medium relevant publication remained (see Appendix 9.3.1). They were analyzed in detail on their domains included in the analysis as well as on used methods and their underlying basic methods.

Concerning the applied or developed methods, the results of this analysis to a large extent comply with the findings of Helms et al. (2014) and Jarratt et al. (2011). For classification the method clusters identified in Helms et al. (2014, pp. 212–214) were used and refined, if necessary. Figure 4-4 visualizes the results and clearly shows that the school of EDC Cambridge and the **Change Prediction Method with some extensions dominates the research** in this field. Other clusters of methods identified by the previous reviews vanish, as they have a different focus. The category "others" summarizes methods, which could not be directly assigned to a specific category, for example the multilayer network model of Pasqual and Weck (2012), which unites the product view with the organization and individuals.

As identified in the previous section and Figure 4-4, the Change Prediction Method plays a central role in ECM publications with the relevant focus. However, a view into the basic methods used within these publications reveals the picture shown in Figure 4-5. The **basic method,** on which the vast majority of all publications rely **are matrices** (i.e. DSM and DMM). Further methods usually only supplement matrices or the Change Prediction Method (CPM). The most prominent examples therefore are the Function Behavior State (FBS), the Contact Channel Model (C&CM) and the Quality Function Deployment (QFD).

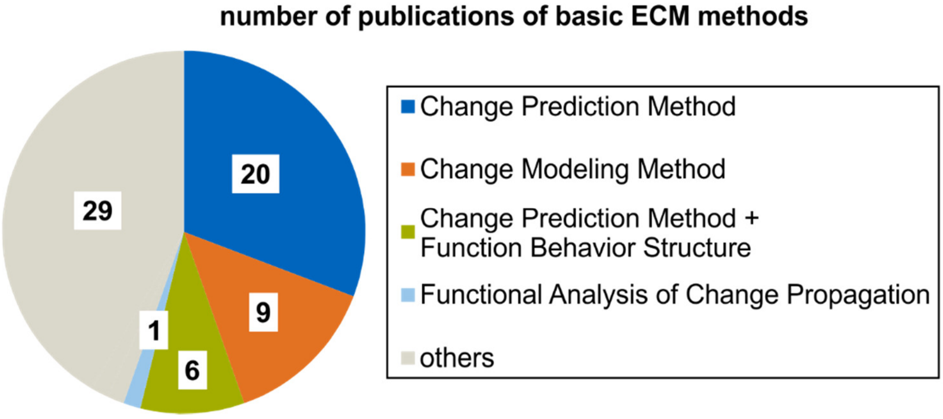


Figure 4-4: Method classification of relevant ECM publications

The analysis of domains identified **eleven different domains** considered in the publications, which are listed in Figure 4-5. Components were identified as central element of all relevant publications. The reason is that the publications usually define the product structure based on components and consider component changes. Furthermore, requirements and functions are often involved in the publications. Moreover, some publications on a more detailed level include design parameters or component properties. In addition, processes and resources are included in multiple publications, despite the focus of this analysis. As already identified in section 3.1, faults and safety aspects only play a marginal role in the published ECM methods.

In summary, the knowledge framework from an ECM perspective mainly has to provide compatibility with matrices and the Change Prediction Method. It moreover has to incorporate components, functions, and requirements as most important domains.

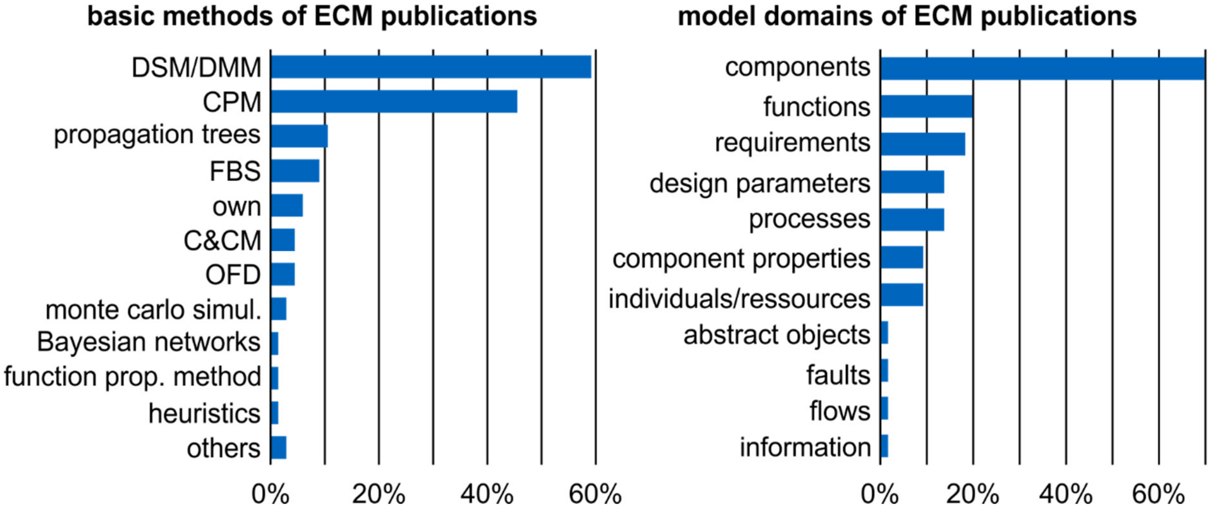


Figure 4-5: Domains and methods incorporated in relevant ECM publications

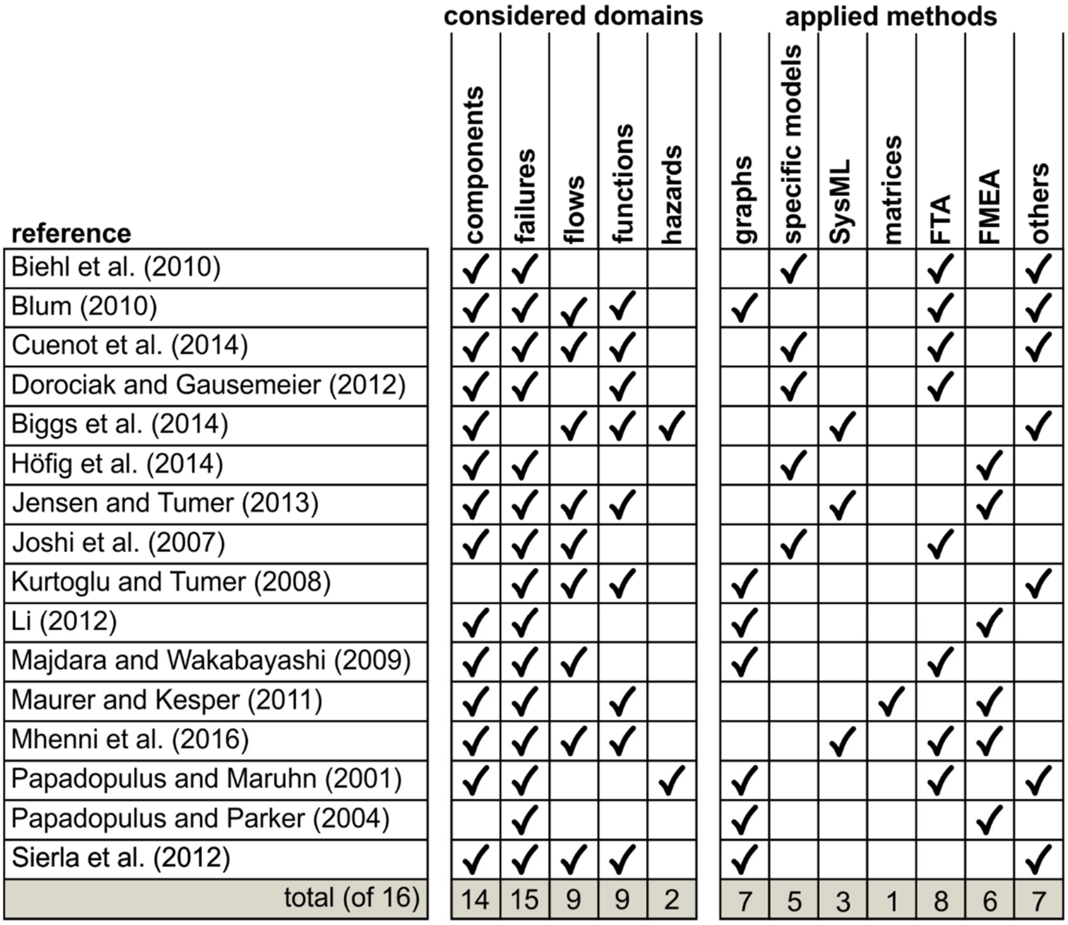
As second element for the framework, the **relevant domains from safety analysis** were identified. This identification picked up the findings on applied traditional methods from Subsection 2.3.2 and the review on current developments given in Subsection 2.3.3. As FMEA and FTA are dominantly used, only representative model-based methods for safety analysis were selected for a detailed analysis. This selection aimed to cover all essential impacts at the interface of safety analysis to customization (see Section 3.1) and the challenges of safety analysis (see Subsection 2.3.4). The selection criteria were that the publication introduces models or frameworks and strives to increase efficiency and automation of safety analysis.

The detailed analysis of the underlying **basic methods** is shown in Figure 4-6. As expected, the traditional methods FMEA and FTA play an important role. Moreover, graph-based methods are commonly used to model and analyze the product. In contrast to ECM, also SysML is used in multiple publications. However, most methods rely on specific methods like the Architecture Description Language.

Regarding the **domains**, the analysis results in Figure 4-6 clearly show that in safety analysis failures are the central domain. Moreover, components and functions both play a central role to set up the product structure. To establish links within the product structure and to identify possible failure propagations, often flows are also included in the models. Depending on the scope of the specific publication, further elements like hazards are considered as well.

In summary, the knowledge framework from a safety analysis perspective mainly has to provide compatibility with FMEA and FTA. Moreover, compatibility with matrices and SysML is advantageous. In addition, the framework should include the domains of failures, components, and functions as well as flows.

As the fields of ECM and safety analysis do not provide a consistent set of methods and domains, the **knowledge framework of the ESMK integrates both fields**. It consolidates domains of both fields and merges the results of the analyses shown in Figure 4-5 and Figure 4-6. Moreover, the consolidated domains and methods are aligned with the perceptions of safety analysts presented in Subsection 3.3.2.



	considered domains					applied methods						
reference	components	failures	flows	functions	hazards	graphs	specific models	SysML	matrices	FTA	FMEA	others
Biehl et al. (2010)	✓	✓					✓			✓		✓
Blum (2010)	✓	✓	✓	✓		✓				✓		✓
Cuenot et al. (2014)	✓	✓	✓	✓			✓			✓		✓
Dorociak and Gausemeier (2012)	✓	✓		✓			✓			✓		
Biggs et al. (2014)	✓		✓	✓	✓			✓				✓
Höfig et al. (2014)	✓	✓					✓				✓	
Jensen and Tumer (2013)	✓	✓	✓	✓				✓			✓	
Joshi et al. (2007)	✓	✓	✓				✓			✓		
Kurtoglu and Tumer (2008)		✓	✓	✓		✓						✓
Li (2012)	✓	✓				✓					✓	
Majdara and Wakabayashi (2009)	✓	✓	✓			✓				✓		
Maurer and Kesper (2011)	✓	✓		✓					✓		✓	
Mhenni et al. (2016)	✓	✓	✓	✓				✓		✓	✓	
Papadopulus and Maruhn (2001)	✓	✓			✓	✓				✓		✓
Papadopulus and Parker (2004)		✓				✓					✓	
Sierla et al. (2012)	✓	✓	✓	✓		✓						✓
total (of 16)	14	15	9	9	2	7	5	3	1	8	6	7

Figure 4-6: Domains incorporated in relevant model-based methods for safety analysis

From both fields **components** clearly elicit as central element of a knowledge framework, which unites safety analysis and change propagation in the context of UDC. In addition, the domain of **functions** is object of most publications and a further core element of the framework.

ECM methods usually establish the links between and within both domains in form of abstract propagation dependencies, which are identified through expert knowledge. Instead, most publications from the field of safety analysis follow a more detailed approach. They use material, energy, or information **flows** to establish the propagation links between the system elements. Moreover, the safety analysis perspective also requires the domain of **failures** or faults as mandatory element of a knowledge framework.

Hence, the core of the ESMK knowledge framework consists (as indicated in Figure 4-7) of components, functions, flows, failures and their interrelations. Additionally, the framework can be extended by different domains depending on the specific aim of the analysis. Recommended domains are requirements (i.e. safety requirements) and hazards.

Moreover, to adjust the framework to different levels of abstraction, a **hierarchical decomposition** is needed (van Beek & Tomiyama, 2008, p. 165; Wölkl & Shea, 2009, p. 639). The knowledge framework provides this decomposition for the domains of requirements, components and functions. This for example allows to consider only assembly groups within the component domain or to decompose components further into design parameters.

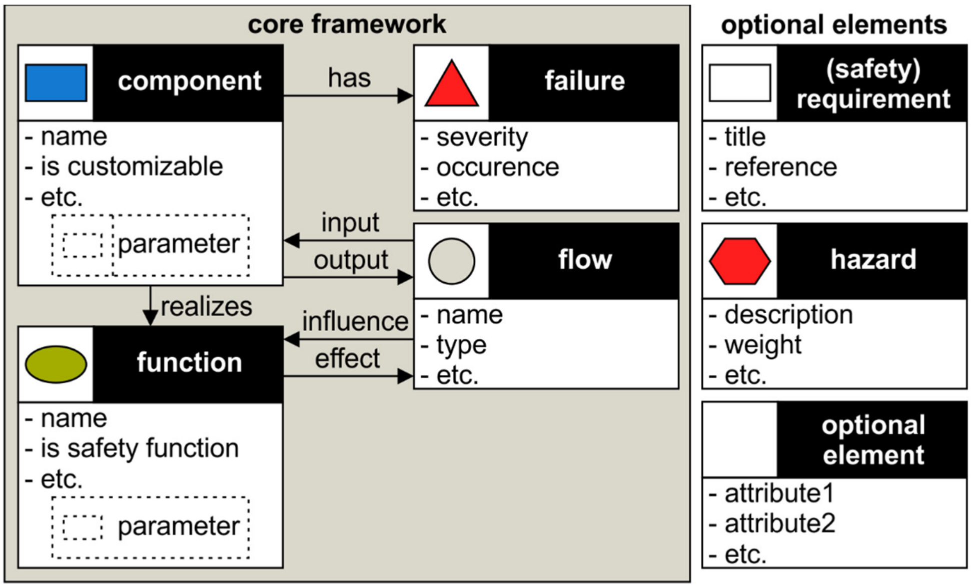


Figure 4-7: Domains and simplified meta-model of the ESMK knowledge framework

These domains and relationships define the structure of the knowledge framework. However, it is advantageous to consider not only the elements and their relations, but to include **element properties** in the framework as well. One example is the assessed severity of a failure or hazard, which is a mandatory element of a FMEA.

In addition, the knowledge framework and the included dependencies can quickly result in large data volumes (Lindemann et al., 2008, pp. 4–5; van Beek & Tomiyama, 2008, p. 169). Nevertheless, the framework has to be compatible with the major methods identified in the previous analysis (i.e. CPM, FMEA, FTA, and DSM). At the same time, due to the need for efficiency and automation (*REQ1*) and the large data volumes, the framework has to be suitable for **automated analyses** (van Beek & Tomiyama, 2008, p. 169; Wölkl & Shea, 2009, p. 639).

To comply with these constraints, a matrix representation is not suitable even though it is the basis of most ECM methods. It especially provides limitations in terms of the manageable amount of data (Browning, 2001, p. 302). Instead, graph-based models are very common in safety analysis. Thus, this thesis relies on typed attributed graphs and principles of graph-rewriting (Heckel, 2006; Helms, 2013, pp. 55–56). Graphs have the advantage of high performances when they are used as data storage concept (Robinson, Webber, & Eifrem, 2013, pp. 8–9). Especially attributed graphs in a simple manner allow assigning attributes to elements of specific domains. Moreover, as shown by Kissel (2014), these graphs allow an automation of workflows and to efficiently analyze and process the framework through graph-rewriting. Lastly, the dependencies of a typed attributed graph can be easily translated into matrices and vice versa (Lindemann et al., 2008, p. 98), which ensures compatibility with matrices.

Typed attributed graphs are composed by nodes and edges, both having attributes. The basic knowledge framework consists of 16 node types, representing the domains and auxiliary information, and 23 edge types, which represent the interrelations. They align with the meta-model of the framework introduced in Figure 4-7. A full overview of the included nodes and edges as well as their attributes is provided in Appendix 9.3.2.

4.3 The Efficient Safety Method Kit (ESMK)

Based on the concept of the ESMK defined in Section 4.1 and the common knowledge framework developed in the previous section, this section introduces the ESMK in detail. Distributed to its four phases, the **ESMK provides twelve support methods**. Figure 4-8 provides an overview of the specific tasks supported by these methods and their assignment to the four phases. As described above, the contribution focus of this thesis lies on the elicitation of safety functions, the identification of propagation effects, the conduction of preliminary safety analyses, and the assessment of elements (see bold letters in Figure 4-8).

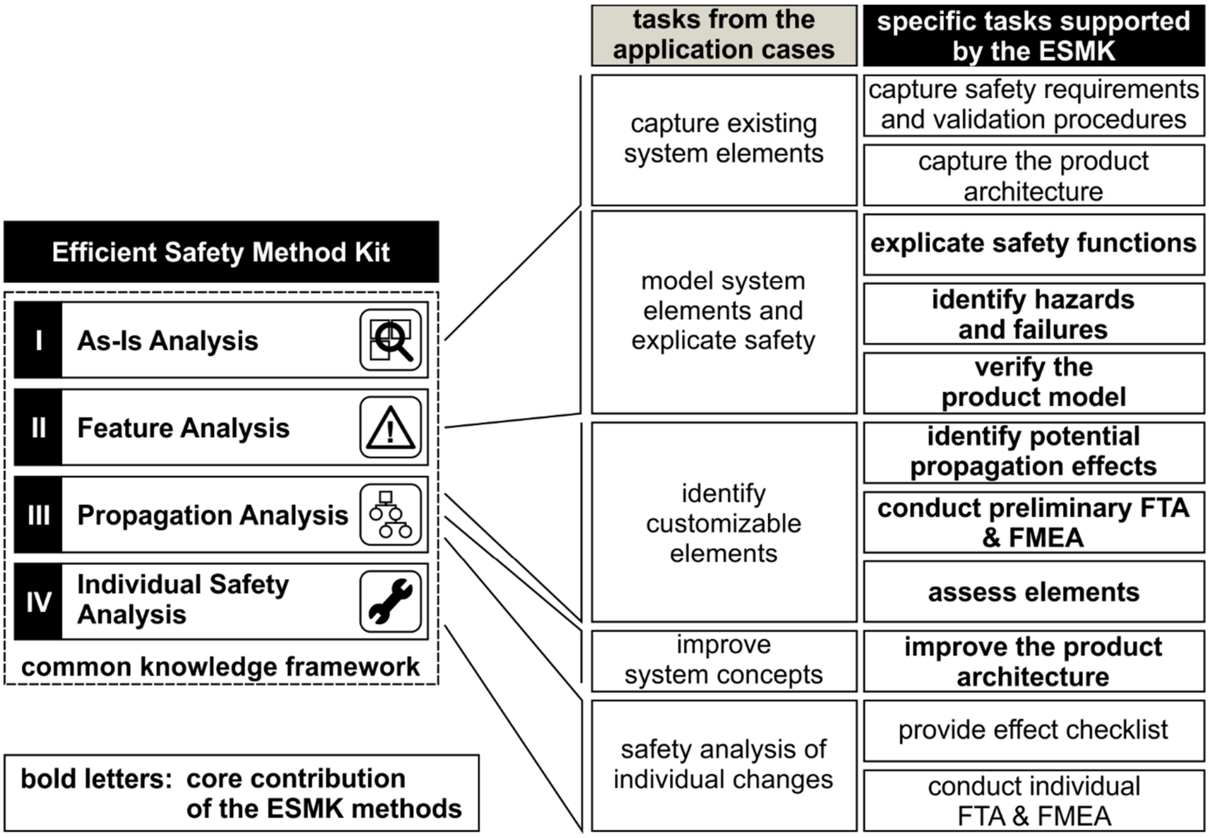

tasks from the application cases
specific tasks supported by the ESMK
Efficient Safety Method Kit
I As-Is Analysis
II Feature Analysis
III Propagation Analysis
IV Individual Safety Analysis
common knowledge framework
bold letters: core contribution of the ESMK methods
capture existing system elements
model system elements and explicate safety
identify customizable elements
improve system concepts
safety analysis of individual changes
capture safety requirements and validation procedures
capture the product architecture
explicate safety functions
identify hazards and failures
verify the product model
identify potential propagation effects
conduct preliminary FTA & FMEA
assess elements
improve the product architecture
provide effect checklist
conduct individual FTA & FMEA

Figure 4-8: Overview of the specific tasks supported by the methods of the ESMK

In the following subsections, the ESMK and its support methods are introduced. For each phase, the specific tasks in respect to the application cases are defined. Within these phases, the contribution focus of the ESMK is highlighted in detail and alternative methods are suggested.

Furthermore, for each specific task, the ESMK provides a support method, which is developed and described in detail. The descriptions of the specific methods are structured as follows. First, an overview of the method and its in- and outputs as well as its application situation and its effects is given. This overview and characterization of the methods relies on the description scheme provided by Lindemann (2009, pp. 61–62). A summary of these descriptions for the core contribution methods is provided in Appendix 9.4. Following that, the development of each support method based on the methodology introduced in the first paragraphs of chapter 4 is described. Finally, the support method as part of the ESMK is presented and explained using the exemplary case of a cordless screwdriver.

4.3.1 Phase I: As-is Analysis

This section describes the **first phase of the ESMK** including its supported specific tasks and support methods. The As-is Analysis prepares the basis for subsequent steps. The ESMK only provides minor contributions to the supported tasks. The following paragraphs give an overview these tasks and contributions. In detail, the Zwicky box of methods to elicit safety requirements and validation procedures and methods to model the product architecture are introduced.

Overview on Tasks and Contribution Focus of the As-Is Analysis

The **As-Is Analysis** aims to analyze the existing product and transfer the connected knowledge into the ESMK knowledge framework. This knowledge mainly consists of the product architecture, which comprises the product's components, its functions, as well as their interrelations (Ulrich, 1995, p. 420). However, in order to provide full transparency and integrate different views, also requirements and validation procedures should be integrated. The resulting relevant in- and outputs of this phase can be summarized as shown in Figure 4-9.

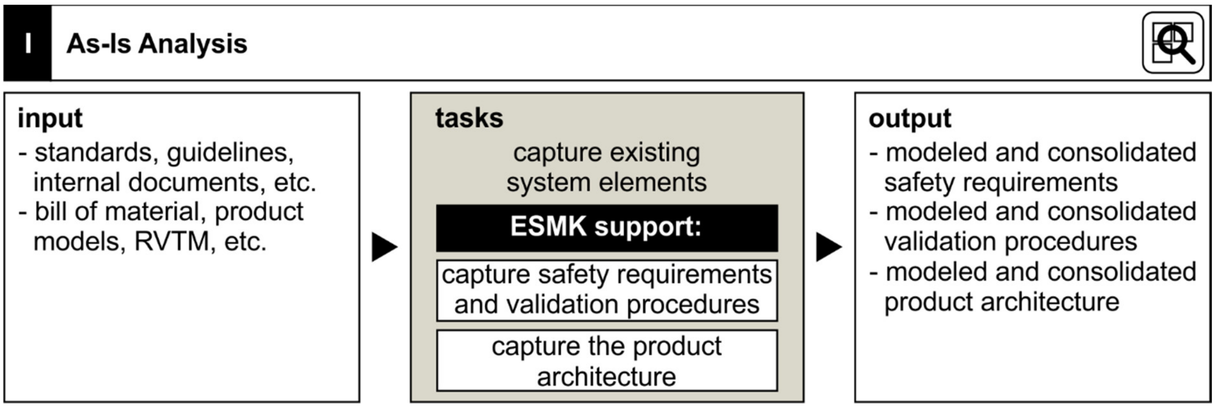

I
As-Is Analysis
input
- standards, guidelines, internal documents, etc.
- bill of material, product models, RVTM, etc.
tasks
capture existing system elements
ESMK support:
capture safety requirements and validation procedures
capture the product architecture
output
- modeled and consolidated safety requirements
- modeled and consolidated validation procedures
- modeled and consolidated product architecture

Figure 4-9: Overview of the in- and outputs and supported specific tasks of phase I (As-Is Analysis)

Broken down to **specific tasks**, the As-Is Analysis according to Figure 4-9 comprises the following two tasks:

- capture requirements (i.e. safety requirements) and validation procedures
- capture the product architecture

The identification and modeling of requirements are an essential element of engineering activities. This applies especially in connection to classical customization. For the acquisition and specification of general requirements, many support methods exist (see paragraph below). From a safety perspective, as the focus-interviews (Section 3.3.2) identified, the engineers mainly rely on standards and guidelines. However, the interviewees highlight that these documents are often challenging to read or interpret. In this context also implicit knowledge and the manufacturer's or individual's interpretation of safety plays an important role. This applies for validation procedures to a similar extent. To support the definition of safety requirements and validation procedures as well as to increase the transparency (*REQ5*) of these processes, the ESMK for both tasks provides a **Zwicky box of methods to support the systematic elicitation of safety requirements and validation procedures**.

The product architecture is a central element of the ESMK knowledge framework (see Section 4.2). Only if the product architecture is modeled in the framework, its safety-oriented preparation (*REQ2*) based on the ESMK is possible. In addition, a consistent model of the product architecture improves transparency and documentation (*REQ5*). As the ESMK covers the transfer to UDC as well as the redesign for UDC, two different origins of the product architecture are possible. In the first case, the architecture can be captured from existing documents or models. In the second case, it has to be modeled during the design process. To support both cases, the ESMK provides a collection of **methods to capture and model the product architecture**.

In summary, the As-Is Analysis phase of the ESMK provides support to capture safety requirements, validation procedures, and the product architecture. This support on the one hand is the Zwicky box of methods to support the systematic elicitation of safety requirements and validation procedures, which specifically aims at normative safety requirements. On the other hand, a collection of methods to capture and model the product architecture is provided. In other situations, **alternative methods** might be better suitable or provide valuable extensions. The following paragraph provides selected examples.

The field of requirements engineering provides tools and methods to support the elicitation of requirements and their specification. An overview is for example given in Hood (2008) and Pohl and Rupp (2015). In addition, specific methods to support the elicitation of non-normative requirements are published. They for example rely on misuse cases (Sindre & Opdahl, 2005) or are based on scenarios of hazard mitigation use cases (Allenby & Kelly, 2001).

Zwicky Box of Methods to Elicit Safety Requirements and Validation Procedures

The Zwicky box of methods to elicit safety requirements and validation procedures supports the task of capturing these elements and integrating them in the ESKM knowledge framework. As Figure 4-10 summarizes, it relies on existing documents like standards, guidelines, or internal documents to model and consolidate safety requirements and validation procedures. The reason why both aspects are integrated in one task is that most standards and regulations not only define safety requirements but do also prescribe specific procedures to validate their fulfillment. The Zwicky box of methods is based loosely on a student project (Rapp, 2015).

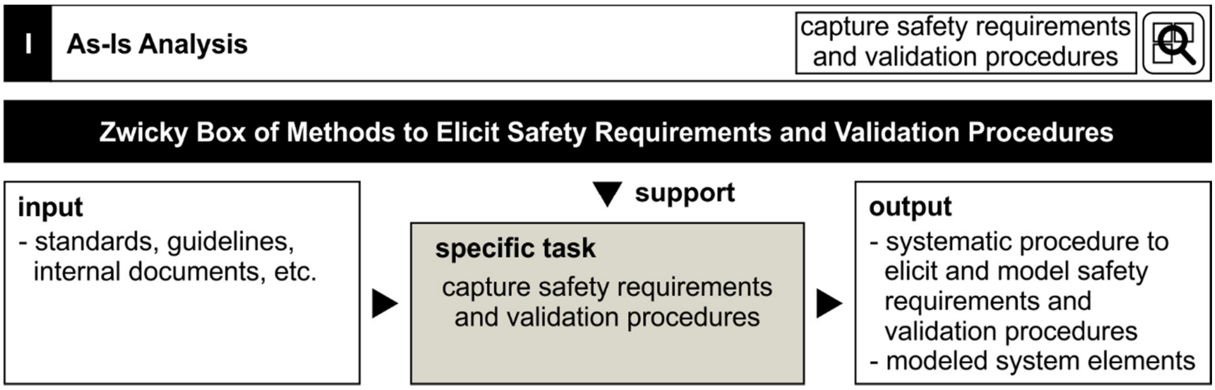

I
As-Is Analysis
capture safety requirements and validation procedures
Zwicky Box of Methods to Elicit Safety Requirements and Validation Procedures
input
- standards, guidelines, internal documents, etc.
▼ support
specific task
capture safety requirements and validation procedures
output
- systematic procedure to elicit and model safety requirements and validation procedures
- modeled system elements

Figure 4-10: Overview of the in- and outputs and the supported task of the Zwicky box of methods

The **purpose** of the Zwicky box of methods is the support of a systematic identification, extraction, and documentation of relevant safety requirements and validation procedures. Through the systematic approach, it also follows the aim to make the implicit interpretation of safety requirements and validation procedures as well as of their interdependencies explicit. Thus, its **effect** is a systematic procedure to elicit and document safety requirements and validation procedures. By that, it moreover supports to reduce the overall amount of implicit expert knowledge. The Zwicky box of methods can be applied in **situations**, when various sources of requirements and validation procedures exist, the connected knowledge mostly is implicit expert knowledge, or the actual information is difficult to extract from existing documents.

Development of Support

The task clarification for the development of a support to capture safety requirements and validation procedures first defined the relevant aspects to be considered during the elicitation process. To capture existing requirements and validation procedures, it was necessary to analyze possible sources, extraction methods, existing validation approaches, and ways of documentation. For each of the fields, existing sources or methods were identified from literature and analyzed on their suitability. Moreover, the Zwicky box was identified as existing solution to structure the methods and aspects. It was adjusted and the identified sources or methods were structured within it.

Provided Support (Zwicky Box of Methods to Elicit Safety Requirements and Validation Procedures)

The following paragraphs introduce the **Zwicky box of methods to elicit safety requirements and validation procedures**. This includes the sources of safety requirements, methods to extract information, validation procedures, and documentation methods. Moreover, the synthesis of the Zwicky box and its application are described.

In general, **sources of requirements** can be classified into the three categories of stakeholders, systems in use, and documents (Pohl & Rupp, 2015, p. 21). In the As-Is Analysis, the existing system in use can provide requirements for improvements, but the knowledge of safety requirements usually originates from documents. Most common documents are norms and standards, which however usually are specific for a branch or organization (Pohl & Rupp, 2015, p. 21). With focus on safety requirements, these documents can be classified into laws, standards, guidelines, and internal documents.

From these documents, important **information** to derive requirements can be **extracted** (Pohl & Rupp, 2015, p. 21). To extract information manual and computer-aided methods exist. The simplest method on the one hand is manual reading of the documents. On the other hand, computer-aided document analysis methods comprise two stages: document analysis and document understanding (Tuot, 2015, p. 92). The document analysis aims to extract information from written text, while the document understanding adds the interpretation and analysis of interdependencies (Tuot, 2015, pp. 91–93).

To **validate** the conformance of the product with extracted safety requirements, various methods exist. In the following, a selection of major and most common methods is given (based on Blum (2010, p. 25) and Nair, de la Vara, Jose Luis, Sabetzadeh, and Briand (2014)). These methods on the one hand include **qualitative analyses** as for example:

- expert analysis (e.g. manual inspection)) (Haskins, 2011, p. 127; Nair et al., 2014, p. 701)
- FTA and FMEA (qualitative) (see Subsection 2.3.2)

On the other hand, the methods include **quantitative analyses**, which for example are:

- reliability/risk analyses (e.g. count failures, reliability (Gottschalk, 2010, p. 87), mean time between failures (Gottschalk, 2010, p. 85), and Reliability block diagrams (IEC 61078))
- FTA/ETA and FMEA (quantitative) (see Subsection 2.3.2)
- simulations (e.g. Hardware-in-the-Loop (VDI 2206, p. 40), Monte-Carlo simulation (Mooney, 1997))
- tests (Haskins, 2011, p. 127)

The **documentation** of the identified requirements can be conducted in free natural language or with more formal techniques, which can be further classified in conceptual models and hybrid forms (Pohl & Rupp, 2015, p. 35). In practical application natural language is widely spread. Examples for conceptual models are for example use case or activity diagrams (Pohl & Rupp, 2015, pp. 37–39). The ESMK knowledge framework instead uses a hybrid form.

To structure the previously introduced methods and support the systematic procedure, the ESMK arranges them in a **Zwicky box** (see Zwicky (1966)). It is specifically suitable to condense and structure information (Lindemann, 2009, p. 281). The Zwicky box assigns the specific subproblems to the rows of a matrix and in each row inserts alternative solutions for the subproblem. Once, the box is filled, the subproblems are combined to a complete solution (Lindemann, 2009, pp. 281–282).

To systematically plan and conduct the requirements elicitation, documentation, and validation, the Zwicky box as shown in Figure 4-11 includes the rows source (i.e. documents), information extraction, documentation, and validation procedure. This Zwicky box moreover includes the basic methods and principles described above. Instead of the original purpose of the Zwicky box, it also allows multi-allocations.

As visualized in Figure 4-11, the ESMK moreover suggests refining and concretizing the Zwicky box depending on situation and product in an iterative manner. There, for example the validation procedure of a requirement is concretized in an iterative manner from manual inspection to the inspection with a specific probe. This supports the documentation and traceability of the capturing of requirements and improves transparency. If applied consequently, the Zwicky box on a detailed level can be translated to a requirements verification and traceability matrix (RVTM) (Haskins, 2011, p. 91).

In **summary**, the Zwicky box of methods to elicit safety requirements and validation procedures supports the identification of requirements and validation procedures based on documents. By providing a methodology to structure and document the connected procedure, it improves traceability, transparency, and helps to better systemize the activities. It contributes to the improved transparency and documentation of the resulting requirements and validation procedures regardless if stored in the ESMK knowledge framework or in other forms. By that, it supports the transfer of implicit safety knowledge into the knowledge framework.

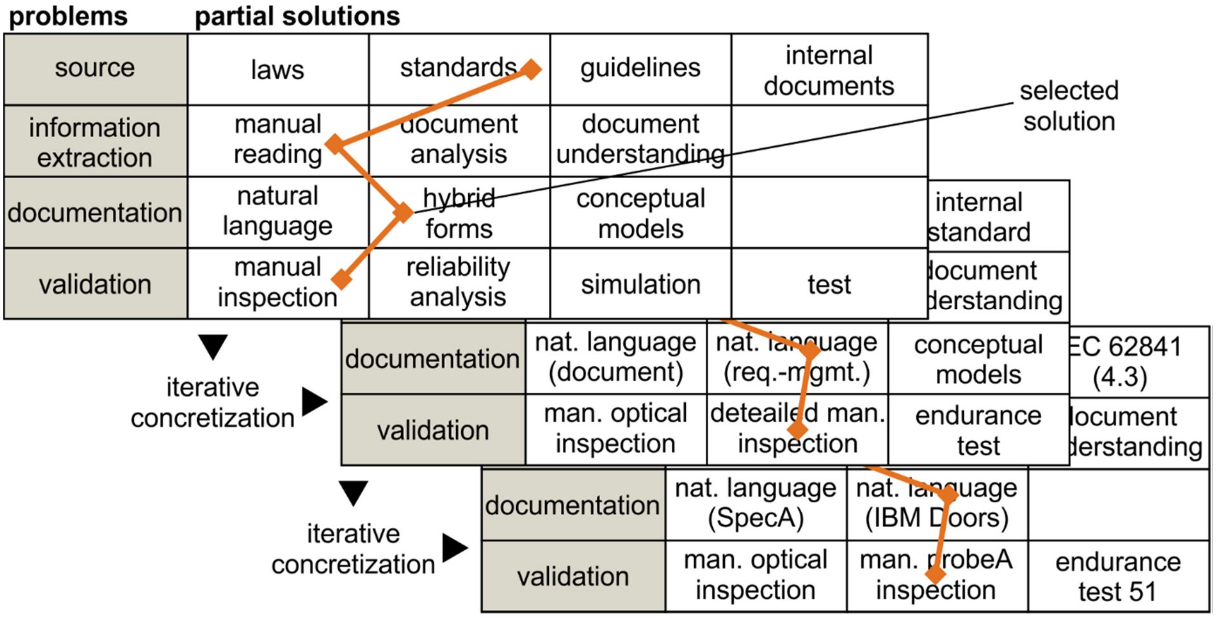


Figure 4-11: The Zwicky box of methods to elicit safety requirements and validation procedures

Methods to Capture and Model Product Architectures

Methods to capture the product architecture model of the product architecture of an existing product or of a new product concept. As summarized in Figure 4-12, they rely on documents like the bill of material (BoM) or existing product models. The result is a model of the product architecture, which comprises components, functions, as well as their dependencies (Ulrich, 1995, p. 420). The ESMK knowledge framework moreover integrates flows. As a wide variety of suitable documents or models and modeling methods exists, the ESMK only offers an overview of the most important modeling methods as well as suitable documents.

The general **purpose** of these methods is to support the systematic modeling of the product architecture. Their **effect** usually is a modeled product architecture with a specific purpose and level of detail. They are applied in **situations**, when the system understanding or analyses require a model of the product architecture. The selection of a specific method depends on the specific boundary conditions and situation.

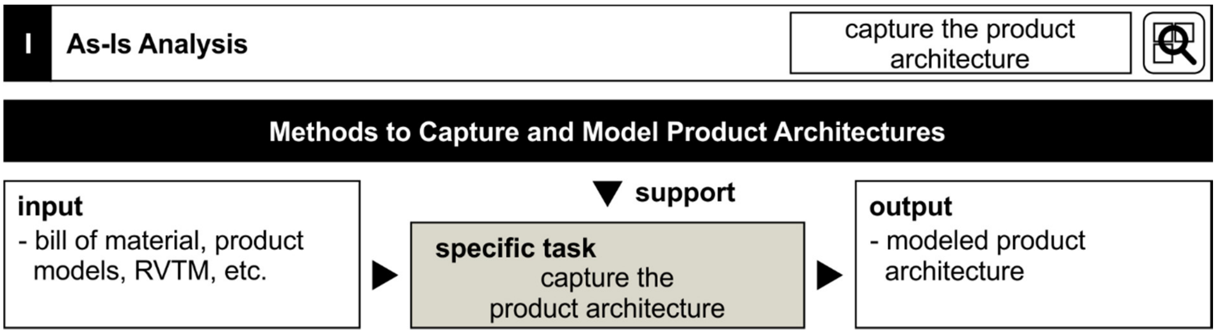

I
As-Is Analysis
capture the product architecture
Methods to Capture and Model Product Architectures
input
- bill of material, product models, RVTM, etc.
support
specific task
capture the product architecture
output
- modeled product architecture

Figure 4-12: Overview of the in- and outputs and the supported task of methods to capture the product architecture

Provided Support (Methods to Capture and Model Product Architectures)

The desired output of the specific supported task is a **model of the product architecture** stored in the ESMK knowledge framework or similar. From an engineering design perspective, a model can be described as simplified and purposeful representation of an original (Lindemann, 2009, p. 333). It is an "[…] incomplete representation of the reality, an abstraction" (Buede, 2009, p. 75). Kohn (2014, pp. 25–27) highlights with reference to Stachowiak (1973) that models include three important characteristics:

- They are only representations of an original.
- They only represent a reduced set of attributes of the original, dependent on their purpose.
- They are only a pragmatic representation valid for specific individuals within a specific period. Therein, an original can be a model itself.

To support the transfer from original to a purposeful specific representation, especially **systems thinking** provides support. It according to Haberfellner (2012, pp. 33–35) describes a system as a sum of elements, which interact through relations, within a system boundary. The system itself interacts with its environment, which can include other elements or other systems. Moreover, systems thinking supports the modeling through the principles of hierarchical decomposition, the black-box principle and the principle of different perspectives on a system (Haberfellner, 2012, pp. 38–40).

To describe the resulting models, **modeling languages** are defined. They prescribe a meta-model, which defines the basics and syntax of a model (Kohn, 2014, pp. 35–36). The ESMK's definition of the knowledge framework given in Section 4.2 is one example of such a meta-model. Other examples of modeling languages commonly used in practical application are the Systems Modeling Language (SysML) provided by the Object Management Group, Inc.[13] and Modelica provided by Modelica Association[14]. To describe product structures in engineering design, apart from SysML, for example also the Design Structure Matrix (DSM) (Browning, 2001) or the Function Behavior Structure (FBS) framework are applied. The ESMK knowledge framework is defined to be compatible with the main concepts of these modeling languages.

In the phase of the As-Is Analysis, especially in the case of a transfer to UDC, many **existing models or documents** can be used to extract the needed attributes and to translate them according to the meta-model of the knowledge framework. Apart from models described in the modeling languages mentioned above, the following paragraphs suggest a selection of suitable documents or other models.

The bill of material is a commonly used document in companies. It provides information on the hierarchical product structure (Schuh, 2005, p. 140). Hence, bills of material can be a basis to capture the structural decomposition of the product.

CAD models are another central element of product development. They represent the geometry of a product in a computer-based format (Kohn, 2014, p. 231). They store for example information of contact relationships between components.

[13] Source: http://www.omg.org, last access: 2016/09/29

[14] Source: https://www.modelica.org, last access: 2016/09/29

Requirements management software also is a commonly used tool used in larger development projects. For example, it stores a consistent set of requirements, their decomposition, dependencies, and their relations to components in a database (Pohl & Rupp, 2015, pp. 151–152).

In **summary**, many existing documents can support the modeling of the product architecture in the ESMK knowledge framework. Their suitability depends on the situation and product. The ESMK knowledge framework allows the integration of many of these models. However, when these models are transferred into the knowledge framework, it is necessary to keep the model's pragmatic, reduction, and representation character in mind.

4.3.2 Phase II: Feature Analysis

This section describes the **second phase of the ESMK** including its tasks and support methods. The Feature Analysis mainly aims to integrate safety aspects in the ESMK knowledge framework and make it explicit. These aspects are a major contribution of the ESMK. The following subsections provide an overview of the supported tasks and the ESMK's contribution. In detail, the method to explicate safety functions, the model-based hazard analysis, and the pattern-based model verification are introduced. The latter aims to verify all modeling activities made during the first two phases of the ESMK.

Overview on Tasks and Contribution Focus of the Feature Analysis

The **Feature Analysis** aims to identify safety-relevant aspects of the existing product or concept and make them explicit within the ESMK knowledge framework. As visualized in Figure 4-13, this phase analyzes the product architecture model resulting from the As-is Analysis (see Subsection 4.3.1) or from any other source. The Feature Analysis identifies hazards, failures, and safety functions as well as their relationships in this model. This identification especially follows the objective to integrate design and safety models (*REQ3*) and to provide transparency and a consistent documentation (*REQ5*). The resulting relevant in- and outputs of the Feature Analysis and its supported specific tasks can be summarized as shown in Figure 4-13.

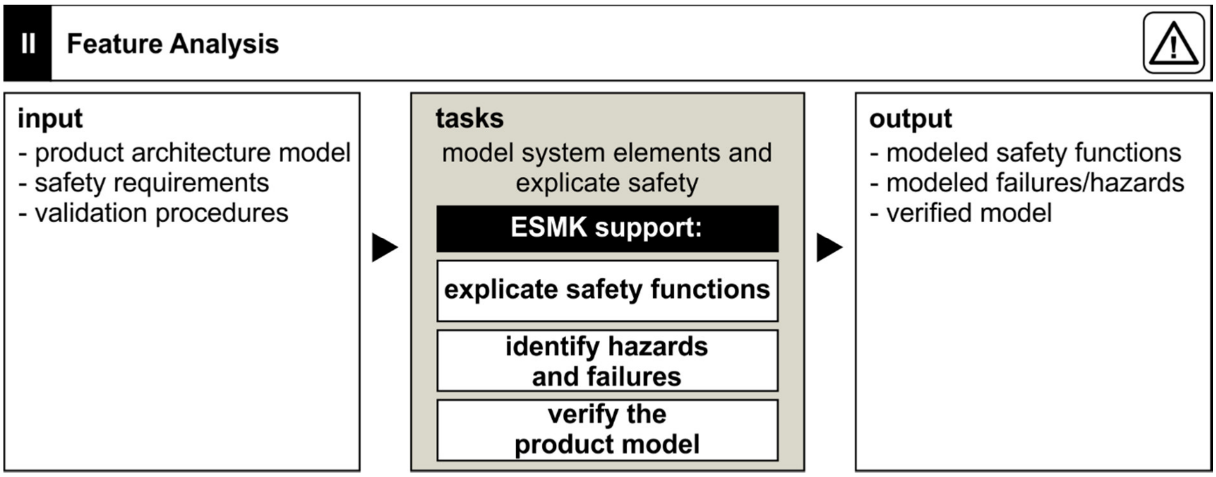

II Feature Analysis
input
- product architecture model
- safety requirements
- validation procedures
tasks
model system elements and explicate safety
ESMK support:
explicate safety functions
identify hazards and failures
verify the product model
output
- modeled safety functions
- modeled failures/hazards
- verified model

Figure 4-13: Overview of the in- and outputs and supported specific tasks of phase II (Feature Analysis)

Broken down to **specific tasks**, the Feature Analysis according to Figure 4-13 comprises the following two tasks:

- make safety functions explicit
- identify hazards and failures

Moreover, the Feature Analysis marks the end of the modeling activities within the ESMK knowledge framework. Yet, the quality of the model and data stored in the knowledge framework determine the quality of the subsequent analyses (Kissel, 2014, p. 166). As modeling processes underlie uncertainties (Kasperek, Kohn, & Maurer, 2013, p. 44; Walker et al., 2003, p. 5), human errors (Swain & Guttmann, 1983, pp. 2-7-2-8), and variations (Kohn, 2014, p. 8), it is necessary to verify the model. This activity can be conducted in an integrated manner during all modeling processes in phases I and II or after the complete model is developed in phase II. Hence, the third task of the Feature Analysis is:

- verify the product model

As described in Subsection 2.3.1, hazards are an important element of product safety. To ensure, the product remains in the safe space, not only hazards need to be made explicit in the knowledge framework. In addition, their counterpart, which helps to keep the product in the safe state, needs to be integrated. This counterpart are the so-called safety functions (see Subsection 2.3.1). When component changes are in the focus, according to the interviewees of the focus-interviews (Subsection 3.3.2), often some of these safety functions are neglected. The reason is that they are only implicit knowledge of safety analysts but not known to the designers. The non-expert changes through UDC deteriorate this situation. Hence, the ESMK provides a **method to make safety functions explicit**, to support the specific task of explicating safety functions. The method intervenes in the modeling and supports making implicit safety functions explicit as well as integrating them in the knowledge framework. The method mainly contributes to the fulfillment of *REQ3*, *REQ4* and *REQ5*.

As already mentioned, hazards and failures are necessary elements to enable and determine the product safety. Both elements have to be identified within the product architecture and their dependencies and relationships need to be modeled. To identify possible hazards and failures, various methods exist (see paragraph below). As UDC can lead to changes, which have an unforeseen impact on the product safety (see Subsection 3.4.1), it is necessary to identify all possible hazards or failures (*REQ3*). This especially applies for hazards, which in the original product are not relevant and hazards connected to misuse. To support the specific task of the identification of hazards and failures, the ESMK provides a **model-based hazard analysis**, which mainly contributes to *REQ4*.

As described above, the quality of the model within the knowledge framework determines the quality of subsequent analyses. To uncover errors within the model and contribute to the specific task of verifying the model, the ESMK provides a **pattern-based model verification**. As the knowledge framework is represented by typed attributed graph, the pattern-based verification provides algorithms and principles to identify invalid patterns. By that, it supports the improvement of the model quality (*REQ5*) and increases automation (*REQ1*).

In summary, the Feature Analysis phase of the ESMK provides support to make safety functions explicit, to identify hazards and failures, as well as to verify the model within the knowledge framework. The provided support methods aim at specific purposes and situations. In other situations, **alternative methods** might be better suitable for the given tasks. The following paragraphs provide selected examples.

To model safety functions, the simple relation-oriented functional modeling by Lindemann (2009, pp. 125–126) can be a fast and simple alternative. Moreover, with more emphasize on mechatronic systems, also the method of Jensen and Tumer (2013) is a possible approach. In addition, for special safety-critical products, the holistic methodology of Mhenni et al. (2016) can be suitable as well.

To identify hazards, various analysis methods exist. Alternative methods like the Preliminary Hazard Analysis are introduced in Subsection 2.3.2. Moreover, for example, the SafeML proposed by Biggs, Sakamoto, and Kotoku (2014) might be another suitable alternative.

To verify the model within the knowledge framework, it might be beneficial to apply model checking techniques. They are formal methods to verify design models (Clarke, Grumberg, & Peled, 1999, p. 1). One example is the methodology proposed by Hehenberger, Egyed, and Zeman (2010). An overview of further methods can be found in Feldmann et al. (2015). In addition, also simulations provide a possible alternative to verify the model. Especially the combination with model checking techniques is promising (Vogel-Heuser, Folmer, Aicher, Mund, & Rehberger, 2015).

Method to Explicate Safety Functions

The method to explicate safety functions, as the name suggests, supports the task of making safety functions explicit. It aims to improve the understanding of the safety-relevant features of the product. As Figure 4-14 summarizes, the method relies on the product architecture modeled in the knowledge framework as well as on existing hazard documents. Based on this, the method models safety functions explicitly within the ESMK knowledge framework. The method to explicate safety functions is published in Roth, Münzberg, and Lindemann (2016).

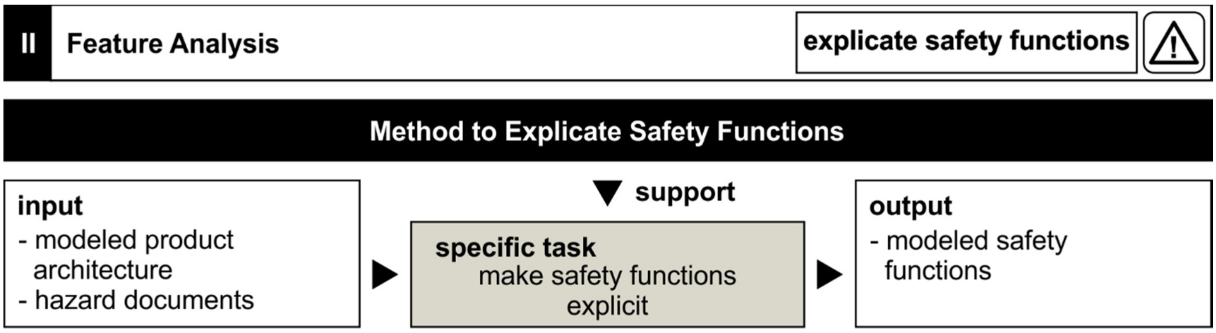

II Feature Analysis
explicate safety functions
Method to Explicate Safety Functions
input
- modeled product architecture
- hazard documents
support
specific task
make safety functions explicit
output
- modeled safety functions

Figure 4-14: Overview of the in- and outputs and the supported task of the method to explicate safety functions

The **purpose** of the method to explicate safety functions is to translate implicit expert knowledge on safety functions into explicit knowledge. Thus, the **effects** are defined and modeled safety functions within a product architecture. Moreover, a functional structure can be achieved, in which all decomposition levels and subfunctions provide a safe solution space. The method to explicate safety functions can be applied in **situations**, when it is necessary to explicate safety-related knowledge or to make this knowledge through a model accessible for multiple persons. Moreover, the method supports situations, in which the gap between design and safety needs to be bridged and awareness on the relations between product design and product safety needs to be fostered.

Development of Support

The development of the method to explicate safety functions to clarify the problem, builds on a review of existing methods to model product functions as well as specific approaches to model safety functions. A set of requirements on the method was defined based on this review, specific challenges in model-based safety analysis (see Subsection 2.3.3), and the general requirements of the ESMK (see Subsection 3.4.2). The mentioned review already proposes solutions, which in respect of this set of requirements are evaluated. As none of the existing methods sufficiently fulfilled the requirements, the most promising approaches were adapted and improved to obtain the method to explicate safety functions. This development procedure is described in detail in the following paragraphs.

The existing fundamental works in engineering design (e.g. Ulrich and Eppinger (2004), Pahl, Beitz, Feldhusen, and Grote (2007), and Lindemann (2009)) all propose methods to model products starting from early phases of design. In their core, they all use and **abstract description of functions and their interrelations**. The variation between approaches usually lies in the type and detail level of these interrelations, which is modeled. For example, Pahl et al. (2007, pp. 31–34) suggest to model the functional structure through flows of material, energy, and information.

The theory of inventive problem solving (TRIZ) (see Altshuller (2004)) uses similar concepts to abstract problems. It uses a component analysis and analysis of their interactions in the sense of physical contact (interaction analysis) to build a functional model (Münzberg, Hammer, Brehm, & Lindemann, 2014, p. 334). To derive a problem-specific model, TRIZ suggests the **Substance-Field-Analysis**. It uses fields as representation of interactions between system elements. Valid fields are mechanical, acoustic, thermal, chemical, electric and magnetic, intermolecular, and biological fields, abbreviated with MATChEMIB (Belski, 2007, pp. 16–17).

Extensions to include safety aspects in the analysis exist. For example, Belski, Belski, Chong, and Kwok (2013) apply the Substance-Field-Analysis to systematically identify and analyze possible failures. They rely on the **MATChEMIB fields** to identify all possible failures and ensure completeness. Also Regazzoni and Russo (2011) acknowledge the advantages of the Substance-Field-Analysis and use it to improve and simplify the FMEA. Based on substance-field models, they derive preventive or corrective measures, which can be interpreted as a type of safety measure.

As alternative to the flow- or field-based modeling of interrelations, Lindemann (2009, pp. 125–126) adopts the idea of Terninko, Zusman, and Zlotin (1998) and suggests a **relation-oriented modeling**. Supportive relations and causalities represent the interrelations between functions. This approach distinguishes between harmful and useful functions and helps to identify all relevant functions through standard questions (Lindemann, 2009, pp. 301–302; Terninko et al., 1998). The approach inherently models safety functions by modeling the functions that inhibit harmful functions. However, harmful is interpreted widely and not limited to safety aspects. Moreover, a link to the product structure is missing.

The domain of systems engineering mainly relies on **SysML**, which supports the specification, analysis, and design of complex systems. It similarly to the previously described approaches distinguishes between structural and behavioral diagrams. The latter are mainly modeled in activity, sequence and state machine diagrams. There, transitions, flows, and allocations are used to model interrelations (Friedenthal, Moore, & Steiner, 2015; Weilkiens, 2007).

Also for **SysML extensions** addressing safety issues, exist. For example Biggs et al. (2014) extend the standard to model safety and design information in an integrated manner. Their SafeML-profile introduces seven new elements (e.g. hazards and detection measures) and improves traceability and consistency. However, it does neither consider the functional architecture, nor provide modeling support. It moreover requires a detailed and formal SysML model. As described in Section 2.3.3, Jensen and Tumer (2013) use SysML to model safety in early design. However, their approach induces the constraint that safety functions are not decomposable and they do not allow a mapping of low-level failures. Nevertheless, they provide a systematic modeling support.

To evaluate and, if necessary, adapt the existing methods, the challenges identified in Subsection 2.3.3 and the general requirements of the ESMK (see Subsection 3.4.2) were used to define the following three **requirements**:

- integrate safety aspects in functional and structural modeling to support the modeling of safety aspects in early phases of design (Subsection 2.3.3, *REQ3* and *REQ4*)
- make safety functions explicit in functional modeling to bridge the gap between design and safety (Subsection 2.3.3and *REQ2* to *REQ5*)
- model the link of components to hazards and safety functions, as failures occur on structural level (Jensen and Tumer (2013, p. 826), *REQ3* and *REQ4*)

Based on these requirements, the author evaluated the models and methods introduced above. In summary, some existing approaches provide a simple modeling procedure, but lack of a simple and sufficient explication of safety aspects or do not establish a link between the structural and functional perspective. Others extensively model safety aspects, but rely on very detailed models and only focus on active safety functions. To provide a simple, but complete explication of safety functions within the ESMK, an adapted method is required.

According to the evaluation, the **most suitable approaches** are the relation-oriented function modeling (Lindemann, 2009, pp. 301–302) and the modeling of safety functions by Jensen and Tumer (2013). While the first provides a simple and flexible modeling, the latter provides a specific explication of safety aspects. This thesis combined both approaches and further adapted them to satisfy the defined requirements.

Provided Support (Method to Explicate Safety Functions)

The resulting **method to explicate safety functions** as part of the ESMK builds on the definition of safety functions given in Subsection 2.3.1. It supports the explication through the four step modeling procedure shown in Figure 4-15. These steps comprise the preparation of the product model, the modeling of flows, the mapping of hazards, and the explication of safety functions. Each of these steps is in detail described in the following. The examples use the graphical notation of the ESMK knowledge framework summarized in Figure 4-15.

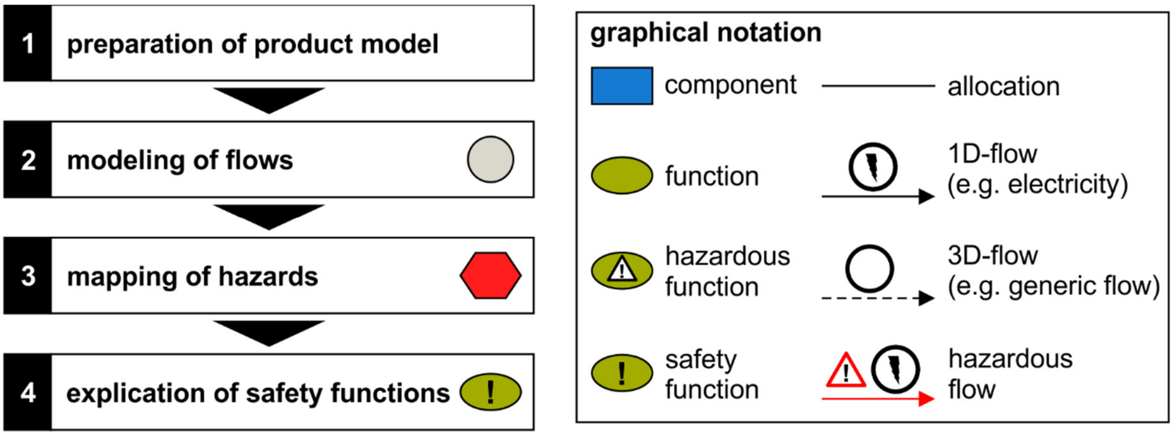


Figure 4-15: Procedure of the method to explicate safety functions (left) and the used graphical notation (right)

The first step of the method to explicate safety functions is to **prepare the required data and product model**. Especially the scope, system boundaries and granularity of the analysis have to be defined.

The method first requires a product architecture model, which includes the functional and structural decomposition as well as their linkages. If the ESMK is used, this data is stored in its knowledge framework from the As-is Analysis. In this case, the functional and structural views can be accessed directly. If the product architecture is not available, it has to be modeled. Support for this task is discussed in Subsection 4.3.1. Figure 4-16 provides an extract of the resulting models, and indicates boundaries for the example used in the following. The figure shows the functional structure of the cordless screwdriver and the decomposition of the considered function "generate torque". Moreover, the link from functions to the components "engine" and "electronics" is established.

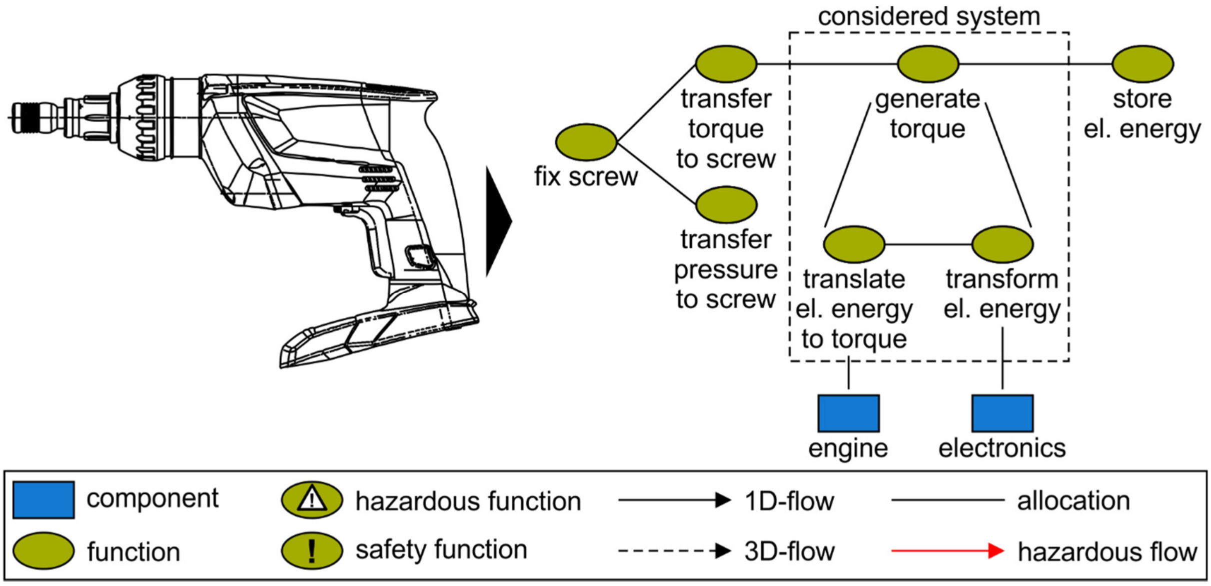


Figure 4-16: Example of the functional and structural model of the cordless screwdriver (source: HILTI AG)

In addition to the product architecture model, the method to explicate safety functions requires information on occurring hazards. Possible hazards have to be identified and collected. Existing norms and standards for example provide support through hazard collections or checklists (e.g. ISO 12100). Moreover, internal hazard checklists for the specific products in companies often exist as well. Other support methods are indicated in the section on alternative methods (see beginning of Section 4.3.2).

In the second step of the method to explicate safety functions, the focus is shifted to a detailed analysis of the **interactions between components**. Flows are used to model these interactions out of the following two reasons. First, as already mentioned above, failures occur on the component level (Jensen & Tumer, 2013, p. 826). Hence, the structural component perspective is the starting point, when safety is made explicit. Second, risks occur at interactions of components with other components or of components with the environment (Ghemraoui et al., 2009, p. 162). As also stated by Belski et al. (2013, p. 484), the interactions of fields and substances, which also can be considered as flows, help to systematically identify all possible failures. Thus, the method to explicate safety functions combines the Substance-Field Analysis with the concept of energy, material, and information flows. It models the following two types of flows:

- 1D-flows (energy, material, information), which are bound to a local interaction. Examples are electrical control signals or mechanical torque on a shaft.
- 3D-flows spread more or less freely and correspond to the fields of the Substance-Field Analysis. The MATChEMIB fields support to distinguish the two types of flows. Examples of 3D-flows are heat radiation around an engine or electromagnetic fields of a transformer.

The task in this step is, to systematically analyze the components' interactions and model those as 1D- and 3D-flows. If the ESMK knowledge framework is used, the interactions are already stored in the framework and only the flow types need to be analyzed. However, especially interactions with the environment and 3D-flows should undergo a detailed analysis as they play an important role for product safety. For the given example, this detailed analysis results in the model shown in Figure 4-17. There, for example, the engine translates the 1D-flow "transformed voltage" into the 1D-flow "torque". The engine additionally emits the two 3D-flows "electromagnetic field (emf)" and "heat" to the environment.

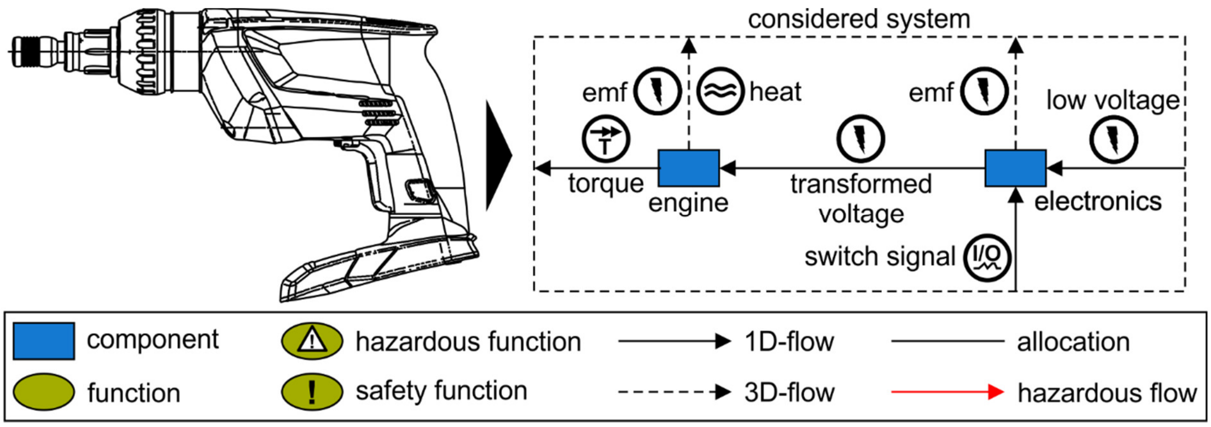


Figure 4-17: Example of the structural model with 1D- and 3D-flows (source: HILTI AG)

The method to explicate safety functions moreover suggests to model user contact as an additional abstract 1D-flow to the environment. However, if also misuse needs to be considered in detail, a subsequent, more detailed model-based hazard analysis (see next method of the Feature Analysis) might be beneficial.

Finally, the flow interactions additionally should be transferred to the functional structure. If the knowledge framework is used, this can be achieved via the allocation of functions to components. However, as this reduces the clarity of the visualization, it is not a mandatory perquisite for the following steps.

The third step of the method to explicate safety functions **maps the identified hazards**. As stated above, risks occur on interactions. This step examines the modeled flows on their risks (i.e. hazards) by mapping the interactions and the hazards identified in the first step. If the flow bears a hazard, this relationship is added to the model and the ESMK knowledge framework. It is important to note that flows can bear multiple hazards or no hazard at all. This allocation of hazards is shown in Figure 4-18 for the given example. The flows "emf" and "heat" emitted by the engine are mapped to the corresponding hazards "emf" and "burning".

Moreover, this step identifies hazardous functions. This is achieved using the mapped hazards and the allocation of functions to components or flows. In this context, a hazardous function is related to a hazard and can lead to a mishap concerning this hazard. These hazardous functions are assigned to the corresponding useful or regular functions and are temporarily added to the functional structure. Figure 4-18 also visualizes this temporal assignment. For the hazard "burning", for example, the hazardous function "produce heat" is added.

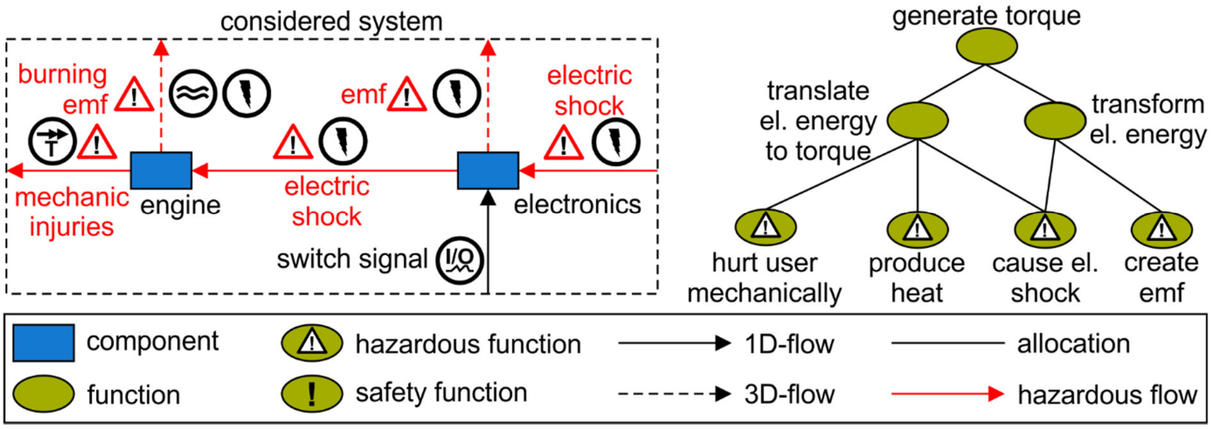


Figure 4-18: Example of the hazards mapped to flows in the structural model (left) and hazardous functions allocated in the functional structure (right)

The fourth and last step **makes the safety functions explicit**. Systematically, for each hazardous function, at least one safety function has to be identified or defined, which prevents the transition from hazard to mishap. The safety functions have to be allocated on the same decomposition level as the corresponding hazardous function and have to be linked to the hazard they address. After this allocation, the temporarily added hazardous functions can be removed. The safety functions in the functional structure can be decomposed and allocated on different levels. For the given example, this step results in the model shown in Figure 4-19. For example, "produce heat" is replaced by the safety function "insulate housing".

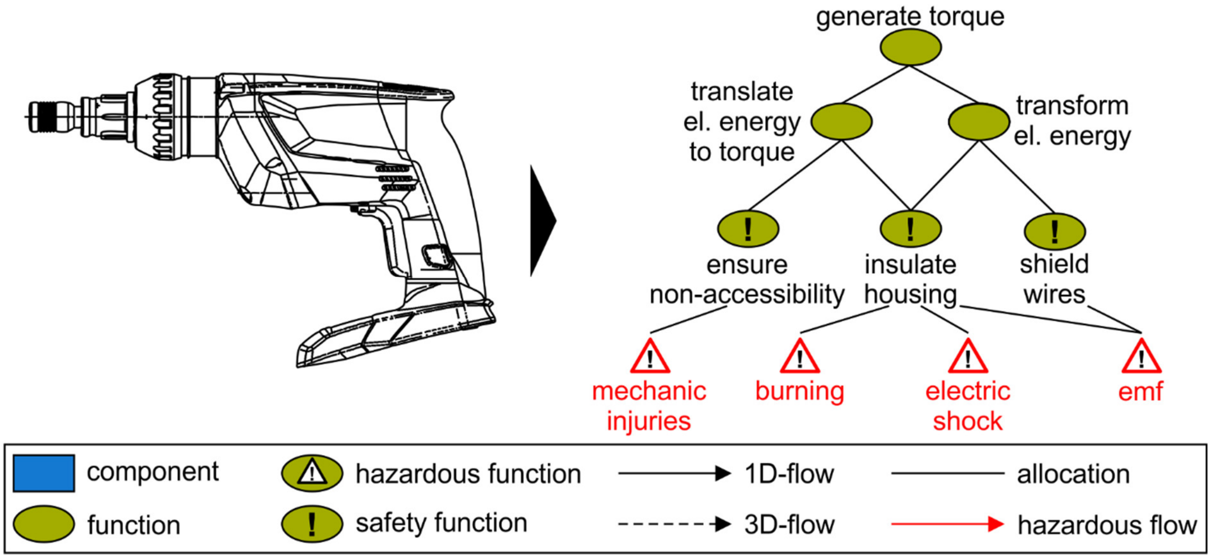


Figure 4-19: Example of the safety functions allocated in the functional structure and their corresponding hazards (source: HILTI AG)

Lastly, this step allocates the defined safety functions to the structural elements (components). Based on the hazards and flows, the safety functions are assigned to one or multiple realizing components. The safety functions can be very generic. For example, to avoid an electric shock, the safety function "isolate current" can be defined. This function can be realized simultaneously by multiple components. Moreover, it is possible that multiple safety functions address one hazard. Concerning the electric shock, for example "prevent contact" is a potential additional safety function.

In **summary**, the method to explicate safety functions provides support to understand the interrelations between safety and design and to increase awareness for safety aspects. It moreover helps to improve the completeness of the product model and the ESMK knowledge framework by integrating safety functions explicitly in the model. The method to explicate safety functions provides a safety-oriented preparation of the product model for analyses and decisions connected to UDC. Safety aspects can be identified directly in the model so that analyses of UDC scenarios can consider safety without involving safety analysts and their implicit knowledge.

Model-Based Hazard Analysis

The model-based hazard analysis supports the identification of hazards and failures within the product model of the knowledge framework. As Figure 4-20 summarizes, it mainly relies on a model of the product architecture and, if available, hazard documents. The model-based hazard analysis is a visual analysis and mainly focuses on graph-based representations. It supports the task of identify hazards and failures by efficiently modeling them in the knowledge framework, with special focus on misuse cases. SysML is a very common visual approach. The model-based hazard analysis was originally developed as a SysML-profile within a student project (Müller, 2015) and published in Müller, Roth, and Lindemann (2016). Nevertheless, it can be directly transferred to the representation of the ESKM knowledge framework and vice versa.

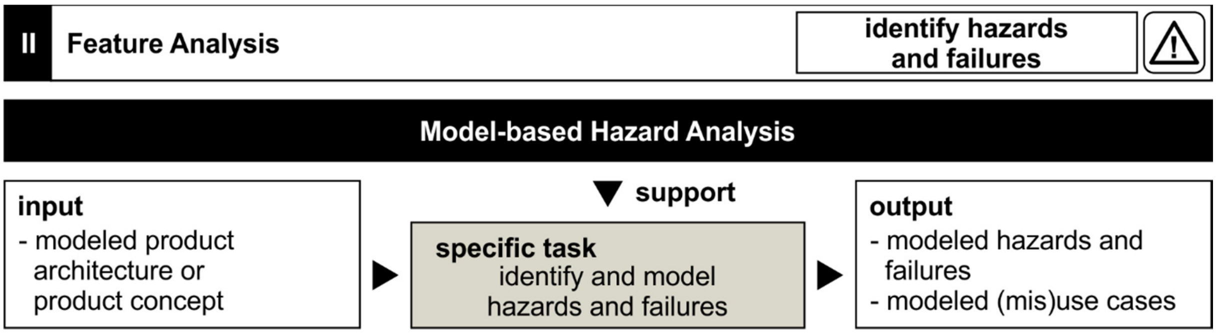

II
Feature Analysis
identify hazards and failures
Model-based Hazard Analysis
input
- modeled product architecture or product concept
▼ support
specific task
identify and model hazards and failures
output
- modeled hazards and failures
- modeled (mis)use cases

Figure 4-20: Overview of the in- and outputs and the supported task of the model-based hazard analysis

The **purpose** of the model-based hazard analysis is to support the process of identifying all possible failures and hazards based on a product model with special focus on use and misuse cases. The **effects** are knowledge about occurring hazards and possible countermeasures modeled in a product model. Moreover, a hazard analysis based on the model is conducted. The model-based hazard analysis can be applied in **situations**, when a detailed hazard analysis needs to be conducted based on a common graph-based product model. Moreover, it is especially suitable in situations when a detailed model is existent or is built and based on this model all possible hazards need to be identified systematically. In addition, it is beneficial, when the interaction of users and possible cases of misuse also need to be considered.

Development of Support

The development of the model-based hazard analysis in its task clarification builds on the systematic literature review on existing methods of hazard and failure analysis, especially in combination with SysML. Moreover, a set of requirements on the approach was derived. Based on this, the literature was analyzed to identify factors, which influence:

- the method selection for hazard analysis,
- the selection of diagram types in SysML, and
- the integration of both aspects in one procedure.

Using these factors and the evaluation of existing solution approaches, the underlying hazard analysis method was selected. For this analysis, a minimal set of diagram types was defined and the model-based hazard analysis was developed. The following paragraphs provide a short overview of the review and the derived requirements.

The **review** identified various approaches to combine safety analysis and SysML. Despite the special focus, most of these approaches are already included in the extensive literature review in Subsection 2.3.3. The following paragraphs only provide a short overview.

A first group of approaches extends the standard SysML through new stereotypes. For example Hause and Thom (2007) define new stereotypes to distinguish between safety requirements and other types of requirements. Biggs et al. (2014) increase traceability and consistency of design and safety information through their profile SafeML. They for example introduce the new stereotypes hazards, harms, and their transition context. Moreover, they also integrate measures to detect and prevent these transitions.

The second group uses SysML models as basis for safety analyses. This includes the approaches of Mhenni et al. (2014), respectively Mhenni et al. (2016), and Xiang et al. (2011), described in Subsection 2.3.3. The third group of approaches propagates the concurrent development of systems from a functional and safety perspective within SysML. The most relevant example is the safety-centric modeling by Jensen and Tumer (2013) also discussed in Subsection 2.3.3.

In summary, all approaches focus on analyses in a specific phase of the development process. An approach, which provides a combined model-based safety or hazard analysis, is missing. This need together with the general requirements of the ESMK (see Subsection 3.4.2) was translated into 42 requirements. Out of these 42 requirements, the following **central requirements** address major aspects:

- identification and modeling of use cases
- model the system architecture (*REQ2* and *REQ4*)
- identification and modeling of hazards and failures with their effects (*REQ2* to *REQ5*)
- ensure traceability between causes and effects for hazards and failures (*REQ3* and *REQ5*)

Based on these requirements and the analysis of the existing approaches, the **minimal set of diagrams** for the approach was defined. This set includes the requirements diagram (REQ), the block definition diagram (BDD), the internal block diagram (IBD), the use case diagram (UC), and the activity diagram (ACT). Instead of using SysML, the major information of these diagrams can be obtained from and modeled in the ESMK knowledge framework as well.

Provided Support (Model-based Hazard Analysis)

The resulting **model-based hazard analysis** combines a system design and safety analysis procedure. It supports the modeling of the system design in the ESMK knowledge framework or with SysML standard elements and conducts the hazard analysis in this model in an integrative manner. Contrary to the ESMK, SysML therefore needs to be extended by eight new elements and six new relationships defined in the Hazard Analysis SysML-profile (see Appendix 9.5). By that, the analysis complies with existing standards like the IEC 60812.

The model-based hazard analysis comprises the three stages indicated in Figure 4-21. They cover the whole design process (left branch of VDI 2206) and are compliant with the first two phases of the ESMK. However, the major focus lies on the hazard analysis and hence, the Feature Analysis. The three stages of the model-based hazard analysis are derived from Weilkiens (2007). The first stage deals with the requirements definition and specification of use cases. Based on this, the second stage establishes the functional architecture, which in the third stage is implemented by components. In the following, each stage is discussed in detail.

The **first stage** of the model-based hazard analysis addresses **requirements and use cases**. The requirements specification as first step determines and analyzes requirements. Support methods like the ESMK's Zwicky box of methods or alternatives indicated in the beginning of Section 4.3.1 can be applied. Safety requirements play a central role and should be indicated explicitly. The model-based hazard analysis in the SysML thus, introduces the stereotype *safety requirement* in addition to standard requirement stereotypes. The traceability during the requirements decomposition is ensured through a *deriveReqt*-relation. The ESMK knowledge framework similarly provides safety requirements-nodes and refines-edges.

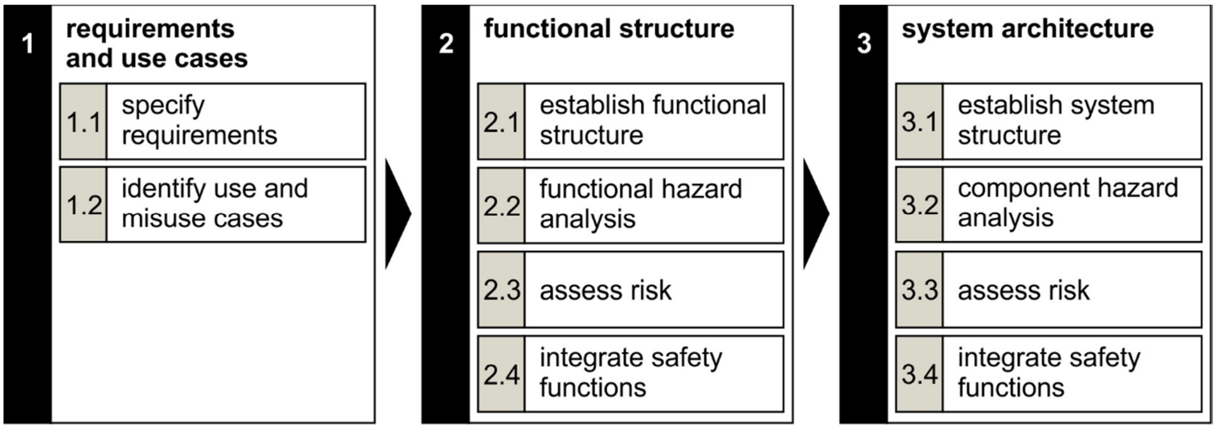

1
requirements and use cases
1.1 specify requirements
1.2 identify use and misuse cases
2
functional structure
2.1 establish functional structure
2.2 functional hazard analysis
2.3 assess risk
2.4 integrate safety functions
3
system architecture
3.1 establish system structure
3.2 component hazard analysis
3.3 assess risk
3.4 integrate safety functions

Figure 4-21: Procedure of a system architecture design with integration of the model-based hazard analysis

To connect requirements and functions, following Weilkiens (2007), use cases can be utilized. They refine functional requirements and relate them to stakeholders like users. To ensure completeness from a safety perspective, additionally misuses need to be considered (Thramboulidis & Scholz, 2016, pp. 5–6). Especially from an UDC perspective, it is necessary to identify all possible uses and misuses, even when the actual design would prevent them. They potentially still can cause failures. Hence, every use case has to be in detail examined for potential misuse and general misuse has to be identified as well. To model those, the SysML-profile provides the stereotype *misuse* and the *derivedMisuse*-relationship. Similarly, the knowledge framework provides the optional node type "use case", which can be attributed as misuse.

As first step of the **second stage development of a functional architecture**, the use cases and requirements are implemented by functions. In SysML, functions are modeled in ACTs. This process-oriented view represents the transformation from in- to output as well as object and control flows. Here, the multi-perspective functional modeling approach of Becerril, Kasperek, Roth, and Lindemann (2014) is suggested to support the systematic decomposition. The ESMK knowledge framework models the flows via effect and impact relations and specific flow nodes instead.

In the second step, a functional hazard analysis is conducted. It is derived from the Functional Hazard Assessment (see MIL-STD-882E) and the functional FMEA. The analysis systematically identifies malfunctions together with their causes and effects. This identification considers every possible failure that may cause malfunctions. Depending on the detail level, generic malfunctions can be derived by negation as explained in the ESMK's multi-hierarchy fault tree generation and evaluation (see Subsection 4.3.3). The SysML-profile models the malfunctions with the stereotype *malfunction* and relates them to their original function via the *derivedFct*-relationship, as shown in Figure 4-22. Following the Functional Hazard Assessment, the causes and effects of malfunctions are subsequently evaluated. The causes as well as possible failure propagation to further malfunctions are modeled through a *cause*-relation. If the malfunction causes a process interruption, it is linked to the end node in the ACT. The ESMK knowledge framework instead, treats malfunctions as failures and models cause and effect relationships between them with propagation edges.

If possible, in the third step, for each malfunction a qualitative assessment of severity and probability of occurrence can be made. This helps to identify safety-critical malfunctions qualitatively. If the knowledge framework is used, this qualitative assessment can be stored in the failure attributes or determined in the subsequent phase of Propagation Analysis. The Hazard Analysis SysML-profile instead, stores this information in annotations of the malfunctions as shown in Figure 4-22

The fourth step of this stage integrates safety functions for each relevant malfunction. The corresponding stereotype *safety function* represents all corrective actions and is related to the malfunction via the *prevent*-relation. The model-based hazard analysis assumes a proper integration so that no additional malfunctions are added to safety functions and the previous steps are not iterated. If the knowledge framework is used, safety functions are modeled as functions with a specific attribute. If the safety functions are already modeled in the framework (e.g. through the method to explicate safety functions described previously in the Feature Analysis phase), this step is limited to their confirmation and the validation of the model. In Figure 4-22, an example for the described procedure on functional level is given. It exemplarily indicates instances of all hazard analysis elements in a standard SysML diagram.

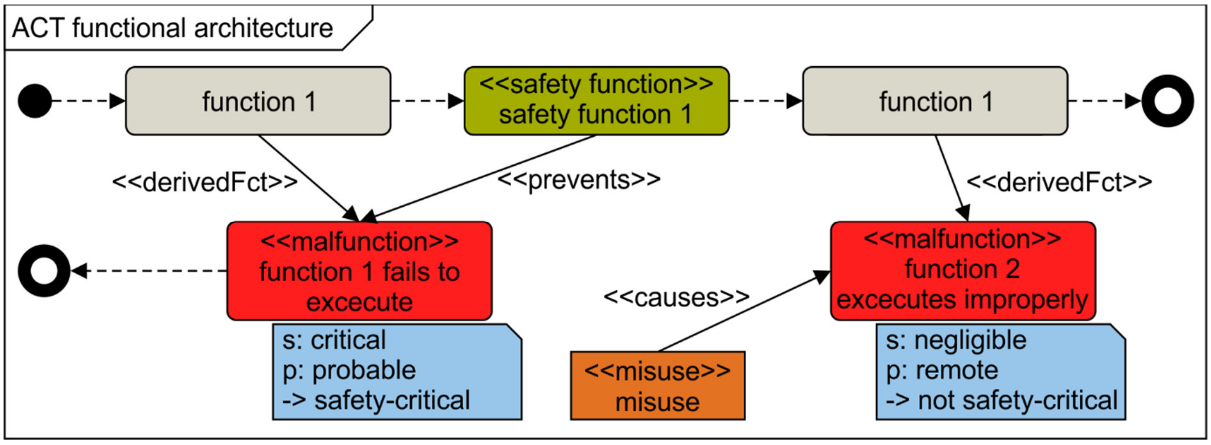


Figure 4-22: Model elements and principle of the model-based hazard analysis on functional level

The **third stage** of the model-based hazard analysis is analogue to the second, but addresses the **structural level**. In a first step, the components implementing the functions (i.e. safety functions) are modeled in BDDs and IBDs. These diagrams allow for a variable level of abstraction. The ESMK knowledge framework follows the same principle.

In the second step, the component hazard analysis is performed in compliance with the Preliminary Hazard Analysis. Alternatively, the method to explicate safety functions, described previously in the Feature Analysis phase, can be used. The resulting information is modeled by the stereotypes *hazard*, *hazard cause,* and *hazard effect,* as shown in Figure 4-23. The *trigger*-relation is used to model the relation from causes to hazards and from hazards to effects. Depending on the level of detail, only a limited range of abstract causes and effects can be modeled. Possible causes (e.g. misuse, component failures, etc.) provide information how to prevent or mitigate the hazards. The severity and number of possible effects helps to classify the elements. Here, the ESMK knowledge framework not directly establishes a connection between components and hazards. Instead, it links both elements via the domain of flows.

The third step, the risk assessment for hazards and the fourth step remain the same as for malfunctions and safety functions in the second stage of the model-based hazard analysis. The SysML-profile models the correspondent safety measures via the stereotype *safety measure* and the *prevent*-relationship. The effect of a safety measure is qualitatively classified by a tagged value (prevention or mitigation), as shown in Figure 4-23. Analogue to safety functions, the model-based hazard analysis assumes that no additional hazards are caused by a safety measure. If the ESKM knowledge framework is used, this step is only necessary for safety functions, which require new components to be realized. Otherwise, the information is already stored through the link between components and their safety functions. Figure 4-23 illustrates the procedure and stereotypes on structural system level. It exemplarily draws a model including all mentioned elements and relations.

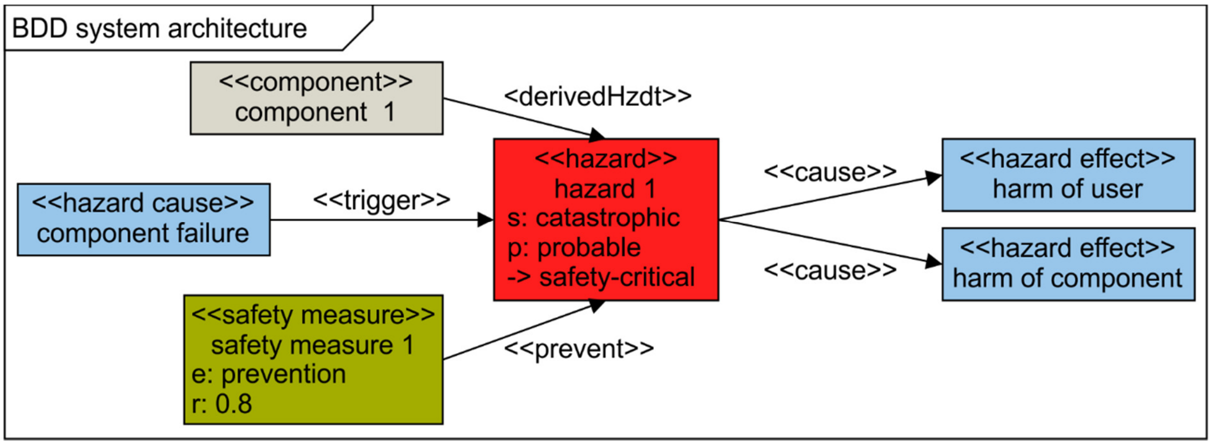


Figure 4-23: Model elements and principle of the model-based hazard analysis on structural level

In **summary**, the model-based hazard analysis provides an environment to concurrently develop a system design and perform a hazard analysis. It integrates both perspectives in a common model, either in SysML or in the ESMK knowledge framework. It mainly contributes to the identification and integration of safety-related information in the model. It puts a special emphasize on misuse cases and applies a worst-case perspective. By that, it prepares design decisions, especially in the context of UDC. Its applicability is not only limited to the second phase of the ESMK. Especially in the second application case (redesign for UDC), the method can be used through all stages of the design process prior to customization to integrate development and safety analysis activities.

Pattern-based Model Verification

The pattern-based model verifications supports to minimize errors in the models of the ESMK knowledge framework. As Figure 4-24 summarizes, it uses the product architecture and safety aspects modeled in the ESMK knowledge framework together with a library of verification principles. Based on these principles, the pattern-based model verification analyzes the model and identifies errors. These errors can be fixed automatically or manually. By that, the method supports the verification of the model. The pattern-based model verification was developed in a student project (Schürmann, 2016).

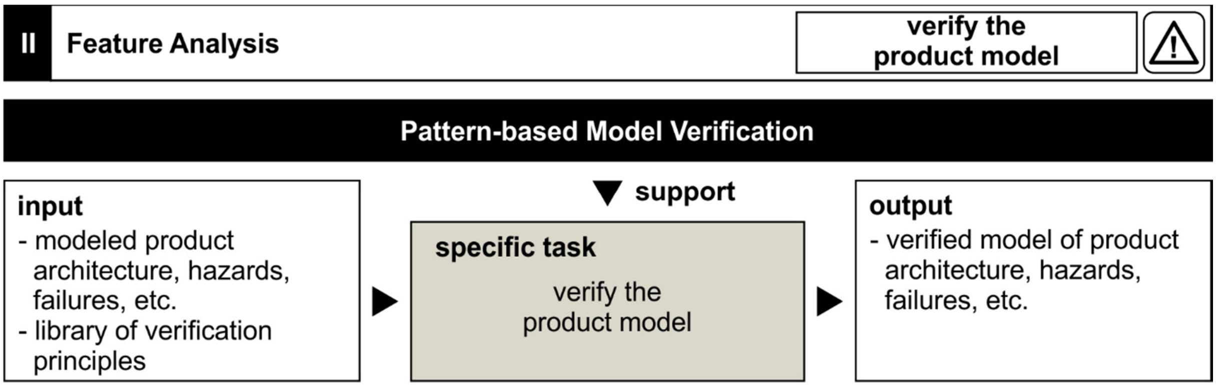

II
Feature Analysis
verify the product model
Pattern-based Model Verification
input
- modeled product architecture, hazards, failures, etc.
- library of verification principles
support
specific task
verify the product model
output
- verified model of product architecture, hazards, failures, etc.

Figure 4-24: Overview of the in- and outputs and the supported task of the pattern-based model verification

The **purpose** of the pattern-based model verification is the identification and elimination of modeling errors in the knowledge framework. Its **effect** is an automated analysis based on a library of defined verification principles. Through this analysis, invalid model patterns are indicated. The pattern-based model verification can be applied in **situations**, when the ESMK knowledge framework stores a large and complex model, which is affected by human errors or uncertainty. In these situations, the resulting complexity is too large to conduct a manual model verification with a similar reliability. In addition, the pattern-based model verification can be applied, when models of different sources are integrated in the knowledge framework or when uncertainties during modeling are high.

Development of Support

The development of the pattern-based model verification builds on the ESMK knowledge framework introduced in Section 4.2 and its graph-based model. To clarify the task, sources of errors or uncertainty during the modeling process were analyzed based on literature. These findings were transferred to the specifics of the knowledge framework to identify possible types of errors. To generate a solution, the basic idea of a pattern-based identification of model errors of Kissel (2014, pp. 107–110) was adapted. Different fields of science were analyzed to identify suitable principles for a verification of the model and define verification patterns. The identified principles were evaluated and selected in two stages. The final selection was assessed on the cost/benefit ratios in a Pareto analysis (Samuelson, 1995). The most promising principles were translated to patterns and supplemented with methods to generate a suitable support. The methods can automatically identify errors in the model and, if possible, automatically fix those.

The modeling process out of different reasons involves a wide variety of **uncertainties or sources of errors**. The literature mainly identifies the following sources:

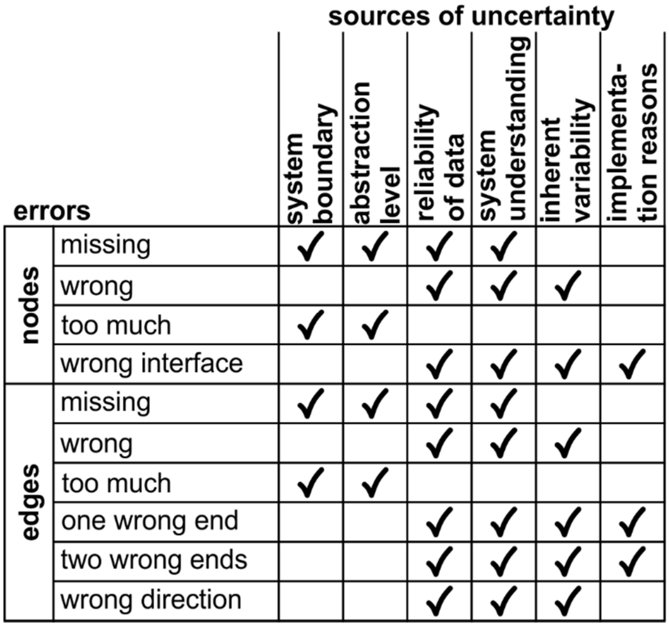
- system boundaries (Kasperek et al., 2013, p. 44; Walker et al., 2003, p. 9)
- level of abstraction (Refsgaard, van der Sluijs, Jeroen P., Brown, & van der Keur, 2006, pp. 1586–1587)
- reliability of data sources (Kasperek et al., 2013, p. 44; Refsgaard et al., 2006, p. 1586; Walker et al., 2003, p. 14)
- system understanding (Kasperek et al., 2013, p. 44; Walker et al., 2003, p. 13)

- natural data variability or inherent variability (Walker et al., 2003, pp. 14–15)
- implementation reasons (Kasperek et al., 2013, p. 44; Walker et al., 2003, p. 13)
- human errors (Swain & Guttmann, 1983, p. 2-7-2-8)
- unknown factors (Walker et al., 2003, p. 15)

To clarify how these general sources of uncertainty imply **modeling errors**, they were mapped to the ESMK knowledge framework. Based on this, generalized model errors within the knowledge framework were defined. Figure 4-25 provides an overview of these model errors and from which sources of uncertainty they might originate. The errors, either for example are missing, wrong, or not required nodes, or not necessary edges and edges with wrong directions. The errors can originate from multiple sources. Wrong data or missing understanding can lead to wrong nodes or edges, while uncertainties concerning the system boundary or abstraction level can lead to missing or not necessary elements. Unknown factors and human errors were not directly considered, as they might be the origin of every possible error. In summary, the requirements on the solution approach were concretized as follows:

- identify automatically (*REQ1*) missing, wrong, or not required nodes, or nodes with wrong interfaces in the knowledge framework
- identify automatically (*REQ1*) missing, wrong, or not required edges, or edges with wrong directions or connections in the knowledge framework
- identify the errors resulting from uncertainties concerning system boundaries, abstraction level, system understanding, data reliability, and variability or implementation reasons

Existing research tackles the aspects uncertainty and resulting errors (e.g. Walker et al. (2003), Refsgaard et al. (2006) and Kasperek et al. (2013)). However, methods to verify a model in this context are not addressed. The other researchers primarily focus on formalized model checking and consistency checks between different models (see the paragraph on alternative methods).



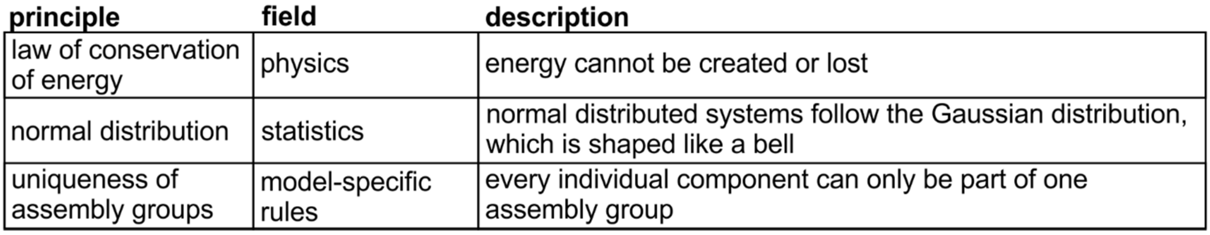
		sources of uncertainty					
errors		system boundary	abstraction level	reliability of data	system understanding	inherent variability	implementa-tion reasons
nodes	missing	✓	✓	✓	✓		
	wrong			✓	✓	✓	
	too much	✓	✓				
	wrong interface			✓	✓	✓	✓
edges	missing	✓	✓	✓	✓		
	wrong			✓	✓	✓	
	too much	✓	✓				
	one wrong end			✓	✓	✓	✓
	two wrong ends			✓	✓	✓	✓
	wrong direction			✓	✓	✓	

Figure 4-25: Types of general model errors in the ESMK knowledge framework and their origins

Hence, the ESMK generated a new solution and **adapts the basic idea of a pattern-based identification of model errors** by Kissel (2014, pp. 107–110). The challenge was to define patterns, which help to identify model errors originating from the above-defined uncertainties. Therefore, the following selected fields of science and their basic literature were analyzed on principles, which help to define errors or invalid patterns:

- physics (Hahn, 2007; Oppen & Melchert, 2005)
- statistics (Fahrmeir, Künstler, Pigeot, & Tutz, 2011; Kreyszig, 1988; Tiemann, 2003)
- heuristics (Michalewicz & Fogel, 2004)
- logics (Barnes & Mack, 1975; Barwise & Keisler, 1977)
- model-specific rules (see Section 4.2 and specific rules of the individual ESMK methods)

Based on these fields and works, a total set of 121 principles was identified and listed in Appendix 0. Thereof, Figure 4-26 provides an overview of three selected principles.



principle	field	description
law of conservation of energy	physics	energy cannot be created or lost
normal distribution	statistics	normal distributed systems follow the Gaussian distribution, which is shaped like a bell
uniqueness of assembly groups	model-specific rules	every individual component can only be part of one assembly group

Figure 4-26: Examples of identified principles from selected fields of science

Provided Support (Pattern-based Model Verification)

The **pattern-based model verification** uses the library of identified principles as starting point for the procedure shown in Figure 4-27. In a first step, the principles are assessed on a scale from one to five. This assessment evaluates their capability to identify the model errors (see Figure 4-25) within the model and their transferability to a pattern-based description.

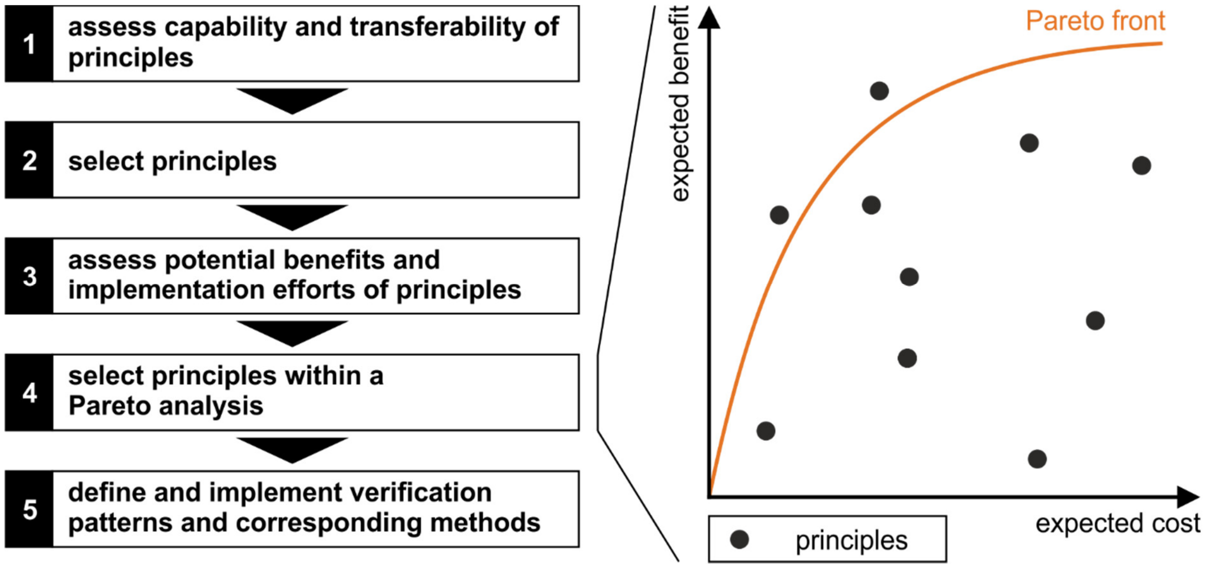
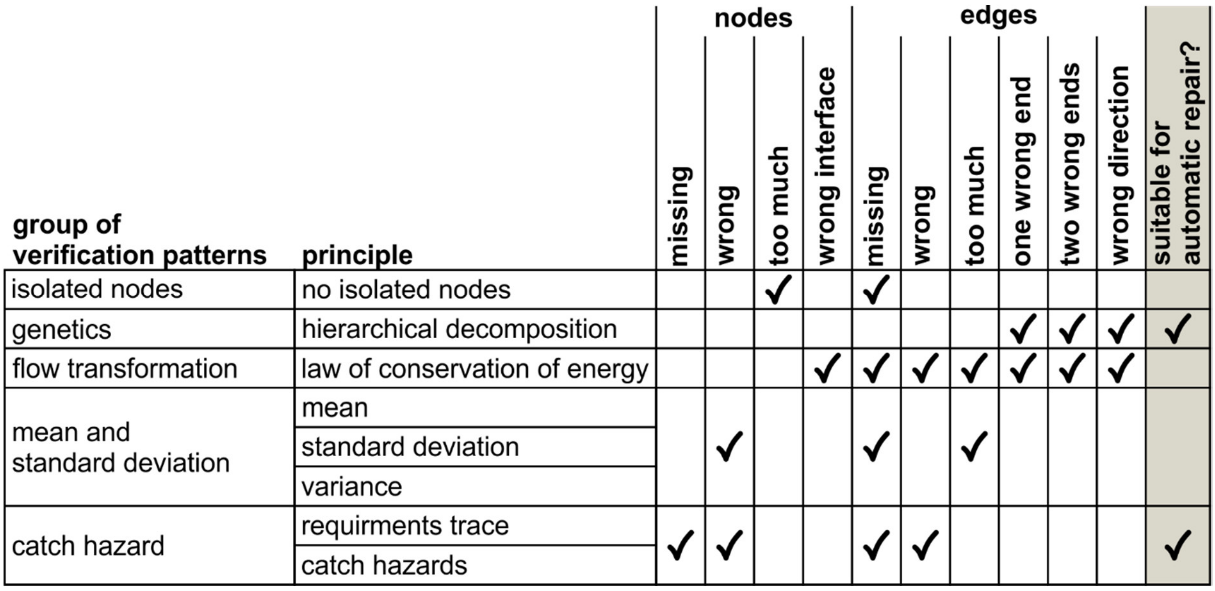

1 assess capability and transferability of principles
2 select principles
3 assess potential benefits and implementation efforts of principles
4 select principles within a Pareto analysis
5 define and implement verification patterns and corresponding methods
expected benefit
Pareto front
expected cost
● principles

Figure 4-27: Procedure of the pattern-based model verification (left) and principle of the Pareto chart (right)

From this assessment, the principles with ratings higher than three are selected for a second assessment. Using the same scale, they are analyzed on the efforts to apply them to graph-based models and on their expected benefit. A Pareto analysis based on these dimensions, leads to the selection of the principles with the best cost/benefit ratio. In the last step, the corresponding valid or invalid patterns for those principles are defined. Moreover, the methods to verify the model according to these principles are implemented.

Based on the library of principles and the two-stage selection including the Pareto-chart, the ESMK suggests applying the principles listed in Figure 4-28 for an automated pattern-based model validation of the ESMK knowledge framework. The following paragraphs describe the application of the pattern-based model verification using these principles.



		nodes				edges						
group of verification patterns	principle	missing	wrong	too much	wrong interface	missing	wrong	too much	one wrong end	two wrong ends	wrong direction	suitable for automatic repair?
isolated nodes	no isolated nodes			✓		✓						
genetics	hierarchical decomposition								✓	✓	✓	✓
flow transformation	law of conservation of energy				✓	✓	✓	✓	✓	✓	✓	
mean and standard deviation	mean		✓			✓		✓				
	standard deviation											
	variance											
catch hazard	requirments trace	✓	✓			✓	✓					✓
	catch hazards											

Figure 4-28: Groups of verification patterns for the ESMK and their link to model errors

Moreover, Figure 4-28 describes, which types of errors these principles address. It also evaluates, if the principle can potentially be used for an automated repair of the error. The figure additionally assigns the principles to five groups. These groups define clusters of similar principles, which can be transferred to and implemented in integrated methods. These **five groups of verification patterns** identify invalid patterns and support the verification of the model in the ESMK knowledge framework. They are explained in the following:

- The verification pattern *"isolated nodes"* identifies nodes without any edges. Hence, it identifies not required nodes or missing edges.
- The verification pattern group *"genetics"* identifies errors in the hierarchical decomposition and connected inheritance errors. It identifies missing or wrong edges. Using the node attributes, invalid hierarchical patterns can be defined. For the connection of multiple domains, patterns for inheritance are defined. As shown in Figure 4-29, the ESMK distinguishes between heredity-based and level-based inheritance patterns.
- The *"flow transformation"* verification patterns aim to identify errors in the flow-based component or functional structure. They identify missing or wrong edges and wrong

interfaces. The ESMK defines valid and invalid flow transformation patterns. They mainly are based on the principle of conservation of energy and material. Figure 4-29 provides some examples of these invalid flow transformation patterns.

- The *"mean and standard deviation"* verification patterns aim to identify wrong or not required edges as well as wrong nodes. They identify nodes, whose edges significantly deviate from the average of the model. This not directly identifies model errors but identifies conspicuous elements, which might be potential errors. However, for specific nodes a deviation from the average might be valid.
- The *"catch hazard"* verification patterns are the model-specific group. They aim to identify hazards, which in the in the knowledge framework are not prevented by safety functions or are not properly connected to flows and safety requirements. The checked patterns are illustrated in Figure 4-29. This group specifically supports the ESMK's As-Is Analysis and Feature Analysis. It mainly identifies missing or wrong nodes and edges.

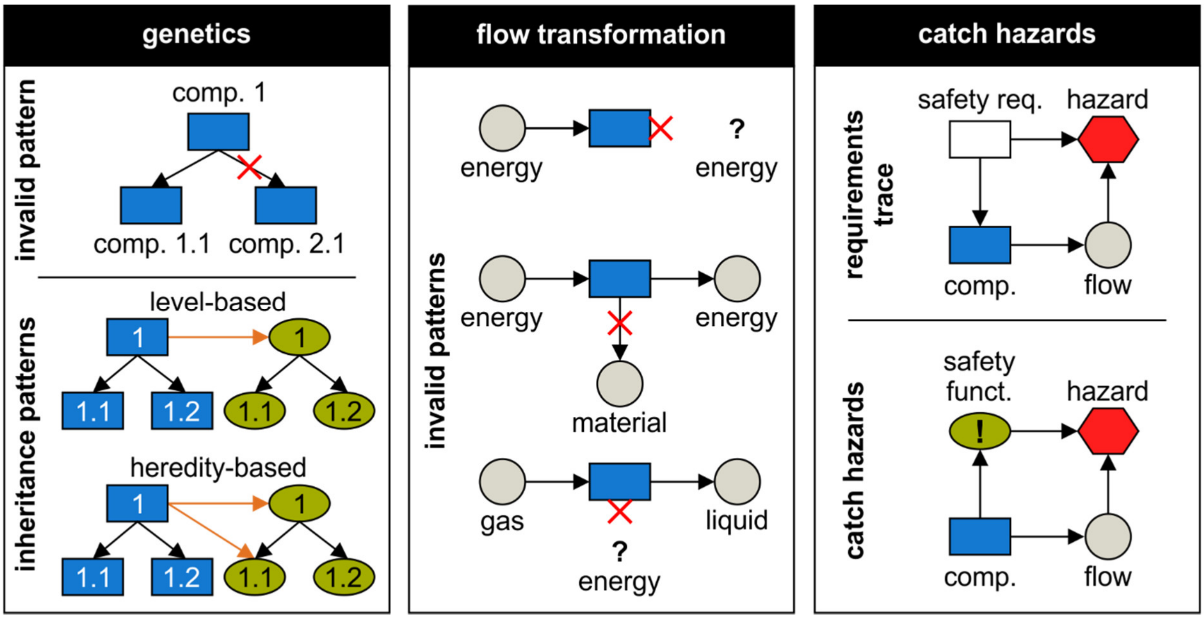


Figure 4-29: Exemplary overview of verification patterns

The **verification patterns** described above are specifically tailored to the ESMK knowledge framework. Using these patterns, graph-rewriting tools can be applied to automate the pattern search. In a specific situation, it might be necessary to adapt or concretize these patterns. In general, the library of principles and the pattern-based verification can be used for other situations and models as well. Then, the steps of selection, Pareto analysis, and definition of patterns need to be specifically adapted to the situation.

In **summary**, the pattern-based model verification provides automated support for the verification of typed attributed graph models. By defining patterns based on general science principles and based on model-specific rules, the method makes modeling knowledge explicit and consolidates different views on the model. Moreover, it can support the identification of human errors. It reduces manual verification efforts and improves the quality of the model. This in turn improves the effectiveness and quality of subsequent analyses.

4.3.3 Phase III: Propagation Analysis

This section describes the **third phase of the ESMK** including its supported specific tasks and support methods. The Propagation Analysis mainly aims to evaluate the potential safety impact of UDC options, to balance the UDC demand with safety restrictions, and to improve the product architecture. It represents the core contribution of the ESMK. The following paragraphs e provide an overview of the tasks and contributions. In detail, the model-based hazard and propagation assessment, the multi-hierarchy fault tree generation and evaluation, the preliminary model-based FMEA, and the UDC safety-relevance portfolio are introduced. Moreover, the safety-oriented Modular Function Deployment, which specifically aims at application case II (redesign for UDC) is described.

Overview on Tasks and Contribution Focus of the Propagation Analysis

The **Propagation Analysis** in general aims to identify customizable elements and prepare the safety analysis based on the product model within the ESMK knowledge framework. This phase one hand analyzes the product components on their possible change propagations. This supports the assessment of the suitability of components for UDC. The Propagation Analysis thus, contributes to the balancing of safety aspects and offered degrees of freedom (*REQ3*). On the other hand, this phase uses the knowledge of the product architecture and propagations to conduct preliminary safety analyses (FTA and FMEA) and to improve their efficiency (*REQ1*). Moreover, the safety analyses are integrated into the knowledge framework of the ESMK (*REQ4*). In addition, exclusively addressing the second application case (redesign for UDC), the knowledge on propagations and the assessment of elements is used to derive modular architectures optimized from a safety perspective (*REQ2*). The relevant in- and outputs of this phase can be summarized as shown in Figure 4-30.

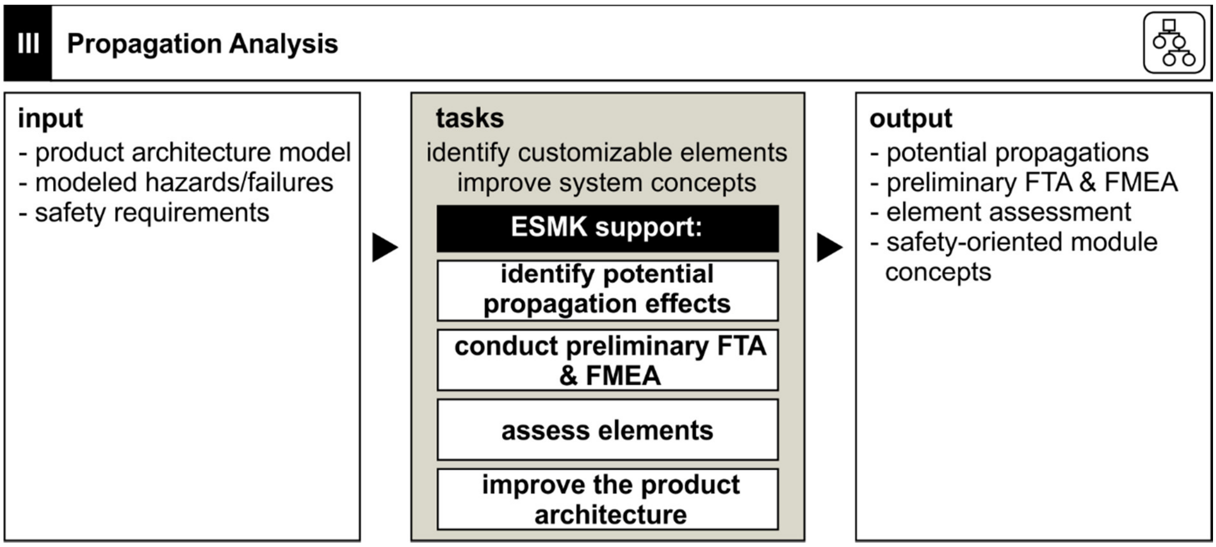

III
Propagation Analysis
input
- product architecture model
- modeled hazards/failures
- safety requirements
tasks
identify customizable elements
improve system concepts
ESMK support:
identify potential propagation effects
conduct preliminary FTA & FMEA
assess elements
improve the product architecture
output
- potential propagations
- preliminary FTA & FMEA
- element assessment
- safety-oriented module concepts

Figure 4-30: Overview of the in- and outputs and supported specific tasks of phase III (Propagation Analysis)

Broken down to **specific tasks**, the phase of Propagation Analysis according to Figure 4-30 comprises the following five tasks:

- identify propagation effects

- conduct preliminary FTA
- conduct preliminary FMEA
- assess of system elements (safety-relevance)
- improve the product architecture

As described in Subsection 3.4.1, the user-induced changes challenge methods of ECM and the safety of a product. Possible propagations of these changes need to be identified efficiently. In addition, the expert judgement to identify change propagations within existing ECM methods (see Subsection 2.2.3) might reach its limits, when due to UDC all possible changes and their propagations need to be examined. Yet, to fulfill *REQ2*, *REQ3*, and *REQ4*, a link to safety-relevant aspects (i.e. existing hazards) needs to be established. To solve these challenges and support the identification of propagation effects, the ESMK provides the **model-based propagation and hazard assessment**.

The knowledge on propagations and hazards can be used as input to safety analyses (i.e. FTA and FMEA). They help to identify critical states and changes with respect to product safety and are a mandatory part of the development (see Subsection 2.3.2). However, as stated in Subsection 2.3.4, the manual efforts for safety analysis need to be reduced in order to realize UDC products. The ESMK provides partially automated methods to conduct a preliminary FTA and FMEA from a worst-case perspective. First, the method for the automated **multi-hierarchy fault tree generation and evaluation** supports the improvement of the efficiency of the FTA and helps to identify critical elements. Second, the **preliminary model-based FMEA** automatically prepares the FMEA-form for the individual analysis and helps to identify necessary restrictions, which are needed to balance product safety and UDC options (*REQ3*).

However, the UDC options do not only have to be balanced with safety efforts (*REQ3*). Many other restrictions and influences are involved in this decision (see Section 1.1). Amongst those, the actual UDC demand of the customers plays an important role. To allow decisions, which incorporate all perspectives, the product elements have to be assessed. To support this from a safety perspective, the ESMK consolidates all information from the knowledge framework to assess the safety-relevance of all components. It visualizes this assessment within the **UDC safety-relevance portfolio** as input for the decision-making.

Moreover, as described above, the ESMK supports the improvement of the product architecture from a safety perspective. As existing modularization methods (see Section 3.1) do not involve an explicit consideration of safety aspects, the ESMK provides the **safety-oriented Modular Function Deployment**. It supports the preparation of safety-oriented architectures (*REQ2*) and helps to integrate this perspective in modularization decisions (*REQ4*).

In summary, the Propagation Analysis of the ESMK provides support to identify change propagations, conduct FTAs and FMEAs, assess the safety-relevance and improve product architectures. The ESMK's support methods aim at a specific purposes and situations. In other situations, **alternative methods** might be better suitable for the given tasks. The following paragraph provides selected examples.

For example, the propagation effects can be assessed using the Change Prediction Method by Clarkson et al. (2004). Another option would be the adaption of the software change impact analysis (Bohner & Arnold, 1996). Moreover, the methodology of Mhenni et al. (2016) might be suitable to develop a safety-oriented system concept based on SysML and automatically derive FTAs and FMEAs. Alternatively, for example a generation of fault trees based on Simulink models (see Papadopoulos and Maruhn (2001)) might be suitable. To ensure the completeness and improve the efficiency of the FMEA, the approach of Maurer and Kesper (2011) may be beneficial as well. The same applies for many other specific methods introduced in Subsection 2.3.3. Furthermore, to improve the product architecture depending on the influences it might be suitable to follow the design for adaptability methodology introduced in Section 3.1 with special focus on safety aspects.

Model-based Hazard and Propagation Assessment (MBHPA)

The model-based hazard and propagation assessment (MBHPA) supports the task of identifying potential propagation effects in order to identify elements (i.e. components), which can be offered for UDC. As Figure 4-31 summarizes, it relies on the modeled product architecture including hazards and safety-relevant aspects stored in the knowledge framework. It derives possible propagations, which are integrated in the ESMK knowledge framework. The model-based hazard and propagation assessment roughly is based on a student project (Gantenbein, 2016) and is partially published in Roth and Gantenbein (2016).

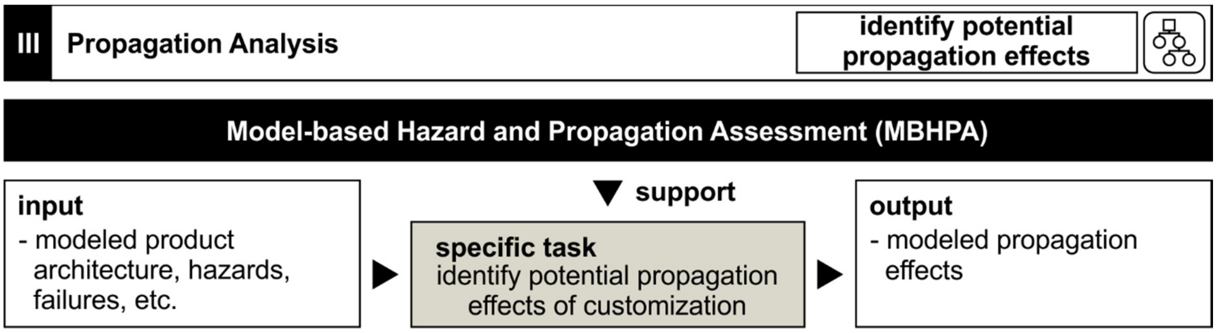

III
Propagation Analysis
identify potential propagation effects
Model-based Hazard and Propagation Assessment (MBHPA)
input
- modeled product architecture, hazards, failures, etc.
support
specific task
identify potential propagation effects of customization
output
- modeled propagation effects

Figure 4-31: Overview of the in- and outputs and the supported task of the model-based hazard and propagation assessment

The **purpose** of the model-based hazard and propagation assessment is the support of the efficient identification of potential propagation effects of user-induced changes. Its **effect** is a systematic procedure to identify propagation effects within a product model and the knowledge of potential propagations including their connection to hazards. The model-based hazard and propagation assessment can be applied in **situations**, when propagations have to be considered from a worst-case perspective and when expert knowledge concerning those is limited. Especially considering the increasing complexity of mechatronic systems, the reliance on expert knowledge and experience becomes critical (Sierla et al., 2012, p. 138). Moreover, the method can be applied, when the potential impact of individual changes needs to be evaluated on a general level.

Development of Support

The development of the model-based hazard and propagation assessment is based on the ESMK knowledge framework (see Section 4.2) and its graph-based representation of the product and relevant knowledge. To clarify the task, the development was built on the literature review on ECM methods and their consideration of change propagations given in Subsection 2.2.3. Moreover, works addressing failure propagation like the Functional Failure Identification and Propagation Framework (see Subsection 2.3.3) were included in the analysis. The major findings align with the challenges at the interfaces highlighted in Subsection 3.4.1: Existing methods mainly rely on experience and ingenuity to identify propagation paths (Sierla et al., 2012, p. 138), which contradicts the trend of UDC and resulting demands for efficiency.

These findings were consolidated and condensed together with general requirements derived from the objective of this thesis (see Section 3.4.2). This resulted in the **formulation of the following requirements** on a method to assess the potential hazard impact of product changes and their propagations within the knowledge framework:

- provide an identification of change propagations (*REQ4*)
- provide an identification and analysis of possibly affected hazards due to changes (*REQ3* and *REQ4*)
- provide a clear and understandable visualization (*REQ5*)
- provide an increased efficiency (time, experience, and resources) of propagation and hazard analyses (*REQ1*)
- increase the awareness for changes' impacts on safety (*REQ2* to *REQ4*)
- facilitate the safety-oriented preparation of user-induced changes (*REQ2* and *REQ3*)
- improve the transparency and documentation of the conducted analyses (*REQ5*)

Based on these requirements, in an **iterative generation of solutions** the model-based hazard and propagation assessment was developed. First, existing approaches identified in the literature review were evaluated on their fulfillment of the defined requirements. This was conducted within a simple score assessment (Ehrlenspiel, 2009, p. 515) on a scale from one to three. By that, the most suitable approaches were identified. As the approaches are not able to meet all requirements, they were adapted and combined to develop the model-based hazard and propagation assessment.

For each step of the model-based hazard and propagation assessment procedure, the most suitable existing approaches were analyzed in detail and adapted according to the requirements. If existing approaches were not sufficient, new approaches were developed. Throughout all these activities, the compatibility and integration of all steps was maintained through the ESMK knowledge framework. This resulted in the method described in the following.

Provided Support (Model-based Hazard and Propagation Assessment)

The **model-based hazard and propagation assessment**, as shown in Figure 4-32, comprises two interconnected analysis workflows. Prerequisite for the application of both workflows is a graph-based product model comparable to the ESMK knowledge framework (see Section 4.2), which comprises the domains of components, flows, functions, and hazards, as well as their interconnections. For both workflows, Figure 4-32 indicates the procedure including analysis and visualization.

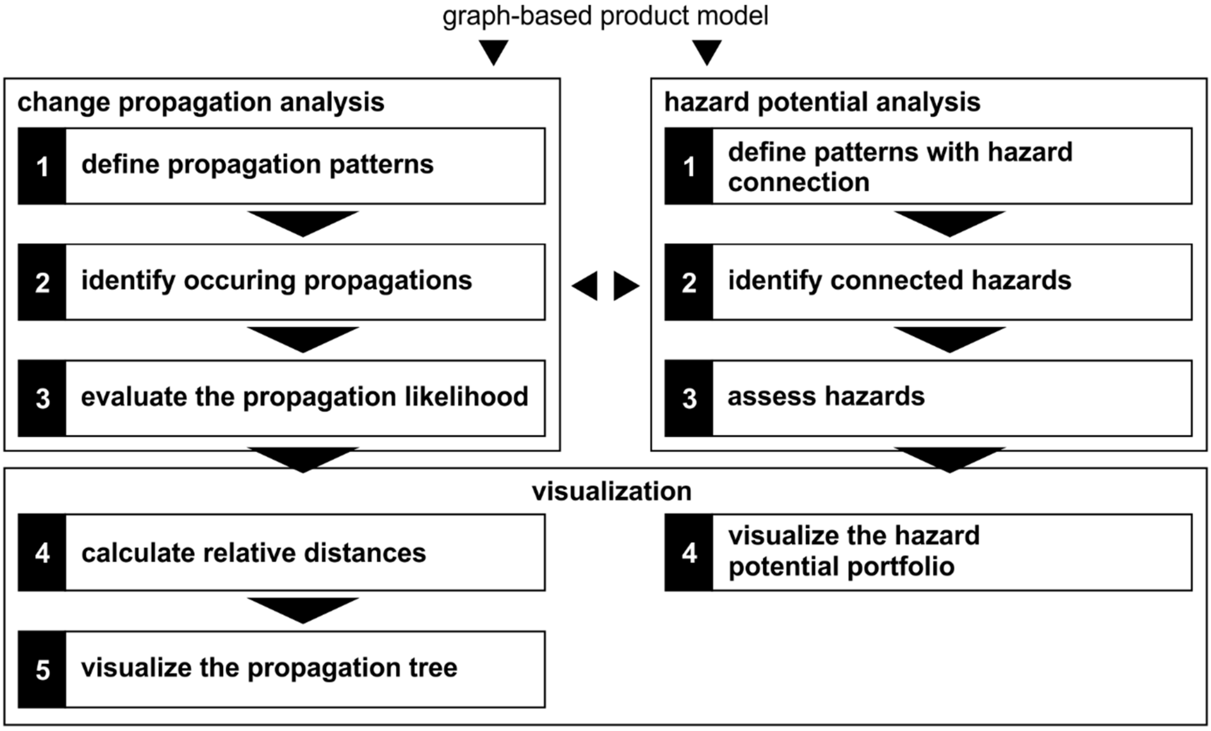

graph-based product model
change propagation analysis
1 define propagation patterns
2 identify occuring propagations
3 evaluate the propagation likelihood
hazard potential analysis
1 define patterns with hazard connection
2 identify connected hazards
3 assess hazards
visualization
4 calculate relative distances
5 visualize the propagation tree
4 visualize the hazard potential portfolio

Figure 4-32: Procedure and steps of the model-based hazard and propagation assessment workflows

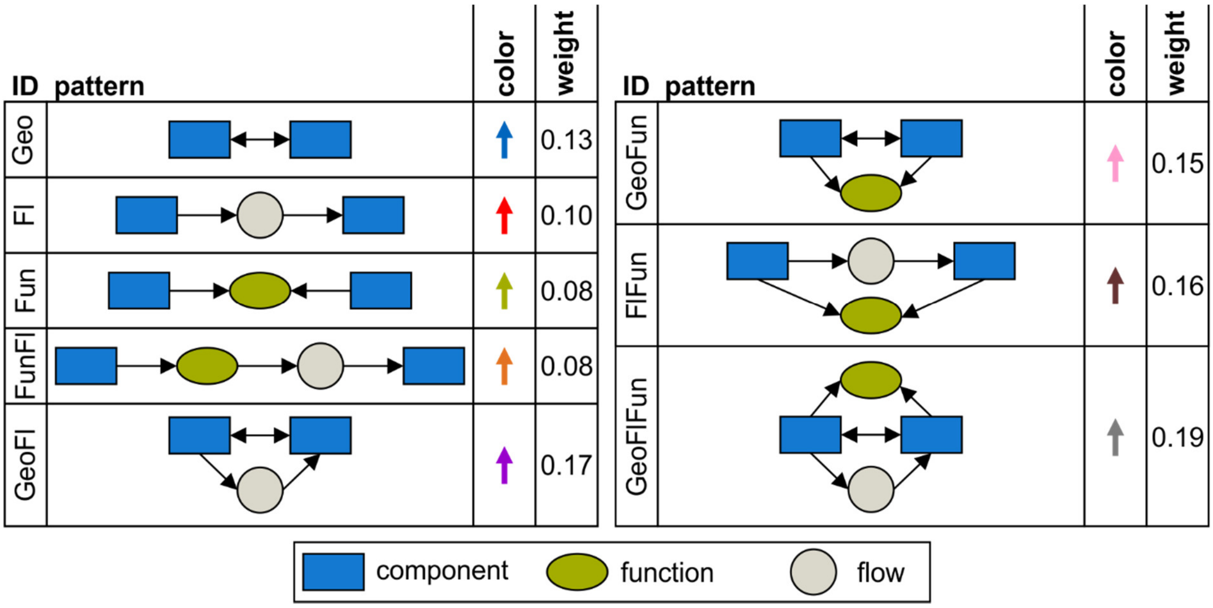
The **change propagation analysis** identifies all components, which are effected by the considered change. These effects are visualized in a propagation tree, which includes the potential likelihood of the propagation and is enriched with further information. In parallel, the **hazard potential analysis** provides an estimation of the hazard potential of a component. It includes the hazard's severity and an estimation of its occurrence. This information is visualized in a hazard potential portfolio, which provides a detailed analysis for individual components identified in the propagation tree.

The basic goal of the change propagation analysis workflow is the identification of all affected components. Starting from a defined initiator component, all possible propagations are extracted from the product architecture. As highlighted above, existing methods for this task mostly rely on experience, which represents a major limitation.

The model-based hazard and propagation assessment resolves this limitation by applying graph-rewriting (Heckel, 2006, p. 188). Similar to the verification patterns defined in Subsection 4.3.2, the method defines graph grammars (Helms, 2013, pp. 55–56), which **describe patterns of change propagation**. Based on these grammars, graph-rewriting algorithms identify and insert propagation paths in the model. Thus, the usually experience- and ingenuity-based knowledge on which propagations might occur in the specific product is translated to rules. These rules define patterns in the model, which will result in a propagation relationship.

The model-based hazard and propagation assessment initially derives the **eight generic patterns** depicted in Figure 4-33. They are based on the ESMK knowledge framework and existing research on change propagations. The generic patterns primarily include four elementary patterns. For example, the knowledge formalized in the pattern “Fl” can be formulated as follows: “If a component (*C1*) has a flow as output, which in turn is input to another component (*C2*), a change to *C1* can propagate to *C2*.” This interpretation can be applied to the other generic patterns of Figure 4-33 accordingly. The elementary patterns can be combined to further patterns. They do not add additional propagation effects to the ruleset, but allow differentiating the likelihood or propagations, if necessary.

The patterns in Figure 4-33 are defined on a generic level. Using the attributes of the typed attributed graph within the knowledge framework, they can be adapted according to the analysis objective and the considered product. By that, the analysis can be transferred from a very generic to a specific and concrete level. For example, the types of flows can be distinguished when patterns and their likelihood are defined. Nevertheless, when preparing products for UDC, all potential propagations need to be considered, so that these generic patterns provide a valid representation of a worst-case perspective.



ID	pattern	color	weight
Geo		↑	0.13
Fl		↑	0.10
Fun		↑	0.08
FunFl		↑	0.08
GeoFl		↑	0.17
GeoFun		↑	0.15
FlFun		↑	0.16
GeoFlFun		↑	0.19

Figure 4-33: Overview of the generic propagation patterns of the model-based hazard and propagation assessment

Figure 4-33 moreover indicates weights of the patterns, which represent the **relative likelihood of the propagation** to occur. Especially on a generic level, it is difficult to define these values. The model-based hazard and propagation assessment suggests to either rely on direct estimations through the experts who define the rules, or to derive values from a pairwise comparison (Ehrlenspiel, 2009, p. 514). The resulting scores for each pattern can then be transferred to a percentage value. For the generic patterns, Figure 4-34 proposes a general evaluation. However, values defined through such a comparison should in the application be challenged and, if necessary, be adapted in respect of the considered product and the objective of the analysis. Furthermore, instead of a likelihood estimation, also other propagation qualities like intensity or adaption efforts can be used.

The product architecture model can be **transformed to a propagation graph** through graph-rewriting using the defined patterns and their likelihood. This transformation is visualized in Figure 4-35. It identifies all components, which are potentially affected by a propagation.

ID	Geo	FI	Fun	FunFI	GeoFI	GeoFun	FIFun	GeoFIFun	**likelihood**
Geo		+	+	+	-	-	o	-	**13%**
FI			+	+	-	-	-	-	**10%**
Fun				+	-	-	-	-	**8%**
FunFI					-	-	-	-	**6%**
GeoFI						+	+	-	**17%**
GeoFun							+	-	**15%**
FIFun								-	**13%**
GeoFIFun									**19%**

- row is less likely than column
o row and column are same likely
+ row is more likely than column

Figure 4-34: Pairwise comparison of the generic propagation patterns' likelihood

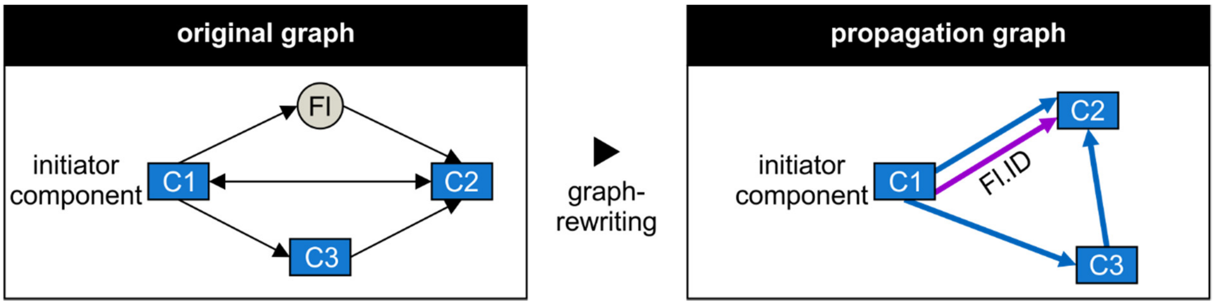


Figure 4-35: Graph-rewriting applied to a product model and the resulting propagation graph

The propagation graph does not allow for an efficient analysis and easy understanding. Thus, the defined likelihood values are used to structure the graph. The likelihood determines the **distance between the initiating and the affected components** in the visualization. The calculation of these distances uses the following two conventions:

- If two components are connected via multiple patterns, only the pattern with the highest likelihood is considered for the evaluation of the distance.
- If a component is affected by more than one component, the minimal distance to the initiator is calculated from a worst-case perspective; the overall minimal distance is used.

The geometrical distance $d_{geo,y}$ between any component y and the initiator component x_0 is calculated based on the geometrical distance of the components, affecting y ($d_{geo,xi}$) and the weight of the corresponding worst-case propagation effect k_{xi} as follows:

$$d_{geo,y} = \min\left(d_{geo,x_i} + \frac{d_{geo,ref}}{k_{x_i}}\right)$$

Whereas x_i are all affecting components of component y. Moreover, a reference distance $d_{geo,ref}$ can be used to scale the visualization. In addition, the color codes introduced in Figure 4-33 improve clarity and allow the tracing of the propagation's origin. The rewritten propagation edges are colored according to their worst-case pattern. Moreover, information on the origin can be stored as attributes of the propagation edges. This visualization supports the prioritizing and structuring of subsequent analyses and activities.

The resulting visualization of the change propagation analysis is a **propagation tree** according to the principle shown in Figure 4-36. In compliance with the distance conventions above, it only displays the worst-case edges (highest weight) between two components. Otherwise, combined patterns would result in multiple edges, which increases the complexity of the visualizations but does not add any value. Moreover, if the same type of pattern occurs between two components multiple times, only one edge is created. It in turn represents the number of patterns in its line width and stores the origins of all contributing patterns in its properties.

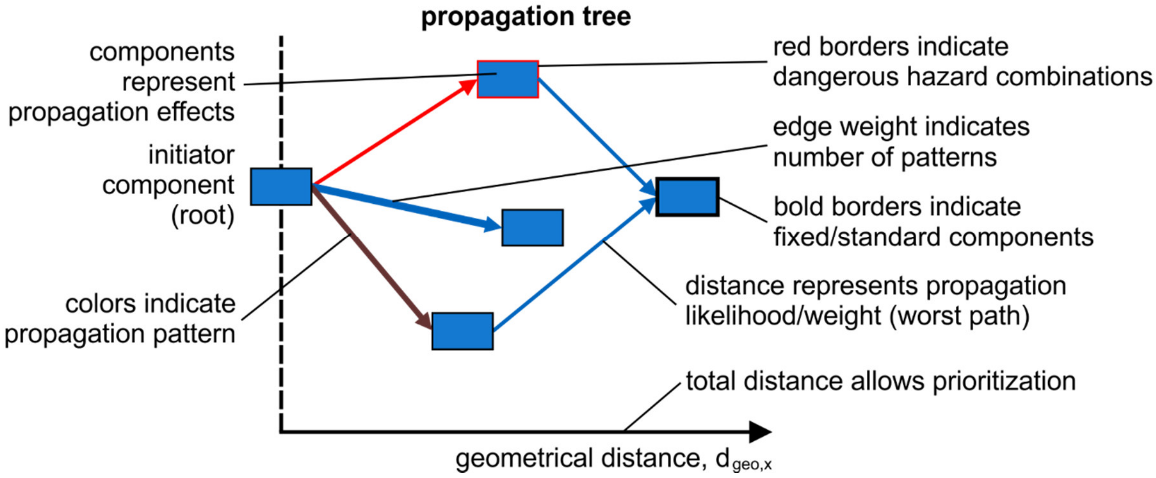

propagation tree
components represent propagation effects
initiator component (root)
colors indicate propagation pattern
red borders indicate dangerous hazard combinations
edge weight indicates number of patterns
bold borders indicate fixed/standard components
distance represents propagation likelihood/weight (worst path)
total distance allows prioritization
geometrical distance, $d_{geo,x}$

Figure 4-36: The principles of the propagation tree as visualization of the change propagation analysis

The propagation tree is enriched with information not directly connected to the change propagation. Changes to standard components or their environment conditions contradict existing efficiency strategies (see Section 3.3.2) and might lead to critical changes and additional costs. The propagation tree highlights these components, which are identified by a respective attribute through a thicker black border. Additionally, they are considered as dead ends in the analysis, which do not have further propagations, as changes to these components have to be avoided. Finally, based on the results of the hazard potential analysis, components bearing a dangerous combination of hazards are highlighted with a red border.

Once, the potential propagations are identified, the second workflow, the model-based hazard and propagation assessment's **hazard potential analysis** in detail identifies potentially affected hazards for each involved component. The first step of the workflow starts with the identification of propagations. Again, graph grammars and rules are applied. In this workflow, the specific knowledge on how a hazard might be affected by a component is translated to patterns.

Same as for change propagations, the model-based hazard and propagation assessment defines the three generic patterns indicated in Figure 4-37 based on existing research and the ESMK's knowledge framework. These generic patterns establish the connection between components and hazards via the domain of flows. For example if a component produces a flow (e.g. heat) as output and this flows bears a hazard (e.g. burning), a change to the component can affect the risk of the hazard. Additionally, a link via safety functions is established, which aim to prevent a hazard's transition to mishap. Again, depending on the specific product and objective of the analysis, the patterns can be concretized by using the element's attributes.

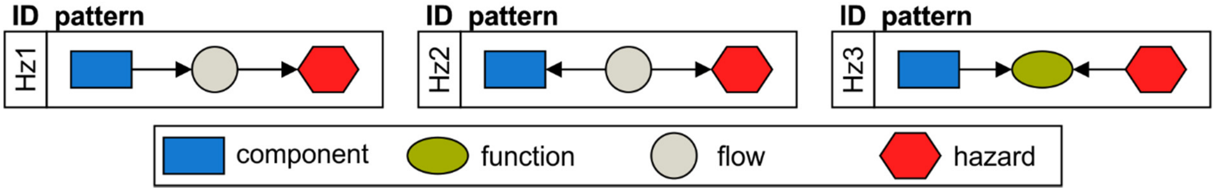


Figure 4-37: Overview of the generic hazard affection patterns of the model-based hazard and propagation assessment

Based on the defined patterns again graph-rewriting is applied. To transfer the information on connected hazards to an understandable and easy-to-evaluate format, the model-based hazard and propagation assessment creates a **hazard potential portfolio** for the analyzed component. As shown in Figure 4-38, it classifies the connected hazards according to their severity and likelihood.

The hazard potential portfolio draws the hazard's severity on the x-axis. It is evaluated through experts and in accordance with the FMEA (see Section 2.3.2), the assessment uses a scale from one (least) to ten (most). For example, a lethal hazard is rated ten, while a hazard causing minor injuries will be assigned to three or four. This information is stored as an attribute of the hazards in the ESMK knowledge framework.

On the y-axis, the hazard potential portfolio draws the likelihood of the hazards. It is derived from the rewritten graph and represents the total number of hazards connected to the considered component through the defined patterns. It represents an absolute value and allows the prioritization of further analyses.

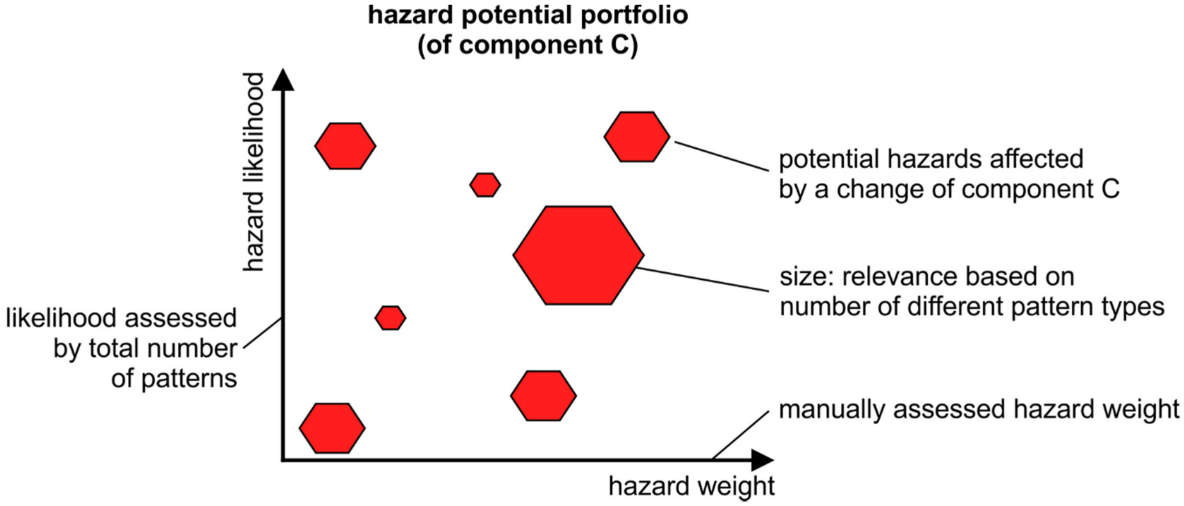

hazard potential portfolio
(of component C)
hazard likelihood
potential hazards affected
by a change of component C
size: relevance based on
number of different pattern types
likelihood assessed
by total number
of patterns
manually assessed hazard weight
hazard weight

Figure 4-38: The principles of hazard potential portfolio as visualization of the hazard analysis

The size of the hazards in the model-based hazard and propagation assessment's hazard portfolio can be used to represent the hazard's relevance for the specific component. The model-based hazard and propagation assessment suggests to determine the relevance on a scale from one (very low) to ten (very high) based on a decision tree (Maimon & Rokach, 2010, pp. 165–167) and the rewritten graph. The decision tree considers the number and diversity of identified propagation patterns. For the generic patterns defined above, Figure 4-39 proposes a simple classification scheme. It distinguishes, if the hazards are connected to the considered component through incoming or outgoing patterns and, if multiple pattern types are involved. Analogue to the patterns, this classification needs to be adapted to the specific situation, product, and objectives of the analysis.

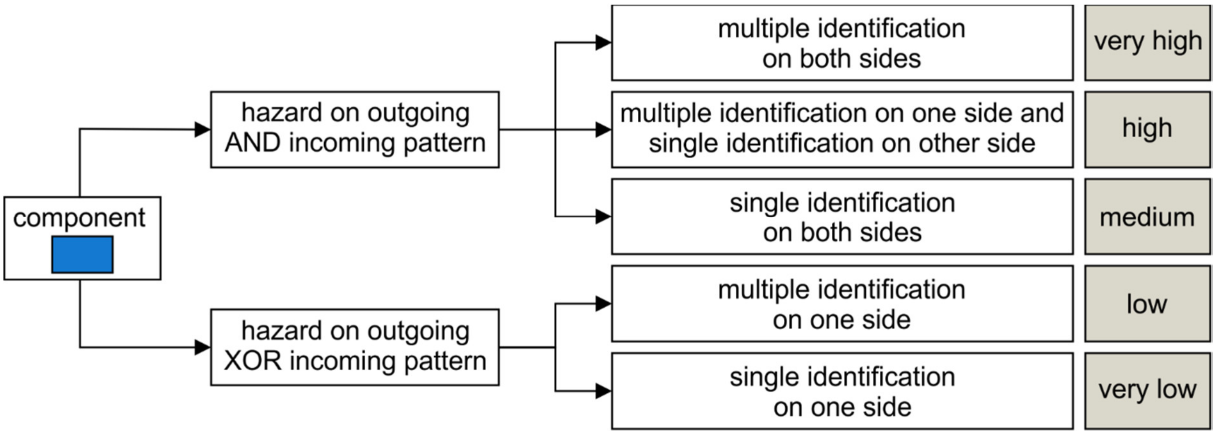

component
hazard on outgoing AND incoming pattern
hazard on outgoing XOR incoming pattern
multiple identification on both sides
multiple identification on one side and single identification on other side
single identification on both sides
multiple identification on one side
single identification on one side
very high
high
medium
low
very low

Figure 4-39: Exemplary decision tree for the evaluation of the hazard relevance in the hazard potential portfolio

In **summary**, the model-based hazard and propagation assessment with its change propagation analysis and hazard potential analysis provide support for the identification of potential propagation effects of product changes. The propagation tree and the hazard potential portfolio visualize the relevant information in a condensed form. Hence, the method can support the identification of customizable elements during the preparation or development of an UDC product. Moreover, the pattern-based identification on the one hand allows for an adaptation to a specific product and environment. It on the other hand improves efficiency by formalizing and automating involved knowledge, which is based on experience or expertise.

Preliminary Multi-hierarchy Fault Tree Generation and Evaluation (MHFTA)

The multi-hierarchy fault tree generation and evaluation (MHFTA) supports the preliminary FTA. This further supports the identification of elements suitable for UDC. As Figure 4-40 summarizes, the method uses the product architecture model including hazards and failures. It moreover uses information on occurring propagations, which can originate from the model-based hazard and propagation assessment described above or from other sources. Based on this data stored in the knowledge framework, the multi-hierarchy fault tree generation and evaluation synthesizes preliminary fault trees and provides an evaluation. It is based on two student projects (Beetzen, 2015; Wolf, 2014) and is partially published in Roth, Wolf, and Lindemann (2015) and Roth, Beetzen, and Lindemann (2016).

The **purpose** of the multi-hierarchy fault tree generation and evaluation is to efficiently conduct preliminary FTAs from a worst-case perspective. The **effect** are automatically generated fault trees and the evaluation of their elements in a graphical form. This results in knowledge on the criticality of specific failures within the product. The method can be applied in **situations**, when preliminary FTAs need to be conducted for large and complex systems and a manual FTA is not suitable due to complexity or resource restrictions. Moreover, it can be used to compare failure propagations and the role of different failures in alternative product architectures.

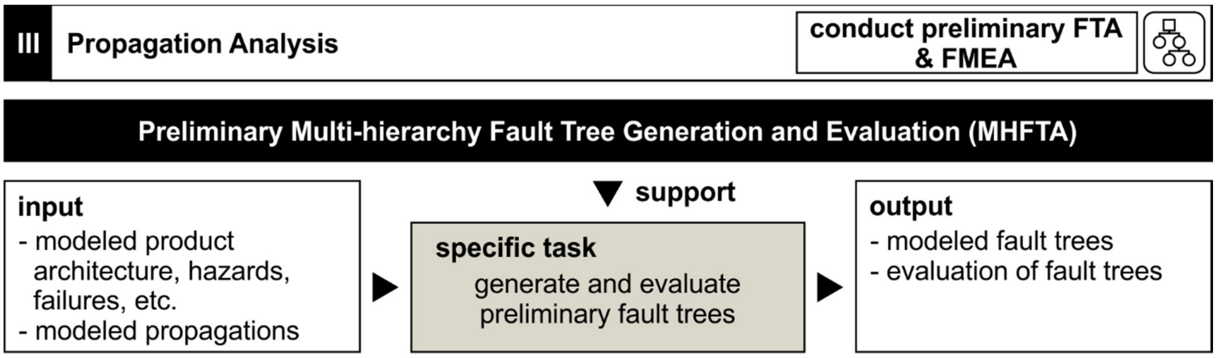

III
Propagation Analysis
conduct preliminary FTA & FMEA
Preliminary Multi-hierarchy Fault Tree Generation and Evaluation (MHFTA)
input
- modeled product architecture, hazards, failures, etc.
- modeled propagations
support
specific task
generate and evaluate preliminary fault trees
output
- modeled fault trees
- evaluation of fault trees

Figure 4-40: Overview of the in- and outputs and the supported task of the multi-hierarchy fault tree generation and evaluation

Development of Support

The task clarification of the development of the multi-hierarchy fault tree generation and evaluation builds on the literature on current methods of safety analysis (see Subsection 2.3.3), of which methods improving the FTA were analyzed in detail. These existing solutions in a first step were evaluated in respect of the requirements defined in Subsection 3.4.2, in particular the improved efficiency (*REQ1*), an early consideration of safety (*REQ3*) as well as integration with other methods (*REQ4*). The evaluation showed that no existing approach is able to fulfill all these requirements.

Thus, based on the findings and the limitations of existing approaches, a new method was developed in two iterations. First, the basic principle of the method was developed and evaluated. Based on this, limitations of the method were identified, in a second iteration. These limitations were translated to requirements, which were then prioritized and realized in an improved method. In the following, the methodology of both iterations is discussed in detail.

Existing methods to improve the efficiency of the FTA are briefly introduced in Subsection 2.3.3. An extensive overview can be found in Mhenni et al. (2014) and Majdara and Wakabayashi (2009). The major difference of these approaches are the models they build on.

For example, Xiang et al. (2011) derive fault trees from **SysML** models by using functional dependencies from diagrams and include an additional reliability configuration and static fault tree model. By that, they automatically derive fault trees with reduced manual efforts. However, the reliability configuration model requires detailed information, which contradicts *REQ3*. Similarly, Mhenni et al. (2014) use standard flow ports to model interactions in SysML and transform diagrams to directed graphs. From this graphs, fault trees are derived based on graph traversal algorithms and pattern recognition. This approach can comply with the requirements on efficiency (*REQ1*) and early consideration of safety (*REQ3*). However, the modeling of flow ports in SysML can be a limitation.

Other approaches rely on **Simulink** models. For example Papadopoulos and Maruhn (2001) automatically generate fault trees from a hierarchical system structure and component dependencies modeled in Simulink. A Hazard and Operability Study is conducted to identify failures. This approach decreases efforts to generate the fault tree, while preparation efforts due to the Hazard and Operability Study remain high. Hence, the efficiency (*REQ1*) and early applicability (*REQ3*) are limited. Tajarrod and Latif-Shabgahi (2008) also rely on Simulink models enhanced with information on failures to automatically derive fault trees. However, they classify components according to their impact and redundancies manually and the efficiency (*REQ1*) and early applicability (*REQ3*) are limited as well.

Other approaches rely on **specific modeling languages** or representations. For example, Majdara and Wakabayashi (2009) use trace-back algorithms to generate fault trees automatically based on directed graphs and functional tables. The modeling of these functional tables induces efforts and has a limited efficiency (*REQ1*). Moreover, it requires detailed knowledge, which limits the applicability in early phases (*REQ3*). Moreover, for example Bieber et al. (2002) derive fault trees from models built in AltaRica and Joshi et al. (2007) generate fault trees from the Architecture Description Language. These special models only provide none or limited compliance with the demand for an integration of methods and models (*REQ4*).

In summary, the existing approaches are not able to fulfill the defined requirements. Even though most use components and abstract functional concepts, they fail to either provide a sufficient integration with other methods and models, or provide limited efficiency. Thus, a new approach in the context of the ESMK was developed.

To ensure integration (*REQ4*), a flexible and adaptable model is required. **Matrix-based representations** like DSMs (Browning, 2001) and DMMs (Danilovic & Browning, 2007) offer this flexibility. As described in Section 4.2, they can be transferred into and deduced from graph-based models. This ensures the integration into the ESMK knowledge framework as well as compatibility to other methods. Additionally, Eppinger, Joglekar, Olechowski, and Teo (2014, pp. 334–335) identify a potential to improve hazard studies trough DSMs. Hence, the basic principle of the method was developed in the first iteration using the DSM-based Structural Complexity Management methodology proposed by Lindemann et al. (2008).

The applicability and success of the method resulting from the first iteration were discussed with an engineer from industrial application using the screwdriver example. Based on this, **requirements for improvement** and general method requirements were defined and decomposed into detailed requirements. These **requirements on a general level** are:

- provide automatic FTA for early stages of design (*REQ1* and *REQ3*)
- allow understanding of failure propagation within the product structure (*REQ5*)
- include interactions in different domains (e.g. material, spatial, etc.) (*REQ4*, *REQ5*)

The **requirements** aiming at an **improvement** are the flowing:

- connect flows over multiple hierarchies (*REQ3*, *REQ5*)
- use functions or components as starting point (resulting from the general definition of customization)
- generate Boolean AND-gates automatically (*REQ1*)

These requirements were prioritized in a pairwise comparison (Ehrlenspiel, 2009, p. 514). This prioritization clearly showed that apart from an automatic FTA, the connection of flows and propagations over multiple hierarchies is the most important improvement. Therefore, the following publications, which discuss **multi-hierarchy aspects** were additionally analyzed on their suitability to fulfill the requirements: Deubzer and Lindemann (2009), Eben, Daniilidis, and Lindemann (2010); Becerril et al. (2014); Gofuku, Koide, and Shimada (2006); Tilstra, Seepersad, and Wood (2012). To identify most suitable approaches for improvement, these approaches and the existing approaches to generate FTAs were assessed in respect of the defined requirements. Figure 4-41 visualizes the results of the simple score assessment. It shows that especially the approaches of Deubzer and Lindemann (2009) and Eben et al. (2010) offer promising solutions.

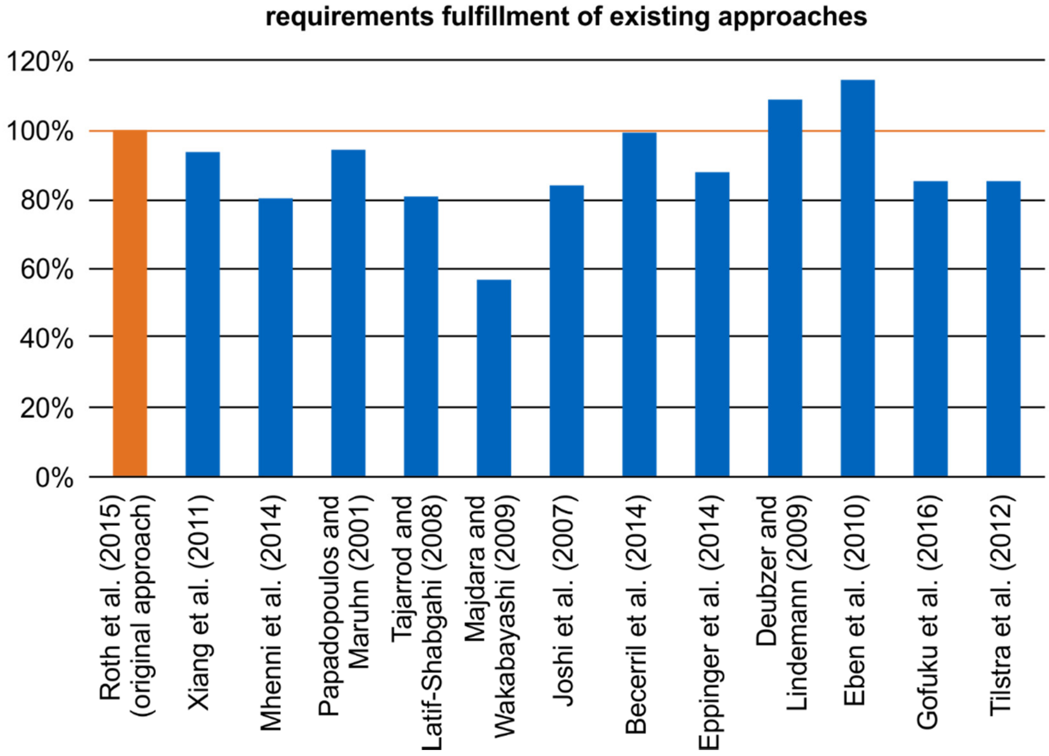


Figure 4-41: Assessment of existing approaches and their fulfillment of the requirements on an improvement

Based on this, the most suitable approaches were integrated in the first approach. To achieve this, the approach resulting from the first iteration was decomposed to identify, where the integration of promising approaches was possible and advantageous. These integrations were conducted, which resulted in the final multi-hierarchy fault tree generation and evaluation presented in the following.

Provided Support (Multi-hierarchy Fault Tree Generation and Evaluation)

The **multi-hierarchy fault tree generation and evaluation** adapts the Structural Complexity Management procedure (Lindemann et al., 2008) and consists of the four stages and six steps shown in Figure 4-42. Starting with the System Definition and Information Acquisition, the considered product is modeled or the product model is extracted from the ESMK knowledge framework. After deriving the indirect dependencies of failures, the failure network is used to generate fault trees automatically and to identify the minimal cut sets. These results are evaluated and visualized afterwards. The following paragraphs discuss each stages of the procedure in detail.

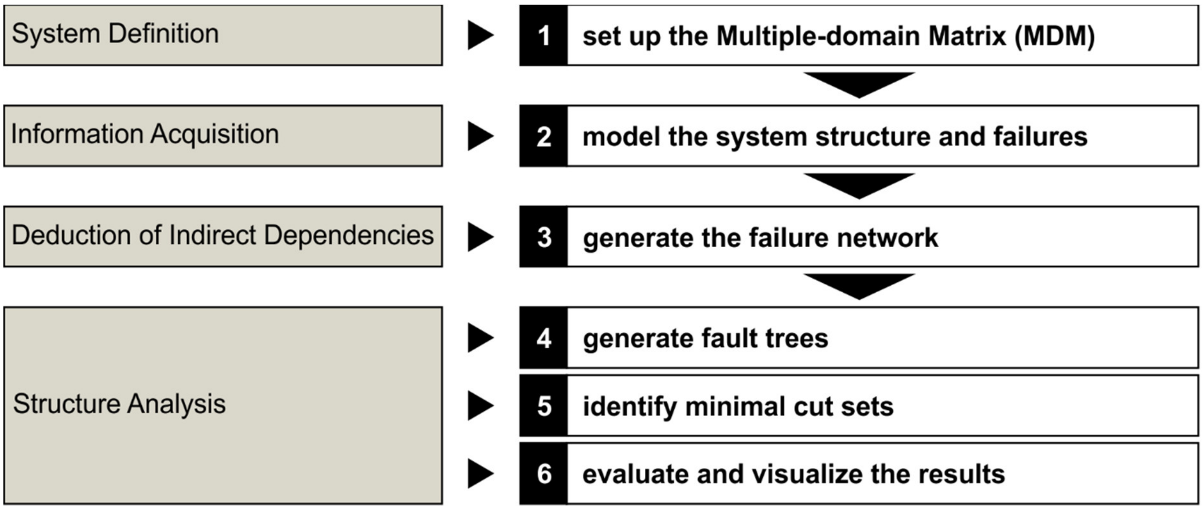

System Definition
1 set up the Multiple-domain Matrix (MDM)
Information Acquisition
2 model the system structure and failures
Deduction of Indirect Dependencies
3 generate the failure network
Structure Analysis
4 generate fault trees
5 identify minimal cut sets
6 evaluate and visualize the results

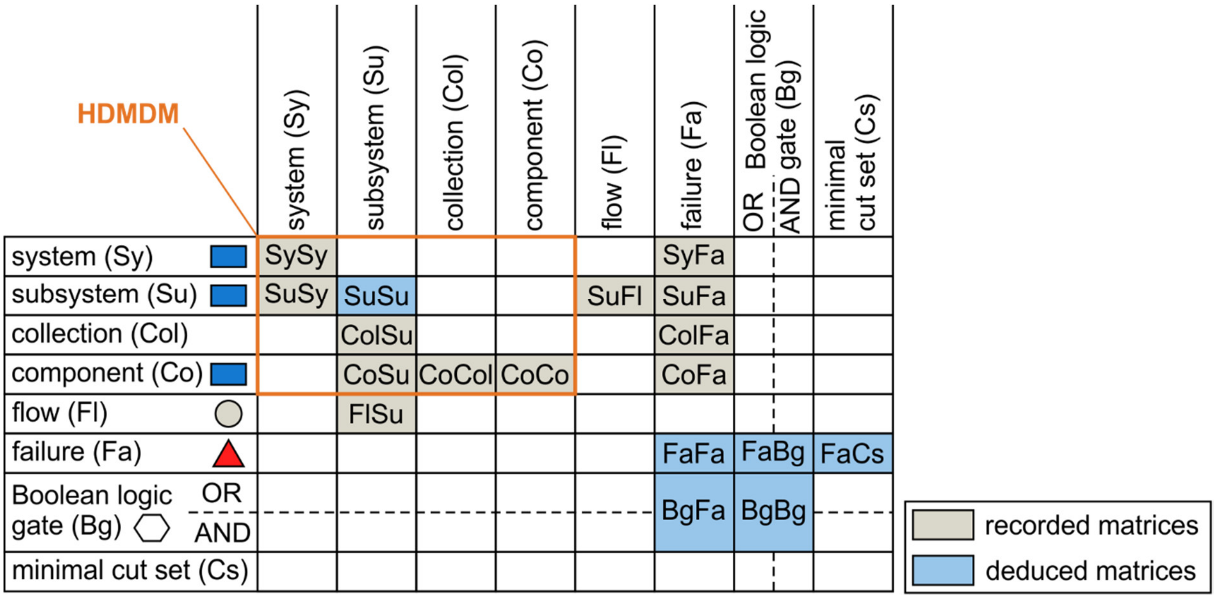
Figure 4-42: Stages and steps of the multi-hierarchy fault tree generation and evaluation

The first stage of the multi-hierarchy fault tree generation and evaluation, the **system definition**, **establishes the Multiple-domain Matrix (MDM)** or meta-model of the analysis. As shown in Figure 4-43, its main domains are the product model as well as the relevant elements of a fault tree (see Subsection 2.3.2). The latter includes failures, Boolean logic gates and minimal cut sets.

The product model comprises the elements of the product and their dependencies in order to model all possible propagations within the product. If this information is not available or obtained from the ESMK knowledge framework (i.e. results of the model-based hazard and propagation assessment), the multi-hierarchy fault tree generation and evaluation follows the ideas of Deubzer and Lindemann (2009) and Eben et al. (2010). It establishes a hierarchical decomposition of the system. This decomposition can be considered as independent MDM within the meta-model and is called the hierarchical decomposition MDM (HDMDM). As indicated in Figure 4-43, the basic HDMDM contains the domains of system, subsystem, and component. These three levels of decomposition represent a basic decomposition of the product structure. Depending on the aspired granularity of the analysis, the domains can be adapted or additional levels can be inserted.

Inspired by Alizon, Shooter, and Thevenot (2007), the HDMDM models both, interhierarchical and intrahierarchical dependencies. Intrahierarchical dependencies are horizontal connections within one hierarchical level and are represented by the DSMs of the HDMDM. Whereas DMMs model the interhierarchical (vertical) dependencies between different hierarchies.

Depending on the available information, it is necessary to identify, which intrahierarchical relations cannot be determined directly. They need to be derived as indirect dependencies in later steps. From a safety perspective, flows are an important domain within the product (see Section 4.2 and the Feature Analysis). Thus, the method proposes to use flows as auxiliary domain to deduce indirect dependencies. In Figure 4-43, this domain is exemplarily inserted to derive dependencies in the domain of components. If required, the auxiliary domain can be inserted in every hierarchical level. In addition, it can be adapted and extended, for example to include states (see Roth, Kasperek, & Lindemann, 2013).



	system (Sy)	subsystem (Su)	collection (Col)	component (Co)	flow (Fl)	failure (Fa)	OR Boolean logic AND gate (Bg)	minimal cut set (Cs)
system (Sy) 🟦	SySy					SyFa		
subsystem (Su) 🟦	SuSy	SuSu			SuFl	SuFa		
collection (Col)		ColSu				ColFa		
component (Co) 🟦		CoSu	CoCol	CoCo		CoFa		
flow (Fl) ○		FlSu						
failure (Fa) ▲						FaFa	FaBg	FaCs
Boolean logic gate (Bg) ⬡ OR AND						BgFa	BgBg	
minimal cut set (Cs)								

Figure 4-43: MDM-framework of the multi-hierarchy fault tree generation and evaluation with its HDMDM

Moreover, the HDMDM shown in Figure 4-43 introduces the domain collection. This domain is adapted from Xiang et al. (2011) and models system redundancies. If, in the given example, components redundantly contribute to the element in the next hierarchical level, they are combined via this domain. A collection can be considered as virtual level between two hierarchical levels.

In addition to the HDMDM, the meta-model of the multi-hierarchy fault tree generation and evaluation includes the domain of failures. It represents the failures, which can occur on all hierarchical levels of the HDMDM. Moreover, the domain of Boolean logic gates includes the AND- and OR-gates of fault trees. Other types of gates are not considered in the approach, as the two considered gates are sufficient to take a worst-case perspective. Even though an FTA does not consider dependencies between Boolean logic gates, they are included in the meta-model as shown in Figure 4-43. This dependency is required for the automatic generation of fault trees. In addition, minimal cut sets as important element of the FTA are included as domain.

If the ESMK knowledge framework and the previously described propagation patterns of the model-based hazard and propagation assessment are used, the meta-model of the HDMDM is simplified. In this case, it consists of the domain of components and their hierarchical relations stored in the framework. Moreover, the dependencies within one hierarchical level are included in the knowledge framework represented by propagation edges. However, if redundant elements occur, they have to be identified manually within the ESMK knowledge framework.

The **Information Acquisition** as the second stage of the multi-hierarchy fault tree generation and evaluation populates the HDMDM and thus, **develops the necessary model**. Support to record dependencies can be for example be found in Lindemann et al. (2008). If the hierarchical decomposition is known, the method suggests modeling dependencies within one hierarchical level and simplifying the modeling in the other levels through usage of heredity principles. If the HDMDM uses auxiliary domains, they also need to be recorded in this stage.

Moreover, failures have to be identified during the Information Acquisition stage within all hierarchical levels. Depending on the aspired level of detail, the multi-hierarchy fault tree generation and evaluation suggests two alternatives:

- For a detailed analysis, each component and its functions need to be analyzed in detail (for example through the model-based hazard analysis introduced in Subsection 4.3.2). By that, every possible failure, which can cause noncompliance with safety restrictions is identified and the respective dependencies are recorded in the MDM.
- For a lower level of detail, the negation of the functions can be sufficient (Lindemann, 2009, p. 209). This step can be automated and will result in DMMs, which connects the product domains and failures. These DMMs only have diagonal entries. The detail level can be increased, if instead of general negation, a differentiation between execution and value failure is made.

If the ESMK knowledge framework and the propagation patterns of the model-based hazard and propagation assessment (see above) are used, the Information Acquisition is limited to the identification of redundant components and their assignment to collections.

The **Deduction of Indirect Dependencies** as third stage of the multi-hierarchy fault tree generation and evaluation aims **to generate a failure network**. First, the relations within the HDMDM, which cannot be directly recorded in the Information Acquisition, are deduced by matrix multiplication (for details see Lindemann et al. (2008) and Roth et al. (2015)).

Once the HDMDM is completed, the failure network can be deduced. For each hierarchical level, at least one DSM of the failure network (*DSM FaFa*) has to be created. This results in an intrahierarchical failure network. In addition, for each interhierarchical transition, one *DSM FaFa* has to be calculated.

To calculate the **intrahierarchical** failure network, the intrahierarchical dependencies (e.g. *DSM SySy*) and the dependencies of the elements of this hierarchical level to failures (e.g. *DMM SyFa*) are required. Examples of intrahierarchical dependencies are geometrical contacts of flow relations between components. The computation follows Figure 4-44. If multiple DSMs of intrahierarchical dependencies are modeled (e.g. differentiation of functional and geometrical dependencies), the computation has to be conducted for each of them and the results are superposed qualitatively.

To calculate the **interhierarchical** failure network, the hierarchical decomposition (e.g. *DMM SuSy*) and the dependencies of elements of both hierarchical levels to failures (e.g. *DMM SyFa* and *DMM SuFa*) are required. An example of an interhierarchical dependency is the allocation of components to assembly groups. The computation follows a similar scheme as above and is visualized in Figure 4-44. If needed, also propagations, which skip one hierarchical level, can be determined. If collection domains are used, they have to be treated as additional hierarchical level within the computation.

Finally, all deduced failure networks are qualitatively superposed to obtain the complete worst-case failure network. Instead, if the ESMK knowledge framework is used, the model-based hazard and propagation assessment (see above) and the created propagation edges can be used. In this case, the propagations only have to be transferred to the domain of failures.

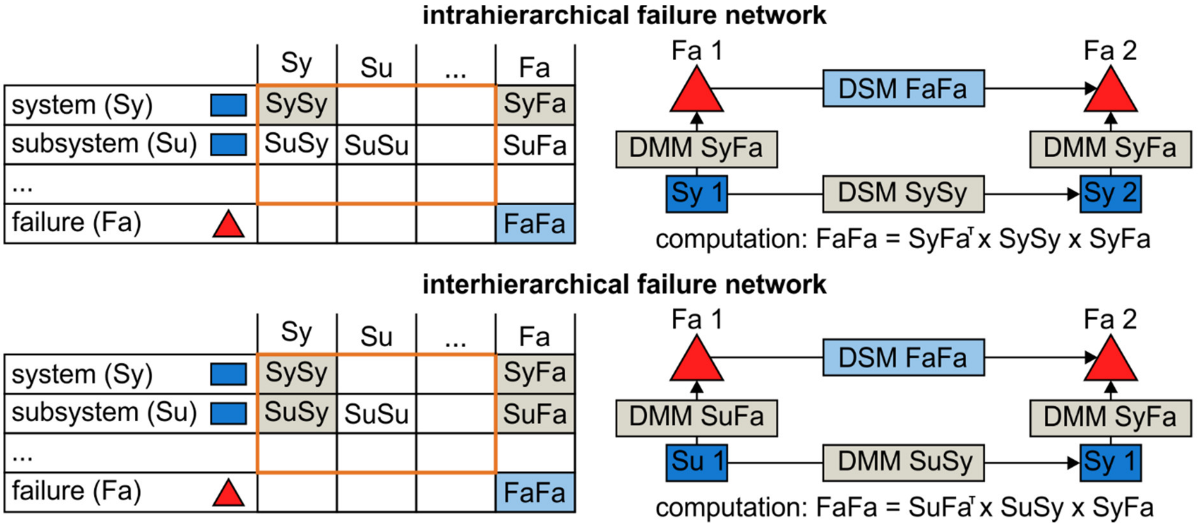


Figure 4-44: Computation of the intrahierarchical (top) and interhierarchical (bottom) failure network

The fourth stage of the multi-hierarchy fault tree generation and evaluation, the **Structure Analysis,** comprises the generation of fault trees, the identification of minimal cut sets, and the evaluation and visualization of the results. To define top events first, the method suggests using the hazard perspective and considering the failures directly linked to hazards as top events.

To generate a fault tree for a specific top event, a **failure chain** (*DSM FaFa_TE*) is extracted from the failure network. First, the failure network in the *DSM FaFa* is transposed to align with the deductive character of the FTA. The reason is that the relations in the failure network due to its generation originally describe an inductive relationship (failure might cause failure). Next, the distance matrix (Lindemann et al., 2008, p. 229) of the transposed network (*DSM FaFa_TE*) is calculated. Based on this distance matrix, all elements, which have no defined distance to the top event, are removed from the failure network. The same applies for ingoing dependencies of the top event. This procedure is visualized in Figure 4-45 and results in the failure chain stored in the *DSM FaFa_TE*.

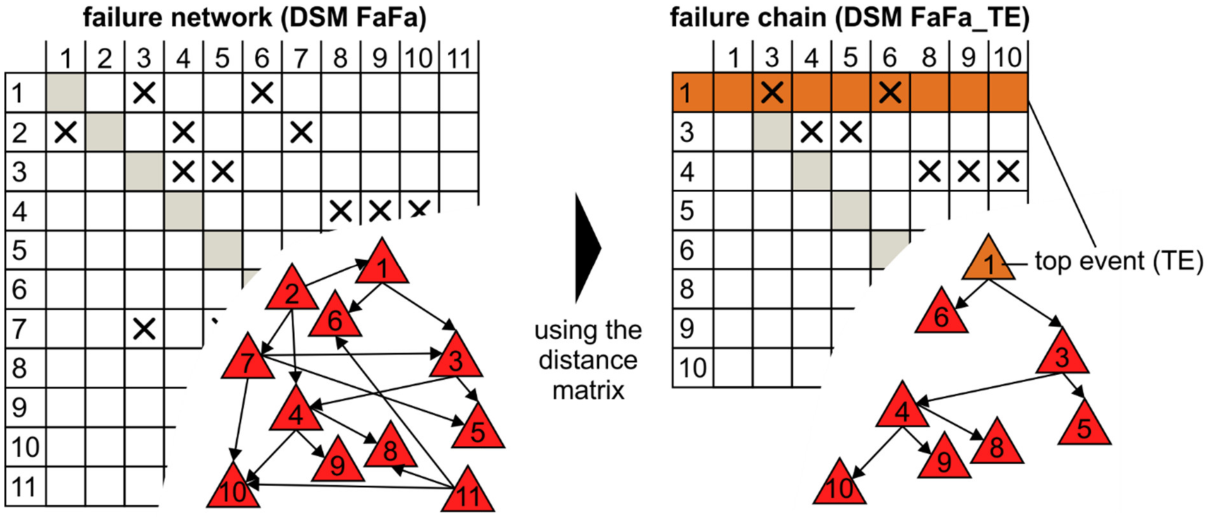


Figure 4-45: Conversion of the failure network into a top event-specific failure chain via the distance matrix

To **transform the failure chains into fault trees**, a Boolean logic gate needs to be inserted at the output of each failure. For each failure in the failure chain, which has an active sum above zero, one element in the domain of Boolean gates is created and the correspondent dependencies are established as indicated in Figure 4-46. For failures assigned to regular hierarchical levels, OR-gates are inserted and for failures assigned to the collection domain, AND-gates are created. The collection elements are deleted afterwards and the dependencies are consolidated accordingly.

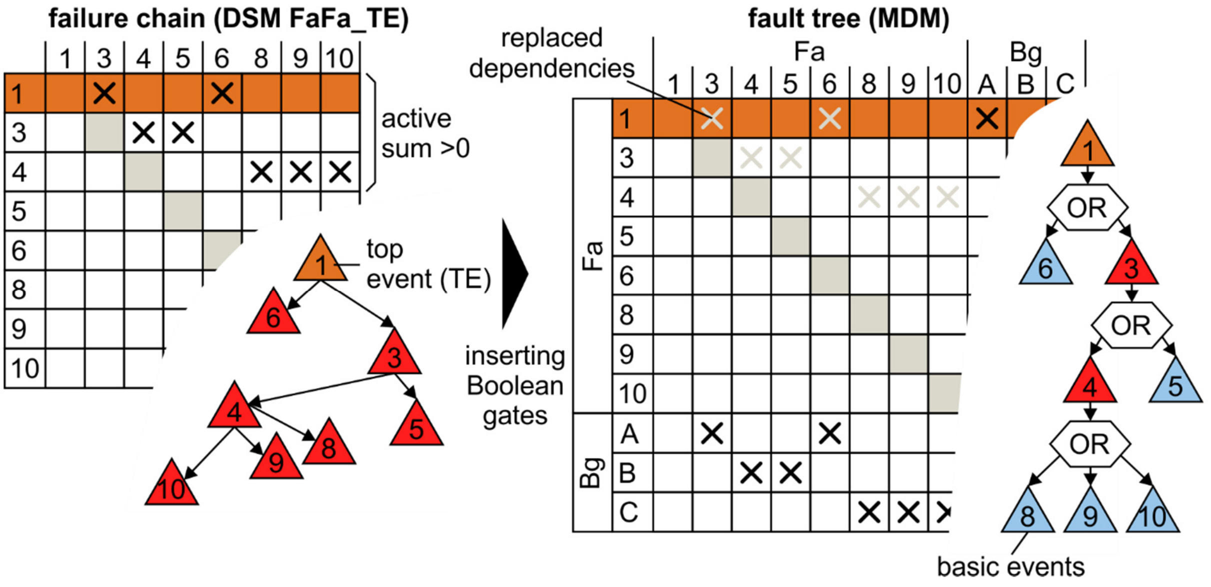


Figure 4-46: Insertion of Boolean logic gates into the failure chain to obtain a fault tree

To finalize the fault tree, occurring loops have to be broken. When no AND-gate is located between the loop and the top event, the distance matrix is evaluated. Based on this, the dependency between the two elements within the loop, which have the smallest and largest distance to the top event, is removed. When an AND-gate is located above the loop, the same rule is applied. In this case, the distances to the AND-gate are considered instead of the distances to the top event.

To **calculate the minima cut sets**, the multi-hierarchy fault tree generation and evaluation uses the algorithm proposed by Hauptmanns, Knetsch, and Marx (2004). It requires the *DMM BgFa* and the *DSM BgBg* as input. From the failure domain, only basic events (active sum in the fault tree is equal to zero) are considered. The algorithm iteratively replaces Boolean gates through their influences and identifies all minimal cut sets. For each minimal cut set, an element in the minimal cut set domain is created and the corresponding basic events are recorded in the *DMM FaCs*.

Due to the worst-case perspective and the abstract definition of failures and propagations, it is not expedient to determine probabilities in the fault tree. Instead, the failures are **visualized and classified** similar to the FMEA (see Subsection 2.3.2) and the model-based hazard and propagation assessment (see above). According to their severity, they are assessed on a scale from one to ten. The multi-hierarchy fault tree generation and evaluation considers a failure as severe, if it has a strong individual impact on the top event and if it is often involved in minimal cut sets, causing the top event.

A strong individual impact is given, if the distance of the failure to the top event is small. To classify basic events according to that the distance matrix of the fault tree is evaluated. For each basic event, the distance to the top event d is normalized to the interval [1; 10] based on the maximum occurring **distance** d_{max} as follows:

$$d_n = (d - 1)\frac{10 - 1}{d_{max} - 1} + 1$$

As second dimension of classification, the **occurrence** of the failures in minimal cut sets is used. For all basic events, the occurrence o is derived from their active sum in the *DMM FaCs*. The occurrence moreover is normalized to [1; 10] based on the maximal and minimal occurrences o_{max} and o_{min}, as follows:

$$o_n = (o_{max} - o)\frac{10 - 1}{o_{max} - o_{min}} + 1$$

The occurrence of the intermediate events is determined in a bottom-up manner based on the occurrences of the basic events. In case of an OR-gate below, the occurrence of the intermediate event is the sum of its basic events' occurrences. If an AND-gate is below, the occurrence of the intermediate event is the maximum of the basic events' occurrences. This process is iteratively repeated, until the top event is reached. To distinguish between intermediate and basic events in the visualization, the intermediate events' occurrences are normalized to the interval [0.1; 1].

Based on both classification dimensions, the preliminary generated fault trees can be quickly assessed and critical elements can be identified. To visualize the results, the multi-hierarchy fault tree generation and evaluation proposes to arrange the failures in a **FTA-portfolio** as shown in Figure 4-47. Moreover, based on the assumption that a failure, which can directly cause the top event, and the failure with maximum occurrence in the minimal cut sets are most critical, a combined severity is inserted for both types of fault tree elements. This combined severity can for example be used in a subsequent preliminary FMEA.

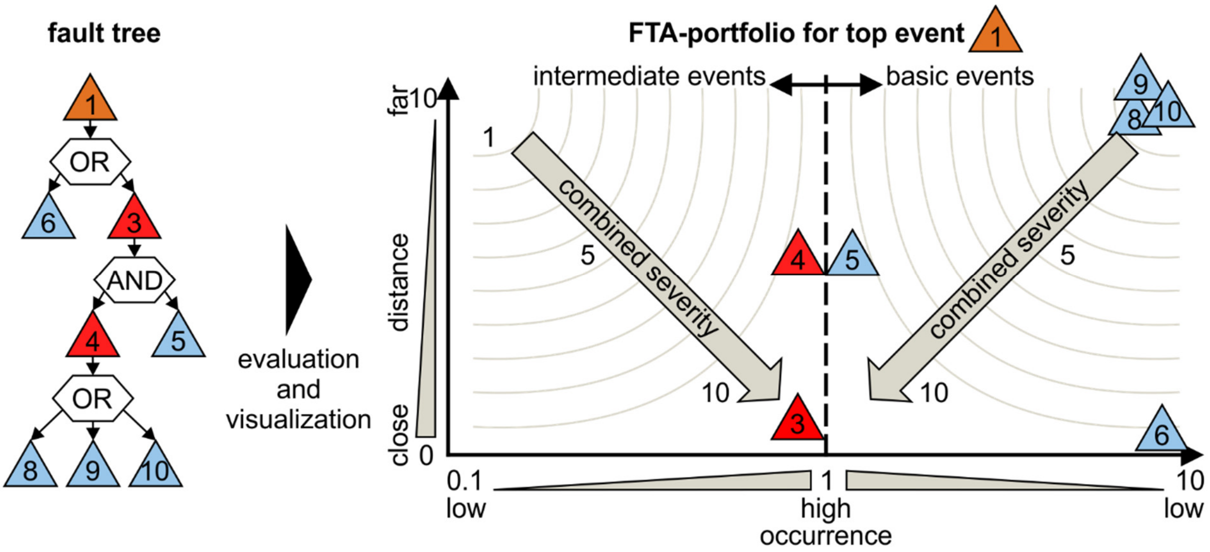


Figure 4-47: FTA-portfolio to visualize the evaluation of the fault tree including basic and intermediate events and their combined severity

In **summary**, the multi-hierarchy fault tree generation and evaluation provides support to automatically generate a preliminary qualitative FTA and enable a fast evaluation. The HDMDM or the usage of the ESMK knowledge framework enable a systematic generation of the product model. The method based on this model provides an automated synthesis of worst-case fault trees. Using these fault trees, the multi-hierarchy fault tree generation and evaluation supports the identification of customizable elements and provides a worst-case preliminary FTA. The latter can be used as basis for an efficient individual safety analysis of UDC products.

Preliminary Model-based Failure Mode and Effects Analysis

The preliminary model-based FMEA specifically supports the task of conducting a preliminary FMEA. By that, it supports the evaluation of occurring risks and the definition of restrictions or countermeasures in the context of UDC. As Figure 4-48 summarizes, it consolidates the information of the ESMK knowledge framework and combines it with the results of a previous FTA. Using this data, the preliminary model-based FMEA provides a prefilled FMEA-form to prepare the manual analysis. The method is based loosely on a student project (Isemann, 2015).

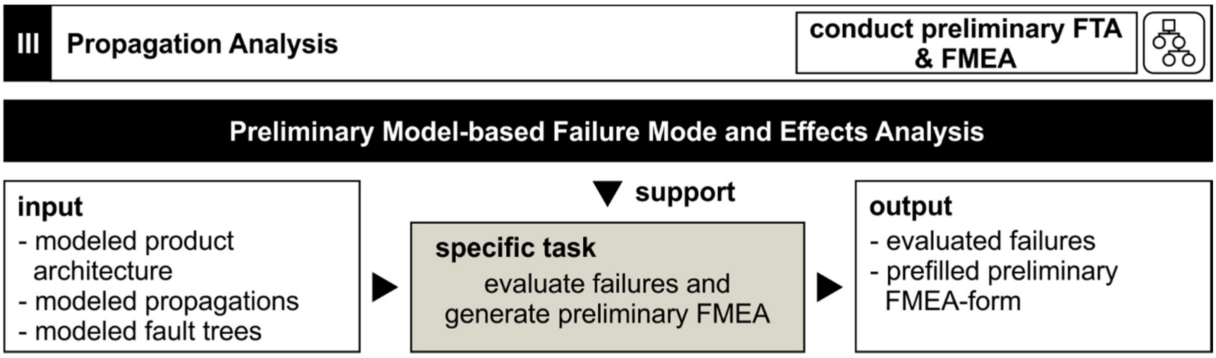

III
Propagation Analysis
conduct preliminary FTA & FMEA
Preliminary Model-based Failure Mode and Effects Analysis
input
- modeled product architecture
- modeled propagations
- modeled fault trees
support
specific task
evaluate failures and generate preliminary FMEA
output
- evaluated failures
- prefilled preliminary FMEA-form

Figure 4-48: Overview of the in- and outputs and the supported task of the preliminary model-based FMEA

The **purpose** of the preliminary model-based FMEA is to automatically prepare and prefill a FMEA-form. Its **effect** a consolidation and structuring of information on occurring failure modes, their possible causes, and their effects within a prefilled FMEA-form. Moreover, it ensures the completeness of the analysis. The preliminary model-based FMEA can be applied in **situations**, when existing knowledge needs to be automatically prepared for an FMEA and the manual preparation efforts have to be reduced. In addition, through its completeness, it is suitable for situations, in which a worst-case perspective needs to be taken and every possible failure needs to be considered.

Development of Support

The task clarification of the development of the preliminary model-based FMEA is based on the review of the FMEA in Subsection 2.3.2 and the current developments in this field discussed in Subsection 2.3.3. In combination with the challenges through UDC and the ESMK's basic requirements (see Subsection 3.4.2), a set of requirements was defined. These **requirements on the model-based preliminary FMEA** are the following:

- automate parts of the FMEA (Subsection 2.3.3, *REQ1*)
- indicate dependencies of failures and propagations automatically (Subsection 3.3.3, *REQ1*)

- provide traceability of results to support manual post processing (*REQ1*, *REQ5*)
- allow manual adjustments to handle complexity of the analysis (*REQ1*, *REQ3* and *REQ5*)
- indicate customizable components (*REQ3*)
- support the identification of potential failures induced or influenced through UDC (*REQ2*, *REQ3*)

To fulfill these requirements and generate a support, the basis FMEA was transferred and adapted to the ESMK knowledge framework. To achieve this, concepts of the current developments in this field as well as concepts of other ESMK methods were used. This resulted in the preliminary model-based FMEA presented in the following.

Provided Support (Preliminary Model-based Failure Mode and Effects Analysis)

The procedure of the **preliminary model-based FMEA** comprises the steps indicated in Figure 4-49. In a first automated step, a basis FMEA is generated based on the ESMK knowledge framework. This FMEA is manually structured in the next step to improve the overview. Based on this, the basis FMEA is manually completed. If the manual analysis is conducted extern of the ESMK knowledge framework, the final step requires an integration of the manual adaptions back into the knowledge framework.

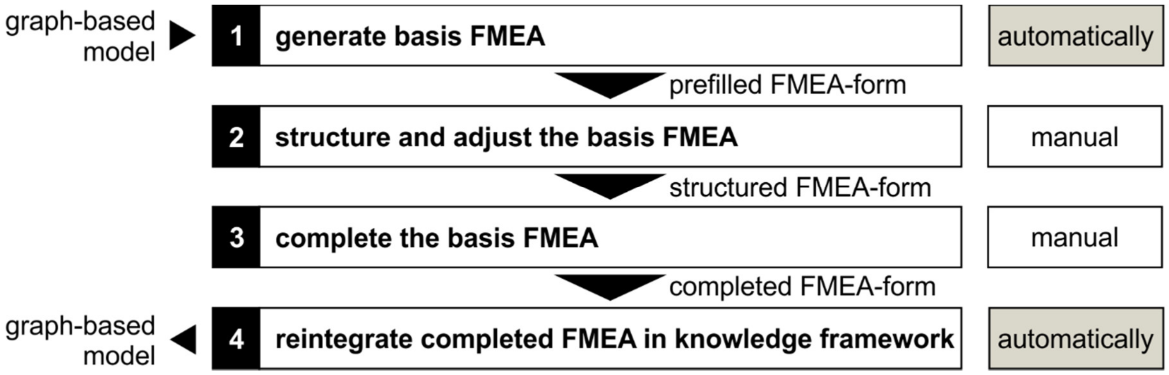


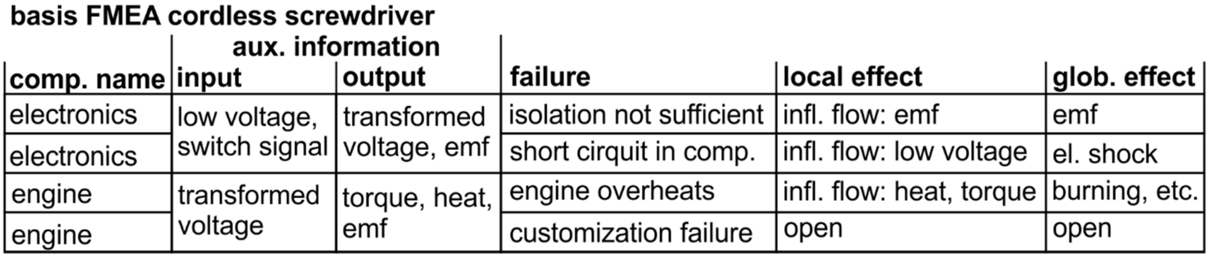
Figure 4-49: Procedure of the preliminary model-based FMEA with automated and manual tasks

To enable the integration of the FMEA, the ESMK knowledge framework provides an **auxiliary node type** (FMEArow). This node type can collect all information, which is consolidated in a row of the FMEA in its attributes. Using this element, the first step of the preliminary FMEA **automatically creates the basis FMEA**. For each component within the system boundary of the analysis, the failures are identified and analyzed. The identified failures are extracted from the framework and consolidated in the nodes, which represent the rows of the basis FMEA. This can be conducted on any decomposition level of the model in the knowledge framework. As result, the following information is stored in the **FMEA rows** for each occurring failure (for detailed overview see the corresponding node in Appendix 9.3.2):

- name and identifier of the component to structure the basis FMEA by components
- auxiliary information on the component’s functions and flow relations to improve manual understanding
- name and identifier of the component’s specific failure

- local failure effects of the considered node; the effects depend on the information stored in the knowledge framework. They comprise failures of parent assemblies or through flow relations between components. However, if the model-based hazard and propagation assessment or multi-hierarchy fault tree generation and evaluation (see above) were conducted, all direct propagations and directly connected failures are considered.
- global failure effect; this requires a previously conducted multi-hierarchy fault tree generation and evaluation. All top events influenced by the considered failure are indicated.
- failure cause; here the same principle like for the local effect is followed. However, instead of outgoing, the incoming relations are identified.
- prevention measure; if the failure is connected to a defined safety function, it is indicated.
- tracing to the top event; if a FTA was conducted, the branch from considered fault to top event can be indicated as further support for the manual analysis.

If a component is marked as customizable in the knowledge framework, the model-based preliminary FMEA also highlights this fact in the basis FMEA. Moreover, for each customizable component, an additional failure is introduced. In this case, child elements of the components from lower decomposition levels are included and integrated. Figure 4-50 provides an exemplary overview of the basis FMEA including regular and customization failures.



basis FMEA cordless screwdriver

	aux. information				
comp. name	input	output	failure	local effect	glob. effect
electronics	low voltage, switch signal	transformed voltage, emf	isolation not sufficient	infl. flow: emf	emf
electronics			short cirquit in comp.	infl. flow: low voltage	el. shock
engine	transformed voltage	torque, heat, emf	engine overheats	infl. flow: heat, torque	burning, etc.
engine			customization failure	open	open

Figure 4-50: Overview of the basis FMEA-form including faults induced through customization

In the next step, the **manual analysis** starts. The user has to structure and adjust the automatically generated basis FMEA first. Depending on the scope of the analysis, this includes sorting and filtering. However, it is also possible to remove elements, which are too detailed. Similarly, it can be advantageous to replace parts through a basis FMEA conducted on a more detailed decomposition level.

Once the basis FMEA is manually prepared, **the FMEA is manually completed**. This includes the removal of not occurring effects or propagations. Especially, when the preliminary model-based FMEA relies on propagations and fault trees generated through the ESMK's worst-case perspective, the completeness will result in some faults or effects, which will never occur in reality. Moreover, if necessary discovery or mitigation measures can be defined and the severity, occurrence and detection values can be assessed. Moreover, it is possible to determine the RPN or deduce risk matrices (see Subsection 2.3.2). In this case, the results of the model-based hazard and propagation assessment and the multi-hierarchy fault tree generation and evaluation (see above) can be supportive. Moreover, to uncover all possible failures, failures induced through customization need to be intensively discussed. Especially the misuses defined in the model-based hazard analysis (see Subsection 4.3.2) can provide valuable support.

Once the manual FMEA is conducted, the **information is transferred back** to the ESMK knowledge framework. By that, the analysis can be reused and the efforts for subsequent analyses are reduced, as not all the manual work has to be repeated.

In **summary**, the preliminary model-based FMEA supports the generation of a FMEA based on the ESMK knowledge framework. Through the automation of parts of the analysis and the provided auxiliary information, the manual work is reduced in terms of efforts and experience. The method especially introduces failures caused through UDC. Thus, it supports the definition and balancing of both, restrictions and degrees of freedom for customization. Moreover, it consolidates many knowledge created through other methods of the ESMK for manual analysis and integrates the manual adaptions back into the ESMK knowledge framework. By that, it allows the reuse of data and the improvement of the efficiency of subsequent analyses.

UDC Safety-relevance Portfolio

The UDC safety-relevance portfolio supports the task to assess the suitability of elements (i.e. components) for UDC from a safety perspective. As Figure 4-51 summarizes, it uses the product architecture model as well as the results of the ESMK's model-based hazard and propagation assessment and the ESMK's multi-hierarchy fault tree generation and evaluation. Based on this, the UDC safety-relevance portfolio assesses the safety-relevance of components and creates a portfolio, which supports the balancing of the safety-relevance and UDC demands.

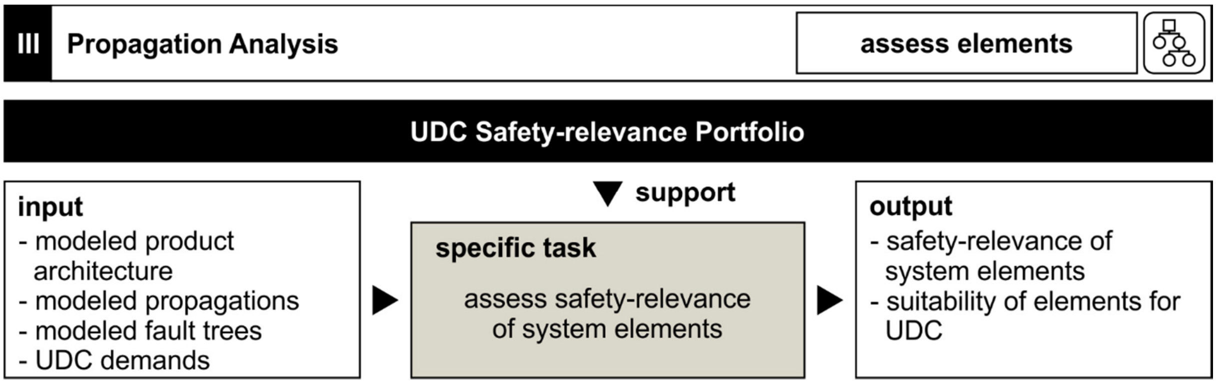

III Propagation Analysis
assess elements
UDC Safety-relevance Portfolio
input
- modeled product architecture
- modeled propagations
- modeled fault trees
- UDC demands
support
specific task
assess safety-relevance of system elements
output
- safety-relevance of system elements
- suitability of elements for UDC

Figure 4-51: Overview of the in- and outputs and the supported task of the UDC safety-relevance portfolio

The **purpose** of the UDC safety-relevance portfolio is to identify elements suitable for UDC. This includes the evaluation of the safety-relevance of components in contrast to a demand for UDC. Its **effect** is an assessment, which represents the safety-relevance of a component on different detail levels. Thus, knowledge on the criticality and relevance of components in terms of safety is created on different detail levels. The UDC safety-relevance portfolio can be applied in **situations**, when the elements of an existing product or product concept need to be examined on their suitability for UDC. Connected to this, it supports the preparation of decision on the balancing of UDC and safety.

Development of Support

The UDC safety-relevance portfolio was developed as consolidating visualization and decision-making support of the ESMK's analysis methods. Thus, no specific review provided input for the development. Nevertheless, the task clarification derived aims for the development from general requirements of the ESMK (see Subsection 3.4.2). The development of the UDC safety-relevance portfolio mainly targeted a visualization and decision support that enables the balancing (*REQ3*) and improves the transparency (*REQ5*).

The visualization in a portfolio and the idea of its composition was **derived from the influence portfolio** proposed by Lindemann et al. (2008, pp. 161–163) and the individualization portfolio proposed by Holle, Gronemann, and Lindemann (2015, p. 14).

Provided Support (UDC Safety-relevance Portfolio)

The **UDC safety-relevance portfolio** consists of two aspects: The assessment of the safety-relevance and its visualization in the portfolio.

To **assess the safety-relevance**, the UDC safety-relevance portfolio suggests applying different levels. Depending on the phase of design and preparation for UDC, a different level of detail should be chosen. Hence, different metrics to assess the safety-relevance of components on varying levels of detail are necessary.

The ESMK suggests a set of three metrics on different levels of detail. However, depending on the actual product and boundary conditions, they require and adaption or other metrics are better suitable. The three assessment levels suggested by the UDC safety-relevance portfolio are:

- ***Level 1 - Rough estimation through hazards and safety requirements:*** The safety-relevance is assessed based on the number of hazards or safety requirements connected to the considered component. The safety-relevance is considered high, when a component is connected to many hazards. This assessment can be conducted already with data of the initial phase of the ESMK. Alternatively, the hazard potential portfolio output of the model-based hazard and propagation assessment (see above) can be used.
- **Level 2 - Estimation through qualitative relations:** The safety-relevance is similar to level 1 assessed by the number and weight of connected hazards or safety requirements. However, a qualitative assessment on the strength of the relation is included. The safety-relevance is considered high, when a component is connected to many high weighted hazards through a strong relationship. Thus, a qualitative assessment of the dependencies is necessary. This assessment is similarly applied to the impact of safety categories in the safety-oriented Modular Function Deployment (see in the following).
- **Level 3 - Quantitative assessment through FTA:** The safety-relevance is assessed by the contribution of a component to the occurrence to top events within an FTA. The safety-relevance is considered high, when a component strongly contributes to the occurrence of multiple top events. For this assessment, the results of the ESMK's multi-hierarchy fault tree generation and evaluation or a model-based FMEA (see above) can be used.

Based on the safety-relevance assessment, the components are visualized in the **UDC safety-relevance portfolio**. To support the balancing of UDC and safety, the portfolio consists of the dimensions safety-relevance and UDC demand, as shown in Figure 4-52. While the safety-relevance is determined as described above, the UDC demands are not in the scope of the ESMK. They for example can be determined following the methodology of Holle et al. (2015).

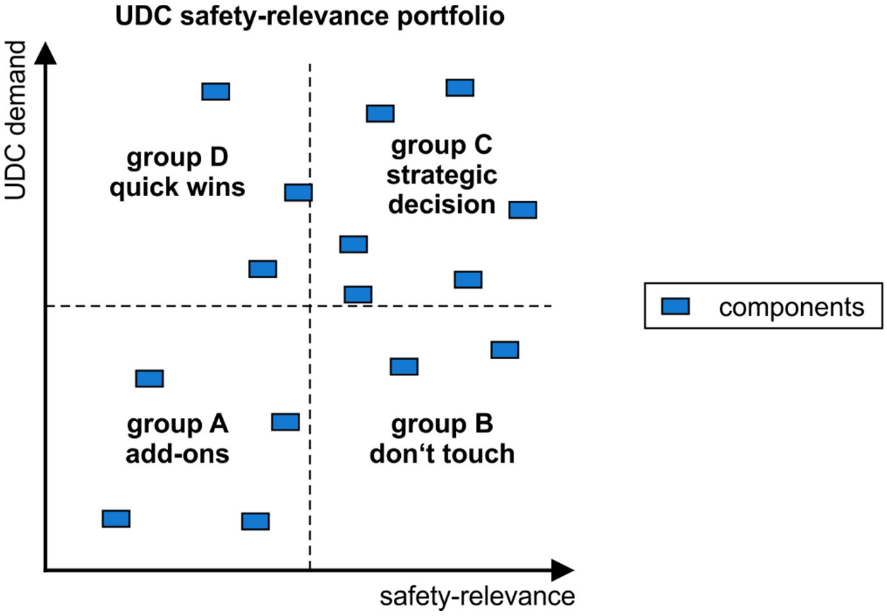


Figure 4-52: The UDC safety-relevance portfolio and its four groups of elements

As shown in Figure 4-52, the portfolio can classify the elements in four groups. Elements of *group A* (add-ons) are elements with a low safety-relevance and a low UDC demand. They do not necessarily have to be defined as UDC options, but if it suits to the final concept, they can be added as UDC option with limited effort.

Elements of *group B* (don't-touch) are elements with a high safety-relevance and a low UDC demand. They do not provide UDC benefit and are very critical from a safety perspective. They should be defined as fixed and standardized core of the product.

Elements of *group C* (strategic-decision) are elements with a high safety-relevance and a high UDC demand. They provide large benefit for UDC but also have a strong impact on product safety. Thus, they should be analyzed in detail on their specific restrictions. Moreover, a strategic decision is necessary, if the efforts are taken and the elements are offered for UDC. Another suggestion can be to adapt the product architecture (see in the following).

Elements of *group D* (quick-wins) are elements with a low a safety-relevance and a low UDC demand. They provide a good potential for UDC compared to low safety-related impacts and efforts. Hence, these elements are most suitable for UDC.

For lager products, the efforts to assess the safety-relevance of components are immense. In this case, the UDC safety-relevance portfolio suggests **proceeding iteratively** as illustrated in Figure 4-53. Starting with a rough assessment (e.g. level 1), potentially suitable elements for UDC can be identified. For those elements, a second more detailed analysis (e.g. level 2) is conducted and the portfolio is applied again. This process is iteratively repeated until the required level of detail is reached and a decision on the UDC options for each element is made.

In **summary**, the UDC safety-relevance portfolio prepares the decision-making for UDC. It assesses the safety-relevance of product elements on different and adaptable levels. It combines this information with the demands for UDC and allows to visualize the trade-offs between UDC options and efforts related to safety. It provides the basis for a balancing of safety and UDC.

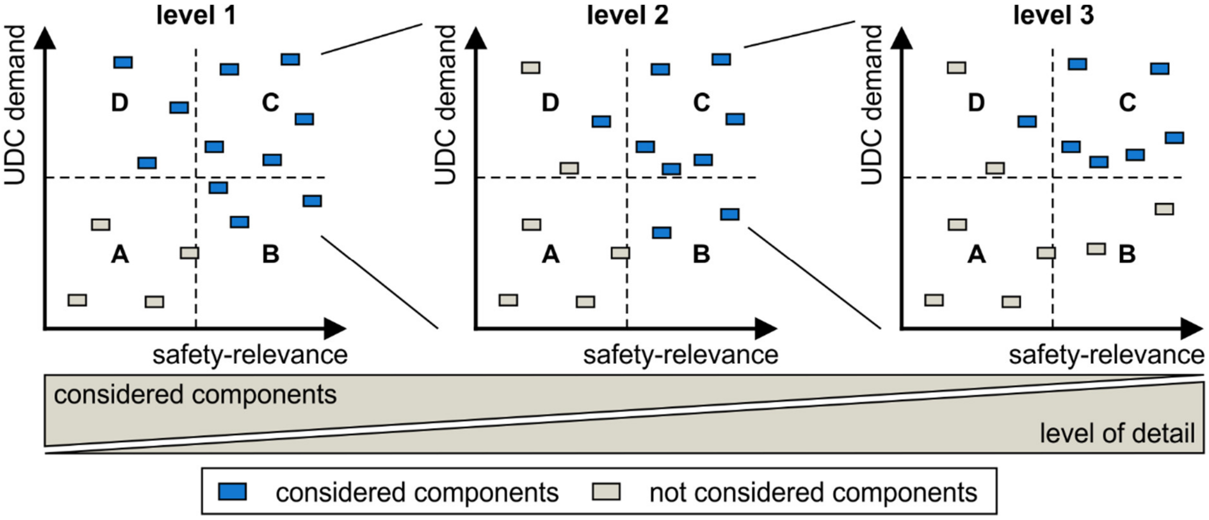
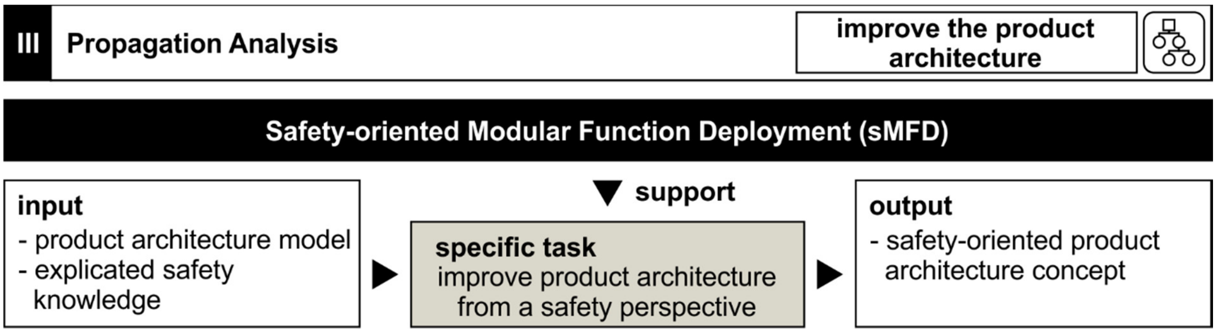


Figure 4-53: Iterative application of the UDC safety-relevance portfolio with increasing level of detail

Safety-oriented Modular Function Deployment (sMFD)

The safety-oriented Modular Function Deployment (sMFD) specifically supports the improvement of the product architecture in the ESMK's application case II (redesign for UDC). As Figure 4-54 summarizes, it uses an existing product architecture model and modeled safety aspects (i.e. safety requirements) stored in the ESMK knowledge framework or from other sources. Based on this, the safety-oriented Modular Function Deployment improves the product architecture. It moreover provides a safety-oriented product architecture. The sMFD is based on a student project (Kohl, 2015) and is published in Kohl, Roth, and Lindemann (2016).


III Propagation Analysis

improve the product architecture

Safety-oriented Modular Function Deployment (sMFD)

input
- product architecture model
- explicated safety knowledge

▼ support

specific task
improve product architecture from a safety perspective

output
- safety-oriented product architecture concept

Figure 4-54: Overview of the in- and outputs and the supported task of safety-oriented Modular Function Deployment

The **purpose** of the safety-oriented Modular Function Deployment is to improve product architectures from a safety perspective. Its **effect** is a module concept, which considers safety aspects and represents a safety-oriented architecture. This architecture clusters elements with similar safety restrictions in modules. It supports to form decoupled modules with limited impact on the product safety. The safety-oriented Modular Function Deployment, can be applied in **situations**, in which the efforts for safety analysis of products derived from a modular product portfolio need to be decreased or situations, when flexible modules (e.g. for customization) with limited impact on product safety need to be established.

Development of Support

The development of the safety-oriented Modular Function Deployment in its task clarification builds on a review of existing methods for modularization. Based on this review and the general ESMK requirements (see Subsection 3.4.2), the requirements on a support method were defined. They include general requirements on modularization methods identified within the review as well as specific requirements derived from the ESMK. The existing solutions were evaluated in respect of these requirements. Especially the demand for a safety-oriented architecture definition (*REQ2*) and for a support to balance safety and degrees of freedom (*REQ3*) provided major input. As the evaluation led to the conclusion that no existing approach satisfies the demands, the existing solutions were further analyzed for their adaptability. Based on this, the most suitable methods were selected, integrated, and adapted within the safety-oriented Modular Function Deployment. In the following, the development of the support is discussed in detail.

As described above, the **requirements on a modularization method**, which supports the safety-oriented improvement of product architectures, comprise two fields. The method has to fulfill general requirements on modularization methods as well as requirements addressing the inclusion of safety aspects. The resulting requirements and their sources are:

- establish a system understanding (from Daniilidis, Enßlin, Eben, and Lindemann (2011, p. 402) and *REQ5*)
- provide quantitative evaluation of module drivers (from Ericsson and Erixon (1999, p. 35) and *REQ5*)
- deliver suitable number of modules (from Ericsson and Erixon (1999, p. 37))
- consider safety as central driver for formation of modules (*REQ2*)
- include functional dependencies (from Koppenhagen (2014, pp. 121–122))
- build on functional structures (from Holtta and Salonen (2003, p. 536))
- consider the safety-relevance of functions (from Bishop and Bloomfield (1998, p. 201) and *REQ3*)
- provide traceability and comprehension (from Blees (2011, p. 27) and *REQ5*)
- provide formation of independent modules (from Blees (2011, p. 11), *REQ2* and *REQ3*)
- provide possibility for adaptions (from *REQ4*)

In the last years, a large number of **modularization methods** with different foci was introduced (Holtta & Salonen, 2003, p. 533). According to Daniilidis et al. (2011, p. 402), the DSM, Function Heuristics (FH), the Modular Function Deployment (MFD) and the Design for Variety (DfV) are the most important. Their requirements fulfillment was assessed using a simple score assessment (Ehrlenspiel, 2009, p. 515). Figure 4-55 provides an overview of this assessment, which is briefly explained in the following.

The **DSM** is applied as modularization method by Pimmler and Eppinger (1994). It represents the decomposition of the system into elements and documents their interactions (e.g. spatial, energy or information). Depending on these interactions, the elements can be clustered into chunks, from which modules can be derived (Pimmler & Eppinger, 1994).

requirement	DSM	FH	MFD	DfV
establish system understanding	◕	◕	◕	◕
provide quantitative evaluation of module drivers	●	●	●	◑
deliver suitable number of modules	●	○	●	●
consider safety as central driver	●	●	○	◕
include functional dependencies	◔	○	◑	◑
build on functional structures	◔	○	◕	◔
consider the safety-relevance of functions	●	●	●	●
provide traceability and comprehension	○	○	●	◔
provide formation of independent modules	●	●	●	◑
provide possibilities for adaptions	●	○	●	○
total	29	19	32	22

○ not fulfilled (0)
◔ marginally fulfilled (1)
◑ partially fulfilled (2)
◕ mostly fulfilled (3)
● completely fulfilled (4)

Figure 4-55: Simple score assessment of established modularization methods based on the defined requirements

The evaluation of the DSM shows that its main strength is the condensed representation of functional dependencies, while the incorporation of safety parameters seems difficult. Moreover, the DSM has an important limitation in delivering a suitable number of modules. Yet, its traceability and adaptability are assessed positively. Nevertheless, extensive adaptions are needed to fulfill the complete set of requirements.

The **Function Heuristics** by Stone, Wood, and Crawford (2000) derive the modularization based on major flows in the functional structure. The connections between subfunctions are modeled by material, energy, and signal flows. Based on these flows, four heuristics provide suggestions to identify possible modules (Stone et al., 2000).

The flows not directly allow an integration of safety aspects and the evaluation of modules remains qualitative. In addition, traceability is limited due to the method's subjectivity. The Function Heuristics method is not able to meet the defined requirements on a level suitable for further adaptions.

Instead, the **Modular Function Deployment** by Ericsson and Erixon (1999) focuses on product strategic aspects and builds on a functional structure. It defines module drivers, which represent influences from various fields (e.g. development and design, manufacturing). For the modularization, the Modular Function Deployment relies on the module indication matrix (MIM). It quantitatively evaluates the influence of module drivers on the technical solutions and derives module candidates based on this evaluation (Ericsson & Erixon, 1999).

The Modular Function Deployment can consider safety aspects indirectly represented in the defined module drivers, but does not include functional dependencies in the modularization. While the formation of modules is clear and understandable, its traceability is not fully ensured. Nevertheless, the Modular Function Deployment provides potential for adaptions to integrate safety aspects directly.

The **Design for Variety** methodology by Martin and Ishii (2002) considers functional dependencies and the product strategy for modularization. It uses the general variety index and the coupling index to define decoupled product architectures with reduced redesign efforts (Martin & Ishii, 2002).

Through these indices, Design for Variety achieves reproducible quantitative results. In addition, the indices can be adapted to include safety aspects. However, the understanding of the system is limited due to the abstract character of the indices and a suitable number of independent modules is not guaranteed.

In summary, the Modular Function Deployment in the assessment in Figure 4-55 achieves the best score and provides adaption potentials. It was **selected as basis** to develop a modularization method, which fulfills the defined requirements. The method was adapted to integrate functional dependencies and specific parameters, which represent safety aspects.

To integrate functional dependencies, the ideas of Koeppen (2008) and Koppenhagen (2014) were adopted and the DSM was integrated into the Modular Function Deployment. Moreover, to include safety aspects, the original module drivers of the Modular Function Deployment were adapted to represent safety aspects and associated efforts. As the literature does not provide suggestions for specific drivers, the so-called safety categories were introduced as module drivers. They can be defined according to situation and product and for example, cluster safety requirements or different standards. In addition, the global safety-relevance was introduced as module driver. It can adopt the assessment of the UDC safety-relevance portfolio or consider safety integrity levels during the modularization. These adaptions of the Modular Function Deployment resulted in the method described in the following.

Provided Support (Safety-oriented Modular Function Deployment)

The safety-oriented Modular Function Deployment builds on the Modular Function Deployment and has a similar, but extended procedure. It comprises the four steps visualized in Figure 4-56, which are determine functional dependencies, analyze functional centralities, identify safety aspects and conduct modularization, as well as define modules.

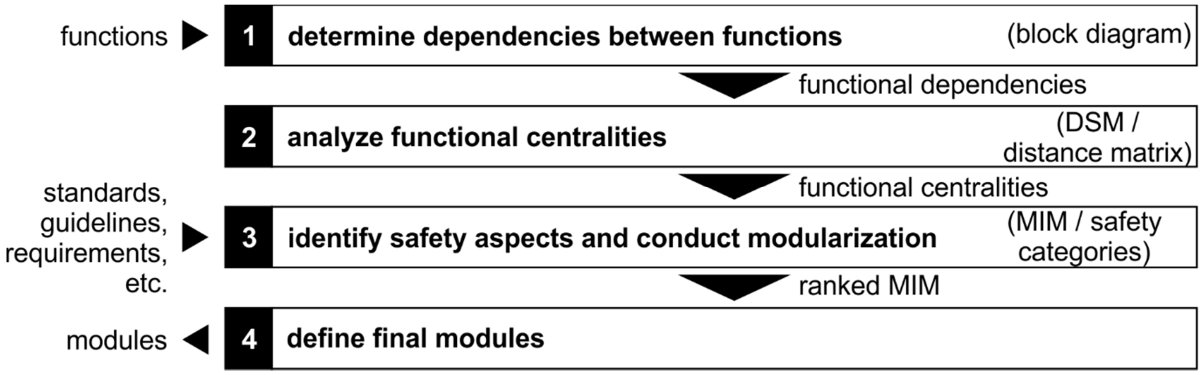
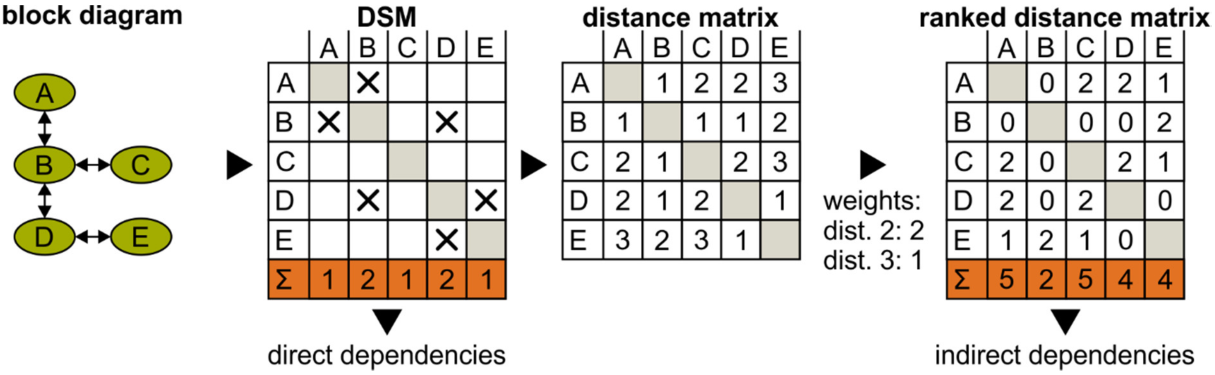

functions
1 determine dependencies between functions
(block diagram)
functional dependencies
2 analyze functional centralities
(DSM / distance matrix)
functional centralities
standards, guidelines, requirements, etc.
3 identify safety aspects and conduct modularization
(MIM / safety categories)
ranked MIM
modules
4 define final modules

Figure 4-56: Procedure and tasks of the safety-oriented Modular Function Deployment

The first step **determines the dependencies between functions**. If the ESMK knowledge framework is used, this information is already available. Otherwise, the functions have to be defined and converted into a functional structure. The safety-oriented Modular Function Deployment suggests to establish the functional structure through material, energy, and information flows, as proposed by Stone et al. (2000) and the ESMK's As-is Analysis (see Subsection 4.3.1). This results in a block diagram as shown in Figure 4-57, which is compliant with the knowledge framework. To cover a worst-case perspective, the safety-oriented Modular Function Deployment interprets dependencies as bidirectional (undirected graph).

The second task **analyzes the centralities in the functional structure**. The block diagram or the functional structure stored in the knowledge framework is translated into a DSM. Moreover, the DSM's distance matrix (Lindemann et al., 2008, p. 229) is derived. An example is given in Figure 4-57. The safety-oriented Modular Function Deployment then derives the centrality of the functions based on the number of direct and indirect dependencies. The direct dependencies are obtained through the active and passive sums of the DSM (Lindemann et al., 2008, p. 201). The indirect dependencies are derived from the distance matrix. There the distances of functional dependencies are aggregated in a weighted sum. Figure 4-57 exemplarily shows the weighted sum for the given weighting factors. Both centralities provide a rough estimation of the importance of a function within the functional structure. If a more detailed perspective is needed, other structural centrality metrics can be used (for a review see Biedermann (2015)).



DSM

	A	B	C	D	E
A		×			
B	×			×	
C					
D		×			×
E				×	
Σ	1	2	1	2	1

distance matrix

	A	B	C	D	E
A		1	2	2	3
B	1		1	1	2
C	2	1		2	3
D	2	1	2		1
E	3	2	3	1	

ranked distance matrix

	A	B	C	D	E
A		0	2	2	1
B	0		0	0	2
C	2	0		2	1
D	2	0	2		0
E	1	2	1	0	
Σ	5	2	5	4	4

Figure 4-57: Determining the functional centralities in the safety-oriented Modular Function Deployment through a DSM and the distance matrix

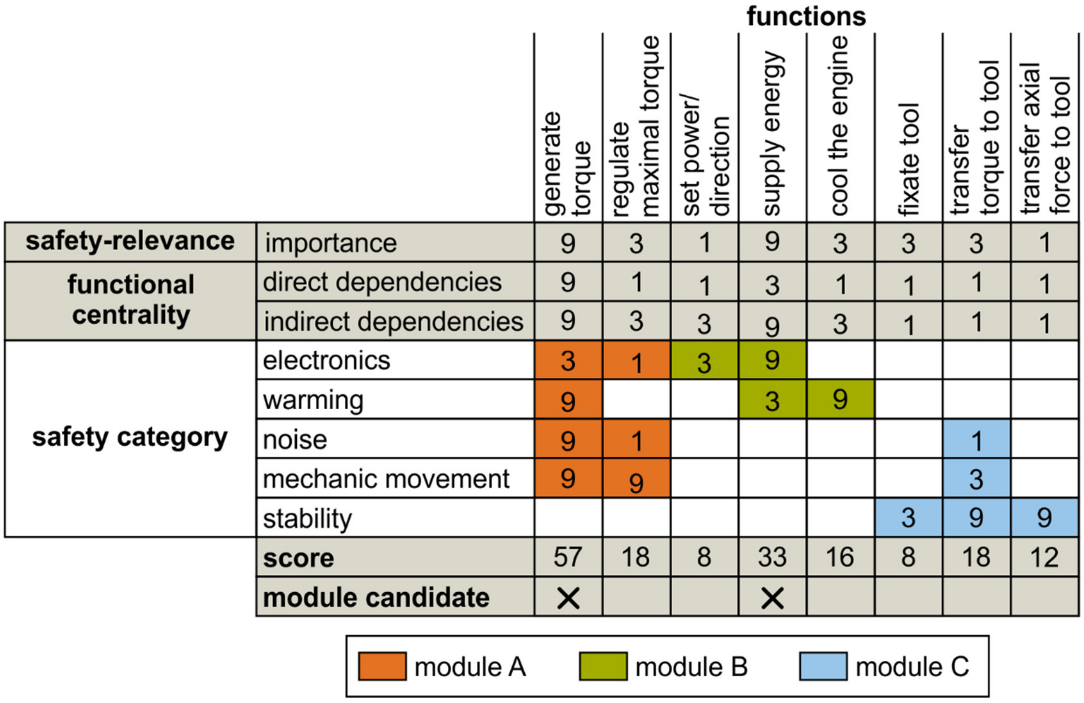
The third step of the safety-oriented Modular Function Deployment **identifies safety aspects** and combines them with the functional dependencies to conduct the modularization. It first defines the **safety-oriented module drivers**. As described above, the safety-oriented Modular Function Deployment suggests defining the functional centrality and safety-relevance as well as the identified safety categories as module drivers. They provide information on the importance of a function from a safety perspective and characterize its type of connection to safety aspects. Hence, they are suitable to determine the safety-oriented composition of modules.

The **module driver safety-relevance** is defined as general indicator for the importance of a function from a safety perspective. Examples for functions with a high safety-relevance are emergency functions. If other indicators like the safety integrity levels or protective classes exist, they also can be incorporated. If available, information from the knowledge framework, for example safety functions and connected hazards can be used as well. Moreover, the safety-relevance determined within the UDC safety-relevance portfolio (see above) can be used. The safety-relevance and the functional centralities both represent a module driver, which not directly influences the composition of modules. Instead, it helps to identify important module or platform candidates.

The **safety categories** define multiple module drivers. They are used as a representative of the safety requirements on the product. The safety categories are the main drivers determining the composition of modules. Similar safety requirements induce similar solutions, validation procedures or documentation requirements. To reduce the efforts connected with safety analysis, they should be clustered to modules to reduce resulting efforts and complexity. As the safety requirements and their impact vary for different products, the safety category module drivers are flexible and need to be adapted to the specific product and situation. The safety-oriented Modular Function Deployment suggests defining these safety categories as groups or clusters of similar safety requirements, standards, or guidelines.

Once all module drivers are defined, the safety-oriented Modular Function Deployment follows the original Modular Function Deployment and assesses the impact of the module drivers in the **safety-oriented module indication matrix**. The cumulated scores of each function help to determine the overall safety-criticality of a function. Same as the original Modular Function Deployment, the safety-oriented Modular Function Deployment clusters similar functions within the module indication matrix. As indicated in Figure 4-58, functions, which are similarly influenced by the module drivers, are grouped by colors. This process starts with the functions having the highest safety-criticality. Aligning with Ericsson and Erixon (1999), the suggested number of modules is approximately equal to the square root of the number of functions. In case of uncertainties during the module decision, information from the ESMK knowledge framework or the created DSM should be used to favor modules with a smaller number of interfaces. Furthermore, it has to be mentioned that clustering too many highly safety-critical functions in one module can result in enormous complexity and might not be a suitable concept.

The fourth step finalizes the safety-oriented Modular Function Deployment. It **defines the modules** based on the suggestions of the module indication matrix. For this definition, the functional modules need to be transferred to component-based modules. Moreover, this selection and definition of modules from a safety perspective has to be documented in a comprehensible form.



		functions							
		generate torque	regulate maximal torque	set power/ direction	supply energy	cool the engine	fixate tool	transfer torque to tool	transfer axial force to tool
safety-relevance	importance	9	3	1	9	3	3	3	1
functional centrality	direct dependencies	9	1	1	3	1	1	1	1
	indirect dependencies	9	3	3	9	3	1	1	1
safety category	electronics	3	1	3	9				
	warming	9			3	9			
	noise	9	1					1	
	mechanic movement	9	9					3	
	stability						3	9	9
	score	57	18	8	33	16	8	18	12
	module candidate	×			×				

🟧 module A 🟩 module B 🟦 module C

Figure 4-58: Example of a clustered safety-oriented module indication matrix with modules indicated by colors

In **summary**, the safety-oriented Modular Function Deployment provides support for the development of safety-oriented product architectures. It defines safety categories and uses them in connection with the safety-relevance and functional dependencies as drivers for the module composition. This modularization helps to cluster safety-relevant functions and decouple these modules from other functions. The resulting modules then provide the flexibility needed for UDC. Thus, the safety-oriented Modular Function Deployment supports the product architecture design and improvement tailored to UDC. However, the product architecture has to be balanced with other restrictions as for example, manufacturing, assembly, and variant management. Moreover, strategic decisions regarding UDC options also have to be considered during the development of the modular product architecture.

4.3.4 Phase IV: Individual Safety Analysis

This section describes the **last phase of the ESMK**, which is situated after the customization through the user (UDC). The Individual Safety Analysis aims at the safety analyses of the resulting individual product. In this phase, the ESMK relies on the knowledge framework and methods of previous phases. Hence, its contributions mainly represent a consolidation and processing of the existing knowledge. The following subsections provide an overview of the addressed tasks and the ESMK's contributions. In detail, the effect checklist as well as the individual adaptions of FMEA and FTA are introduced.

Overview on Tasks and Contribution Focus of the Individual Safety Analysis

The **Individual Safety Analysis** phase starts after the customization through the user is implemented in the UDC-toolkit. This phase in general aims to evaluate and analyze the safety impact of the conducted UDC. As indicated in Figure 4-59, this phase provides a checklist of the effects of these changes including affected safety requirements and validation procedures. The phase moreover conducts an individual safety analysis (FTA and FMEA) of the product, which considers the discrete user-induced changes. By that, the Individual Safety Analysis phase contributes to a more efficient safety analysis of the customized products (*REQ1*) and provides transparency and documentation (*REQ5*). Figure 4-59 summarizes the in- and outputs of this phase including the individual UDC as input from the UDC-toolkit.

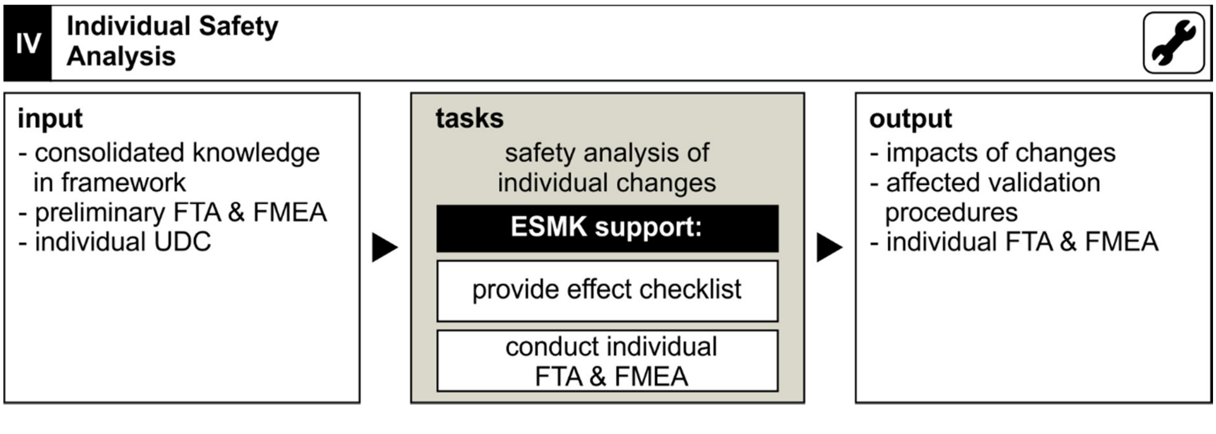

IV
Individual Safety Analysis
input
- consolidated knowledge in framework
- preliminary FTA & FMEA
- individual UDC
tasks
safety analysis of individual changes
ESMK support:
provide effect checklist
conduct individual FTA & FMEA
output
- impacts of changes
- affected validation procedures
- individual FTA & FMEA

Figure 4-59: Overview of the in- and outputs and supported specific tasks of phase IV (Individual Safety Analysis)

Broken down to **specific tasks**, the Individual Safety Analysis phase according to Figure 4-59 comprises the following two tasks:

- provide checklist of identified effects of the user-induced changes
- conduct and document individual FTA and FMEA

The user-induced changes through UDC can have an impact on various elements of the ESMK knowledge framework. At the current stage according to the focus-interviews (see Subsection 3.3.2), these impacts have to be manually evaluated, to identify if any safety constraints are violated. This process needs to be made efficient in terms of experience and time (*REQ1*). In addition, its documentation and traceability have to be improved (*REQ5*). It moreover is necessary to establish a link between safety-related aspects and the impacts within the product architecture (*REQ4*). To solve these challenges and to support the task of providing an overview of the potential effects, the ESMK provides an **effect checklist** to systemize and support the manual analysis of the possible impacts of the specific UDC.

While the impact of each change has to be analyzed, also the general safety analysis needs to be conducted for the individual product. This analysis has to prove either that the UDC has no impact on the product safety, or that the product remains safe even though an impact occurs. To solve the challenge of efficiency (*REQ1*), it is necessary to automate these methods as described in Subsection 2.3.3 at least partially and to reuse previous analyses. Hence, the ESMK supports the task of conducting an individual FTA and FMEA. It reuses the preliminary FTA and FMEA and integrates the user-induced changes in these analyses within the **individual FTA and individual FMEA**.

In the Individual Safety Analysis phase, the ESMK provides support methods to identify possible effects of user-induced changes as well as to conduct FMEAs and FTAs efficiently. These methods build on the previously introduced preliminary analyses and aim at specific purposes and situations. In other situations, other methods might be better suitable. The following paragraph provides a selection of **alternatives**.

Instead of the provided effect checklist, also commonly used requirement management tools can provide an overview of affected safety requirements by using the traceability of requirements. Moreover, the requirements verification and traceability matrix (Haskins, 2011, p. 91) can be applied to identify affected validation procedures. To conduct an individual model-based FMEA, the same alternatives apply as described in Subsection 4.3.3. For example, the individual changes can be translated into a SysML model and an individual FMEA can be derived using the method of Mhenni et al. (2014). Alternatively, the individual FMEA in specific situations can be derived from a metaFMEA as proposed by Höfig et al. (2014).

Effect Checklist

The effect checklist supports creating a checklist of effects of customized UDC-products and their individual user-induced changes. As Figure 4-60 summarizes, it uses the consolidated knowledge framework including the results of the model-based hazard and propagation assessment (i.e. the propagation tree) together with information on the changed components provided by an UDC-toolkit. Based on this, the effect checklist identifies and consolidates the potential impacts and propagations of the discrete user-induced changes in a structured form.

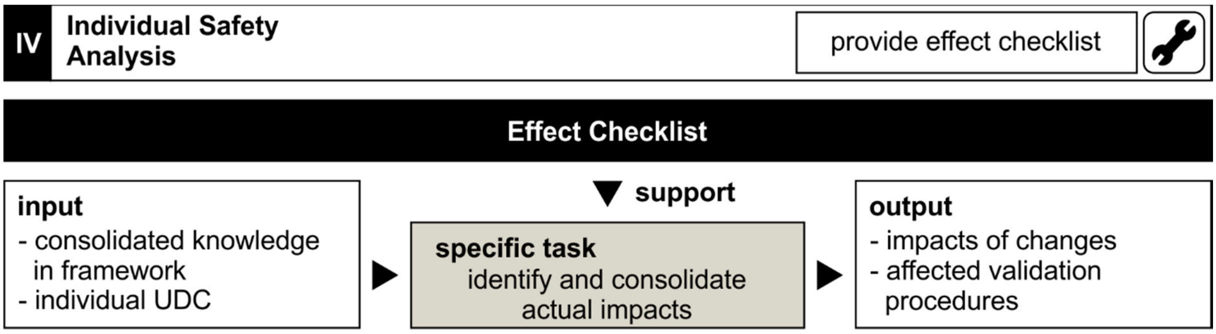

IV
Individual Safety Analysis
provide effect checklist
Effect Checklist
input
- consolidated knowledge in framework
- individual UDC
support
specific task
identify and consolidate actual impacts
output
- impacts of changes
- affected validation procedures

Figure 4-60: Overview of the in- and outputs and the supported task of the effect checklist

The **purpose** of the effect checklist is to prepare and condense data on potential impacts of changes. Its **effect** is a systematic overview of potential impacts and a guided procedure to analyze them. The effect checklist can be applied in **situations**, when the effects of an individual UDC or engineering change need to be evaluated comprehensively. It is suitable, when the comprehension of these impacts needs to be supported due to limited experience.

Development of Support

The development of the effect checklist mainly relies on principles of the model-based hazard and propagation assessment and its propagation tree. Hence, the task clarification was limited to the definition of requirements concerning the bundling and representation of the data. This resulted in the following two **specific requirements** on the effect checklist:

- consolidate all affected elements of the knowledge framework (*REQ1*, *REQ4,* and *REQ5*)
- allow for prioritization of analysis activities (*REQ1*)

Based on these requirements, the generation of a solution combined the principle of a checklist (Lindemann, 2009, p. 254) and the propagation tree of the model-based hazard and propagation assessment (see Subsection 4.3.3). Checklists were chosen as they are suitable to guide and support complex tasks and to ensure completeness (Lindemann, 2009, p. 254). This procedure is loosely based on a student project (Kowalski, 2016).

Provided Support (Effect Checklist)

The **effect checklist** uses the propagation tree of the model-based hazard and propagation assessment with an iterative procedure as a backbone to set up a checklist of occurring effects and influenced elements. Figure 4-61 depicts the iterative procedure based on the propagation tree. The procedure in its first step uses the information of the UDC-toolkit on manipulated components. For those components, it **establishes propagation trees** according to the model-based hazard and propagation assessment.

The actual solution to identify manipulated elements depends on the nature of the applied UDC-toolkit. For example, an UDC-toolkit, which uses a CAD system, can compare the structure trees and indicate parts with changes. Another option are specifically defined exchange formats for UDC. One example is the Extensible Markup Language (XML). An example of these XML-files is provided in the evaluation case (see Section 5.2). As input for the ESMK, the information on changed components can be extracted from these formats.

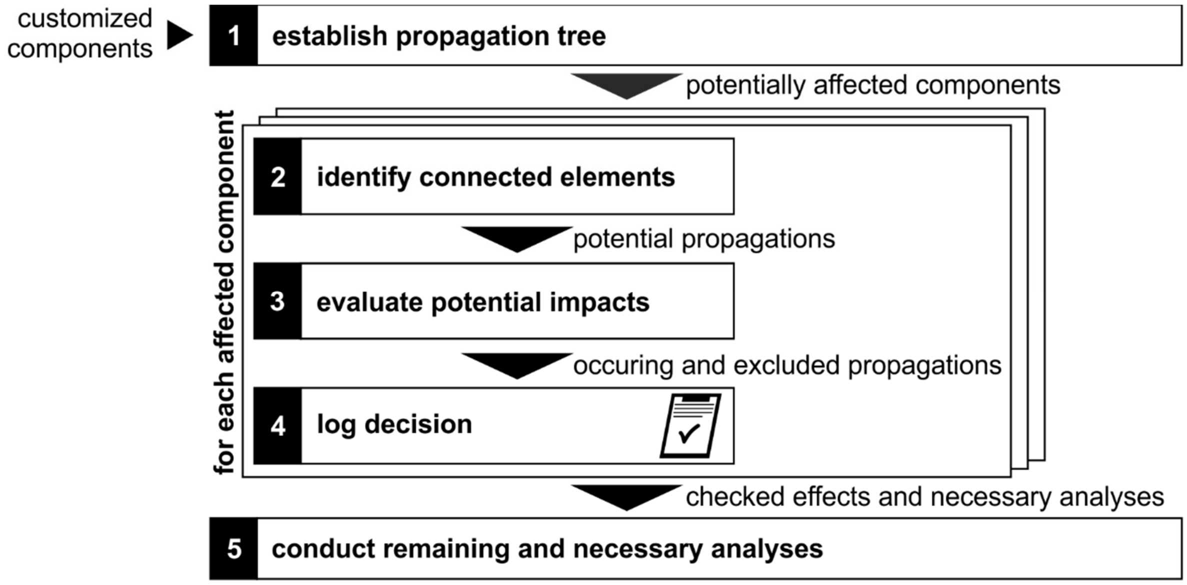
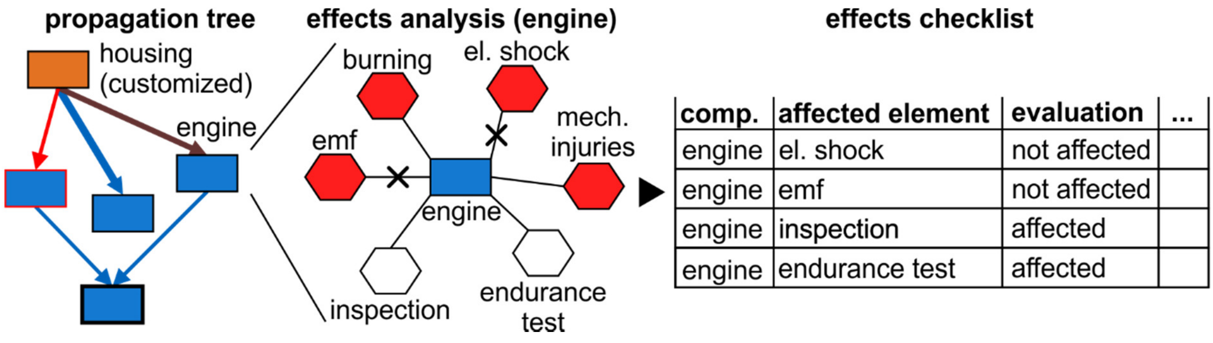

customized components
1 establish propagation tree
potentially affected components
for each affected component
2 identify connected elements
potential propagations
3 evaluate potential impacts
occuring and excluded propagations
4 log decision
checked effects and necessary analyses
5 conduct remaining and necessary analyses

Figure 4-61: Procedure of the effect checklist

In the second step, the customized component with the highest safety-relevance is used as a starting point and **its connected elements are identified** as shown in Figure 4-62. These elements are primarily safety requirements, hazards, and especially tests and validation procedures. The identified connected elements are manually **evaluated** if the user-induced change at the considered component affects them. Once all directly affected elements are analyzed in an iterative manner, the component at the closest distance in the propagation tree is selected next. First, the actual occurrence of the propagation is analyzed. If it can be excluded, the whole branch of the propagation tree is cut. Otherwise, the effect on the elements connected to the considered component is again analyzed. These steps are iteratively repeated until the whole propagation tree is evaluated or the last branch is cut. Then, the procedure is analogously repeated for the next customized component.

To ensure the traceability, all **decisions are logged** into the actual effect checklist. If an impact is excluded, this decision is documented in the checklist. If not, the checklist provides the basis to guide and plan further analyses or further required validation activities. This resulting checklist and the analysis of a specific affected component are visualized in Figure 4-62.



comp.	affected element	evaluation	...
engine	el. shock	not affected	
engine	emf	not affected	
engine	inspection	affected	
engine	endurance test	affected	

Figure 4-62: Example of the effect checklist procedure for the engine of the cordless screwdriver with a customized housing

In **summary**, the effect checklist consolidates the knowledge acquired during the first three phases of the ESMK and uses it to guide the analysis of the impacts of user-induced changes efficiently. By that, it supports the efficiency of the safety-oriented analysis of individual UDC products. Hence, it not only prepares the individual FMEA and FTA but also efficiently documents the analysis of the customized products.

Individual FTA and FMEA

The individual FTA and FMEA support the task of conduction the safety analysis of the customized products. As Figure 4-63 summarizes, it relies on the consolidated knowledge within the ESMK knowledge framework and information of the customization provided by an UDC-toolkit. Moreover, it reuses the preliminary safety analyses described in the Propagation Analysis (see Subsection 4.3.3). In combination with the effect checklist, the preliminary FTA and FMEA build the base to create the final safety analyses and the corresponding documentation for the customized product.

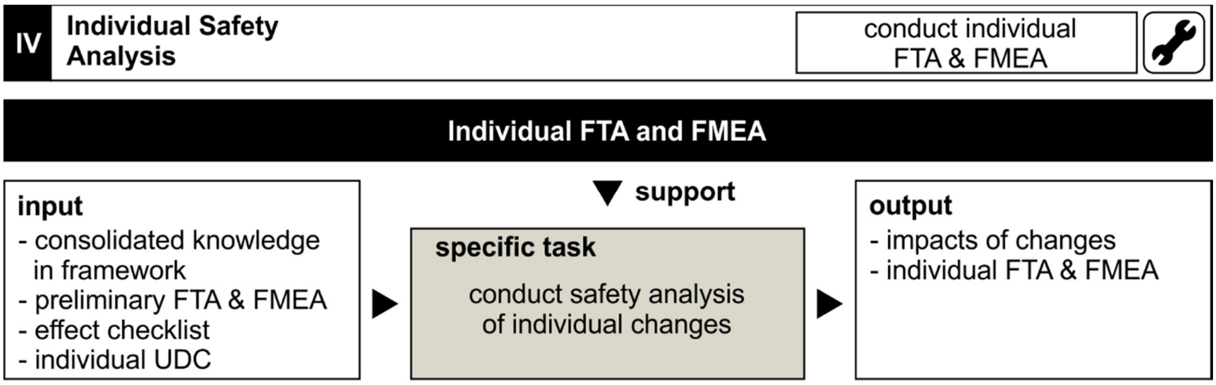


Figure 4-63: Overview of the in- and outputs and the supported task of the individual FTA and FMEA

The **purpose** of the individual FTA and FMA is to conduct safety analyses of an individual UDC product efficiently. Their **effect** is a safety analysis specifically incorporating the user-induced changes, which is reused. The individual FTA and FMEA are applied in **situations**, when an individual UDC or change occurs and a safety analysis needs to be conducted efficiently. They require a previously conducted preliminary analysis.

Development of Support

The development of the individual FTA and FMEA strongly relies on the principles of the multi-hierarchy fault tree generation and evaluation and the preliminary model-based FMEA introduced in Subsection 4.3.3. Thus, no further task clarification is necessary, as the only requirement is to indicate and highlight the impact of the user-induced change within the existing analyses. Hence, the basic methods are adopted and combined with the idea of the effect checklist introduced above.

Provided Support (Individual FTA and FMEA)

As described above, the **individual FTA and FMEA** use the results of the multi-hierarchy fault tree generation and evaluation and the preliminary model-based FMEA. They are manually completed and stored in the ESMK knowledge framework. Relying on these basic safety analyses, the individual FMEA and FTA have two steps. First, to identify changed elements and second, to indicate and prioritize effects in the knowledge framework. The identification of manipulated elements follows the same principle like the effect checklist (see above).

Using information on customized components from the UDC-toolkit, the **individual FTA** reuses the fault trees obtained through the multi-hierarchy fault tree generation and evaluation (see Subsection 4.3.3). It highlights the affected faults in the trees and the FTA-portfolio. As shown in Figure 4-64, the affected failures as well as their branches to the top event are highlighted in red. Moreover, the affected failures are marked in the FTA-portfolio. This helps to prioritize subsequent manual analysis activities according to the combined severity of affected failures.

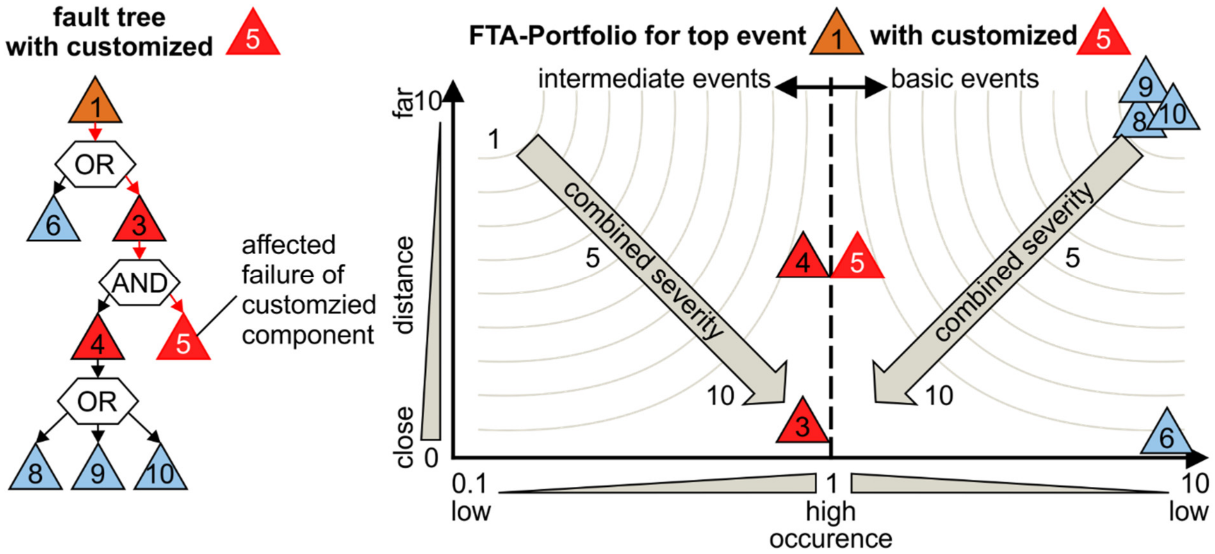
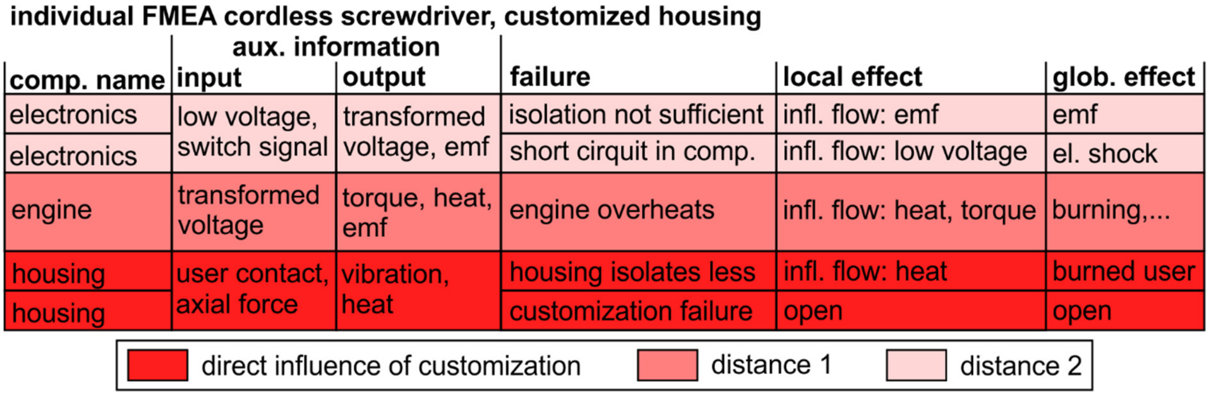


Figure 4-64: Example of an individual FTA including the fault tree (left) and the FTA-portfolio (right)

Analogue, the **individual FMEA** reuses the FMEA-form obtained from the preliminary model-based FMEA (see subsection 4.3.3) combined with information on affected elements (i.e. failures). The failures with direct impact are highlighted with red rows. For indirect failures, the highlighting color is faded with increasing distance. This helps to prioritize the manual analyses and to exclude possible indirect effects. Figure 4-65 visualizes the resulting FMEA-form. Moreover, the specific failure mode for failures induced by customization (introduced in the preliminary model-based FMEA) supports to consider all potential effects of the user-induced changes.

In **summary**, the individual FTA and FMEA reuse the knowledge obtained through the preliminary analyses in the Propagation Analysis phase of the ESMK to support the safety analysis of customized products. They combine the stored knowledge with the actual induced changes and condensate both in a supportive format. This efficiently prepares the manual analysis and through the included worst-case perspective ensures completeness. By that, customized UDC products can be analyzed efficiently through analysis support and reuse of data from the ESMK knowledge framework.



individual FMEA cordless screwdriver, customized housing

	aux. information				
comp. name	input	output	failure	local effect	glob. effect
electronics	low voltage, switch signal	transformed voltage, emf	isolation not sufficient	infl. flow: emf	emf
electronics			short cirquit in comp.	infl. flow: low voltage	el. shock
engine	transformed voltage	torque, heat, emf	engine overheats	infl. flow: heat, torque	burning,...
housing	user contact, axial force	vibration, heat	housing isolates less	infl. flow: heat	burned user
housing			customization failure	open	open

🟥 direct influence of customization ▨ distance 1 □ distance 2

Figure 4-65: Example of an individual FMEA-form for the cordless screwdriver with customized housing

4.4 Summary of the Efficient Safety Method Kit's Contribution

The ESMK introduced in the previous sections aims to support the safety analysis and balancing of UDC products and to reduce the overall efforts to ensure the safety of each individual product. It provides a set of methods and tools organized in four phases, which is based on a common knowledge framework. To achieve the defined objectives and especially to enable the balancing of UDC options and connected safety efforts, the ESMK aims at a better understanding of the consequences and impacts of UDC on the safety of the product.

The first three phases of the ESMK follow this objective by establishing a product model and providing model-based analyses of potential customizations and their impact on safety. By that, the **decision on UDC options is prepared**. This includes the identification of UDC options, which result in high safety analysis efforts as well as the evaluation of trade-offs.

One of the ESMK's main contributions is a **support to make safety aspects explicit** and create a model uniting the perspectives of safety and design. The ESMK aims to **reduce the efforts of subsequent analyses** in terms of time and experience by making implicit expert knowledge transparent and accessible.

Based on this accessible knowledge, the second main contribution of the ESMK are **partially automated analyses** of potential change propagations, as well as partially automated FTAs and FMEAs. With these methods, the ESMK aims to reduce time and experience needed to conduct these analyses as well as it improves transparency. The ESMK thus supports the evaluation of potential UDC options. This contribution is the main enabler for the balancing of UDC options prior to the actual customization. In addition, the ESMK contributes to the improvement of the product architecture to reduce the safety impact of UDC options.

In its fourth phase, the ESMK aims to **decrease the efforts of safety analysis and assurance of a defined set of UDC options**. Its main contribution is the reuse of the previously created preliminary analyses and knowledge in order to reduce manual efforts and efficiently prepare and guide the remaining manual activities.

In **summary**, the ESMK provides a set of tools and methods, which supports the modeling and analysis of UDC products as well as their safety analysis. It mainly aims at a reduction of involved efforts and required experience. This applies for both, the evaluation and definition of UDC options under the awareness of their impact on product safety, and the reduction of the connected efforts by reducing the safety impact of UDC options and improving the efficiency of the individual analyses.

5. Evaluation

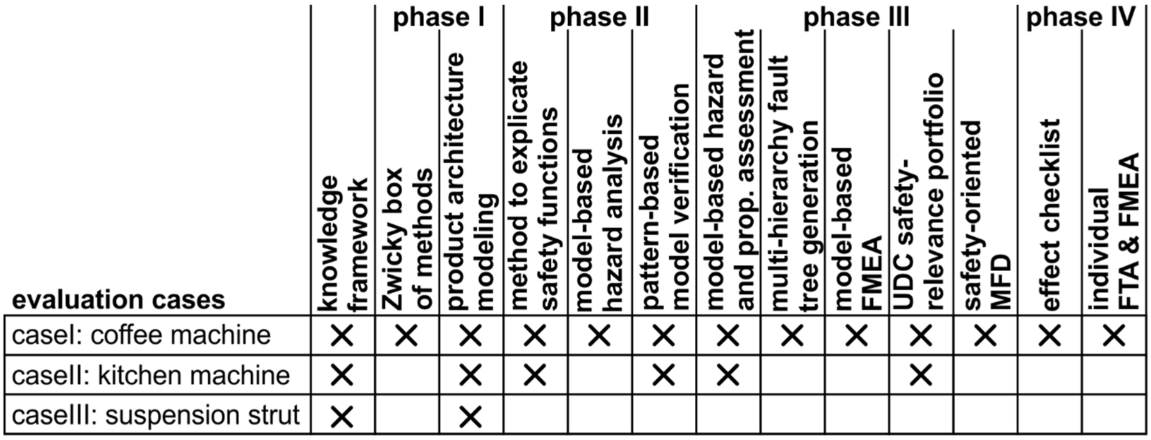
This section evaluates the ESMK developed in the previous chapter. Section 5.1 introduces the evaluation concept, while the three evaluation cases are discussed in Sections 5.2 to 5.4. Finally, Section 5.5 merges the findings and evaluates the ESMK from a holistic perspective.

5.1 Evaluation Concept

In Subsection 5.1.1, this section first introduces the methodology to evaluate the ESMK developed in the previous chapter. Moreover, it describes in Subsection 5.1.2 how the major support methods are implemented in a software application, which is used in the evaluation cases to set up the knowledge framework and apply the methods.

5.1.1 Evaluation Methodology

The ESMK and its support methods are evaluated in a combined application and success evaluation within multiple industrial cases, in conformance with Blessing and Chakrabarti (2009) and the defined research type (see Section 1.4). Figure 5-1 provides an overview of these cases, which consist of one main case (case I) and two auxiliary cases (case II and III). As the UDC concept for all cases is not yet fully realized, the evaluation remains at an initial stage and further activities are required once the products are transferred to UDC.



		phase I		phase II			phase III					phase IV	
evaluation cases	knowledge framework	Zwicky box of methods	product architecture modeling	method to explicate safety functions	model-based hazard analysis	pattern-based model verification	model-based hazard and prop. assessment	multi-hierarchy fault tree generation	model-based FMEA	UDC safety-relevance portfolio	safety-oriented MFD	effect checklist	individual FTA & FMEA
caseI: coffee machine	X	X	X	X	X	X	X	X	X	X	X	X	X
caseII: kitchen machine	X		X	X		X	X			X			
caseIII: suspension strut	X		X										

Figure 5-1: Overview of industrial cases and evaluation activities

The **application evaluation** assesses if the developed ESMK is usable and addresses the key factors defined as general requirements in Subsection 3.4.2 (Blessing & Chakrabarti, 2009, pp. 184–185). The knowledge framework of the ESMK and its methods and tools were applied in three industrial cases as shown in Figure 5-1. All elements of the ESMK were applied to the main use case of a fully-automatic coffee machine. Moreover, the methods providing the major contribution of the ESMK were applied to a kitchen machine of the same company. This second use case specifically aims to reflect reuse and connected efficiency aspects. In addition, the knowledge framework with specific focus on the requirements and the tracing of dependencies was evaluated using the case of a subsystem of a motor cycle (suspension strut).

The **success evaluation** assesses the usefulness of the ESMK as a whole. It examines if the ESMK is able to provide a suitable solution to the research question defined in Section 1.3 (Blessing & Chakrabarti, 2009, p. 185). As described above, the concept of UDC is not yet successfully applied to commercial products due to the various restrictions and challenges. Thus, the success evaluation remains initial and assumptive. Nevertheless, the coffee machine provides a thoroughgoing use case, which allows the evaluation of the ESMK as a whole. The kitchen machine originates from the same company, so that it can be included in the success evaluation as well.

The application and success evaluation is conducted in an integrated manner and is described for each case in Sections 5.2 to 5.4. The description of these cases focuses on the individual evaluation of the ESMK. The findings of all three cases are merged to evaluate the ESMK from a holistic perspective (Section 5.5).

5.1.2 Implementation of Tool Support (The EfficientSafety-Application)

The improvement of efficiency is a major requirement on the ESMK. Thus, many of the ESMK methods automate analysis tasks or workflows. To apply these methods, a tool support is required. Moreover, it is necessary to implement a software support, which establishes the knowledge framework and based on this supports the application of the methods.

The ESMK knowledge framework relies on typed attributed graphs and graph-rewriting. The knowledge framework and a large part of the software support were therefore implemented in the **EfficientSafety-application** using the software tool Soley Studio Professional 2.7[15] (Soley). It uses the programming system GrGen.NET (Jakumeit, Buchwald, & Kroll, 2010) and provides an environment to define individual typed attributed graph meta-models and graph-rewriting rules. These rules can be applied within sequences and are visualized in a graphical environment. Soley allows integrating these rules and sequences in executable workflows and assembles them in an executable application.

In addition to Soley, Microsoft Excel extended through VBA scripts was used to support the application of the multi-hierarchy fault tree generation and evaluation. An interface provides the possibility to exchange data of the knowledge framework between the two tools. Moreover, the SysML-profile of the model-based hazard analysis was realized using the SysML modeling tool Magic Draw 17.0.5[16]. Figure 5-2 in summary provides an overview for which element of the ESMK, which tool is used.

The implemented Soley support is assembled in the EfficientSafety-application. It defines the specific meta-model according to the ESKM knowledge framework defined in Section 4.2. Based on this, it provides a total **set of 26 workflows** structured in seven groups. These groups are listed and briefly described in the following.

[15] Source: https://www.soley.io/en/pr-soley-studio/, last access: 2016/09/29

[16] Source: http://www.nomagic.com/products/magicdraw.html, last access: 2016/09/29

		phase I		phase II			phase III					phase IV	
tool support	**knowledge framework**	**Zwicky box of methods**	**product architecture modeling**	**method to explicate safety functions**	**model-based hazard analysis**	**pattern-based model verification**	**model-based hazard and prop. assessment**	**multi-hierarchy fault tree generation**	**model-based FMEA**	**UDC safety-relevance portfolio**	**safety-oriented MFD**	**effect checklist**	**individual FTA & FMEA**
Soley (EfficientSafety-application)	×		×	×		×	×	×	×	×		×	×
MS Excel								×					
MagicDraw					×								
none		×									×		

Figure 5-2: Overview of the implemented tool support for the ESMK

The first and general group supports the visual modeling and handling of the graph by providing navigation and highlighting functions. The second group provides workflows to import all necessary data elements in the knowledge framework. Additionally, a set of workflows is provided, for each phase of the ESMK.

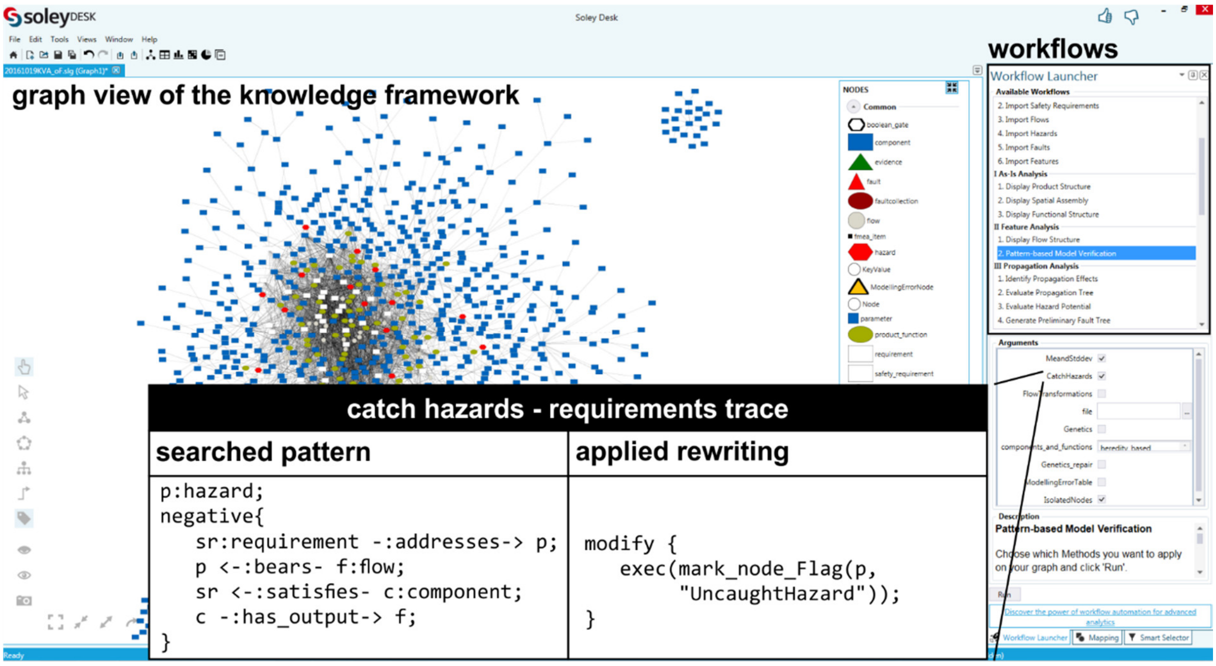
To support the modeling of the product architecture in the As-Is Analysis, the application offers workflows to extract and display the hierarchical decomposition of functions and structures. Moreover, one workflow extracts the spatial assembly of the modeled product.

The workflows of the Feature Analysis on the one hand support to switch between the regular structure of the ESMK knowledge framework and the flow-oriented structures required by the method to explicate safety functions. On the other hand, the pattern-based model verification workflow implements and conducts all selected automatic verification principles defined in Subsection 4.3.2.

The group of workflows for the Feature Analysis provides a workflow to identify propagations according to the model-based hazard and propagation assessment as well as workflows deriving the propagation trees and hazard potential portfolios. Two further workflows support the multi-hierarchy fault tree generation and evaluation and the model-based preliminary FMEA. In addition, three workflows use the information from the knowledge framework to draw the UDC safety-relevance portfolio on the three suggested levels.

Lastly, the workflows of the Individual Safety Analysis use the input from the UDC-toolkit to create the effect checklist and rely on the preliminary FTA and FMEA to highlight the impacts of customization within these analyses additionally. Moreover, a specific adapted group of workflows used in the third evaluation case is provided.

The final **user interface of the EfficientSafety-application** is exemplarily shown in Figure 5-3. It illustrates how the source code implements one of the generic graph-rewriting patterns of the pattern-based model verification introduced in Subsection 4.3.2. The implemented EfficientSafety-application provides a thoroughgoing support, environment, and visualization to apply the ESMK in the industrial cases described in the following.



Pattern-based Model Verification

Choose which Methods you want to apply on your graph and click 'Run'.

catch hazards - requirements trace

searched pattern	applied rewriting

`p:hazard;`
`negative{`
`   sr:requirement -:addresses-> p;`
`   p <-:bears- f:flow;`
`   sr <-:satisfies- c:component;`
`   c -:has_output-> f;`
`}`
	`modify {`
	`   exec(mark_node_Flag(p,`
	`         "UncaughtHazard"));`
	`}`

Figure 5-3: The user interface of the EfficientSafety-application and an exemplary excerpt of the source code

5.2 Evaluation Case I: Coffee Machine

This section describes the application of the ESMK to a fully-automatic coffee machine. The application covers the full range of ESMK methods and represents the central evaluation. First, Subsection 5.2.1 describes the product and situation. The application of the ESMK to this case is then summarized in Subsection 5.2.2. Finally, Subsection 5.2.3 draws a resume and evaluates the capabilities of the ESMK based on this case from a general perspective.

5.2.1 Description of Case I: Coffee Machine

The BSH Hausgeräte GmbH (BSH) with more than 50.000 employees offers a large bandwidth of home appliances under various brands[17]. Among those products, **fully-automatic coffee machines** are an important branch. Coffee machines are a popular lifestyle object and the company expects a demand for customization. Thus, the BSH consumer products (PCP) division in the project InnoCyFer[18] researches if and how UDC can be applied to their fully-automatic coffee machines. Object of the research is a high-end product, which in addition to brewing coffee provides a set of other functions like furthered milk and a pre-heating of mugs.

To prepare the product for UDC, BSH aims to **identify components, which provide potential for UDC** and to find a way, how the resulting **safety and approval efforts can be kept in an acceptable range**. The ESMK was applied to uncover the safety impact of UDC options and

[17] Source: http://www.bsh-group.com/index.php?page=100325&language=uk, last access: 2016/09/29

[18] Source: https://www.innocyfer.de/, last access: 2016/09/29

to provide an environment to increase the efficiency of the connected safety analyses. This situation mainly aligns with application case I (transfer to UDC) of the ESMK, but to generate ideas how the product in future developments can be optimized for UDC, application case II (redesign for UDC) was included in the analysis as well.

5.2.2 Application of the ESMK to a Coffee Machine

As described above, the complete ESMK was applied to the fully-automatic high-end coffee machine. The methods were applied by the author of this thesis and involved students. This was done supported by, and in discussion with the designers and safety analysts of BSH.

The results of all methods were evaluated with these subject-matter experts. The minor methods of the ESMK were evaluated in an open discussion, while the central methods were systematically evaluated using a questionnaire. The following paragraphs describe the application of each method using the EfficientSafety-application (see Subsection 5.1.2) as well as the results of the evaluation.

Phase I: As-Is Analysis

The ESMK provides two support methods for the As-Is Analysis phase (see Subsection 4.3.1). These are the Zwicky box of methods to elicit safety requirements and validation procedures as well as a collection of methods to model the product architecture.

Based on the **Zwicky box of methods**, an exemplary set of requirements was identified and modeled within the ESMK knowledge framework. These requirements for example address maximal surface temperatures of the housing or protection classes of electric components. The most important standards (IEC 60335-1; IEC 60335-2-15) were used as source and the relevant information was extracted through manual reading. A hybrid form was used as documentation, which combines the graph-based representation of the knowledge framework and the textual description within the attributes of the requirement nodes. The validation procedures were derived from the standard and mainly are manual inspections or tests.

To **model the product architecture**, existing data was used as primary source. The components of the coffee machine were imported from the bill of material using the import workflows of the EfficientSafety-application. In addition, geometrical contacts between parts were derived from a CAD model. For the functions, an existing model of their hierarchical decomposition was used and adapted. To model flows, the physical product and the CAD model were analyzed. This resulted in a product model consisting of a total of 808 components, 17 flows, 53 functions, and 160 safety requirements. To handle the huge amount of components, the black-box principle was used to reduce the number of components to 106. The resulting graph of the knowledge framework is visualized in Figure 5-4. The figure also provides an excerpt of the hierarchical component structure of the coffee outlet assembly.

Both above-described methods only represent a minor contribution of the ESMK. Their **evaluation** was reduced to a short open discussion based on the resulting model. The discussion revealed that the ESMK improves the transparency of the model and its origin. However, this state does not allow drawing further conclusions.

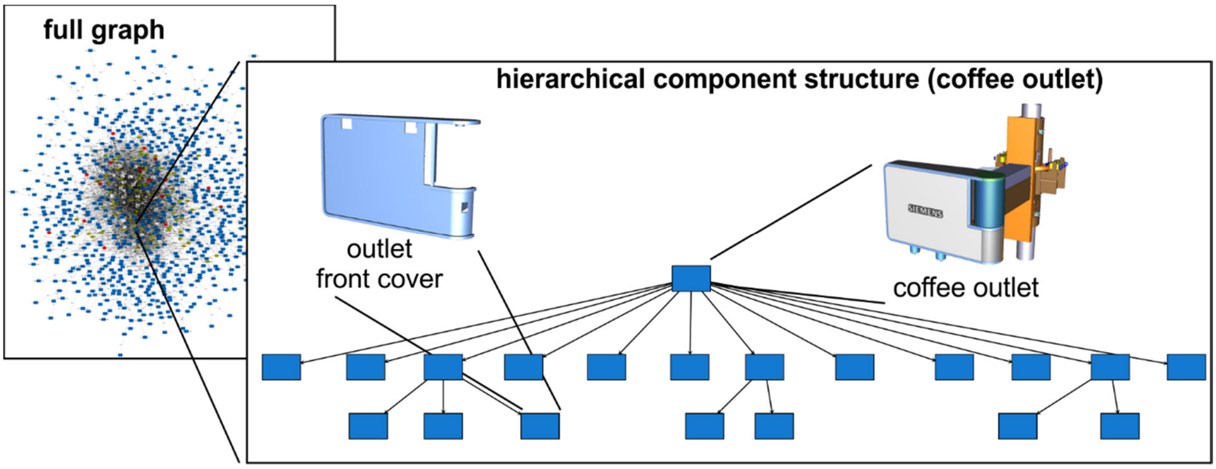


Figure 5-4: The product architecture model and the hierarchical component decomposition of the coffee outlet.

Phase II: Feature Analysis

In the Feature Analysis (see Subsection 4.3.2), the ESMK provides the method to explicate safety functions and the model-based hazard analysis as support. Moreover, the pattern-based model verification supports all modeling activities of the first two phases of the ESMK.

The **method to explicate safety functions** was applied building on the model described above. Due to the ESMK knowledge framework, the method's preparation step was limited to the definition of the lowest abstraction level, which is included in the analysis. Moreover, a list of 16 potential hazards was identified based on the safety requirements derived from the standards (see above) and the knowledge of the BSH safety analyst. The ESMK knowledge framework mostly covered the second step as well. The only remaining task was to classify the modeled flows into 1D- and 3D-flows. As indicated in Figure 5-5, the relevant flows of the coffee outlet are steam/beverage (1D), heat (3D), and the abstract user contact.

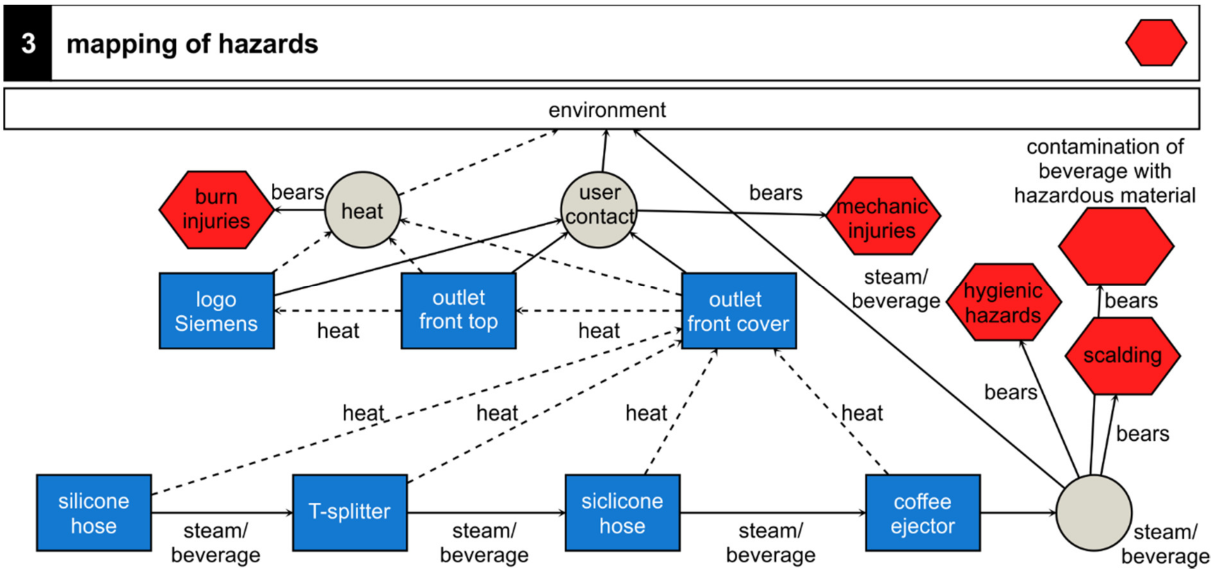


Figure 5-5: Classification of flows and mapping of hazards of the coffee outlet assembly

In the third step, the hazards were assigned to flows and hazardous functions were derived. The assignment of hazards is exemplarily shown in Figure 5-5 as well. The identification of hazardous functions for the complete coffee machine resulted in 46 potentially hazardous functions within the 53 product functions.

In the fourth step of the method to explicate safety functions, 20 safety functions to prevent the modeled hazards were defined and assigned to their realizing components. Figure 5-6 indicates the resulting functional decomposition of the function “deliver beverage”, which mainly corresponds to the functions of the coffee outlet assembly. The safety functions include many functions, which in the functional decomposition are assigned to multiple parent functions. The reason is that multiple components realize the same safety function. For example, the function "avoid contamination of beverage with hazardous material" needs to be realized by all components involved in the coffee brewing and delivery process.

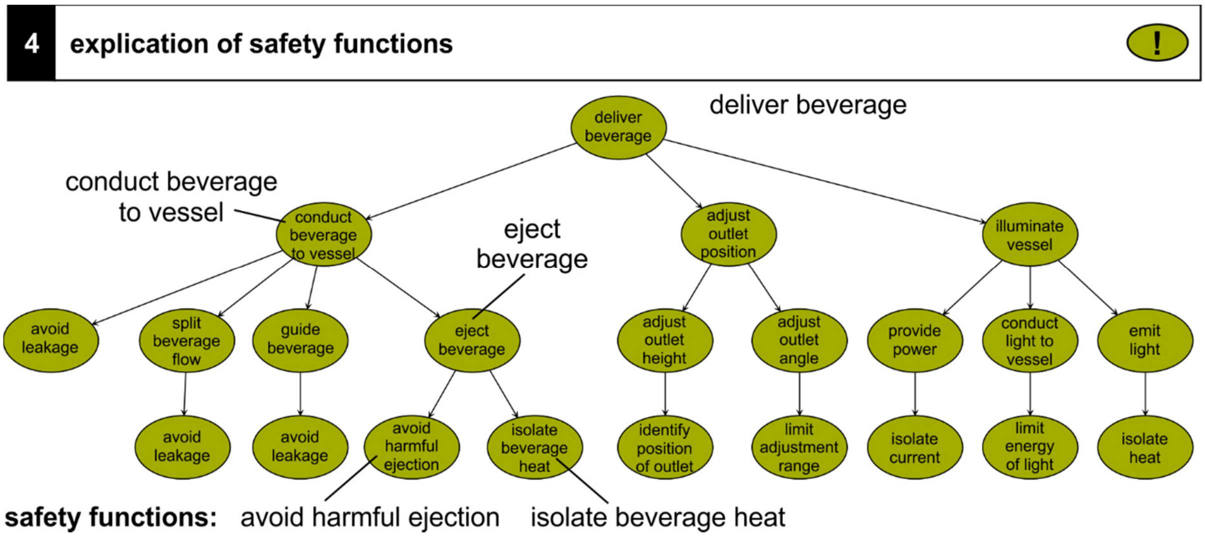


Figure 5-6: Functional decomposition with added safety functions of the coffee outlet assembly

The application of the method to explicate safety functions was **evaluated** within a workshop with a safety analyst and designers of BSH. Especially the differences between the resulting and the original functional structure of a prior product of the product line were discussed.

The basic subject of the discussion was, if the method and its results satisfy the requirements defined in Subsection 4.3.2. The discussion confirmed that the method to explicate safety functions supports the integration of safety aspects in the functional model and helps to make important safety aspects explicit, starting from the early phases of design. Moreover, the discussion showed that also the link of components to hazards and functions is successfully realized even though the modeling of abstract flows (i.e. user contact) is unusual. This aspect underlines the need for a support method to reduce the uncertainty within the model.

The discussion furthermore identified that the method improves the completeness of the model through explicit safety functions. The safety analyst expects an improved understanding of the designers in terms of safety (for example heating of housing components). In addition, the designers emphasized the advantage of safety functions integrated in the functional decomposition. While the old model treated safety functions as a separate branch in the functional decomposition, they now are integrated. As result, the decomposition has safe sub-branches and modules, which include all their necessary safety functions.

Moreover, a student applied the **model-based hazard analysis and its SysML-profile** to the coffee machine. She strictly followed the whole procedure defined in Subsection 4.3.2, which covers a complete model-based development, even though the considered product already existed. The modeling was not conducted within the EfficientSafety-application, but the information was transferred to SysML using MagicDraw and vice versa.

In the first stage of the model-based hazard analysis, the requirements have to be specified. In this case, they were directly extracted from the ESMK knowledge framework mainly relying on IEC 60335. In the next step, the use cases and misuse cases were derived. The analysis focused on the two main stakeholders user and service technician. Exemplarily derived misuses are wrong liquids in the water tank or removed and forgotten parts after cleaning.

In the second stage, a functional architecture was established starting from an abstract level. As described above, the application of the method assumed a new product development even though information on the actual architecture would have been available. The functional architecture was analyzed for potential hazards and malfunctions were inserted accordingly. An excerpt of the resulting diagram is given in Figure 5-7. It shows the function, which starts the water pump together with its two malfunctions. The first is that the pump is not started at all. The second is that a wrong volume stream is created. Moreover, safety functions were defined and compared to the safety functions defined in the knowledge framework. This evaluated the model-based hazard analysis in comparison to the method to explicate safety functions (see above). As exemplarily shown in Figure 5-7, the safety function "control pump volume" was integrated in the diagram to prevent the corresponding malfunction.

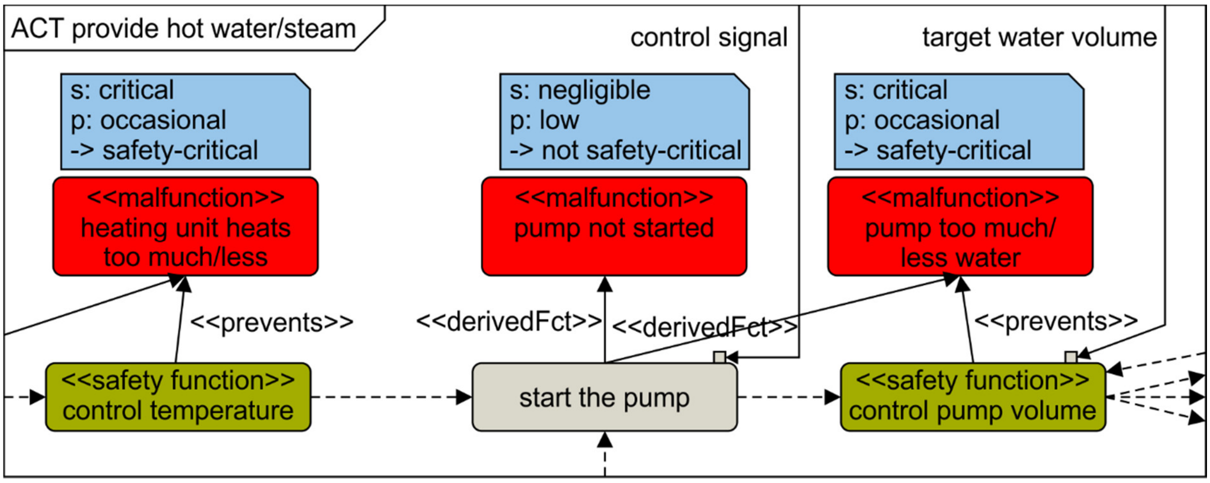

ACT provide hot water/steam
control signal
target water volume
s: critical
p: occasional
-> safety-critical
s: negligible
p: low
-> not safety-critical
s: critical
p: occasional
-> safety-critical
<<malfunction>> heating unit heats too much/less
<<malfunction>> pump not started
<<malfunction>> pump too much/ less water
<<prevents>>
<<derivedFct>>
<<derivedFct>>
<<prevents>>
<<safety function>> control temperature
start the pump
<<safety function>> control pump volume

Figure 5-7: Excerpt of the ACT "provide hot water/steam" created during the model-based hazard analysis

In the third stage of the model-based hazard analysis, the system architecture of the coffee machine was modeled accordingly. This included the definition of components in a BDD, the identification and allocation of hazards, and the definition of corresponding safety measures. Figure 5-8 shows an excerpt of the resulting system architecture corresponding to the functional architecture defined in Figure 5-7. It for example introduces the safety measure "pressure control" related to the above-depicted safety function "control pump volume".

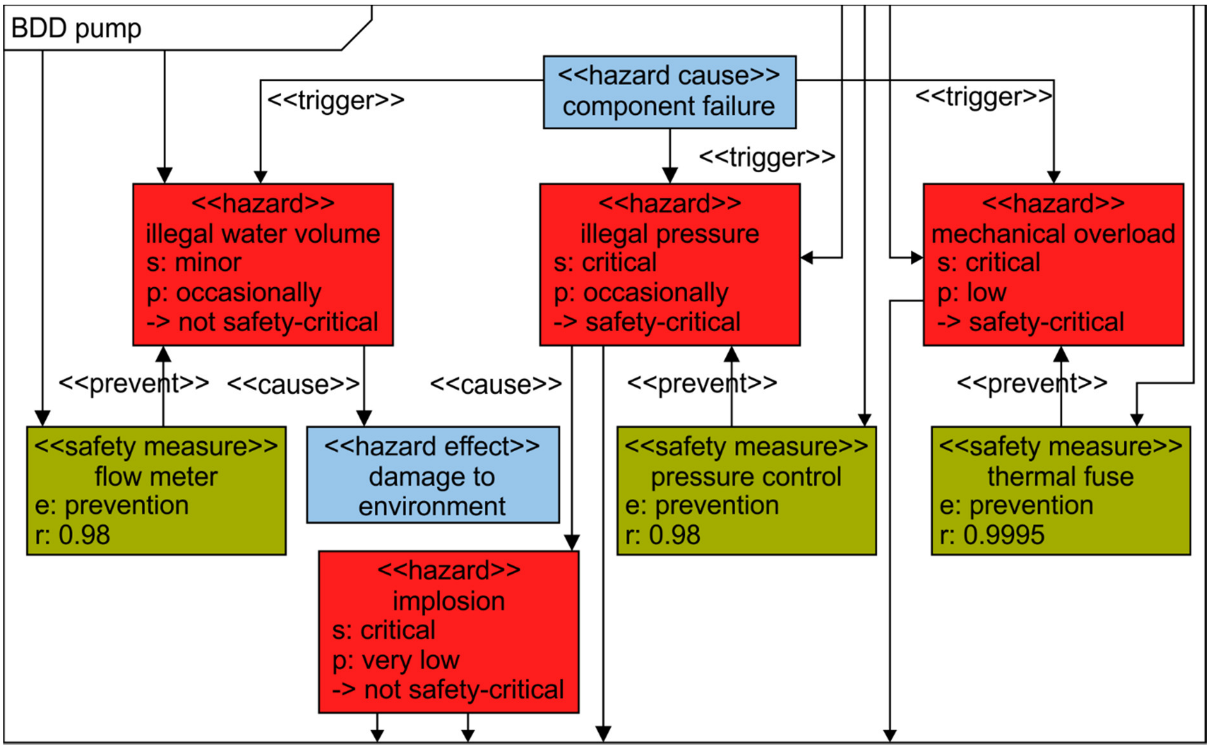


Figure 5-8: Excerpt of the BDD "pump" created in the model-based hazard analysis

The application of the model-based hazard analysis was **evaluated** primarily through a comparison of the results in the SysML model with the model of the ESMK developed together with the industrial experts.

This showed that the method successfully models use cases from a static point of view as well as the system architecture. The comparison moreover demonstrated that the method supports the identification and modeling of hazards together with their causes and effects. The annotations and tagged values provided additional traceability.

Transferred back to the ESMK knowledge framework, the discussion with the safety expert revealed the importance and the benefits of the inclusion of misuses into the ESMK through the model-based hazard analysis. Especially, the example of forgotten and removed parts after cleaning adds important safety aspects to the model. BSH currently prevents this risk through switches and specially adapted geometries.

The **pattern-based model verification** was applied at the end of the ESMK's second phase. The general principles selected in Subsection 4.3.2 and implemented in the EfficientSafety-application, were applied to the model of the fully-automatic coffee machine.

The pattern "isolated nodes" identified 94 nodes without any connections in the ESMK knowledge framework. These nodes were requirement nodes, which are not connected to any component. They for example address not applicable protection classes. Hence, the pattern-based model verification successfully identified not necessary elements in the model. In addition, the "genetics" pattern group identified 20 model errors. They all were traced back to a mismatch between the granularity of the functional and the structural model of the coffee outlet. This mismatch was analyzed and compensated manually.

The pattern group “flow-transformation” reported 18 model errors. These errors were mainly caused by implementation issues. The EfficientSafety-application only provides a pattern library for up to two in- and two outputs. Consequently, for components having more than two flows as in- or output, errors might be identified by mistake. Apart from these implementation issues, the application also detected valid errors. For example, as shown in Figure 5-9, an error for the reed switch was identified. In the original model, this switch consumed an energy flow and only produced an information flow. This constellation violates the law of the conservation of energy. Hence, an additional energy flow had to be added as additional output.

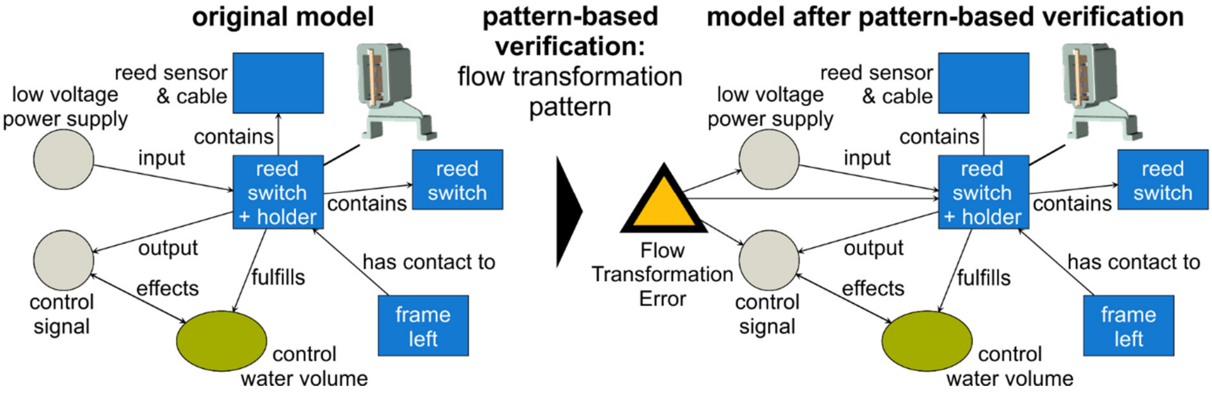


Figure 5-9: Reported error of the pattern-based model-verification for a flow transformation error (reed switch)

The “mean and standard deviation” pattern group identified 65 conspicuous components. A closer inspection showed that the identified components are central elements or add-on parts and are modeled correctly. Examples are the brewing unit (central) or the service interface (add-on). Lastly, the “ESMK-specific verification patterns” identified twelve hazards, which in the model created by the author of this thesis were not connected correctly. These model errors originate from the author’s limited experience. All errors were manually checked and fixed. In case of remaining uncertainty, the subject-matter experts of BSH were consulted. They in every phase of their development ensure that no safety aspects are neglected and based on this experience were able to resolve uncertainties concerning the modeling.

The application of the pattern-based model verification to the coffee machine **proved its contribution**. Even though the model was built carefully and in close cooperation with the designers and safety analysts, it contained errors. The method successfully identified these model errors, which then were fixed to improve the quality of the model. The manual analysis of the detected errors however showed that due to limitations caused by the implementation in Soley, the error detection is not completely reliable. As it rather detects too many errors, the improvement and completeness are ensured. However, the company experts emphasize that the defined patterns are not sufficient and additional and more specific patterns are needed to improve the model quality further.

Phase III: Propagation Analysis

To support the Propagation Analysis (see Subsection 4.3.3), the ESMK provides the model-based hazard and propagation assessment, the multi-hierarchy fault tree generation and evaluation, and the model-based preliminary FMEA. Moreover, the UDC safety-relevance portfolio supports the assessment of components and the safety-oriented Modular Function Deployment provides a safety-oriented modularization. The following paragraphs describe the application of all these methods to the coffee machine.

The **model-based hazard and propagation assessment** was applied to the model of the coffee machine stored in the ESMK knowledge framework. This analysis primarily focused on the parts identified and realized for customization within the cooperation project InnoCyFer. These components are the front cover of the coffee outlet and the dripping plate.

The necessary graph-based product model was obtained from the ESMK knowledge framework and the generic propagation patterns together with their pairwise comparison and derived likelihoods were adopted from Subsection 4.3.3. The identification of propagation patterns was conducted by the implemented EfficientSafety-application. It allows selecting, which of the generic patterns should be considered during the identification. The application calculates the relative distances and draws the resulting propagation trees as shown in Figure 5-10 in variable depth. The figure indicates the two components, which are most likely affected through a change propagation of the outlet front cover. Those are the outlet back cover (via geometrical and flow-based propagation) and the outlet front top (via geometrical, flow-based, and functional propagation). However, the figure illustrates that the visualization of a higher depth than two for complex systems can get overwhelming.

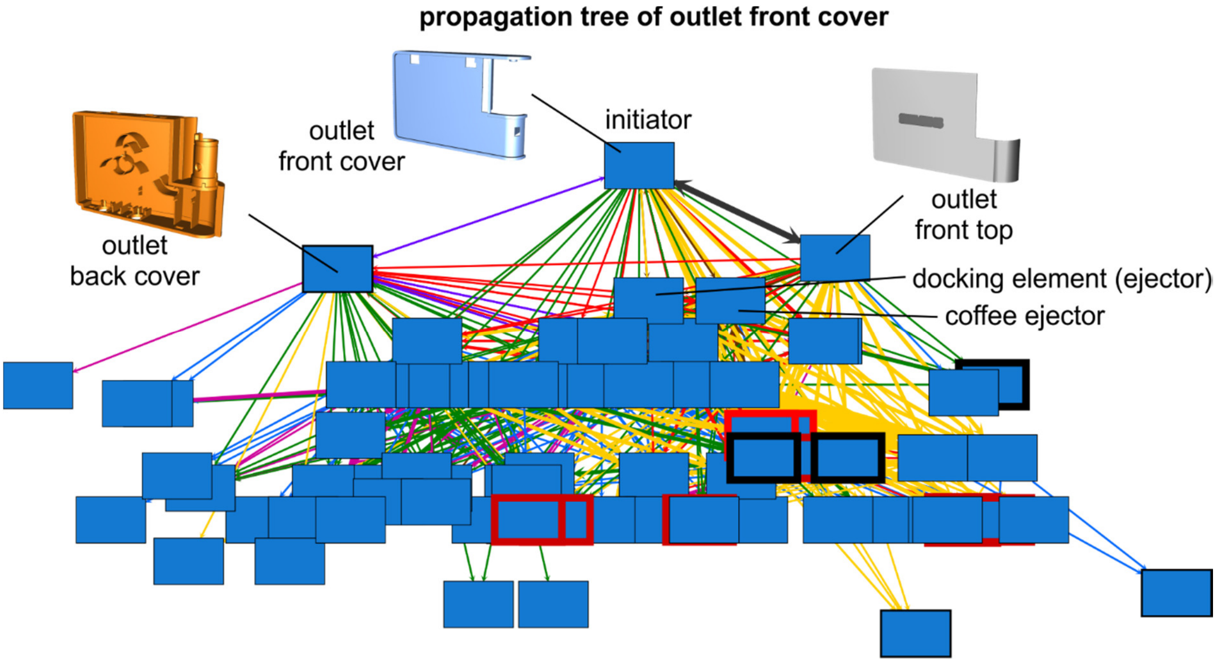


Figure 5-10: Propagation tree for the outlet front cover as initiator component

Analogue, the hazard potential analysis was conducted using the generic patterns defined in Subsection 4.3.3. A safety analyst of BSH manually assessed the hazard weights. Based on this assessment, the application identifies the affected hazards and visualizes them according to Figure 5-11 in the hazard potential portfolio. The figure shows that the outlet front top as potentially affected component is not safety-critical. It only impacts heat-related hazards with a middle weight. In reality, the heat originates from the beverage, so that temperatures, which trigger the hazards, cannot be reached. Only a minimal potential of mechanical injuries remains.

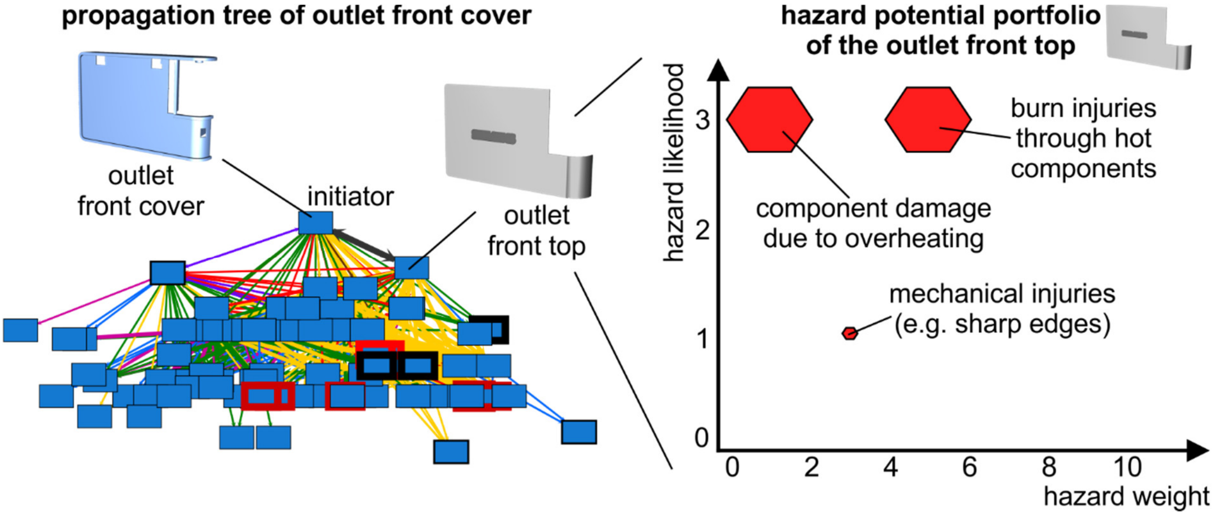


Figure 5-11: Propagation tree (left) and the derived hazard potential portfolio (right) of coffee outlet front cover

The results of the application of the model-based hazard and propagation assessment were discussed with the safety analyst to **evaluate** its capabilities. He assessed the capabilities of the method in a structured questionnaire and gave further feedback in an open discussion. The questionnaire (see Appendix 9.7.1) picks up the specific requirements on the method, defined in Subsection 4.3.3 and the general requirements on the ESMK (see Subsection 3.4.2). It assesses the fulfillment of the requirements on an adapted Likert-scale (McIver & Carmines, 1981, pp. 22–37). In general, the questionnaire addresses the following topics: efficiency, safety awareness and safety-oriented preparation, quality of the propagation analysis, as well as documentation and usability.

From the safety analyst's perspective, the model-based hazard and propagation assessment is not able to reduce time and manual efforts to analyze the effects of potential user-induced changes. He personally expects a 20 to 30 % increased effort. However, he in the discussion admits that this effect is connected with his immense experience. For less-experienced analysts and designers, he expects a decrease in efforts. This complies with his evaluation that the method reduces the amount of required experience.

Moreover, the expert is optimistic that the model-based hazard and propagation assessment increases the awareness for the effects of individual changes and simplifies the safety-oriented preparation of changes. He does not expect a simplification of the actual evaluation of safety aspects by the method and is neutral about its ability to influence the overall safety awareness.

Regarding the quality of the results, the analyst is quite sure that the method allows to at least identify the potential effects of changes and identifies rather too many than too less hazards. Simultaneously, he is quite critical that in every case all potential hazards are identified.

Additionally, he is confident that the method improves the traceability of the effects of individual changes and enables a fast and easy understanding of potential propagation effects. He disagrees that the visualization reduces the complexity to a manageable amount, which complies with the observations made during the application. Nevertheless, he expects a large advantage for the general documentation and the transparency of the connected analyses.

The **multi-hierarchy fault tree generation and evaluation** was applied based on the identified propagations using the model-based hazard and propagation assessment. The identified hazards were defined as top events. The EfficientSafety-application uses the propagations to compute the fault network tailored to UDC and extracts the fault trees for each top event. Due to implementation issues, the calculation of minimal cut sets and the evaluation of the fault trees was conducted by a VBA-script in Microsoft Excel. Figure 5-12 shows an excerpt of the fault tree corresponding to the hazard "burn injuries". It shows that the failures corresponding to the potential UDC options of the coffee outlet can directly cause the hazard. This might be right from a worst-case perspective, however as mentioned above, in reality critical temperatures, which trigger the hazard cannot be reached.

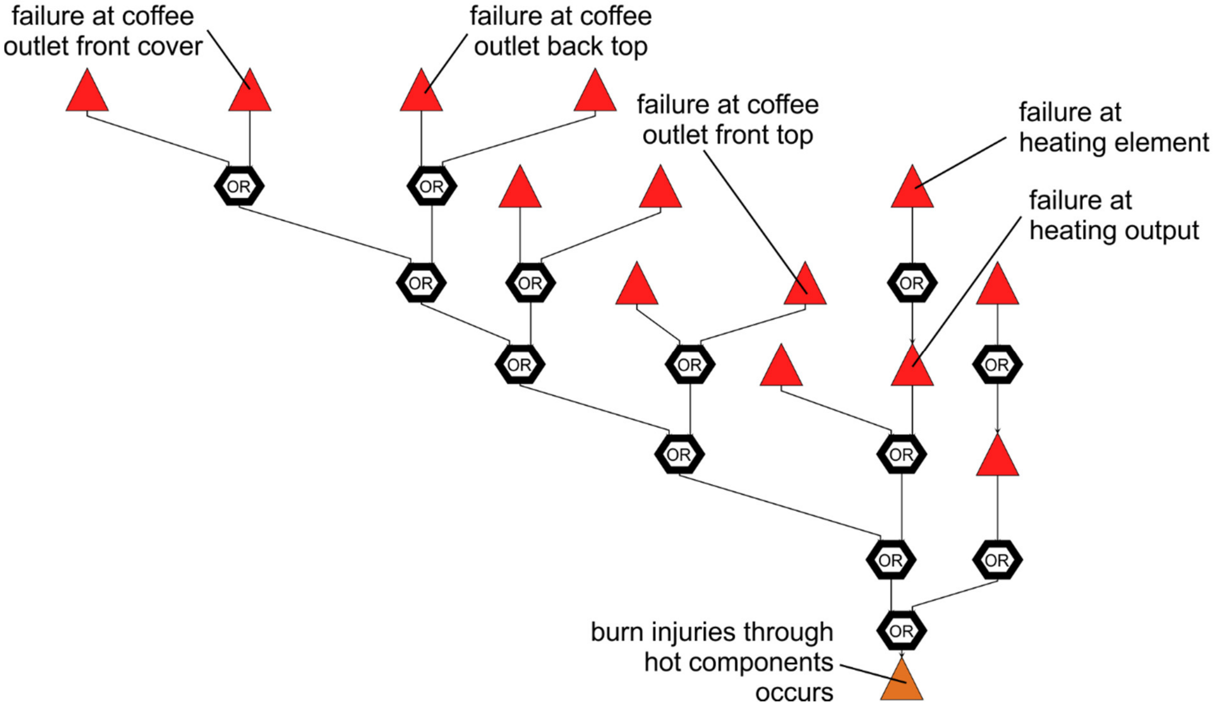
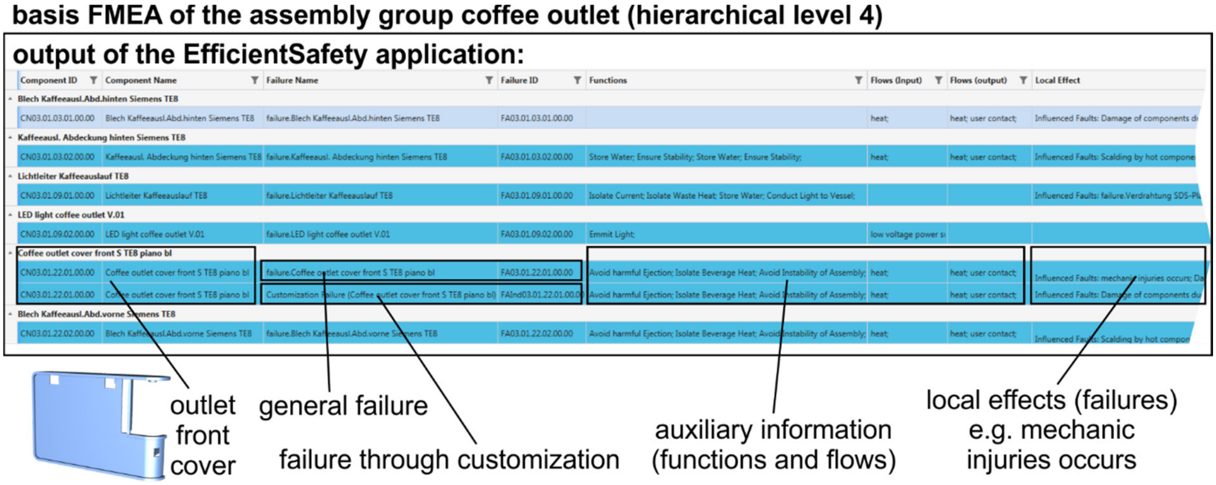

failure at coffee outlet front cover
failure at coffee outlet back top
failure at coffee outlet front top
failure at heating element
failure at heating output
OR
burn injuries through hot components occurs

Figure 5-12: Fault tree of the top event "burn injuries through hot components occurs"

The **preliminary model-based FMEA**, as described in Subsection 4.3.3 consolidates and condenses many parts of the ESMK knowledge framework. The implemented EfficientSafety-application realizes the automatic steps and provides the basis FMEA in form of a table as shown in Figure 5-13. There, the general failure of the outlet front cover is listed together with an additional failure through customization. Moreover, the connected flows of "heat" and "user contact" as well as the allocated safety function "isolate beverage heat" are provided as auxiliary information. In compliance with the fault tree shown in Figure 5-12, the local effects column indicates that the top events "burn injuries through hot components occurs" as well as "mechanic injuries occurs" could directly be influenced by the failures of the outlet front cover. Again, the occurrence of these failures in reality is hardly possible.

The EfficientSafety-application allows selecting on which hierarchical system level the analysis is conducted. To reduce the overall effort, the application and manual completion in this thesis was conducted only for failure modes connected to the previously identified dripping plate and coffee outlet front cover.


basis FMEA of the assembly group coffee outlet (hierarchical level 4)
output of the EfficientSafety application:
outlet front cover
general failure
failure through customization
auxiliary information (functions and flows)
local effects (failures) e.g. mechanic injuries occurs

Component ID	Component Name	Failure Name	Failure ID	Functions	Flows (Input)	Flows (output)	Local Effect
Blech Kaffeeausl.Abd.hinten Siemens TE8							
CN03.01.03.01.00.00	Blech Kaffeeausl.Abd.hinten Siemens TE8	failure.Blech Kaffeeausl.Abd.hinten Siemens TE8	FA03.01.03.01.00.00		heat;	heat; user contact;	Influenced Faults: Damage of components d
Kaffeeausl. Abdeckung hinten Siemens TE8							
CN03.01.03.02.00.00	Kaffeeausl. Abdeckung hinten Siemens TE8	failure.Kaffeeausl. Abdeckung hinten Siemens TE8	FA03.01.03.02.00.00	Store Water; Ensure Stability; Store Water; Ensure Stability;	heat;	heat; user contact;	Influenced Faults: Scalding by hot compone
Lichtleiter Kaffeeauslauf TE8							
CN03.01.09.01.00.00	Lichtleiter Kaffeeauslauf TE8	failure.Lichtleiter Kaffeeauslauf TE8	FA03.01.09.01.00.00	Isolate Current; Isolate Waste Heat; Store Water; Conduct Light to Vessel;			Influenced Faults: failure.Verdrahtung SDS-Pl
LED light coffee outlet V.01							
CN03.01.09.02.00.00	LED light coffee outlet V.01	failure.LED light coffee outlet V.01	FA03.01.09.02.00.00	Emmit Light;	low voltage power s		
Coffee outlet cover front S TE8 piano bl							
CN03.01.22.01.00.00	Coffee outlet cover front S TE8 piano bl	failure.Coffee outlet cover front S TE8 piano bl	FA03.01.22.01.00.00	Avoid harmful Ejection; Isolate Beverage Heat; Avoid Instability of Assembly;	heat;	heat; user contact;	Influenced Faults: mechanic injuries occurs; Da
CN03.01.22.01.00.00	Coffee outlet cover front S TE8 piano bl	Customization Failure (Coffee outlet cover front S TE8 piano bl)	FAInd03.01.22.01.00.00	Avoid harmful Ejection; Isolate Beverage Heat; Avoid Instability of Assembly;	heat;	heat; user contact;	Influenced Faults: Damage of components du
Blech Kaffeeausl.Abd.vorne Siemens TE8							
CN03.01.22.02.00.00	Blech Kaffeeausl.Abd.vorne Siemens TE8	failure.Blech Kaffeeausl.Abd.vorne Siemens TE8	FA03.01.22.02.00.00	Avoid harmful Ejection; Isolate Beverage Heat; Avoid Instability of Assembly;	heat;	heat; user contact;	Influenced Faults: Scalding by hot compon

Figure 5-13: Basis FMEA of the coffee outlet on hierarchical system level 4

As the FTA and FMEA are interconnected analyses, the results of the application of the multi-hierarchy fault tree generation and evaluation and the preliminary model-based FMEA were **evaluated** simultaneously. Both were discussed with the safety analyst based on a questionnaire and an open discussion similar to the evaluation of the model-based hazard and propagation assessment. Again, the questionnaire (see Appendix 9.7.2) picks up the specific requirements on the methods (Subsection 4.3.3) as well as the general requirements on the ESMK and assesses them on an adapted Likert scale. In general, the questionnaire for both methods evaluates the efficiency and the quality of the analyses.

From the safety analyst's perspective, neither the multi-hierarchy fault tree generation and evaluation nor the model-based FMEA can save time regarding his current practice. According to him, the question is how the underlying failure model is updated and maintained. Similar to the model-based hazard and propagation assessment, he is convinced that both methods can reduce the required experience even though experience in some aspects might be irreplaceable for a final FTA. Experienced engineers and an approbation department in combination with a basic training of safety aspects for the designers are essential. In addition, he thinks that the methods support the reuse of the results.

Regarding the quality of the analyses, the safety analyst is also skeptical that the analyses will be able to replace the experience fully. Hence, he does not think that all potential causes and effects are identified. Therefore, a manual check would be always essential. Nevertheless, he thinks that the methods rather identify too much than too less causes and effects. In summary, he therefore is sure that the methods support the identification of potential causes and effects at an early stage without comprehensive analyses.

The **UDC safety-relevance portfolio** was applied in a student course on level one and by the author of the thesis on level two. To quantify the UDC demand, data from the research project InnoCyFer (see Holle et al. (2015)) was used. To determine the safety-relevance, the suggested method for the application was reduced to a 2-level assessment. In a first stage, the requirements and hazards connected to a component were counted to determine the safety-relevance. The results are shown in Figure 5-14. To assess the second level, the elements were analyzed more closely by incorporating the influence of requirements and weight of hazards.

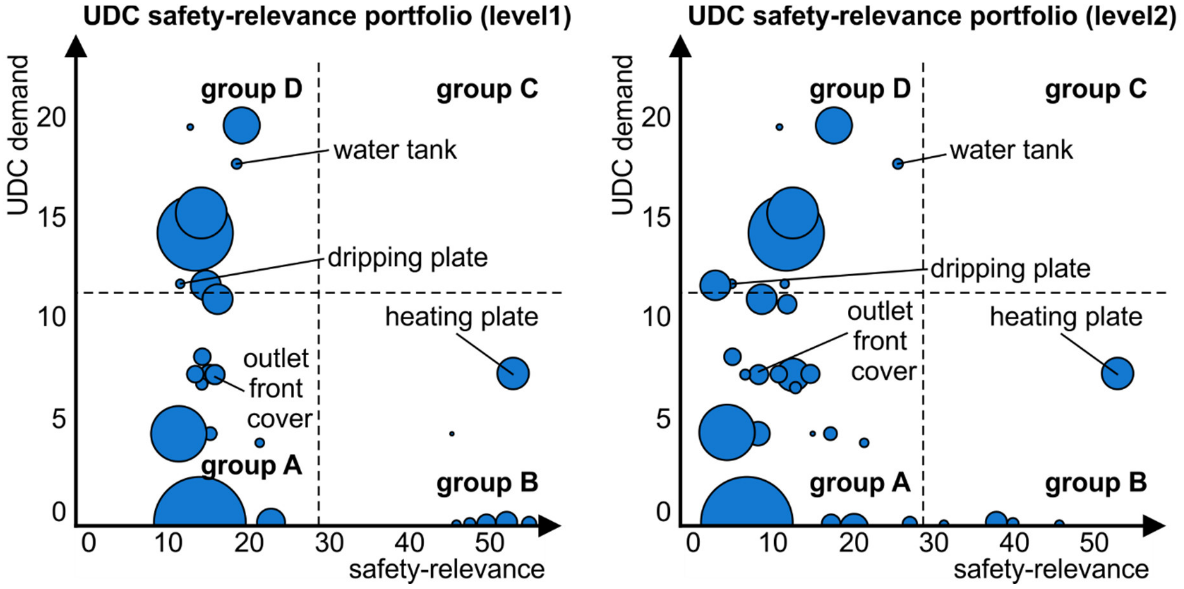


Figure 5-14: UDC safety-relevance portfolios of the fully-automatic coffee machine on two levels

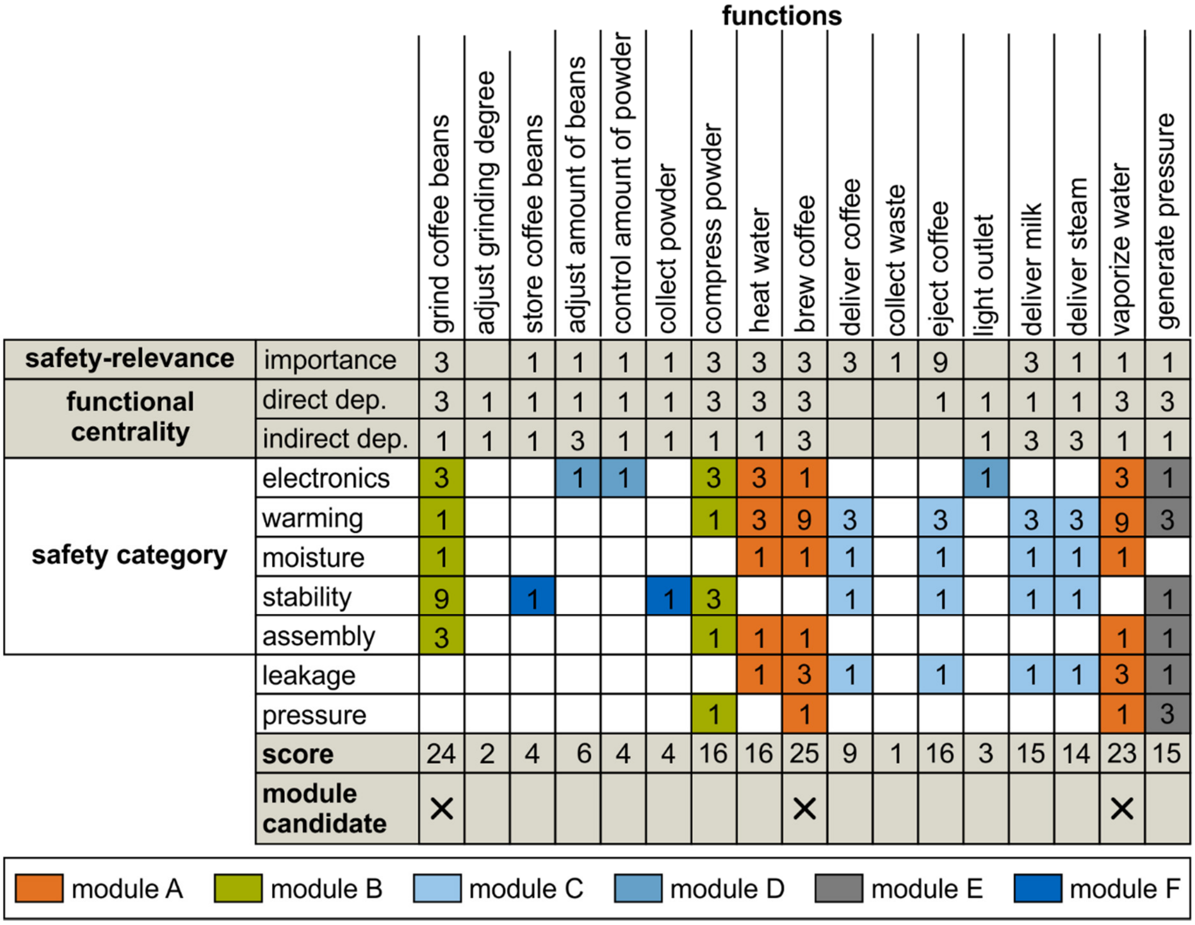
The results in Figure 5-14 show that the two components selected in the UDC project (outlet front cover and dripping plate) are a suitable choice. Another option might be the water tank. However, the second level indicates a significantly higher safety-relevance. The heating plate instead, might be critical. While a potential UDC demand is expected, the connected voltage and heat flows can lead to increased safety efforts. The borders between the quarters of the portfolio in the evaluation case were qualitatively drawn. They might be shifted after a detailed assessment of demands and safety efforts.

The resulting UDC safety-relevance portfolios were **discussed and evaluated** with a designer and a safety analyst of BSH. Both in general confirmed the results. From their experience and intuition, they would have come to a similar rating and classification. In addition, they confirm that the identified group D components are from their point of view most suitable for UDC.

Even though, the situation of the analysis of the fully-automatic coffee machine can be assigned to application case I (transfer to UDC), its product architecture was analyzed on potential improvements for further developments. Thus, the safety-oriented Modular Function Deployment was applied to the existing architecture.

The **safety-oriented Modular Function Deployment** as first step requires the functional structure and their centralities. This information was directly extracted from the ESMK knowledge framework. The dependencies between functions thereby were defined according to the flows. An analysis of the centralities identified "brew coffee" and "deliver coffee" as central functions of the fully-automatic coffee machine. Moreover, the function "vaporize water" plays a central role in the functional architecture. Considering the indirect dependencies additionally, the functions connected to the energy supply elicit as most critical.

To define the safety categories, the requirements resulting from the applicable standard (IEC 60335-1) were clustered thematically. These thematic clusters were used to derive the safety categories. The resulting categories in detail are electronics, warming, moisture, stability, assembly, leakage (materials), and pressure. Based on these safety categories, the functions were assessed on their impact by a student. The assessment resulted in the safety-oriented module indication matrix shown in Figure 5-15. Based on this assessment, the module candidates were identified by selecting the highest scores. For example, the function “brew coffee” was selected as a candidate. Starting from this function, similar functions were identified (e.g. “vaporize water”). In Figure 5-15, these similar functions are highlighted in the same color. The functions of the same color were then combined to modules. For the given example, the resulting module integrates the functions “brew coffee”, “vaporize water”, and “heat water”. This procedure finally delivered eight safety-oriented modules for the fully-automatic coffee machine.



		functions																
		grind coffee beans	adjust grinding degree	store coffee beans	adjust amount of beans	control amount of powder	collect powder	compress powder	heat water	brew coffee	deliver coffee	collect waste	eject coffee	light outlet	deliver milk	deliver steam	vaporize water	generate pressure
safety-relevance	importance	3		1	1	1	1	3	3	3	3	1	9		3	1	1	1
functional centrality	direct dep.	3	1	1	1	1	1	3	3	3			1	1	1	1	3	3
	indirect dep.	1	1	1	3	1	1	1	1	3				1	3	3	1	1
safety category	electronics	3			1	1		3	3	1				1			3	1
	warming	1						1	3	9	3		3		3	3	9	3
	moisture	1							1	1	1		1		1	1	1	
	stability	9		1			1	3			1		1		1	1		1
	assembly	3						1	1	1							1	1
	leakage								1	3	1		1		1	1	3	1
	pressure							1		1							1	3
	score	24	2	4	6	4	4	16	16	25	9	1	16	3	15	14	23	15
	module candidate	×								×							×	

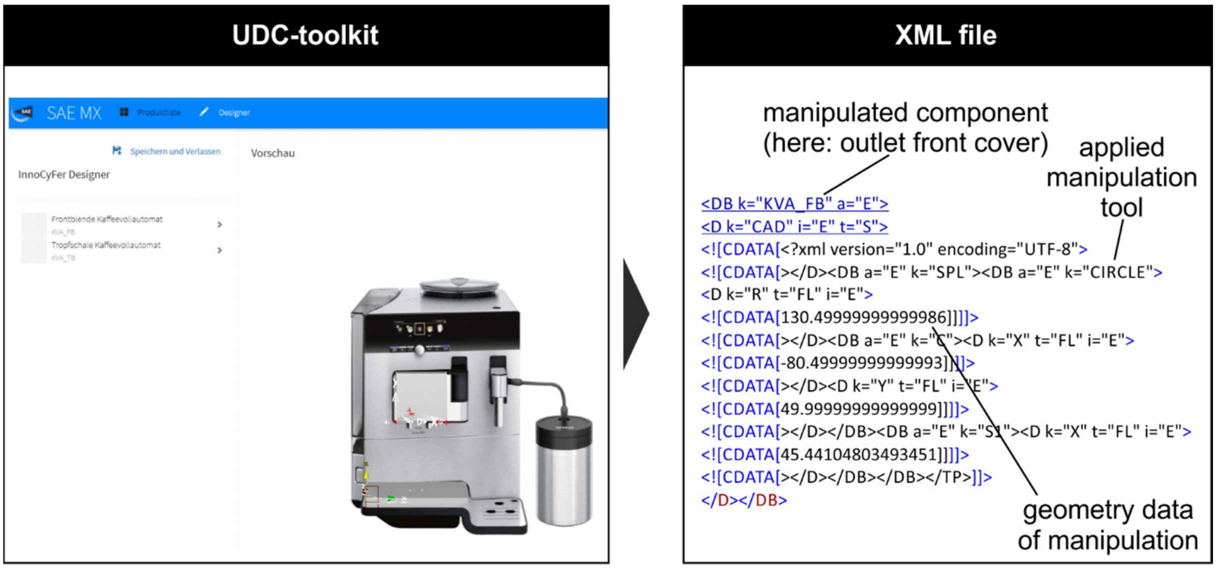
🟧 module A 🟩 module B 🟦 module C 🟦 module D ⬛ module E 🟦 module F

Figure 5-15: safety-oriented module indication matrix of the fully-automatic coffee machine

The resulting eight modules and their composition were **discussed and evaluated** with the safety analyst and designer of BSH. The safety analyst’s judgement is that the resulting modules are reasonable to bundle safety aspects in modules and reduce the dependencies from a safety perspective. Both discussion partners also identified a high accordance between the current module strategy and the modularization suggested by the safety-oriented Modular Function Deployment. The differences originate from other impacts as make-or-buy decisions and design or assembly aspects. Nevertheless, despite these impacts, BSH tries to establish a machine core to reduce the efforts connected to safety and approval. This core at the current stage more or less comprises the most critical modules identified by the safety-oriented Modular Function Deployment.

Phase IV: Individual Safety Analysis

As described above, the objective of the analysis is to identify potentials and to analyze the feasibility of UDC for BSH (PCP). At this stage, an UDC by real users is not available to test the applicability of the ESMK's methods of the Individual Safety Analysis Phase (see Subsection 4.3.4). Instead, a prototype UDC-toolkit (see Figure 5-16), implemented in the context of the project InnoCyFer was used. It offers the UDC of the coffee outlet front cover and the dripping plate. Even though the toolset is limited, it still provides an indefinite solution space. The customization is stored in an XML file, which as shown in Figure 5-16 provides the information which components are customized. However, the limited abilities of the prototype do not allow a more detailed interpretation of the nature of the customization. Nevertheless, the information on the alternated components is used as input for the application of the **effect checklist** and the **individual FTA and FMEA**.


UDC-toolkit
SAE MX
Produktliste
Designer
Speichern und Verlassen
InnoCyFer Designer
Vorschau
Frontblende Kaffeevollautomat
KVA_FB
Tropfschale Kaffeevollautomat
KVA_TB
XML file
manipulated component (here: outlet front cover)
applied manipulation tool
geometry data of manipulation

```
<DB k="KVA_FB" a="E">
<D k="CAD" i="E" t="S">
<![CDATA[<?xml version="1.0" encoding="UTF-8">
<![CDATA[></D><DB a="E" k="SPL"><DB a="E" k="CIRCLE">
<D k="R" t="FL" i="E">
<![CDATA[130.49999999999986]]]]>
<![CDATA[></D><DB a="E" k="C"><D k="X" t="FL" i="E">
<![CDATA[-80.49999999999993]]]]>
<![CDATA[></D><D k="Y" t="FL" i="E">
<![CDATA[49.99999999999999]]]]>
<![CDATA[></D></DB><DB a="E" k="S1"><D k="X" t="FL" i="E">
<![CDATA[45.44104803493451]]]]>
<![CDATA[></D></DB></DB></TP>]]>
</D></DB>
```

Figure 5-16: UDC-toolkit prototype to customize the coffee machine (left) and the XML file storing the customization data (right)

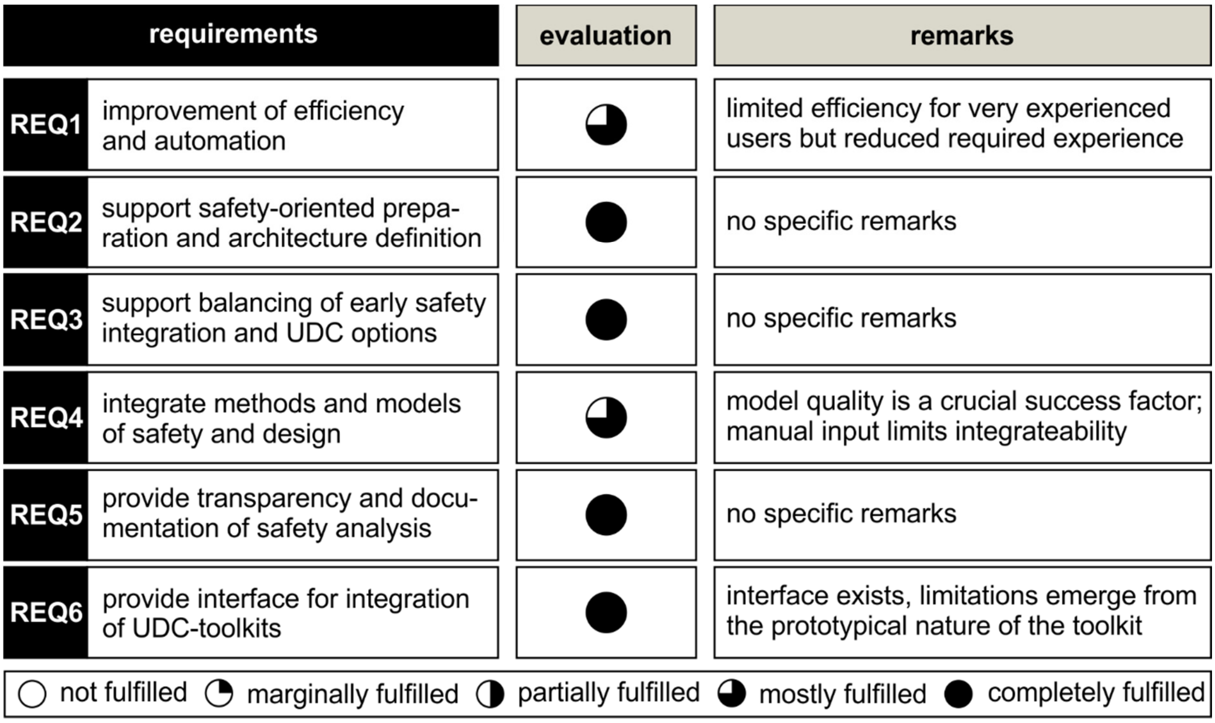
Based on the information on customized parts, the **effect checklist** is generated automatically by the EfficientSafety-application for the considered customizable components. Analogue, the **individual FTA and FMEA** are provided automatically by the EfficientSafety-application based on the input of the UDC-toolkit, respectively the effect checklist.

The results and principles were **discussed** with the safety analyst. From his perspective, the effect checklist as well as the individual FTA and FMEA cannot provide the basis for a faster final safety analysis. From his point of view, the final tests and analyses remain a manual task, which has to be conducted anyways. The application of the methods can be dangerous if some propagations or effects are removed in the preliminary stage and will be forgotten in the final stage. Hence, the worst-case perspective is an important element of these methods. Considering this, for less experienced analysts the methods according to him can provide a good basis for the analyses and a more systematic procedure. In addition, if the most safety critical components are sufficiently separated from the customized components, an improved support through the methods is possible.

5.2.3 Resume of the Application of the ESMK to a Coffee Machine

In summary, the application of the whole ESMK to the fully-automatic coffee machine proves its applicability on a real product and in practical context. The evaluation with experts from BSH shows that the support methods of the ESMK fulfill the majority of the defined requirements and overall help to uncover the safety impact of UDC options. In addition, the ESMK provides an environment for an increased efficiency of connected safety analyses.

The impact on the efficiency is limited for very experienced safety analysts. However, the required amount of experience is reduced and the efficiency and comprehension of the product and safety analyses is improved for less experienced analysts and designers. Hence, the requirements defined in Subsection 3.4.2 are fulfilled with minor limitations. Thereof, Figure 5-17 draws a resume. As mentioned, the factor of experience as well as the maintenance efforts for the knowledge framework limit the fulfillment of *REQ1*. Connected to this, the limited quality of the model is a further limitation, which affects the fulfillment of *REQ3*.



requirements		evaluation	remarks
REQ1	improvement of efficiency and automation	◕	limited efficiency for very experienced users but reduced required experience
REQ2	support safety-oriented preparation and architecture definition	●	no specific remarks
REQ3	support balancing of early safety integration and UDC options	●	no specific remarks
REQ4	integrate methods and models of safety and design	◕	model quality is a crucial success factor; manual input limits integrateability
REQ5	provide transparency and documentation of safety analysis	●	no specific remarks
REQ6	provide interface for integration of UDC-toolkits	●	interface exists, limitations emerge from the prototypical nature of the toolkit

○ not fulfilled ◔ marginally fulfilled ◑ partially fulfilled ◕ mostly fulfilled ● completely fulfilled

Figure 5-17: Summary of the evaluation of the ESMK (coffee machine) and its limitations

5.3 Evaluation Case II: Kitchen Machine

In addition to the central evaluation case described in previous section, this section evaluates the ESKM on a kitchen machine. This evaluation focuses on the major methods of the ESMK. As evaluation case I identified that the efficiency might be a limitation of the ESMK, the second case aims to evaluate if the ESMK supports reuse across products and by that further improves efficiency. The case additionally evaluates the generalizability of the previous result. The product and specific situation are described in Subsection 5.3.1. Subsection 5.3.2 summarizes the application of the ESMK to this case. Finally, Subsection 5.3.3 draws a resume and based on this case evaluates the capabilities of the ESMK from a general perspective.

5.3.1 Description of Case II: Kitchen Machine

BSH (PCP) in addition to coffee machines offers many other home appliances. Amongst those, **kitchen machines** are an important product. Here, the company also identifies a potential value of UDC. Therefore, a scenario of a flexible production is established for an existing model. While the initial planning of UDC options was driven from a manufacturing and marketing perspective, the application of the ESMK aims to validate this selection from a safety perspective. Hence, the ESMK is applied to uncover the safety impact of these options and to support or rebut the choice. The application was limited to the major elements of the ESMK, which mainly range from the modeling of the product architecture in the knowledge framework to the model-based hazard and propagation assessment and the UDC safety-relevance portfolio.

5.3.2 Application of the ESMK to a Kitchen Machine

Similarly to the case described above, mainly student workers and the author of this thesis in discussion with experts from BSH applied the ESMK to the kitchen machine. The following sections describe the application and evaluation in detail.

Phase I: As-Is Analysis

In the As-Is Analysis phase (see Subsection 4.3.1), the safety requirements were not specifically captured. The safety requirements identified for the use case of the fully-automatic coffee machine in Section 5.2 were defined based on the standard IEC 60335-1. This general part of the standard is valid for all household appliances and thus, the relevant foundation for kitchen machines as well. It was possible, to adopt the corresponding safety requirements directly and reuse them within the ESMK knowledge framework and the EfficientSafety-application.

To **model the product architecture**, similar data as for the coffee machine was used. The bill of material provided information on the product structure and was directly imported in the knowledge framework. The flows and dependencies were modeled based on exploded drawings of the existing product. Using this data, a functional structure was established. The resulting model consists of 84 components, 18 flows, and 53 functions.

Phase II: Feature Analysis

In the Feature Analysis phase (see Subsection 4.3.2), the hazards were identified without using the support of the model-based hazard analysis. The reason is that many hazards can be transferred from the coffee machine use case. For example, requirements concerning the maximum temperatures apply for the kitchen machine as well. While safety has the same importance for both cases, the kitchen machine’s complexity is lower. Nevertheless, sensors and other safety devices are integrated. Thus, the hazards are manually defined based on the coffee machine and the comprehension of the kitchen machine as well as its functions. This reduced the efforts required to integrate the hazards in ESMK knowledge framework.

The **method to explicate safety functions** was applied in detail. As described in Subsection 5.2.2, based on the ESMK, the remaining steps are the classification of flows into 1D- and 3D-flows, the assignment of hazards, the identification of connected hazardous functions, as well as the identification and definition of safety functions. These steps were conducted by a student in discussion with the author of this thesis, designers, and safety analysts of BSH. Figure 5-18 shows an excerpt of the resulting flow-based component structure and the derived safety functions. For example, the contact with moving parts at a kitchen machine cannot be avoided. However, the creation of torque bears the hazard of mechanical injuries. To avoid this, the corresponding safety function “avoid a harmful contact with moving parts” is defined. In the product, this function is realized by safety sensors, which stop the movement, if necessary. For some other safety functions, a direct transfer from the coffee machine was possible, when the flows and functions of the components were similar. The final functional structure includes 66 functions of which 13 are the defined safety functions.

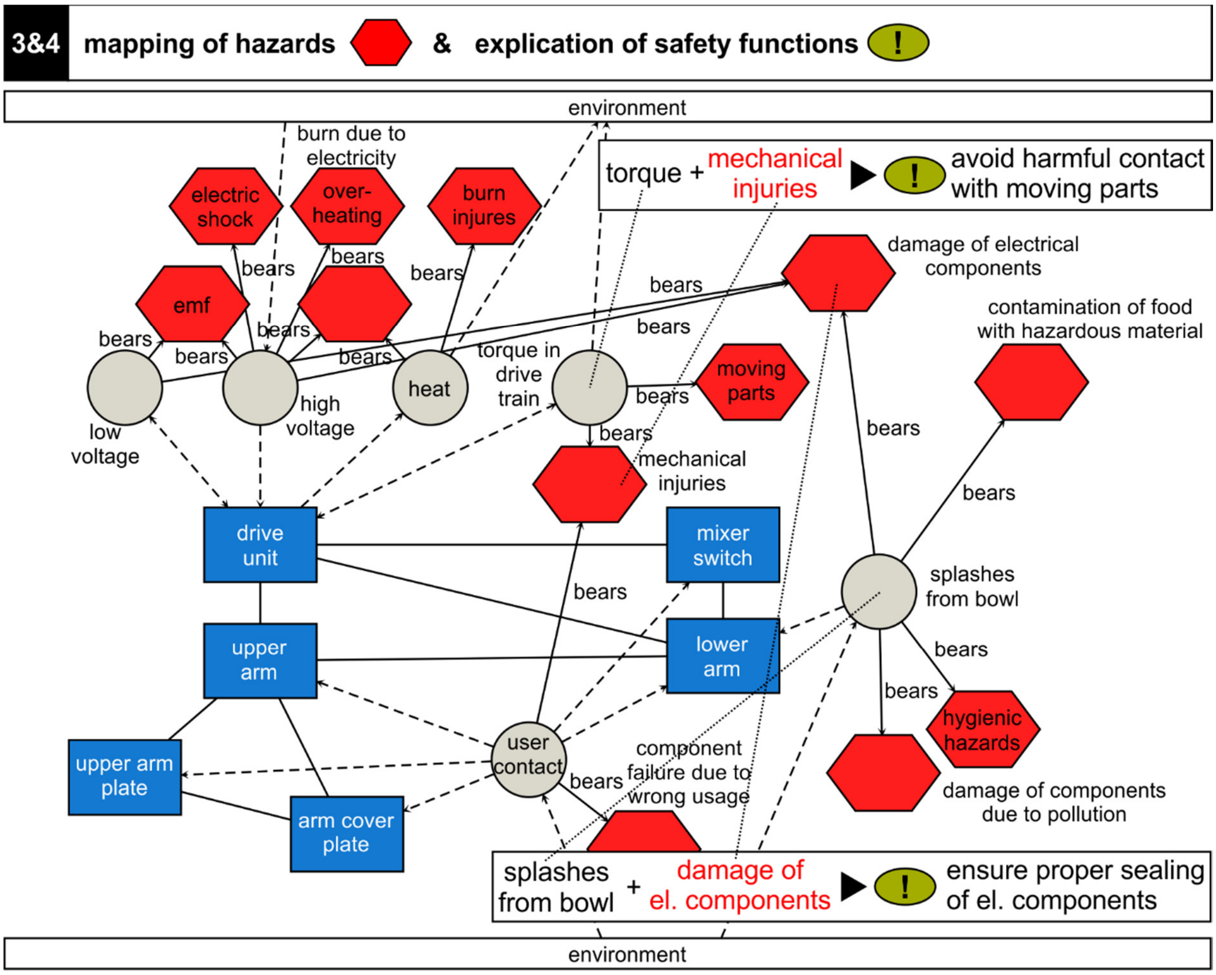


Figure 5-18: Excerpt of the kitchen machine’s component structure for the functional arm and examples of derived safety functions

The resulting model within the ESMK was verified iteratively by the **pattern-based model verification**. Whenever suitable in the modeling process and after several sub-steps, the automated verification was applied to identify and fix model errors. The principles and workflows of the coffee machine, implemented in the EfficientSafety-application, were used. Also in the model of the kitchen machine, the pattern-based verification successfully identified model errors. The iterative application additionally supported the modeling activities. Thus, the modeling abilities and the system understanding of the involved student were improved.

Phase III: Propagation Analysis

Based on the model established within the ESMK knowledge framework in the previous phases, the **model-based hazard and propagation assessment** was conducted for the components, which have been previously selected for customization. The patterns and weights were adopted from the coffee machine. Figure 5-19 shows the resulting propagation tree and hazard potential portfolio of the lower arm of the kitchen machine. It can be seen that many potential propagations to standard components occur, even though the lower arm is considered as potential UDC component. The potentially affected standard components mainly are elements of the drive unit. In addition, the lower arm itself has a large hazard potential, so that its UDC will probably have to be strongly restricted.

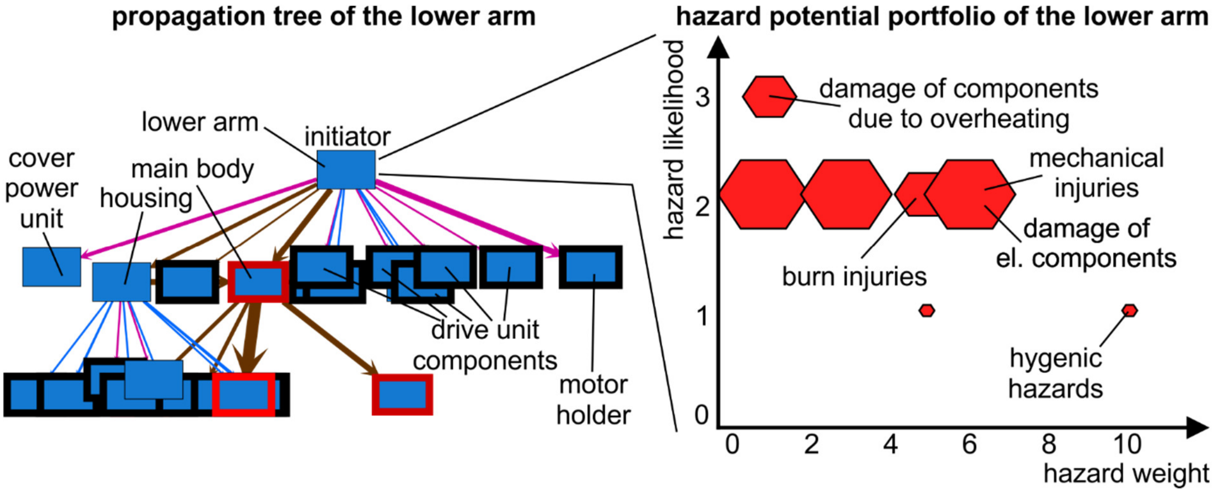


Figure 5-19: Propagation tree and hazard potential portfolio of the lower arm of the kitchen machine

As identified within the model-based hazard and propagation assessment, the choice of the lower arm for UDC might be critical. However, also other housing components and the bowl are subject of the UDC considerations. To evaluate all components, the **UDC safety-relevance portfolio** was established for the kitchen machine. The resulting classification is shown in Figure 5-20. According to the first level assessment, the general housing and the lower arm are assigned to group C (strategic decision). The other housing components as well as the bowl seem to be not very safety-relevant. The assessment on the second level confirms this assumption, but shifts the lower arm and the housing into group D. These components are to some extent suitable for UDC, but they need to be analyzed closely for potential restrictions due to their medium safety-relevance. Finally, the **preliminary FMEA and FTA** were conducted to prepare the documents for a future use.

The results of the application of the ESMK as a whole **were discussed** with the safety analysts and designers from BSH. The discussion confirmed the applicability of the ESMK. While the systematic procedure supported the full and consistent modeling, the visualization figured out to be challenging during the analyses. The experts' intuition on the implications of UDC mostly was confirmed during the analysis. This showed once more the limitations of the ESMK compared to experienced safety analysts and designers. Nevertheless, the applicability and the benefits of the ESMK were confirmed and the time required for application compared to the first evaluation case was significantly reduced due to the large amount of reuse.

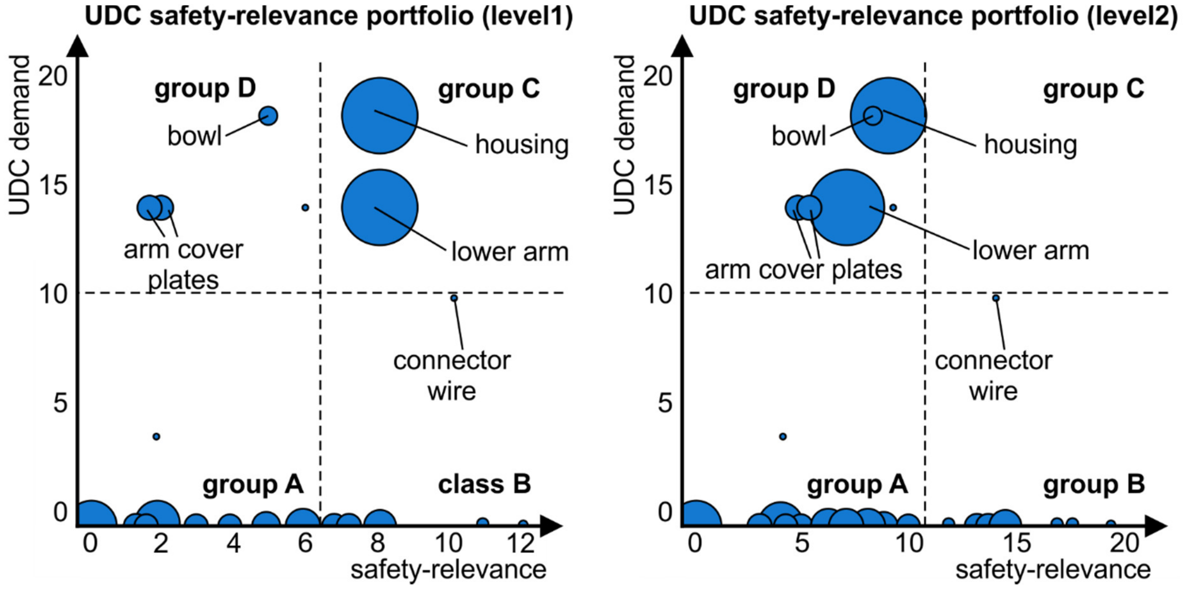
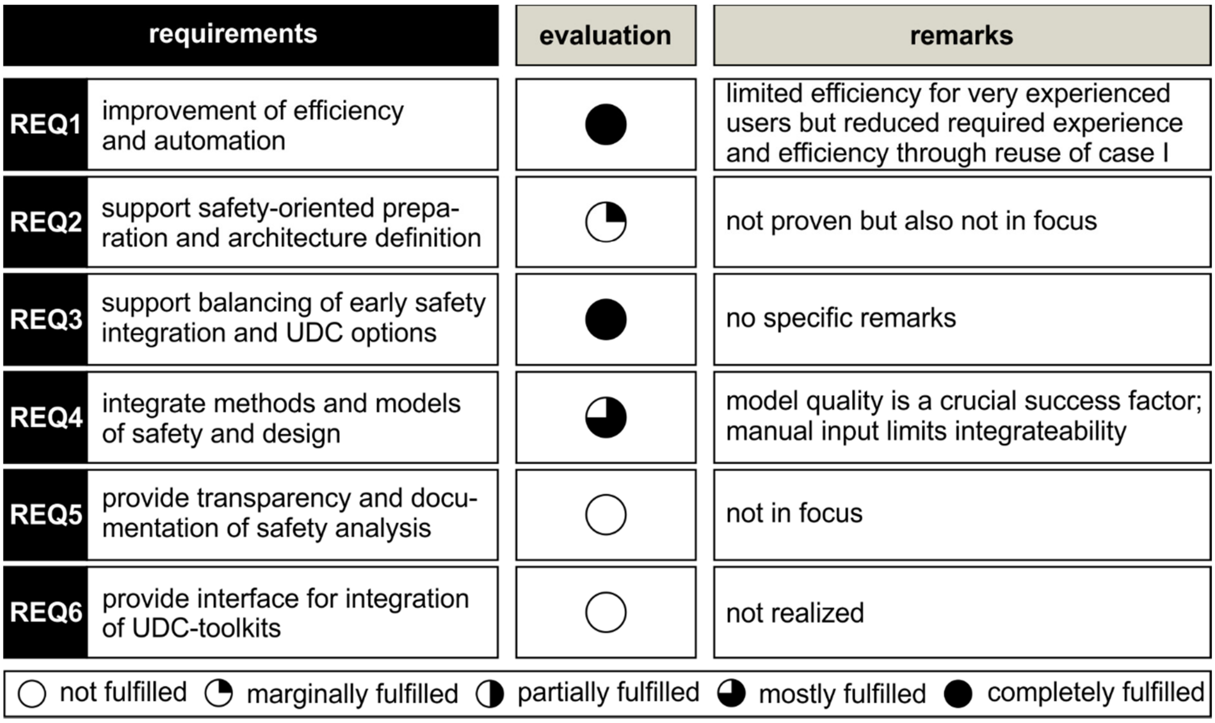


Figure 5-20: UDC safety-relevance portfolios of the kitchen machine on two levels

5.3.3 Resume of the Application of the ESMK to a Kitchen Machine

In summary, the application of major parts of the ESMK combined with the results from evaluation case I to the kitchen machine reconfirms the ESMK's applicability on industrial products in practical context. This evaluation case especially proved that the ESMK and its knowledge framework can be transferred and applied to different products and objectives. The reuse of ESMK methods and models is possible, which can help to resolve the limitations in terms of efficiency. The evaluation with experts from BSH shows that the applied support methods in the case of the kitchen machine fulfill the majority of the defined requirements and overall help to evaluate the safety impact of UDC options. Figure 5-21 summarizes the requirements fulfillment and points out the identified limitations. In this special case, the ESMK helped to evaluate the UDC options selected from a marketing and production perspective. The major finding is that not all previously selected components might be suitable for offering large UDC options.

As students primarily conducted the analysis, the advantage of the ESMK to reduce the required experience was reconfirmed. Moreover, the reuse of requirements and hazards shows that the ESMK knowledge framework can improve the efficiency of all connected tasks. Thus, *REQ1*, which demands an increased efficiency, is fulfilled even though limitations for very experienced engineers remain. Especially the UDC safety-relevance portfolio contributed to the fulfillment of *REQ3*. The trade-offs regarding safety were visualized to balance the safety perspective with other aspects. Yet, the quality of the model remains a bottleneck. The manual modeling is time-consuming and error prone, especially in connection with the missing interfaces (*REQ4*). As indicated in Figure 5-21, the requirements addressing the safety-oriented preparation (REQ2) as well as transparency and documentation aspects (REQ5) were not evaluated. Neither was a connection to an UDC-toolkit established.



requirements		evaluation	remarks
REQ1	improvement of efficiency and automation	●	limited efficiency for very experienced users but reduced required experience and efficiency through reuse of case I
REQ2	support safety-oriented preparation and architecture definition	◔	not proven but also not in focus
REQ3	support balancing of early safety integration and UDC options	●	no specific remarks
REQ4	integrate methods and models of safety and design	◕	model quality is a crucial success factor; manual input limits integrateability
REQ5	provide transparency and documentation of safety analysis	○	not in focus
REQ6	provide interface for integration of UDC-toolkits	○	not realized

○ not fulfilled ◔ marginally fulfilled ◑ partially fulfilled ◕ mostly fulfilled ● completely fulfilled

Figure 5-21: Summary of the evaluation of the ESMK (kitchen machine) and its focus

5.4 Evaluation Case III: Suspension Strut for a Motorcycle

In addition to both previous evaluation cases, the ESMK was applied to a suspension strut for a motorcycle. This subsystem is not planned for UDC but undergoes a regular redesign, where different stakeholders induce changes. This case aims at evaluating the general principle of the ESMK knowledge framework and its capabilities in terms of transparency and documentation. The product and situation are described in detail in Subsection 5.4.1. Subsection 5.4.2 summarizes the application of the ESMK to this case. Finally, Subsection 5.4.3 draws a resume and evaluates the capabilities of the ESMK based on this case from a general perspective.

5.4.1 Description of Case III: Suspension Strut for a Motorcycle

In the third evaluation case, the general concept of the ESMK knowledge framework and its impact on transparency and documentation are specifically evaluated for a subsystem of a motorcycle. As mentioned above, this suspension strut for a motorcycle is not object of UDC considerations but undergoes many changes when existing products are redesigned or new products for specific market segments are developed.

Hence, the changes are not directly induced by the customers. Instead, they are regularly imposed by strategic decisions or through changes at other subsystems. These changes start on a requirement level. Thus, within a requirement management process, the possible propagations and effects are evaluated. In summary, the situation in this case is comparable to the ESMK's second application case and allows evaluating the knowledge framework and its capability to support transparency and documentation.

The subordinate goal of the motorcycle manufacturer is to implement an improved process for the **requirements management**. To support this, a student project (Bermond, 2016) was conducted in cooperation with the manufacturer. Within the development of one specific subsystem of a current motorcycle development project, the application of the ESMK knowledge framework was evaluated. The ESMK was applied as potentially suitable tool to support the identification of interdependencies between requirements and to manage changes in the requirements domain. Thus, especially the As-is Analysis phase and parts of the Propagation Analysis were conducted.

5.4.2 Application of the ESMK to the Suspension Strut for a Motorcycle

To apply the ESMK within the requirements management process of the manufacturer, the ESMK knowledge framework was reduced and slightly adapted in a first step. The analysis only focuses on the product architecture including requirements, components, and functions. Compared to the previous applications, the domain of requirements was enlarged and now contains all relevant requirements in a hierarchical decomposition.

The EfficientSafety-application was modified accordingly in a few aspects. This includes the implementation of additional attributes (e.g. a requirement status and the specific system level, the requirement addresses). Moreover, specific workflows to import the requirements from the existing requirements management tool (IBM Doors) and to improve the navigation through these requirements were implemented.

The model of the suspension strut was imported and modeled in the ESMK knowledge framework using this adapted application. While the requirements were imported from IBM Doors, the components and their dependencies were modeled manually by the involved student. This resulted in a model similar to the simplified view shown in Figure 5-22.

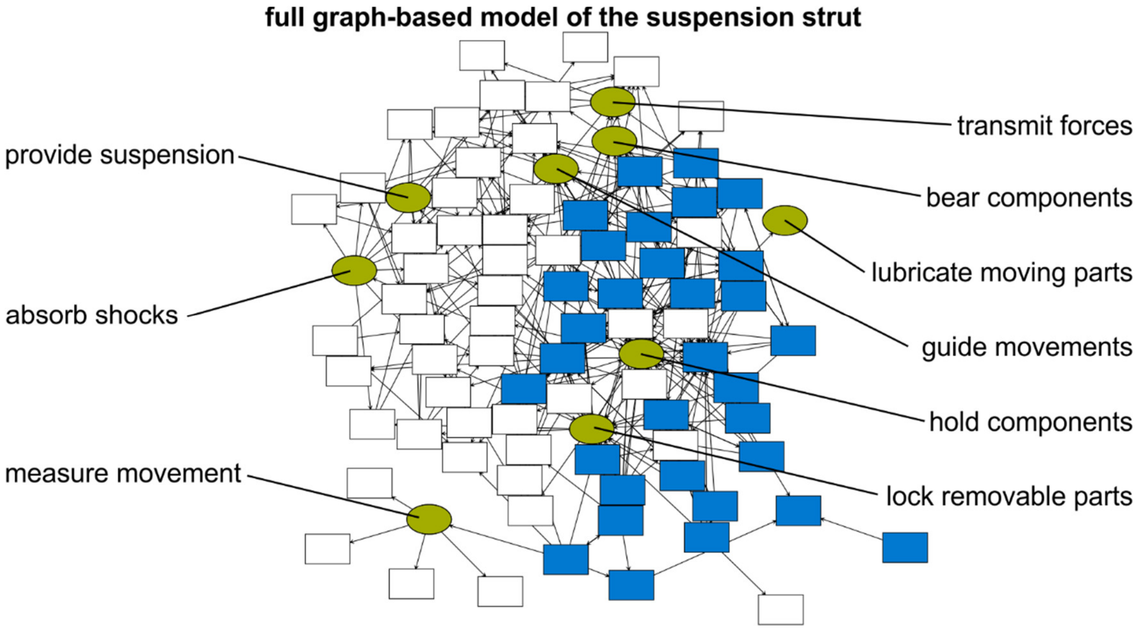
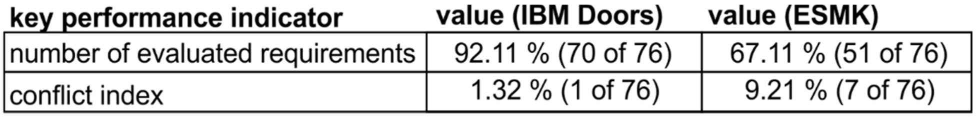


Figure 5-22: Model of the suspension strut and its main functions within the EfficientSafety-application

Supported by this model and the EfficientSafety-application, the tasks of **requirements elicitation**, **coordination**, **classification**, and **distribution** as well as the **analysis of interdependencies** between requirements were conducted. Based on this prototypical implementation, the benefits and limitations of the ESMK compared to the current practices were analyzed.

The comparison and analysis was evaluated in two steps. First, a comparison between the procedure using the ESMK and the current procedure using IBM Doors was conducted based on key performance indicators. Second, a qualitative evaluation through the two involved requirement engineers elaborated the advantages and limitations of the ESMK and its knowledge framework.

Within the requirements management process of the manufacturer, the rate of evaluated requirements and the rate of identified conflicts after requirement coordination meetings are used as important **key performance indicators**. For the comparison, the same process was conducted following the original procedure and the procedure supported by the ESMK within the same amount of time. Figure 5-23 indicates the resulting values of these key performance indicators. They clearly show that the regular procedure is faster, but the procedure supported by the ESMK and its propagation analysis identifies more potential conflicts.



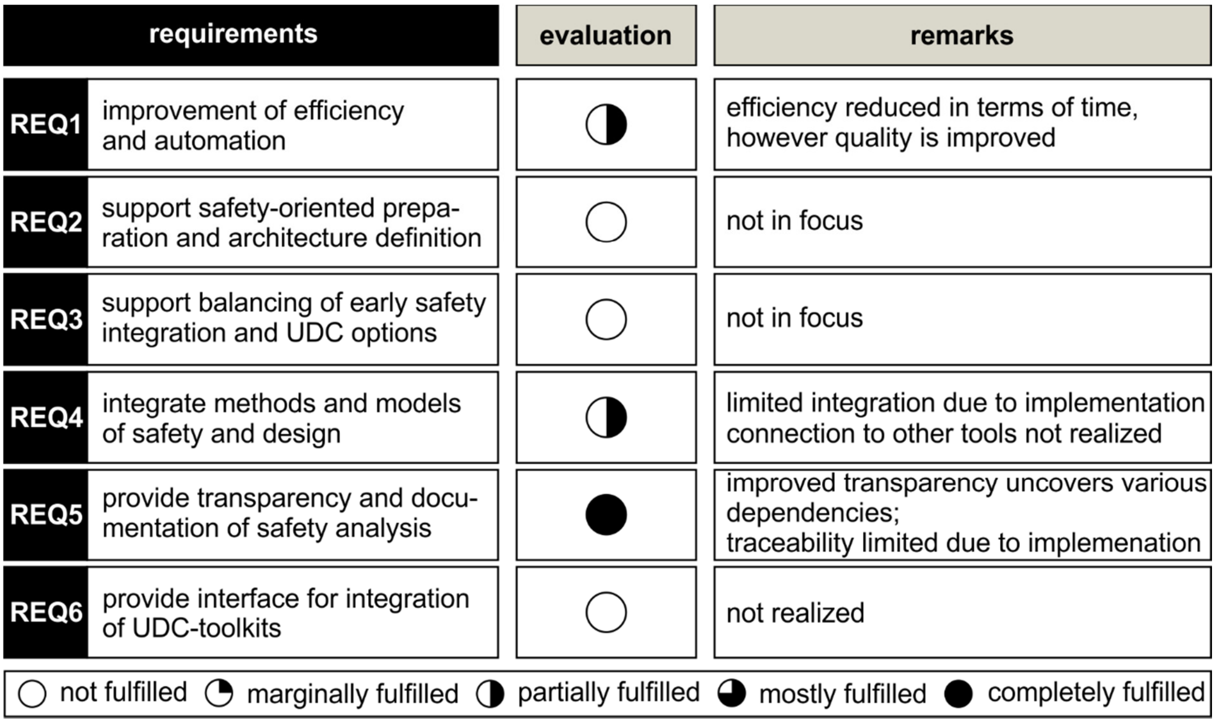
key performance indicator	value (IBM Doors)	value (ESMK)
number of evaluated requirements	92.11 % (70 of 76)	67.11 % (51 of 76)
conflict index	1.32 % (1 of 76)	9.21 % (7 of 76)

Figure 5-23: Resulting key performance indicators of the application to the suspension strut

The **qualitative assessment** in the discussion with the participants supported this impression. According to them, the ESMK provides a large benefit in form of a very good overview and visualization of potential propagations and dependencies. This supports the discussion of potential changes to requirements. Moreover, the visualization of the graph-based model offers benefits for the coordination meetings. Despite these advantages, the participants see limitations in the daily business. They for example relate to baseline management, multi-user modeling, and interfaces to other tools. However, these identified limitations mainly concern the implemented EfficientSafety-application and not the core principles of the ESMK.

5.4.3 Resume of the Application of the ESMK to the Suspension Strut

In summary, the application of the ESMK and its knowledge framework to the suspension strut for a motorcycle underlines the ESMK's capability to identify potential propagations and interrelations within a product architecture. In comparison to the existing procedure and tool of the manufacturer, the ESMK identified more conflicts but also consumed more time. Especially when UDC is realized, the additional time does not have to be an overall disadvantage. Hence, the ESMK is partially able to fulfill its efficiency requirement (*REQ1*). As summarized in Figure 5-24, the ESMK moreover fulfills the requirement on transparency and documentation (*REQ5*) by uncovering more interrelations than the current procedure. Only the integration requirement (*REQ4*) is not completely fulfilled in this evaluation case due to the limitations of the implemented EfficientSafety-application.



requirements		evaluation	remarks
REQ1	improvement of efficiency and automation	◑	efficiency reduced in terms of time, however quality is improved
REQ2	support safety-oriented preparation and architecture definition	○	not in focus
REQ3	support balancing of early safety integration and UDC options	○	not in focus
REQ4	integrate methods and models of safety and design	◑	limited integration due to implementation connection to other tools not realized
REQ5	provide transparency and documentation of safety analysis	●	improved transparency uncovers various dependencies; traceability limited due to implemenation
REQ6	provide interface for integration of UDC-toolkits	○	not realized

○ not fulfilled ◔ marginally fulfilled ◑ partially fulfilled ◕ mostly fulfilled ● completely fulfilled

Figure 5-24: Summary of the evaluation of the ESMK (suspension strut for a motorcycle) and its limitations

5.5 Integrated Evaluation of the Efficient Safety Method Kit

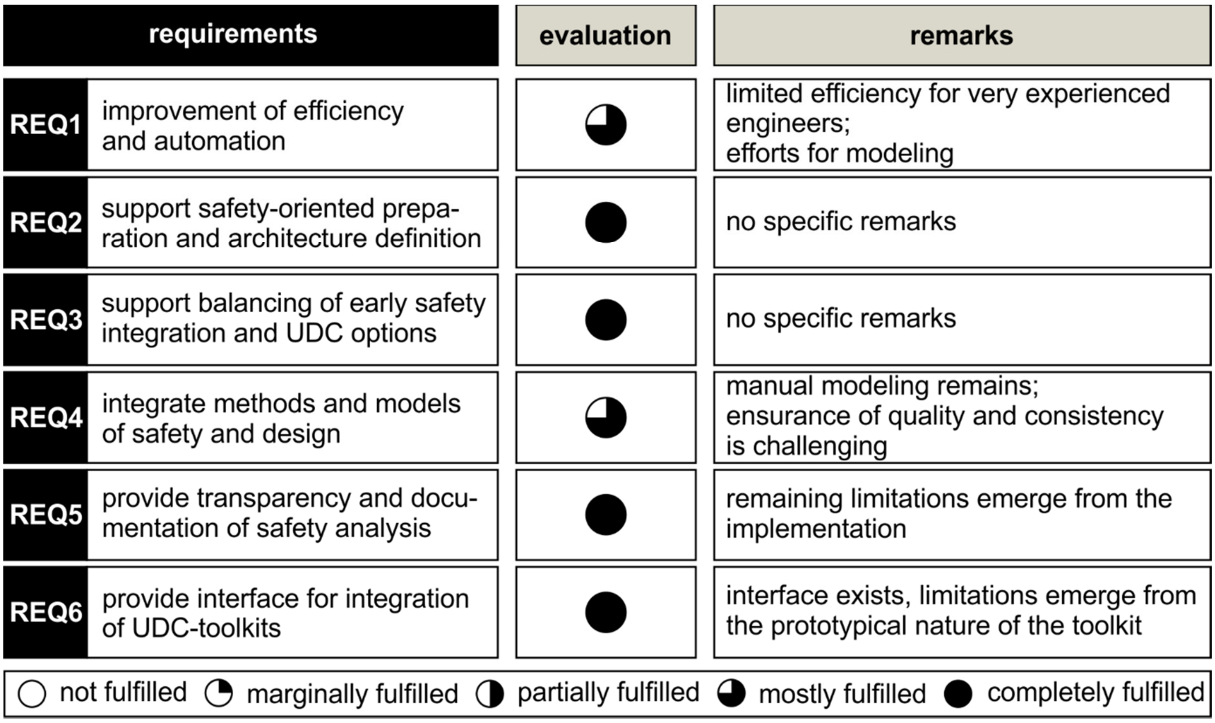
The previous sections apply the ESMK to three different use cases and evaluate specific aspects of the individual support methods. Even though the Descriptive Study II within this thesis remains on an initial stage, it is necessary to evaluate the success of the ESMK as a whole. This includes the evaluation if the ESMK satisfies the needs identified in Section1.3.

As mentioned in Section 5.1, a real application of UDC is missing. This limits the possibilities to evaluate the success of the ESMK in detail. Instead, the evaluations of the individual methods were merged, discussed, and reflected with the involved engineers from a **holistic perspective.** The involved engineers were the designers, safety analysts, and requirement managers who supported the ESMK's application. In a discussion, the compatibility, potential synergies, and conflicts of the ESMK's methods were evaluated. This in summary leads to the evaluation of the requirement fulfillment as shown in Figure 5-25. The ESMK fulfills the majority of the defined requirements. Only minor limitations concerning its efficiency (*REQ1*) and its integration capabilities (*REQ4*) remain.

In addition, the **main goals and connected needs** defined in Section 1.3 were discussed. In this discussion, the involved engineers were asked to evaluate based on their experience and knowledge of their company and products, if the ESMK is able to meet these objectives and satisfy the underlying needs.

The first aspect of the defined goals is to limit the efforts for safety analysis prior to the customization and to balance UDC options. This aspect is mainly addressed by the first three phases of the ESMK. The engineers of all three cases were convinced that the ESMK successfully supports the identification of interrelations and the evaluation of customization options. By that, it can successfully reduce the efforts for the safety analysis of UDC products prior to the customization. However, especially the engineers of BSH (evaluation cases I and II) see an important limitation in the time and efforts required to establish the ESMK knowledge framework. Still, from their point of view, an overall positive effect is possible for a full UDC, when each product is individual.

The second aspect of the defined goals are the limited efforts for the final safety analysis of the customized products. Here, all three cases show that the ESMK is not fully able to achieve this. Especially for the very experienced analysts, the application of the ESMK can increase the time of the analyses. Nevertheless, all involved engineers are convinced that the ESMK reduces the required experience to conduct the analyses. Hence, the ESMK increases the overall resource efficiency. In summary, the discussion shows that the ESMK to a large extent provides the demanded support to identify and shift the optimum in the tension between safety efforts and UDC options.



requirements		evaluation	remarks
REQ1	improvement of efficiency and automation	◕	limited efficiency for very experienced engineers; efforts for modeling
REQ2	support safety-oriented preparation and architecture definition	●	no specific remarks
REQ3	support balancing of early safety integration and UDC options	●	no specific remarks
REQ4	integrate methods and models of safety and design	◕	manual modeling remains; ensurance of quality and consistency is challenging
REQ5	provide transparency and documentation of safety analysis	●	remaining limitations emerge from the implementation
REQ6	provide interface for integration of UDC-toolkits	●	interface exists, limitations emerge from the prototypical nature of the toolkit

○ not fulfilled ◔ marginally fulfilled ◑ partially fulfilled ◕ mostly fulfilled ● completely fulfilled

Figure 5-25: Summary of the evaluation of the ESMK from all evaluation cases

6. Discussion

In this chapter, conclusions from the evaluation are derived in Section 6.1. Based on this, Section 6.2 discusses the contributions and implications of this thesis.

The main objective of this thesis is to find an answer how the safety analysis of UDC products can be improved in order to reduce the overall time and resources needed. It therefore defines the objective to provide a support for the balancing of the UDC options and connected safety efforts. This balancing includes two subgoals. First, the evaluation of the safety implications of UDC options prior to customization and second, the more efficient individual safety analysis after customization. Based on this these goals, the thesis derives requirements, develops, and validates the Efficient Safety Method Kit (ESMK). Figure 6-1 depicts and summarizes this decomposition of objectives in a goal breakdown structure. The following sections discuss the conclusions from the evaluation in the three cases (see Chapter 5) and the resulting contributions and limitations of the ESMK for practical application and science.

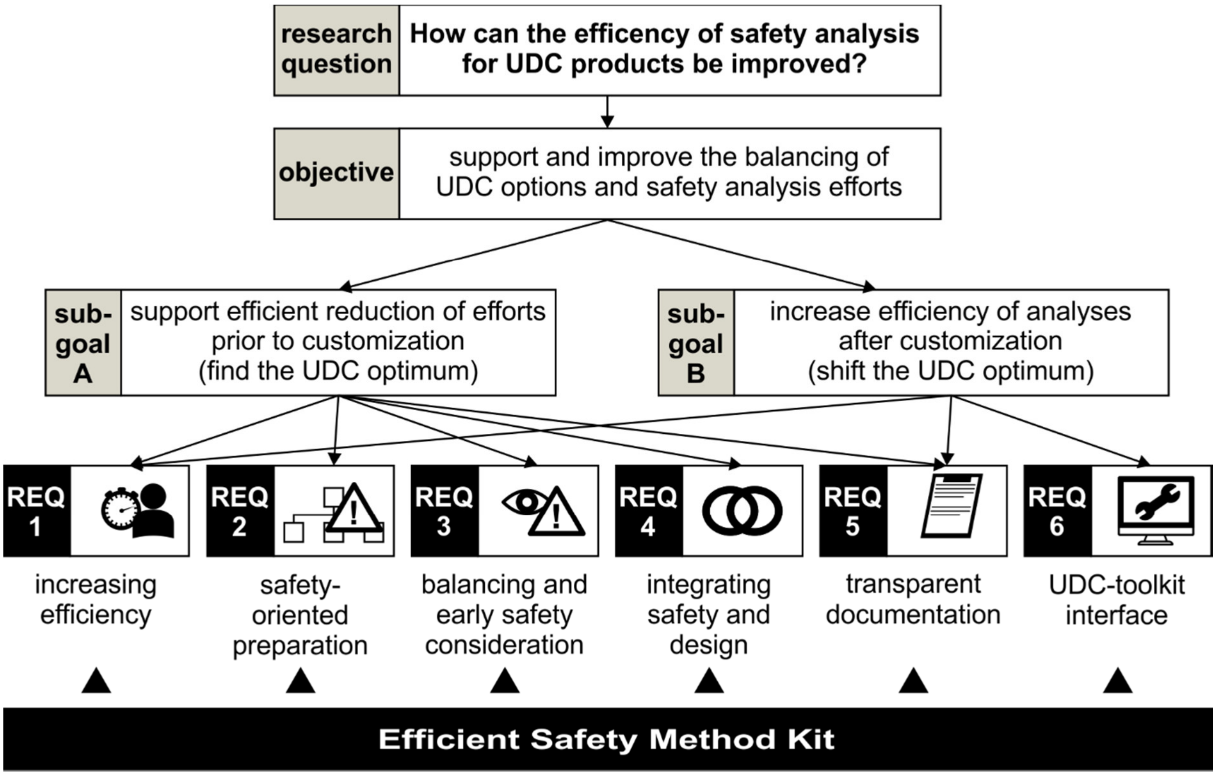

research question
How can the efficency of safety analysis for UDC products be improved?
objective
support and improve the balancing of UDC options and safety analysis efforts
sub-goal A
support efficient reduction of efforts prior to customization (find the UDC optimum)
sub-goal B
increase efficiency of analyses after customization (shift the UDC optimum)
REQ 1
increasing efficiency
REQ 2
safety-oriented preparation
REQ 3
balancing and early safety consideration
REQ 4
integrating safety and design
REQ 5
transparent documentation
REQ 6
UDC-toolkit interface
Efficient Safety Method Kit

Figure 6-1: Goal breakdown structure of this thesis

6.1 Discussion of the Evaluation Cases

The three evaluation cases described in Chapter 5 evaluate and prove the applicability and benefits of the ESMK for different products and situations. The application to different products and companies shows the potentials and generalizability of the ESMK. However, all applications rather build on scenarios of UDC or similar than on full realizations of UDC. Thus, the conducted initial evaluation is not sufficient to prove the general success and benefits of the ESMK. This requires further evaluations in other contexts and for full implementations of UDC. Nevertheless, the following paragraphs discuss the findings of the initial evaluation structured according to the six general requirements of the ESMK.

In all three evaluation cases, it was not possible to identify a completely satisfactory fulfillment of *REQ1*, which demands an increased **efficiency and automation**.

The first reason is that the involved engineers from the industrial partners possess large experience and expertise. They are able to understand the product and potential safety impacts of changes quite fast. In contrast, the support methods of the ESMK focus on a worst-case perspective, consider all possibilities, and produce large amounts of data. Analyzing this data would increase the efforts for the experienced engineers. However, the evaluation cases show that the experience required for the analyses will be reduced and consequently, for less experienced engineers, the efficiency will be improved. Especially for UDC with a large number of individual analyses, experience is likely to be a limited resource and the worst-case perspective gains importance. In addition, the evaluation cases rely on the estimations of the experienced engineers, which can induce a potential overconfidence bias. In summary, the ESMK proved its potential to improve the overall efficiency of safety analysis for an UDC realization. As shown in evaluation case II (kitchen machine), the efficient reuse of the ESMK can contribute to the overall efficiency and can diminish the described limitations.

The second reason for a limited efficiency during the evaluation cases originates from the implementation and the situation in the companies. As not all data for the ESMK was directly available and the EfficientSafety-application was not able to import all available formats automatically, still manual work was necessary. This limitation will be dissolved, when the one-time efforts are taken to establish the ESMK knowledge framework and to implement specific interfaces, which are fully compatible with the tools and formats used in the companies. Moreover, the application to the kitchen machine demonstrated the reuse potentials of data stored in the ESMK knowledge framework. However, it has to be mentioned that even if the model is established, efforts to keep it up-to-date will be necessary.

The fulfillment of *REQ2*, which addresses a **safety-oriented preparation of product architectures,** was only evaluated in the first evaluation case (coffee machine). Nonetheless, the implications of a safety-oriented architecture are also discussed during the applications of other methods. In summary, the methods provided by the ESMK successfully support a safety-oriented preparation. One important aspect is that knowledge on safety is made explicit. Moreover, the safety-oriented Modular Function Deployment provides a modularization method, which is tailored to safety aspects. It defines a module concept, which incorporates safety on a general level, while a detailed consideration of safety is not included. This concept provides a good basis for discussion and for the balancing of different influence factors, when a module concept is defined.

The evaluation cases also underline that the ESMK supports the **balancing of UDC options and connected safety efforts** (*REQ3*). Especially the application of the model-based hazard and propagation assessment and the UDC safety-relevance portfolio in the cases at BSH (cases I and II) helped to uncover potential impacts and to visualize the trade-offs between the added value through UDC options and the increased cost through increased safety efforts. In addition, the application of the ESMK on the suspension strut (case III) demonstrates the importance of the analysis and visualization of interdependencies within the ESMK knowledge framework. This allows to identify potential conflicts of changes, which is not only important for UDC but for ECM and requirements management as well. In the same time, the engineers were able to identify seven times more conflicting relations than without the ESMK. However, for the special case of UDC, the provided safety analyses are not yet able to fully replace the current practices. Still, the applications at BSH (cases I and II) show that the ESMK helps to evaluate UDC options and to early integrate safety considerations.

The **integration of other methods and tools** (*REQ4*) was demonstrated throughout all three evaluation cases. The concept of the ESMK allows to integrate specific attributes or to adjust the scope of the framework to the given situation. As mentioned above, the implemented EfficientSafety-application and the tool Soley impose limitations for integrating other tools and formats. In the evaluation cases, the data of some tools had to be manually analyzed and reproduced in the knowledge framework. From a practical perspective, this limits the benefits of the ESMK. Nevertheless, these limitations primarily concern the implemented application and not the ESMK as solution approach itself.

The ESMK in the evaluation moreover demonstrated its advantages in terms of **transparency and documentation** (*REQ5*). The applications at BSH (cases I and II) showed that the explicit and consistent documentation is key to fulfill *REQ1*. The documentation of the model-based hazard and propagation assessment for example, makes the considerations during the analysis of potential impacts explicit and traceable. As described above, the ESMK in the case of the suspension strut demonstrated its capabilities to make interrelations and the impacts of potential changes explicit. Furthermore, the basis FMEA-form was identified as valuable input and condensation of the relevant information. However, the EfficientSafety-application is not able to fulfill the relevant standards (e.g. ISO 26262) completely. The application at the current stage is for example not able to realize multi-user environments, provide baseline management, or satisfy usability aspects. Especially the worst-case perspective of the ESMK's methods leads to huge data volumes, which can reduce transparency. As the propagation trees of the model-based hazard and propagation assessment showed, suitable tool support is required to manage and visualize the information transparently. These limitations again primarily concern the application and not the general concept of the ESMK.

Finally, the compatibility of the ESMK with an **UDC-toolkit** (*REQ6*) was only shown in the evaluation case of the fully-automatic coffee machine. The largest limitations during the evaluation emerge from the UDC-toolkit. The evaluation case only allowed to use the prototypical toolkit of the InnoCyFer project, which provides limited UDC options. From its accessible output, only information on which components are customized was accessible. Thus, the concept of connecting the ESMK with an UDC-toolkit is proven, an evaluation with a more sophisticated UDC-toolkit remains open.

In summary, the ESMK in the evaluation cases was able to meet most of the requirements. While, the implemented EfficientSafety-application imposed multiple restrictions, the ESMK concept demonstrated its potentials. Despite the initial stage of the evaluation and its scenario-based procedure, the ESMK created multiple contributions and benefits, which were identified and evaluated in industrial cases.

6.2 Contribution and Implications on Practical Application

This thesis researches the field of UDC and develops the ESMK to provide support to realize UDC from a safety perspective. According to the aim defined in Section 1.3, the ESMK provides support at the interface of customization, safety analysis, and ECM. In addition, as shown in Figure 6-2, the ESMK's contributions and implications reach into the dual interfaces between these fields and even in the individual fields. All these levels of contribution are discussed in the following.

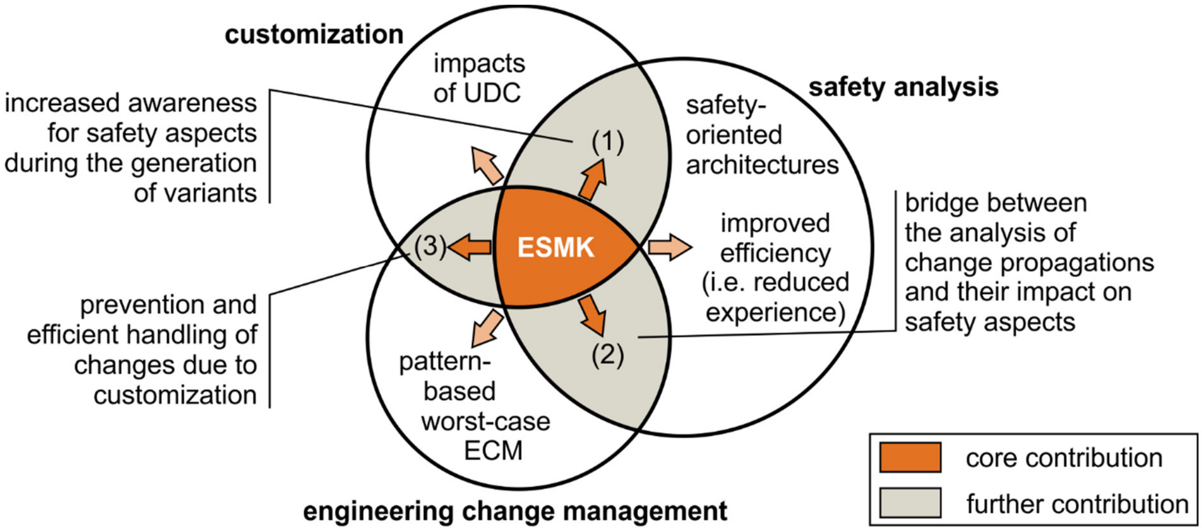

customization
impacts of UDC
increased awareness for safety aspects during the generation of variants
(1)
safety analysis
safety-oriented architectures
(3)
ESMK
improved efficiency (i.e. reduced experience)
bridge between the analysis of change propagations and their impact on safety aspects
prevention and efficient handling of changes due to customization
(2)
pattern-based worst-case ECM
engineering change management
core contribution
further contribution

Figure 6-2: Contribution and implications of this thesis in the research fields

6.2.1 Contribution of the ESMK at the Interface of the Three Fields

The ESMK provides a set of twelve support methods and tools clustered into four phases, which build on a common framework. As demonstrated in the three industrial evaluation cases, it successfully supports the safety analysis of UDC products. The methods and tools of the ESMK integrate the fields of UDC, ECM, and safety analysis to support the balancing of provided UDC options, their impact on product safety, and connected safety efforts.

The ESMK successfully **improves the efficiency** of the safety analyses of individual changes. However, the evaluation cases show that in the case of very experienced analysts, the ESMK is not able to cope with the experience. In these situations, the time efficiency might even decrease. This applies for both, a preliminary analysis to identify the impact of UDC options and the final individual safety analysis after the customization is conducted. For less experienced analysts an increase in time- and resource-efficiency is achieved. The reuse potentials can further improve the overall efficiency.

However, the overall efficiency is limited through the one-time efforts to set up the knowledge framework. In order to provide a valid base for the analyses, the ESMK knowledge framework requires a valid model of the analyzed product architecture. Depending on the availability of information in the company and the nature of the product, this step can be very time- and resource-consuming. Hence, a trade-off analysis is required to determine if the ESMK is a suitable solution for the specific situation.

The quality of the model is another factor, which can have a negative effect. It determines the outcome of the analyses. If the model quality is limited, also the quality and efficiency of the analyses can be limited. Nevertheless, the typed attributed graph-based knowledge framework provides large opportunities for automation. They are to some extent accessed within the pattern-based model verification and are implemented in the EfficientSafety-application. In turn, the implementation using Soley imposes further limitations, especially in terms of interfaces and usability.

In addition, the ESMK successfully **provides an early integration of safety aspects and a preparation of the product architecture** for UDC from a safety perspective. The UDC safety-relevance portfolio represents a tool, which starting from early stages identifies the safety impact of potential UDC options and evaluates the resulting trade-offs. To support the improvement of product architectures from a safety perspective, the ESMK provides the safety-oriented Modular Function Deployment. However, both methods only provide an abstracted analysis in early phases. The actual product safety is strongly determined by the actual geometry of the components and materials. The results of these methods have to be analyzed on plausibility once more detailed information is available. Moreover, safety is not in any situation the most important influence on the product architecture definition. In order to achieve a global optimum, the suggested architecture improvements need to be discussed from other perspectives.

The ESMK **supports the balancing of early safety considerations and the provided UDC options** and their impact on safety as well. The core methods of the ESMK all address the early integration and consideration of safety aspects. They even provide automated preliminary safety analyses. As mentioned above, the validity of analyses strongly depends on the quality of the model in the ESMK knowledge framework. To achieve a high quality, manual crosschecks of the results are required and a final manual check of the analyses might remain mandatory during the next years. Nevertheless, the ESMK methods are adjustable to different levels of abstraction and support the transparency and completeness of the analyses. In turn, the worst-case perspective and the completeness result in large models and complex analyses. These analyses require a profound knowledge of the methods and training.

The flexible nature of the ESMK also successfully **ensures compatibility with other methods and tools**. This allows for the integration of other methods like for example QFD or SysML models. However, the implementation in the prototypical application shows that the ESMK, despite its compatibility, does not solve the problems regarding interfaces and consistency. The pattern-based model verification provides an initial solution for this problem, but further principles need to be integrated and consistency checking will be necessary.

As already mentioned, the ESMK **successfully improves transparency and documentation** of the analyses. Its major contribution is the explicit modeling of implicit safety knowledge and its accessible and transparent documentation in the knowledge framework. In addition, the analyses implemented in the EfficientSafety-application provide a consistent and automated documentation. At the current stage, this documentation is not fully compliant with established standards. As standards slightly vary between different companies, a specific adaption will be necessary to implement UDC and the ESMK. To realize UDC, also a specific UDC-toolkit will be needed, which extends the prototype used in the first evaluation case. This toolkit has to be closely interlinked with the ESMK knowledge framework.

In **summary**, the ESMK successfully addresses the challenges at the interface between UDC, ECM, and safety analysis. It thus represents a **valid answer to the research question** formulated in Section 1.3.

However, the application and evaluation of the ESMK in this thesis is limited to three cases and two companies. These cases only consider an UDC scenario. Thus, the conclusions drawn from these cases are not fully generalizable. Further studies in a wider context and with a realization of the UDC product are required. Nevertheless, the ESMK provides the required basis and support for these studies. It offers an adaptable and flexible knowledge framework and a set of independent, but compatible methods. It is hence adaptable to specific situations and products.

Moreover, the success and benefit of the ESMK in the evaluation cases is only analyzed based on scenarios. The industrial partners involved in the cases proved the benefit based on expectations and assumptions. To evaluate the ESMK's success further, realizations of UDC have to be analyzed and the assumptions of the experts need to be verified.

The applicability of the ESMK is proven in the evaluation cases. However, the methods were applied by the involved students or by the author of this thesis. Only the principles of the methods and the results were discussed with the engineers from the industrial companies. This evaluation does not yet prove the applicability for engineers from practice without assistance and does not allow drawing conclusions on the amount of required training. Nevertheless, the involved students were able to apply the methods after a short introduction on their own.

6.2.2 Contribution of the Efficient Safety Method Kit to Other Fields

The contributions of the ESMK as visualized in Figure 6-2 (page 168) also reach out to further fields. This includes the dual interfaces between the three fields addressed in this thesis as well as the three fields themselves.

At the **interface between safety and customization (1)** (i.e. UDC) the challenge is to reduce the efforts required for safety analysis, approval, and validation of the large amount of variant products resulting from customization. Simultaneously, research demands an early consideration of safety aspects and for a bridging of the gap between design and safety analysis. The ESMK contributes to solve this challenge by offering a knowledge framework, which unites the perspectives of safety and design. Moreover, the ESMK's UDC safety-relevance portfolio is not limited to UDC when supporting the identification of trade-offs between customization and safety aspects.

An important strategy of ECM is the frontloading of changes and their efficient handling. Even though safety is an important factor, existing research does not unite both fields when evaluating and planning changes. Especially the ESMK's model-based hazard and propagation assessment contributes to solve this challenge. It identifies change propagations and their impact on safety by an automatic pattern-based analysis. This contributes to bridge the gap between ECM methods and safety aspects at the **interface of safety analysis and ECM (2)**.

While many researches try to address the challenge at the **interface of ECM and customization (3)** by frontloading only, the ESMK supports two strategies. This includes the prevention of unwanted change impacts and propagations as well as the efficient handling of late changes. The model-based hazard and propagation assessment offers a pattern-based worst-case propagation analysis, which can efficiently help to avoid specific propagations or quickly analyze late changes and their impacts.

In addition, this thesis strongly contributes to the field of **customization** by defining and analyzing UDC. Two studies research the relevant impacts of UDC and their effects. This analysis provides the base for further research of UDC and extends the research field of customization.

The ESMK moreover directly contributes to current challenges in the field of **safety analysis**. This field demands increased efficiency, an early consideration of safety aspects, and products and architectures tailored to safety. These challenges are especially addressed by the methods of the Propagation Analysis phase of the ESMK. The methods are not limited to UDC only and can be applied to other products as well.

Finally, the ESMK contributes to the field of **ECM**. By providing the pattern-based propagation analysis of the model-based hazard and propagation assessment, the ESMK reduces the efforts of the analysis of potential propagations. This increases the efficiency and effectiveness of change propagation analyses. Additionally, it enables the better handling of change propagations in large and complex systems.

In **summary**, the ESMK provides a successful answer on how UDC products can be balanced and how the efforts for the safety analysis of UDC products can be reduced. In addition, the contributions of the ESMK are not limited to this specific case. For example, it contributes to an early safety consideration and it helps to close the gap between safety and design for other products as well.

7. Summary and Outlook

This chapter summarizes the motivation, content and contributions of this thesis. It moreover provides an outlook on unanswered questions and open fields for further research.

7.1 Summary

The goal of this thesis is to support manufacturers to balance User-driven Customization (UDC) products with respect to safety. Therefore, it develops the **“Efficient Safety Method Kit for User-driven Customization” (ESMK)** as support for balancing and safety analysis of UDC products to reduce the time and resources needed to analyze each customized product.

The **motivation** for this support results from the following current trends and challenges. The demand for individual products and customization is increasing. While flexible manufacturing systems and additive manufacturing allow for more degrees of freedom, product safety is a central bottleneck for efficient customization. Especially increasing complexity and stricter legislative regulations increase safety analysis and assurance efforts in product development. This imposes restrictions on customization options. To remain competitive, manufacturers have to find a suitable balance between customization options offered and defined restrictions due to product safety in order to limit the additional efforts.

To develop a suitable support for this challenge, this thesis first analyzes the **state of science** in the fields of **customization, ECM, and safety analysis**. On the one hand, current research in customization shifts the focus towards the users. Methods like user innovation and UDC involve users in product development in order to better satisfy their needs. On the other hand, current research in the field of safety analysis strives for a shift of safety considerations to early phases of product development. Therefore, mainly model-based methods are applied. In combination, these trends lead to a potential conflict, as the early safety considerations are opposed by late changes through users, who are not product development experts.

The handling of regular engineering changes in product development is covered by the field of ECM. Established ECM methods identify propagation effects but neither incorporate user-induced changes nor establish the bridge to safety analysis. However, this thesis identifies that a collaboration of the three discussed fields is essential.

As the current state of science provides neither sufficient support nor sufficient information on challenges and implications through the previously mentioned conflict, especially with focus on UDC, this thesis conducts two **explorative studies**.

First, an explorative questionnaire survey researches the general impact of UDC on the product development process. It shows that the concept of UDC has a strong impact on most phases in classical development processes like the VDI 2206. The main findings are that for successful UDC, the integration of the product development process phases needs to be improved. Moreover, a suitable preparation of the customizable product is essential. This includes extensive product structure planning and the definition of boundaries. Therefore, the **early consideration of product safet**y and other aspects like quality and compatibility becomes crucial. These aspects have to be considered starting from early phases so that the impact of the uncertainties and risks induced by UDC can be minimized.

Second, to explore the challenges in the crucial field of product safety, this thesis conducts three complementary focus-interviews. They confirm the findings of the questionnaire survey and concretize the need for support. The interviewees demanded an **early consideration of** safety aspects, especially in the context of customization. Moreover, for variant or customized products, an **increased efficiency of safety analysis** is needed. In general, the interviewees demanded **better documentation** of safety analysis and a **bridging of the gap** between safety analysts and designers.

To develop the **solution approach**, this thesis derives specific requirements from the findings summarized in the previous paragraphs. It integrates methods and approaches from the three fields of customization, ECM, and safety analysis at their interface. This results in the **"Efficient Safety Method Kit for User-driven Customization"** (ESMK). It provides a set of twelve methods and tools, which support the major tasks in the development of UDC products with respect to safety. These methods not only support the balancing of customization options and restrictions from a safety perspective, but also improve the efficiency of the safety analysis of customized products. The ESMK and its methods cover the transfer of an existing product to UDC as well as the redesign of a product for UDC. The twelve support methods and tools of the ESMK are clustered into four phases and listed in Figure 7-1.

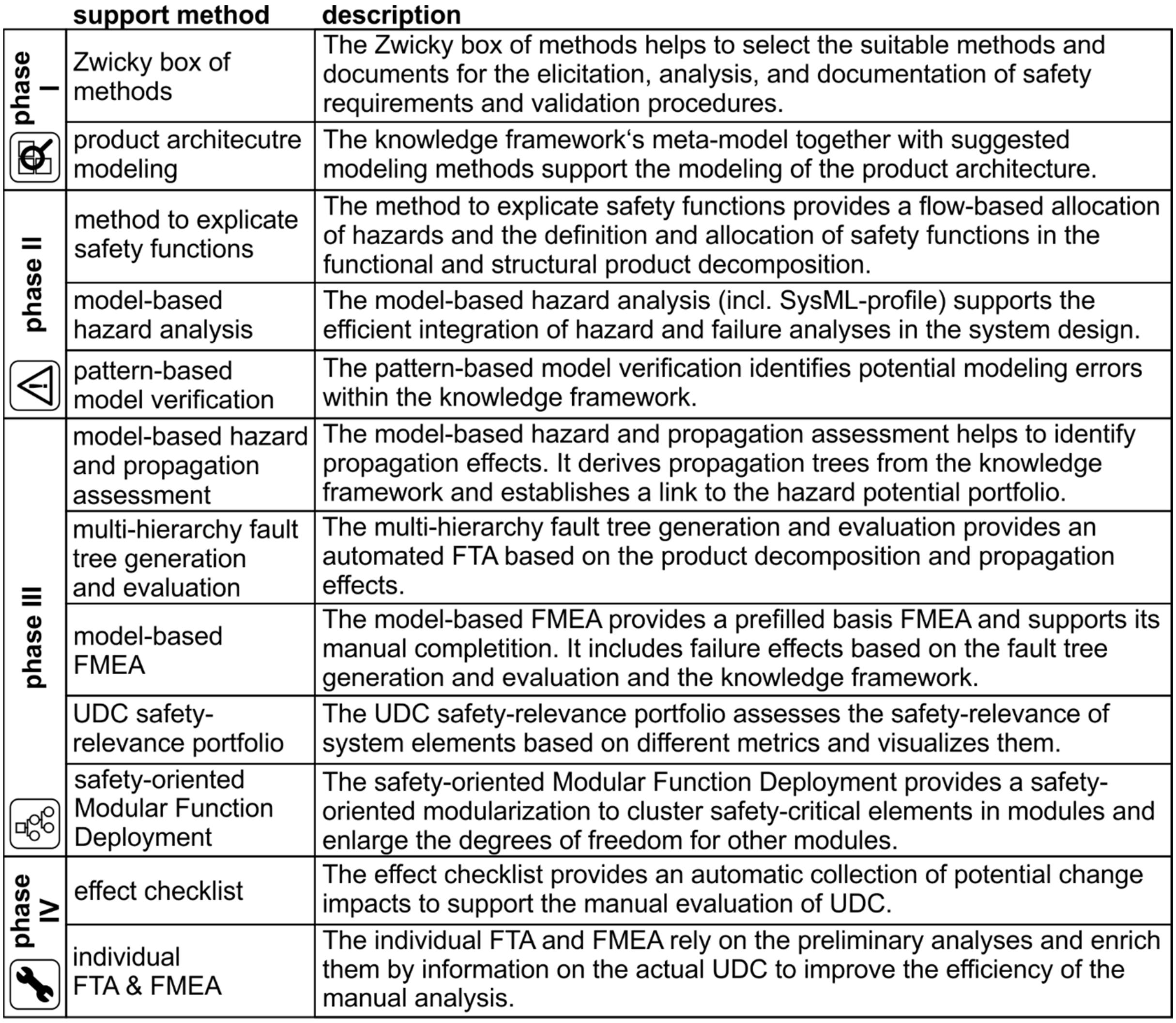
All individual methods of the ESMK are based on a **common graph-based knowledge framework**, which models the product architecture as well as relevant safety aspects and requirements. To reduce manual effort and handle complexity, graph-rewriting algorithms can be used to automate parts of the methods.

The ESMK is applied within **three industrial cases**, which are a fully-automatic coffee machine, a kitchen machine, and a suspension strut for a motorcycle. These cases prove the ESMK's **applicability** and demonstrate that it is mostly able to fulfill the defined requirements.

In summary, the ESMK successfully contributes to the interface between UDC, ECM, and safety analysis. It **supports the realization and balancing of UDC products from a safety perspective**. Hence, the ESMK is a suitable answer to the research question of this thesis and successfully **reduces the time and resources** needed for the safety analysis of customized UDC products. The ESMK and its methods in particular provide the following **contributions**:

- early integration of safety by modeling and evaluating safety aspects explicitly and providing preliminary safety analyses
- safety-oriented product architectures through modularization based on safety aspects
- balancing support for UDC by evaluating the safety-relevance and propagation analyses
- improved transparency and documentation through the explicit and consistent modeling of product architectures in the common knowledge framework
- improved efficiency through automated workflows

These aspects all contribute to increased awareness and improved efficiency (i.e. required experience is reduced). They allow balancing UDC products from a safety perspective by **identifying and shifting the optimum** in the tension between UDC options and safety efforts.



	support method	description
phase I	Zwicky box of methods	The Zwicky box of methods helps to select the suitable methods and documents for the elicitation, analysis, and documentation of safety requirements and validation procedures.
	product architecutre modeling	The knowledge framework's meta-model together with suggested modeling methods support the modeling of the product architecture.
phase II	method to explicate safety functions	The method to explicate safety functions provides a flow-based allocation of hazards and the definition and allocation of safety functions in the functional and structural product decomposition.
	model-based hazard analysis	The model-based hazard analysis (incl. SysML-profile) supports the efficient integration of hazard and failure analyses in the system design.
	pattern-based model verification	The pattern-based model verification identifies potential modeling errors within the knowledge framework.
phase III	model-based hazard and propagation assessment	The model-based hazard and propagation assessment helps to identify propagation effects. It derives propagation trees from the knowledge framework and establishes a link to the hazard potential portfolio.
	multi-hierarchy fault tree generation and evaluation	The multi-hierarchy fault tree generation and evaluation provides an automated FTA based on the product decomposition and propagation effects.
	model-based FMEA	The model-based FMEA provides a prefilled basis FMEA and supports its manual completition. It includes failure effects based on the fault tree generation and evaluation and the knowledge framework.
	UDC safety-relevance portfolio	The UDC safety-relevance portfolio assesses the safety-relevance of system elements based on different metrics and visualizes them.
	safety-oriented Modular Function Deployment	The safety-oriented Modular Function Deployment provides a safety-oriented modularization to cluster safety-critical elements in modules and enlarge the degrees of freedom for other modules.
phase IV	effect checklist	The effect checklist provides an automatic collection of potential change impacts to support the manual evaluation of UDC.
	individual FTA & FMEA	The individual FTA and FMEA rely on the preliminary analyses and enrich them by information on the actual UDC to improve the efficiency of the manual analysis.

Figure 7-1: Overview of methods and phases of the "Efficient Safety Method Kit for User-driven Customization"

7.2 Outlook

Even though the ESMK answers the question of how the efficiency of the safety analysis of UDC products can be improved, need for future research remains. In the following, specific aspects of the ESMK are discussed, followed by an outlook on future research.

7.2.1 Specific Aspects

The evaluation of the ESMK in this thesis remains at the initial level. The industrial cases apply the ESMK to scenarios of potential UDC. To extend the evaluation to a comprehensive stage and improve the significance of the results, **further evaluation** has to be conducted, which also includes actual realizations of UDC.

While the ESMK successfully increases the efficiency of the safety analysis for UDC products in the evaluation cases, the overall efficiency of the product development is not necessarily increased. The creation of the knowledge framework can be very time consuming and these **one-time efforts** can overrun the savings through the method kit. To reduce these efforts, **interfaces** need to be developed to automatically translate and transfer knowledge from existing tools and documents into the knowledge framework. For example, components and geometrical contacts could be obtained from CAD models or flows could be extracted from piping or wiring diagrams. Another useful source are existing safety analysis tools.

Not only the time, but also the **quality of the model** in the knowledge framework can limit the value of the method kit. Errors in the model can cause critical misinterpretations in the automated analyses. At the current stage, this makes manual crosschecks unavoidable. The pattern-based model verification as part of the ESMK reduces the risk of model errors but cannot fully eliminate them. Further methods should be developed to **identify modeling errors, ensure the quality of models, and limit the efforts to keep such models up-to-date**.

The industrial cases show that experience still plays an important role for the manual crosschecks as well as for the analysis of propagations and the individual safety analysis. This circumstance limits the practical efficiency of automated analyses. Very experienced engineers can possibly conduct these analyses faster manually than they interpret the results of the automatic analyses. However, experience is rare and costly. Future research should develop methods, which **explicate and formalize this experience** so that it can be translated and transferred to the knowledge framework. This would allow for a more reliable automatic analysis and reduce the manual efforts.

The decreased efficiency compared to very experienced engineers mainly emerges from the large amount of results produced by the automated analyses. The reason for this amount of data is that the automated analysis identifies every possible effect based on the system elements and their dependencies. In reality, many of those dependencies do not necessarily create an effect. Here, the formalization of experience can also help to reduce the **amount of data**. On the flipside, the model in the knowledge framework could also be enriched by additional information, for example through field data from maintenance. In addition, an interface to simulation tools could be used to more precisely evaluate changes.

Moreover, a dynamic link to UDC-toolkits should be researched. This thesis only realizes a static interface at which the customization from the UDC-toolkit is interpreted by the ESMK's methods. Future work should establish a **dynamic evaluation and feedback loop**. It could dynamically evaluate the customization, conduct safety analyses, and feed these results back to support user who customizes the product in the UDC-toolkit.

7.2.2 General Aspects

From a more general perspective, it is obvious that restrictions, interfaces, and suitable methods vary dependent on the context and company. The ESMK only provides a catalogue of suggestions. Further work should develop **support for selecting and adapting the suitable methods** according to the given context. This arises questions like how the benefit of methods can be evaluated in respect of the given overall context, and how the adaption of methods can be systematically supported.

Moreover, the ESMK only incorporates validation procedures as affected element in the knowledge framework. However, the safety analysis of UDC products is only one challenge. The testing and validation of these products is another hurdle. Future work has to research how **validation tests can be defined and managed** to handle UDC products and how these tests can be efficiently conducted. This includes for example questions, as how products with a customized shape can efficiently be tested on quality issues.

The development of the ESMK relies on the results of the two studies conducted in the Descriptive Study I. These studies reveal **implications of UDC** on the development process, according to which the ESMK was designed. Future research should further validate these implications. In addition, the implications arise questions, as how can the development process for UDC products be designed or how can the pricing strategy of UDC products look like.

Additionally, the evaluation and discussion shows that even though the methods are tailored for the UDC of consumer products, they can also have a **value for other products and settings**. Future research should evaluate if the ESMK can for example support the development of products in an engineer-to-order or mass customization concept. Moreover, the identified contributions of the ESMK to the fields of customization, safety analysis, and ECM should be evaluated in detail. Therefore, the independent value of the ESMK's methods for these fields needs to be assessed.

8. References

Ahmad, N., Wynn, D. C., & Clarkson, P. J. (2011). Information Models Used to Manage Engineering Change: A Review of the Literature 2005-2010. In S. Culley (Ed.), 18th International Conference on Engineering Design (ICED'11) (Vol. 1, pp. 538–549). Glasgow: Design Society.

Ahmad, N., Wynn, D. C., & Clarkson, P. J. (2013). Change impact on a product and its redesign process: A tool for knowledge capture and reuse. Research in Engineering Design, 24(3), 219–244. doi:10.1007/s00163-012-0139-8

AIAG. (2008). Potential failure mode and effects analysis (FMEA): Reference manual (4th ed.). Southfield MI: AIAG.

Alizon, F., Shooter, S. B., & Thevenot, H. J. (2007). Design Structure Matrix Flow for Improving Identification and Specification of Modules. In American Society of Mechanical Engineers (ASME) (Ed.), Proceedings of the ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference 2006 (pp. 399–411). New York: American Society of Mechanical Engineers. doi:10.1115/DETC2006-99524

Allenby, K., & Kelly, T. (2001). Deriving safety requirements using scenarios. In Fifth IEEE International Symposium on Requirements Engineering (pp. 228–235). Piscataway: IEEE. doi:10.1109/ISRE.2001.948563

Altshuller, G. (2004). And suddenly the inventor appeared: TRIZ, the theory of inventive problem solving (6th ed.). Worcester: Technical Innovation Center.

Barnes, D. W., & Mack, J. M. (1975). An algebraic introduction to mathematical logic. New York: Springer.

Barwise, J., & Keisler, H. J. (1977). Handbook of mathematical logic. Amsterdam: North-Holland Pub. Co.

Bauer, W., Chucholowski, N., Lindemann, U., & Maurer, M. S. (2015). Domain-Spanning Change Propagation in Changing Technical Systems. In M.-A. Cardin, D. Krob, P. C. Lui, Y. H. Tan, & K. L. Wood (Eds.), Complex Systems Design & Management Asia (pp. 111–123). Cham: Springer. doi:10.1007/978-3-319-12544-2_9

Baumberger, G. C. (2007). Methoden zur kundenspezifischen Produktdefinition bei individualisierten Produkten. Zugl. Diss. Technische Universität München (2007). München: Dr. Hut.

Becerril, L., Kasperek, D., Roth, M., & Lindemann, U. (2014). Visualization of Interdisciplinary Functional Relations in Complex Systems. In D. Marjanović, M. Storga, N. Pavković, & N. Bojcetić (Eds.), Proceedings of the DESIGN 2014 13th International Design Conference (pp. 1239–1248). Glasgow: Design Society.

Beetzen, C. von. (2015). Refinement of an Approach to Automatically Generate Fault Trees (Semester Thesis). Technical University of Munich, München.

Belski, A., Belski, I., Chong, T. T., & Kwok, R. (2013). Application of substance-field analysis for failure analysis. In A. Aoussat, D. Cavallucci, M. Trela, & J. Duflou (Eds.), Proceedings of the 13th ETRIA World TRIZ Future Conference 2013 (pp. 483–490). Paris: Arts Et Metiers ParisTech.

Belski, I. (2007). Improve your thinking: Substance-field analysis. Melbourne: TRIZ4U.

Bermond, L. (2016). Validierung und Optimierung des Anforderungsmanagementprozesses bei BMW-Motorrad (Master Thesis). Technical University of Munich, München.

Berres, A., & Schumann, H. (2014). Closing the safety process gap: Early integration of safety. In M. S. Maurer & S.-O. Schulze (Eds.), Tag des Systems Engineering (pp. 143–152). München: Carl Hanser.

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

Bertsche, B. (2004). Zuverlässigkeit in Maschinenbau und Fahrzeugtechnik: Ermittlung von Bauteil- und System-Zuverlässigkeiten (3rd ed.). Berlin: Springer.

Bieber, P., Castel, C., & Seguin, C. (2002). Combination of Fault Tree Analysis and Model Checking for Safety Assessment of Complex System. In G. Goos, J. Hartmanis, J. van Leeuwen, A. Bondavalli, & P. Thevenod-Fosse (Eds.), Lecture Notes in Computer Science. Dependable Computing EDCC-4 (Vol. 2485, pp. 19–31). Berlin, Heidelberg: Springer. doi:10.1007/3-540-36080-8_3

Biedermann, W. (2015). A minimal set of network metrics for analysing mechatronic product concepts (Dissertation). Technical University of Munich.

Biehl, M., Chen, D.-J., & Törngren, M. (2010). Integrating safety analysis into the model-based development toolchain of automotive embedded systems. In J. Lee & B. R. Childers (Eds.), Proceedings of the ACM SIGPLAN/SIGBED 2010 Conference on Languages, Compilers, & Tools for Embedded Systems (pp. 125–132). New York: Association for Computing Machinery.

Biggs, G., Sakamoto, T., & Kotoku, T. (2014). A profile and tool for modelling safety information with design information in SysML. Software & Systems Modeling, 1–32. doi:10.1007/s10270-014-0400-x

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. doi:10.1007/978-1-4471-1534-2_14

Blecker, T., Abdelkafi, N., Kaluza, B., & Kreutler, G. (2004). Mass Customization vs. Complexity: A Gordian Knot? In University of Zagreb (Ed.), Anenterprise odyssey. International Conference Proceedings (pp. 890–903). Zagreb.

Blecker, T., Friedrich, G., Kaluza, B., Abdelkafi, N., & Kreutler, G. (2005). Information and management systems for product customization. New York: Springer.

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

Blessing, L. T. M., & Chakrabarti, A. (2009). DRM, a Design Research Methodology. Dordrecht: Springer. Retrieved from http://www.worldcat.org/oclc/432711281

Blum, M. (2010). Effizienter Sicherheitsnachweis für mechatronische Systeme (1st ed.). Göttingen: Sierke.

Bohner, S. A., & Arnold, R. S. (1996). Software change impact analysis. Los Alamitos, Calif.: IEEE Computer Society.

Booker, J. (2012). A survey-based methodology for prioritising the industrial implementation qualities of design tools. Journal of Engineering Design, 23(7), 507–525. doi:10.1080/09544828.2011.624986

Browning, T. R. (2001). Applying the Design Structure Matrix to System Decomposition and Integration Problems: A Review and New Directions. IEEE Transactions on Engineering Management, 48(3), 292–306. doi:10.1109/17.946528

Buede, D. M. (2009). The Engineering Design of Systems. Hoboken, NJ, USA: John Wiley & Sons.

Carlson, C. (2012). Effective FMEAs: Achieving safe, reliable, and economical products and processes using failure mode and effects analysis. Hoboken, NJ, USA: John Wiley & Sons.

Carter, A. (1986). Mechanical reliability (2nd ed.). Basingstoke: Macmillan.

Chesbrough, H. W. (2003). Open innovation: The new imperative for creating and profiting from technology. Boston, Mass: Harvard Business School Press.

Chesbrough, H. W., Vanhaverbeke, W., & West, J. (2014). New Frontiers in Open Innovation. Oxford: Oxford University Press.

Clarke, E. M., Grumberg, O., & Peled, D. A. (1999). Model checking. Cambridge: MIT Press.

Clarkson, P. J., Simons, C., & Eckert, C. M. (2004). Predicting Change Propagation in Complex Design. Journal of Mechanical Design, 126(5), 788. doi:10.1115/1.1765117

Cohen, T., Navathe, S. B., & Fulton, R. E. (2000). C-FAR, change favorable representation. Computer-Aided Design, 32(5-6), 321–338. doi:10.1016/S0010-4485(00)00015-4

Conrad, J., Deubel, T., Köhler, C., Wanke, S., & Weber, C. (2007). Change Impact and Risk Analysis (CIRA)–Combining the COM/PDD Theory and FMEA-Methodology for An Improved Engineering Change Management. In J.-C. Bocquet (Ed.), 16th International Conference on Engineering Design (ICED'07). Glasgow: Design Society.

Cuenot, P., Ainhauser, C., Adler, N., Otten, S., & Meurville, F. (2014, February). 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.

Danilovic, M., & Browning, T. R. (2007). Managing Complex Product Development Projects with Design Structure Matrices and Domain Mapping Matrices. International Journal of Project Management, 25(3), 300–314.

de la Vara, Jose Luis, Borg, M., Wnuk, K., & Moonen, L. (2016). An Industrial Survey of Safety Evidence Change Impact Analysis Practice. IEEE Transactions on Software Engineering, 1–30. doi:10.1109/TSE.2016.2553032

Deubzer, F., & Lindemann, U. (2009). MDM Application to Interrelate Hierarchical Layers of Abstraction. In M. Kreimeyer, J. Maier, G. Fadel, & U. Lindemann (Eds.), Proceedings of the 11th International DSM Conference. Greenville, SC, 12 and 13 October 2009 (pp. 167–178). München: Carl Hanser.

Dorociak, R., & Gausemeier, J. (2012). Modeling of the Failure Propagation of an Advanced Mechatronic System Within the Specification of its Principle Solution. In D. Marjanović, M. Storga, N. Pavkovic, & N. Bojcetic (Eds.), Proceedings of DESIGN 2012, the 12th International Design Conference (pp. 807–816). Glasgow: Design Society.

Dubrova, E. (2013). Fundamentals of Dependability. In E. Dubrova (Ed.), Fault-Tolerant Design (pp. 5–20). New York: Springer. doi:10.1007/978-1-4614-2113-9_2

Dugan, J. B., Bavuso, S. J., & Boyd, M. A. (1992). Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability, 41(3), 363–377. doi:10.1109/24.159800

Eben, K., Daniilidis, C., & Lindemann, U. (2010). Interrelating and Prioritising Requirements on Multiple Hierarchy Levels. In D. Marjanović (Ed.), Design 2010 Proceedings (pp. 1055–1064). Glasgow: Design Society.

Eberhardt, O. (2015). Risikobeurteilung mit FMEA: Die Fehler-Möglichkeits- und Einfluss-Analyse gemäß VDA-Richtlinie 4.2. Die Risikobeurteilung von Maschinen gemäß EU-Richtlinie 2006/42/EG (4th ed.). Renningen: Expert.

Eckert, C. M., Clarkson, P. J., & Zanker, W. (2004). Change and customisation in complex engineering domains. Research in Engineering Design, 15(1), 1–21. doi:10.1007/s00163-003-0031-7

Eckert, C. M., Wyatt, D. F., & Clarkson, P. J. (2009). The elusive act of synthesis: creativity in the conceptual design of complex engineering products. In N. Bryan-Kinns, M. D. Gross, H. Johnson, J. Ox, & R. Wakkary (Eds.), Proceeding of the seventh ACM conference on Creativity and cognition (pp. 265–274). New York: ACM. doi:10.1145/1640233.1640274

Ehrlenspiel, K. (2009). Integrierte Produktentwicklung: Denkabläufe, Methodeneinsatz, Zusammenarbeit (4th ed.). München: Carl Hanser.

Ehrlenspiel, K., Kiewert, A., Lindemann, U., & Mörtl, M. (2014). Kostengünstig Entwickeln und Konstruieren: Kostenmanagement bei der integrierten Produktentwicklung (7th ed.). VDI-Buch. Berlin: Springer Vieweg.

ElMaraghy, H. A. (2005). Flexible and reconfigurable manufacturing systems paradigms. International Journal of Flexible Manufacturing Systems, 17(4), 261–276. doi:10.1007/s10696-006-9028-7

Eppinger, S. D., Joglekar, N. R., Olechowski, A., & Teo, T. (2014). Improving the systems engineering process with multilevel analysis of interactions. Artificial Intelligence for Engineering Design, Analysis and Manufacturing, 28(04), 323–337. doi:10.1017/S089006041400050X

Ericson, C. A. (2005). Hazard Analysis Techniques for System Safety. Hoboken, NJ, USA: John Wiley & Sons.

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

EU Dir.2001/95/EC (2001). Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

EU Dir.2006/42/EC (2006). Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC.

Everdij, M. H. C., Blom, H. A. P., & Kirwan, B. (2006). Development of a Structured Database of Safety Methods (PSAM-0140). In M. G. Stamatelatos & H. S. Blackman (Eds.), Proceedings of the Eighth International Conference on Probabilistic Safety Assessment & Management (PSAM) (pp. 1541–1549). New York: American Society of Mechanical Engineers. doi:10.1115/1.802442.paper191

Fahrmeir, L., Künstler, R., Pigeot, I., & Tutz, G. (2011). Statistik: Der Weg zur Datenanalyse (7th ed.). Berlin: Springer.

Feldmann, S., Herzig, S. J., Kernschmidt, K., Wolfenstetter, T., Kammerl, D., Qamar, A.,. . . Vogel-Heuser, B. (2015). Towards Effective Management of Inconsistencies in Model-Based Engineering of Automated Production Systems. IFAC-PapersOnLine, 48(3), 916–923. doi:10.1016/j.ifacol.2015.06.200

Flanagan, T. L., Eckert, C. M., Eger, T., Smith, J., & Clarkson, P. J. (2003). A Functional Analysis of change propagation. In A. Folkeson, K. Gralen, M. Norell, & U. Sellgren (Eds.), 14th International Conference on Engineering Design. Research for practice : innovation & products, processes and organisations : 19-21 August 2003, the Royal Institute of Technology, Sweden (pp. 441–442). Glasgow: Design Society.

Flaus, J.-M. (2013). Risk analysis: Socio-technical and industrial systems. Hoboken, NJ, USA: John Wiley & Sons.

Fournier, G. (1994). Informationstechnologien in Wirtschaft und Gesellschaft: Sozioökonomische Analyse einer technologischen Herausforderung. Berlin: Duncker & Humblot.

Franke, N., & Hippel, E. von. (2003). Satisfying heterogeneous user needs via innovation toolkits: the case of Apache security software. Open Source Software Development, 32(7), 1199–1215. doi:10.1016/S0048-7333(03)00049-0

Franke, N., & Piller, F. T. (2004). Value creation by toolkits for user innovation and design: The case of the watch market. Journal of Product Innovation Management, 21(6), 401–415.

Fricke, E., Gebhard, B., Negele, H., & Igenbergs, E. (2000). Coping with changes: Causes, findings, and strategies. Systems Engineering, 3(4), 169–179. doi:10.1002/1520-6858(2000)3:4<169::AID-SYS1>3.0.CO;2-W

Fricke, E., & Schulz, A. P. (2005). Design for changeability (DfC): Principles to enable changes in systems throughout their entire lifecycle. Systems Engineering, 8(4). doi:10.1002/sys.20039

Friedenthal, S., Moore, A., & Steiner, R. (2015). A practical guide to SysML: The systems modeling language (Third edition). The MK/OMG Press. Waltham, MA: Elsevier.

Gantenbein, F. (2016). Modellbasierte Auswertungsmethodik zur Gefahrenabsicherung bei Produktindividualisierungen (Semester Thesis). Technical University of Munich, München.

Gassmann, O., & Enkel, E. (2006). Open Innovation. Zeitschrift Führung + Organisation. (3), 132–138.

Gehrlicher, S. (2014). Risiko- und Gefährdungsanalyse von individuellen Produkten (Bachelor Thesis). Technical University of Munich, München.

Ghemraoui, R., Mathieu, L., & Tricot, N. (2009). Design method for systematic safety integration. CIRP Annals - Manufacturing Technology, 58(1), 161–164. doi:10.1016/j.cirp.2009.03.073

Gibson, I., Rosen, D., & Stucker, B. (2015). Additive manufacturing technologies: 3D printing, rapid prototyping, and direct digital manufacturing (2nd ed.). New York: Springer.

Giffin, M., Weck, O. L. de, Bounova, G., Keller, R., Eckert, C. M., & Clarkson, P. J. (2009). Change Propagation Analysis in Complex Technical Systems. Journal of Mechanical Design, 131(8), 81001. doi:10.1115/1.3149847

Goduscheit, R. C., & Jørgensen, J. H. (2013). User toolkits for innovation - a literature review. International Journal of Technology Management, 61(3/4), 274–292. doi:10.1504/IJTM.2013.052671

Gofuku, A., Koide, S., & Shimada, N. (2006). Fault Tree Analysis and Failure Mode Effects Analysis Based on Multi-level Flow Modeling and Causality Estimation. In 2006 SICE-ICASE International Joint Conference (pp. 497–500). doi:10.1109/SICE.2006.315478

Gottschalk, A. (2010). Qualitäts- und Zuverlässigkeitssicherung elektronischer Bauelemente und Systeme: Methoden - Vorgehensweisen - Voraussagen (2nd ed.). Renningen: Expert.

Grantham Lough, K., Stone, R. B., & Tumer, I. Y. (2006). The Risk in Early Design (RED) Method: Likelihood and Consequence Formulations. In ASME 2006 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (pp. 1119–1129). doi:10.1115/DETC2006-99375

Gräßler, I. (2004). Kundenindividuelle Massenproduktion: Entwicklung, Vorbereitung der Herstellung, Veränderungsmanagement. Berlin,: Springer.

Gürtler, M. R., Saucken, C. von, Tesch, T., Damerau, T., & Lindemann, U. (2015). Systematic selection of suitable Open Innovation methods. In International Society for Professional Innovation Management (Ed.), The Proceedings of The XXVI ISPIM Conference 2015. Machester: ISPIM.

Haberfellner, R. (2012). Systems Engineering: Grundlagen und Anwendung. Zürich: Orell Füssli.

Häder, M. (2015). Empirische Sozialforschung: Eine Einführung. Wiesbaden: Springer.

Hahn, U. (2007). Physik für Ingenieure. Berlin: De Gruyter.

Hamraz, B., Caldwell, N. H. M., & Clarkson, P. J. (2012). FBS Linkage Model - Towards an Integrated Engineering Change Prediction and Analysis Method. In D. Marjanović, M. Storga, N. Pavkovic, & N. Bojcetic (Eds.), Proceedings of DESIGN 2012, the 12th International Design Conference (pp. 901–910). Glasgow: Design Society.

Hashemian, M. (2005). Design for Adaptability (PhD Thesis). University of Saskatchewan, Saskatoon.

Haskins, C. (2011). Systems engineering handbook: A guide for system life cycle processes and activities (Version 3.2.2). San Diego: International Council of Systems Engineering.

Hauptmanns, U., Knetsch, T., & Marx, M. (2004). Gefährdungsbäume zur Analyse von Unfällen und Gefährdungen. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin : Forschung: Fb 1028. Bremerhaven: Wirtschaftsverlag NW.

Hause, M. C., & Thom, F. (2007). Integrated safety strategy to model driven development with SysML. In 2nd IET International Conference on System Safety (pp. 124–129). IEEE. doi:10.1049/cp:20070452

Heckel, R. (2006). Graph Transformation in a Nutshell. Electronic Notes in Theoretical Computer Science, 148(1), 187–198.

Hehenberger, P., Egyed, A., & Zeman, K. (2010). Consistency Checking of Mechatronic Design Models. In American Society of Mechanical Engineers (ASME) (Ed.), ASME 2010 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (pp. 1141–1148). American Society of Mechanical Engineers. doi:10.1115/DETC2010-28615

Helms, B. (2013). Object-Oriented Graph Grammars for Computational Design Synthesis (Dissertation). Technical University of Munich, Munich.

Helms, S., Behncke, F. G. H., Lindlöf, L., Wickel, M. C., Maisenbacher, S., & Lindemann, U. (2014). Classification of methods for the Indication of Change Propagation - A Literature Review. In D. Marjanović, M. Storga, N. Pavković, & N. Bojcetić (Eds.), Proceedings of the DESIGN 2014 13th International Design Conference (pp. 211–220). Glasgow: Design Society.

Herfeld, U., Fürst, F., & Braun, T. (2007). Managing complexity in automotive safety development. In U. Lindemann, M. Danilovic, F. Deubzer, M. S. Maurer, & M. Kreimeyer (Eds.), Proceedings of the 9th International DSM Conference (pp. 271–286). Aachen: Shaker.

Hering, E., Triemel, J., & Blank, H.-P. (2003). Qualitätsmanagement für Ingenieure (5th ed.). VDI-Buch. Düsseldorf: VDI.

Hildebrand, V. G. (1997). Individualisierung als strategische Option der Marktbearbeitung: Determinanten und Erfolgswirkungen kundenindividueller. Wiesbaden: Deutscher Universitätsverlag.

Hillenbrand, M. (2012). Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen. Karlsruhe: KIT Scientific Publishing.

Hinterhuber, H. H., Bailom, F., Handlbauer, G., & Matzler, K. (1998). Kundenzufriedenheit durch Kernkompetenzen. In H. Wildemann (Ed.), Innovationen in der Produktionswirtschaft. Produkte, Prozesse, Planung und Steuerung (pp. 339–369). München: TCW.

Hippel, E. von. (2001). Perspektive: User toolkits for innovation. Journal of Product Innovation Management, 18(4), 247–257. doi:10.1016/S0737-6782(01)00090-X

Hippel, E. von. (2005). Democratizing innovation. Cambridge: MIT Press.

Hippel, E. von, & Katz, R. (2002). Shifting Innovation to Users via Toolkits. Management Science, 48(7), 821–833. doi:10.1287/mnsc.48.7.821.2817

Höfig, K., Zeller, M., & Grunske, L. (2014). metaFMEA-A Framework for Reusable FMEAs. In F. Ortmeier & A. Rauzy (Eds.), Lecture Notes in Computer Science. Model-Based Safety and Assessment (Vol. 8822, pp. 110–122). Springer. doi:10.1007/978-3-319-12214-4_9

Holle, M., Gronemann, C., & Lindemann, U. (2015). Customer Individual Product Development - Assessment of Individualisation Potential. In International Society for Professional Innovation Management (Ed.), The Proceedings of The 2015 ISPIM Innovation Summit. Machester: ISPIM.

Holle, M., & Lindemann, U. (2014, December). Design for Open Innovation (DfOI) – Product Structure Planning for Open Innovation Toolkits. International Conference on Industrial Engineering and Engineering Management, Selangor.

Holle, M., Maisenbacher, S., & Lindemann, U. (2015). Design for Open Innovation individualization-oriented product architecture planning. In IEEE (Ed.), 9th Annual IEEE International Systems Conference (SysCon 2015) (pp. 397–402). Piscataway: IEEE. doi:10.1109/SYSCON.2015.7116783

Holle, M., Roth, M., Gürtler, M. R., & Lindemann, U. (2014). From Customer Innovations to Manufactured Products: A Project Outlook. International Journal of Mechanical, Aerospace, Industrial and Mechatronics Engineering, 8(4), 1078–1082.

Holle, M., Straub, I., Roth, M., & Lindemann, U. (2016). Customer individual product development: Methodology for product architecture modification. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 744–749). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490627

Holtta, K. M. M., & Salonen, M. P. (2003). Comparing Three Different Modularity Methods. In American Society of Mechanical Engineers (ASME) (Ed.), ASME 2003 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (3b, pp. 533–541). American Society of Mechanical Engineers. doi:10.1115/DETC2003/DTM-48649

Hood, C. (2008). Requirements management: The interface between requirements development and all other systems engineering processes. Berlin: Springer.

IEC 61078 (2006). Analysis techniques for dependability - Reliability block diagram and boolean methods. Geneva: International Electrotechnical Commission.

IEC 60812 (2006). Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA). Geneva: International Electrotechnical Commission.

IEC 61025 (2006). Fault tree analysis (FTA). Geneva: International Electrotechnical Commission.

IEC 61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission.

IEC 60335-1 (2012). Household and similar electrical appliances - Safety - Part 1: General requirements. Berlin: Beuth.

IEC 60335-2-15 (2012). Household and similar electrical appliances - Safety - Part 2-15: Particular requirements for appliances for heating liquids. Berlin: Beuth.

Inglehart, R. F., Basanez, M., & Moreno, A. (2010). Human Values and Beliefs: A Cross-Cultural Sourcebook. Ann Arbor: University of Michigan Press.

Inness, J. G. (1994). Achieving successful product change: A handbook. London: Financial Times/Pitman.

Isemann, M. (2015). Optimierung der FMEA für individualisierbare Produkte durch Model-Based Systems Engineering (Semester Thesis). Technical University of Munich, München.

ISO 26262 (2011). Road vehicles - Functional safety. Berlin: Beuth.

ISO 12100 (2011). Safety of machinery - General principles for design - Risk assessment and risk reduction. Berlin: Beuth.

ISO 9001 (2015). Quality management systems - Requirements. Berlin: Beuth.

Jakumeit, E., Buchwald, S., & Kroll, M. (2010). GrGen.NET. International Journal on Software Tools for Technology Transfer, 12(3-4), 263–271. doi:10.1007/s10009-010-0148-8

Jarratt, T. A. W., Clarkson, P. J., & Eckert, C. M. (2005). Engineering change. In P. J. Clarkson & C. M. Eckert (Eds.), Design process improvement. A review of current practice (pp. 262–285). London: Springer.

Jarratt, T. A. W., Eckert, C. M., Caldwell, N. H. M., & Clarkson, P. J. (2011). Engineering change: an overview and perspective on the literature. Research in Engineering Design, 22(2), 103–124. doi:10.1007/s00163-010-0097-y

Jensen, D. C., & Tumer, I. Y. (2013). Modeling and Analysis of Safety in Early Design. 2013 Conference on Systems Engineering Research, 16, 824–833. doi:10.1016/j.procs.2013.01.086

Jiang, X., Liang, S., Ding, W., & Wang, W. (2007). Research on Quality Management System for Individualized Customization Based-Customer Satisfaction. In 2007 IEEE International Conference on Automation and Logistics (pp. 1156–1161). doi:10.1109/ICAL.2007.4338743

Joshi, A., Vestal, S., & Binns, P. (2007). Automatic generation of static fault trees from aadl models. In IEEE (Ed.), 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007. Los Alamitos: IEEE Computer Society.

Kamiske, G. F., & Brauer, J.-P. (2011). Qualitätsmanagement von A bis Z: Erläuterungen moderner Begriffe des Qualitätsmanagements. München: Carl Hanser.

Kasperek, D., Kohn, A., & Maurer, M. S. (2013). Identifying Uncertainties Within Structural Complexity Management. In U. Lindemann, S. Venkataraman, Y. S. Kim, S. W. Lee, P. J. Clarkson, & G. Cascini (Eds.), 19th International Conference on Engingeering Design (ICED'13) (Vol. 1, pp. 41–50). Glasgow: Design Society.

Keuneke, S. (2005). Qualitatives Interview. In L. Mikos & C. Wegener (Eds.), Qualitative Medienforschung. Ein Handbuch (pp. 254–267). Konstanz: UVK Verlagsgesellschaft.

Kissel, M. (2014). Mustererkennung in komplexen Produktportfolios. Zugl. Diss. Technische Universität München (2014). München: Dr. Hut.

Koeppen, B. (2008). Modularisierung komplexer Produkte anhand technischer und betriebswirtschaftlicher Komponentenkopplungen. Produktentwicklung. Aachen: Shaker.

Koh, E. C. Y., Caldwell, N. H. M., & Clarkson, P. J. (2012). A method to assess the effects of engineering change propagation. Research in Engineering Design, 23(4), 329–351. doi:10.1007/s00163-012-0131-3

Koh, E. C. Y., Förg, A., Kreimeyer, M., & Lienkamp, M. (2015). Using engineering change forecast to prioritise component modularisation. Research in Engineering Design, 26(4), 337–353. doi:10.1007/s00163-015-0200-5

Kohl, M. (2015). Berücksichtigung sicherheitsrelevanter Aspekte in der Modularisierung (Bachelor Thesis). Technical University of Munich, München.

Kohl, M., Roth, M., & Lindemann, U. (2016). Safety-oriented Modular Function Deployment. In C. Boks, J. Sigurjonsson, M. Steinert, C. Vis, & A. Wulvik (Eds.), Proceedings of NordDesign 2016 (Vol. 2, pp. 103–113). Bristol: Design Society.

Kohn, A. (2014). Entwicklung einer Wissensbasis für die Arbeit mit Produktmodellen. Produktentwicklung. München: Dr. Hut.

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.

Kowalski, S. (2016). Effektchecklisten für die Produktindividualisierung (Semester Thesis). Technical University of Munich, München.

Kreyszig, E. (1988). Statistische Methoden und ihre Anwendungen: Mit zahlr. Tab. Göttingen: Vandenhoeck & Ruprecht.

Krus, D., & Grantham Lough, K. (2007). Risk due to Function Failure Propagation. In J.-C. Bocquet (Ed.), 16th International Conference on Engineering Design (ICED'07). Glasgow: Design Society.

Kurtoglu, T., & Tumer, I. Y. (2008). A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems. Journal of Mechanical Design, 130(5), 51401. doi:10.1115/1.2885181

Kurz, A., Stockhammer, C., Fuchs, S., & Meinhard, D. (2009). Das problemzentrierte Interview. In R. Buber & H. H. Holzmüller (Eds.), Qualitative Marktforschung. Konzepte, Methoden, Analysen (2nd ed., pp. 463–475). Wiesbaden: Gabler.

Lachmayer, R., Gembarski, P. C., Gottwald, P., & Lippert, R. B. (2015). The Potential of Product Customization using Technologies of Additive Manufacturing. In Managing complexity. Proceedings of the 8th World Conference on Mass Customization, Personalization and Co-Creation (MCPC). Springer.

Langer, S. (2016). Änderungsmanagement. In U. Lindemann (Ed.), Handbuch Produktentwicklung (pp. 513–539). München: Carl Hanser.

Leveson, N. (2004). A new accident model for engineering safer systems. Safety Science, 42(4), 237–270. doi:10.1016/S0925-7535(03)00047-X

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

Li, G. (2012). Ontology-Based Reuse of Failure Modes for FMEA: Methodology and Tool. In 2012 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) (pp. 17–18). doi:10.1109/ISSREW.2012.42

Lindemann, U. (2005). Wünsche eines Produktentwicklers an das Controlling. In H. Jander & J. Grasshoff (Eds.), Schriftenreihe Schriften zum betrieblichen Rechnungswesen und Controlling: Bd. 27. Betriebliches Rechnungswesen und Controlling im Spannungsfeld von Theorie und Praxis. Festschrift für Prof. Dr. Jürgen Grasshoff zum 65. Geburtstag (pp. 345–361). Hamburg: Kovač.

Lindemann, U. (2009). Methodische Entwicklung technischer Produkte: Methoden flexibel und situationsgerecht anwenden (3rd ed.). VDI-Buch. Berlin: Springer.

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

Lindemann, U., & Reichwald, R. (1998). Integriertes Änderungsmanagement. Berlin: Springer.

Lindemann, U., Reichwald, R., & Zäh, M. F. (2006). Individualisierte Produkte-Komplexität beherrschen in Entwicklung und Produktion (1st ed.). VDI. Berlin: Springer.

Maier, J. F., Wynn, D. C., Biedermann, W., Lindemann, U., & Clarkson, P. J. (2014). Simulating progressive iteration, rework and change propagation to prioritise design tasks. Research in Engineering Design, 25(4), 283–307. doi:10.1007/s00163-014-0174-8

Maimon, O., & Rokach, L. (2010). Data mining and knowledge discovery handbook (2nd ed.). New York: Springer.

Majdara, A., & Wakabayashi, T. (2009). Component-based modeling of systems for automated fault tree generation. Reliability Engineering & System Safety, 94(6), 1076–1086. doi:10.1016/j.ress.2008.12.003

Martin, M. V., & Ishii, K. (2002). Design for variety: developing standardized and modularized product platform architectures. Research in Engineering Design, 13(4), 213–235. doi:10.1007/s00163-002-0020-2

Maurer, M. S., & Kesper, H. (2011). eFMEA— Raising Efficiency of FMEA by Matrix-Based Function and Failure Networks. In A. Chakrabarti (Ed.), Proceedings of the 3rd International Conference on Research into Design (ICoRD'11) (pp. 179–186).

Mayer, R. (1993). Strategien erfolgreicher Produktgestaltung: Individualisierung und Standardisierung. DUV. Wiesbaden: Deutscher Universitätsverlag.

McIver, J. P., & Carmines, E. G. (1981). Unidimensional scaling. Beverly Hills: Sage Publications.

Mhenni, F., Choley, J.-Y., & Nguyen, N. (2014). Extended Mechatronic Systems Architecture Modeling with SysML for Enhanced Safety Analysis. In IEEE (Ed.), 2014 IEEE International Systems Conference (SysCon 2014) Proceedings (pp. 378–382). Piscataway: IEEE.

Mhenni, F., Nguyen, N., & Choley, J.-Y. (2014). Automatic fault tree generation from SysML system models. In IEEE/ASME (Ed.), International Conference on Advanced Intelligent Mechatronics (AIM) (pp. 715–720). doi:10.1109/AIM.2014.6878163

Mhenni, F., Nguyen, N., & Choley, J.-Y. (2016). SafeSysE: A Safety Analysis Integration in Systems Engineering Approach. IEEE Systems Journal, 1–12. doi:10.1109/JSYST.2016.2547460

Mhenni, F., Nguyen, N., Kadima, H., & Choley, J.-Y. (2013). Safety analysis integration in a SysML-based complex system design process. In 2013 7th Annual IEEE Systems Conference (SysCon) (pp. 70–75). doi:10.1109/SysCon.2013.6549861

Michalewicz, Z., & Fogel, D. B. (2004). How to Solve It: Modern Heuristics (2nd ed.). Berlin: Springer.

MIL-STD-882E (2012). Department of Defense Standard Practice for System Safety: US Department of Defense.

Mooney, C. Z. (1997). Monte Carlo Simulation. Sage university papers series. Quantitative applications in the social sciences: no. 07-116. Thousand Oaks, CA: Sage Publications.

Müller, M. (2015). Sicherheitsanalyse von Architekturkonzepten durch Verbindung von SysML und Fehleranalysemethoden (Master Theses). Technical University of Munich, München.

Müller, M., Roth, M., & Lindemann, U. (2016). The Hazard Analysis Profile: Linking Safety Analysis and SysML. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 123–129). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490532

Münzberg, C., Hammer, J., Brehm, A., & Lindemann, U. (2014). Further Development of TRIZ Function Analysis based on Applications in Projects. In D. Marjanović, M. Storga, N. Pavković, & N. Bojcetić (Eds.), Proceedings of the DESIGN 2014 13th International Design Conference (pp. 333–342). Glasgow: Design Society.

Nair, S., de la Vara, Jose Luis, Sabetzadeh, M., & Briand, L. (2014). An extended systematic literature review on provision of evidence for safety certification. Information and Software Technology, 56(7), 689–717. doi:10.1016/j.infsof.2014.03.001

Neudörfer, A. (2014). Konstruieren sicherheitsgerechter Produkte: Methoden und systematische Lösungssammlungen zur EG-Maschinenrichtlinie (6th ed.). VDI-Buch. Berlin: Springer.

Neufville, R. de, & Scholtes, S. (2011). Flexibility in engineering design. Cambridge, Mass.: MIT Press.

Ollinger, G. A., & Stahovich, T. F. (2001). RedesignIT - A Constraint-based Tool for Managing Design Changes. In American Society of Mechanical Engineers (ASME) (Ed.), Proceedings of DETC'01 (pp. 1–11). American Society of Mechanical Engineers.

Ollinger, G. A., & Stahovich, T. F. (2004). RedesignIT—A Model-Based Tool for Managing Design Changes. Journal of Mechanical Design, 126(2), 208. doi:10.1115/1.1666888

Oppen, G. v., & Melchert, F. (2005). Physik für Ingenieure: Von der klassischen Mechanik zu den Quantengasen. München: Pearson Studium.

Pahl, G., Beitz, W., Feldhusen, J., & Grote, K.-H. (2007). Engineering Design (3rd ed.). London: Springer.

Papadopoulos, Y., & Maruhn, M. (2001). Model-based Synthesis of Fault Trees from Matlab-Simulink Models. In International Conference on Dependable Systems and Networks (DSN 2001) (pp. 77–82). Los Alamitos: IEEE Computer Society. doi:10.1109/DSN.2001.941393

Papadopoulos, Y., Parker, D., & Grante, C. (2004). Automating the failure modes and effects analysis of safety critical systems. In IEEE (Ed.), Eighth IEEE International Symposium on High Assurance Systems Engineering, 2004 (pp. 310–311). doi:10.1109/HASE.2004.1281774

Papakonstantinou, N., Sierla, S., & Koskinen, K. (2011). Generating and validating product instances in IEC 61131–3 from feature models. In Factory Automation (ETFA 2011) (pp. 1–8). doi:10.1109/ETFA.2011.6058977

Pasqual, M. C., & Weck, O. L. de. (2012). Multilayer network model for analysis and management of change propagation. Research in Engineering Design, 23(4), 305–328. doi:10.1007/s00163-011-0125-6

Piller, F. T. (2001). Mass customization: Ein wettbewerbsstrategisches Konzept im Informationszeitalter (2nd ed.). Wiesbaden: Deutscher Universitätsverlag.

Piller, F. T. (2006). Mass customization: Ein wettbewerbsstrategisches Konzept im Informationszeitalter (4th ed.). Wiesbaden: Deutscher Universitätsverlag.

Piller, F. T., Moeslein, K., & Stotko, C. M. (2004). Does mass customization pay? An economic approach to evaluate customer integration. Production Planning & Control, 15(4), 435–444. doi:10.1080/0953728042000238773

Piller, F. T., & Stotko, C. M. (2003). Mass customization und Kundenintegration: Neue Wege zum innovativen Produkt (1st ed.). Düsseldorf: Symposion Publishing.

Piller, F. T., & Walcher, D. (2006). Toolkits for idea competitions: a novel method to integrate users in new product development. R and D Management, 36(3), 307–318. doi:10.1111/j.1467-9310.2006.00432.x

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

Pine, B. J. (1993). Mass customization: The new frontier in business competition. Boston, Mass.: Harvard Business School Press.

Pine, B. J., Peppers, D., & Rogers, M. (1995). Do You Want to Keep Your Customers Forever? Harvard Business Review. (03/04), 103–114.

Pohl, K., & Rupp, C. (2015). Basiswissen Requirements Engineering: Aus- und Weiterbildung zum "Certified Professional for Requirements Engineering" ; Foundation Level nach IREB-Standard (4th ed.). Heidelberg: dpunkt.

Pulm, U. (2004). Eine systemtheoretische Betrachtung der Produktentwicklung. München: Dr. Hut.

Rapp, M. A. (2015). Entwicklung einer Methodik zur Identifikation, Validierung und durchgängigen Dokumentation von Sicherheitsanforderungen (Semester Thesis). Technical University of Munich, München.

Reddi, K. R., & Moon, Y. B. (2009). A framework for managing engineering change propagation. International Journal of Innovation and Learning, 6(5), 461–476.

Refsgaard, J. C., van der Sluijs, Jeroen P., Brown, J., & van der Keur, P. (2006). A framework for dealing with uncertainty due to model structure error. Advances in Water Resources, 29(11), 1586–1597. doi:10.1016/j.advwatres.2005.11.013

Regazzoni, D., & Russo, D. (2011). TRIZ tools to enhance risk management. Procedia Engineering, 9, 40–51. doi:10.1016/j.proeng.2011.03.099

Reichwald, R., Piller, F. T., & Ihl, C. (2009). Interaktive Wertschöpfung: Open Innovation, Individualisierung und neue Formen der Arbeitsteilung (2nd ed.). Wiesbaden: Gabler.

Robinson, I., Webber, J., & Eifrem, E. (2013). Graph databases (First edition). Sebastopol, Calif., Sebastopol, CA: O'Reilly Media.

Roland, H. E., & Moriarty, B. (1990). System Safety Engineering and Management. Hoboken, NJ, USA: John Wiley & Sons.

Roth, M., Beetzen, C. von, & Lindemann, U. (2016). Matrix-based Multi-hierarchy Fault Tree Generation and Evaluation. In IEEE (Ed.), 2016 Annual IEEE Systems Conference (SysCon 2016) (pp. 140–146). Piscataway: IEEE. doi:10.1109/SYSCON.2016.7490535

Roth, M., & Gantenbein, F. (2016). Model-based Hazard and Propagation Assessment of Product Changes. In American Society of Mechanical Engineers (ASME) (Ed.), 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Charlotte: American Society of Mechanical Engineers.

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. Marjanović, & 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.

Roth, M., Harmeling, J., Michailidou, I., & Lindemann, U. (2015). The "Ideal" User Innovation Toolkit - Benchmarking and Concept Development. In C. Weber, S. Husung, G. Cascini, M. Cantamessa, D. Marjanović, & M. Bordegoni (Eds.): Vol. 9. Proceedings of the 20th International Conference on Engineering Design (ICED 15), User-centred design, design of socio-technical systems (pp. 249–260). Glasgow: Design Society.

Roth, M., Kasperek, D., & Lindemann, U. (2013). Functional Analysis and Modeling of Complex, Evolutionary Grown, Mechatronic Products. In IEEE (Ed.), 2013 IEEE International Conference on Industrial Engineering and Engineering Management (pp. 346–350). Piscataway: IEEE. doi:10.1109/IEEM.2013.6962431

Roth, M., Mayr, L., & Lindemann, U. (2016). A Knowledge Framework for Safety Analysis of User-Induced Changes. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 1553–1562). Glasgow: Design Society.

Roth, M., Münzberg, C., & Lindemann, U. (2016). A Method to Explicate Safety Functions. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 463–472). Glasgow: Design Society.

Roth, M., Ulrich, C. M., Holle, M., & Lindemann, U. (2016). The Impact of User-driven Customization on the Development Process. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 1357–1366). Glasgow: Design Society.

Roth, M., Wolf, M., & Lindemann, U. (2015). Integrated Matrix-based Fault Tree Generation and Evaluation. Procedia Computer Science, 44, 599–608. doi:10.1016/j.procs.2015.03.027

Rutka, A., Guenov, M. D., Lemmens, Y., Schmidt-Schäffer, T., Coleman, P., & Rivière, A. (2006). Methods for engineering change propagation analysis. In ICAS (Ed.), Proceedings of 25th Congress of the International Council of the Aeronautical Sciences.

Samuelson, P. A. (1995). Diagrammatic Exposition of a Theory of Public Expenditure. In S. Estrin & A. Marin (Eds.), Essential Readings in Economics (pp. 159–171). London: Macmillan. doi:10.1007/978-1-349-24002-9_8

Saucken, C. von, Gürtler, M. R., Schneider, M., & Lindemann, U. (2015). A Method Model for Distinguishing and Selecting Open Innovation Methods. In C. Weber, S. Husung, G. Cascini, M. Cantamessa, & D. Marjanović (Eds.): Vol. 8. Proceedings of the 20th International Conference on Engineering Design, Innovation and Creativity (pp. 203–212). Glasgow: Design Society.

Schenk, M., Müller, E., & Wirth, S. (2014). Fabrikplanung und Fabrikbetrieb: Methoden für die wandlungsfähige, vernetzte und ressourceneffiziente Fabrik (2nd ed.). Berlin: Springer.

Schuh, G. (2005). Produktkomplexität managen: Strategien - Methoden - Tools (2nd ed.). München: Carl Hanser.

Schürmann, J. (2016). Pattern-Based Validation of Product Models (Master Thesis). Technical University of Munich, München.

Sierla, S., Tumer, I. Y., Papakonstantinou, N., Koskinen, K., & Jensen, D. C. (2012). Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework. Mechatronics, 22(2), 137–151. doi:10.1016/j.mechatronics.2012.01.003

Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. Requirements Engineering, 10(1), 34–44. doi:10.1007/s00766-004-0194-4

Spallek, J., Sankowski, O., & Krause, D. (2016). Influences of Additive Manufacturing on Design Processes for Customised Products. In D. Marjanović, M. Storga, N. Pavković, N. Bojcetic, & S. Skec (Eds.), Proceedings of the DESIGN 2016 14th International Design Conference (pp. 513–522). Glasgow: Design Society.

Stachowiak, H. (1973). Allgemeine Modelltheorie. Wien, New York: Springer Vieweg.

Stamatis, D. H. (2003). Failure mode and effect analysis: FMEA from theory to execution (2nd ed.). Milwaukee: ASQ Quality Press.

Stirgwolt, P. (2013). Effective management of functional safety for ISO 26262 standard. In IEEE (Ed.), The 59th Annual Reliability and Maintainability Symposium (pp. 1–6). Piscataway: IEEE. doi:10.1109/RAMS.2013.6517758

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. doi:10.1016/S0142-694X(99)00003-4

Swain, A. D., & Guttmann, H. E. (1983). Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Washington D.C.: U.S. Nuclear Regulatory Commission.

Tajarrod, F., & Latif-Shabgahi, G. (2008). A Novel Methodology for Synthesis of Fault Trees from MATLAB-Simulink Model. World Academy of Science, Engineering and Technology, 17(5), 1234–1240.

Taylor, Z., & Ranganathan, S. (2014). Designing high availability systems: Design for Six Sigma and classical reliability techniques with practical real-life examples. Hoboken, NJ, USA: John Wiley & Sons.

Terninko, J., Zusman, A., & Zlotin, B. (1998). Systematic innovation: An introduction to TRIZ (theory of inventive problem solving). Boca Raton: St. Lucie Press.

Terwiesch, C., & Loch, C. H. (1999). Managing the process of engineering change orders: The case of the climate control system in automobile development. Journal of Product Innovation Management, 16(2), 160–172. doi:10.1016/S0737-6782(98)00041-1

Thomke, S. H., & Hippel, E. von. (2004). Customers As Innovators: A New Way to Create Value. Harvard Business Review, 80(4), 51–61.

Thramboulidis, K., & Scholz, S. (2016). Integrating the 3+1 SysML view model with safety engineering. In IEEE Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1–8). IEEE. doi:10.1109/ETFA.2010.5641353

Tiemann, V. (2003). Einführung Statistik: Grundlagen, Techniken und Verblüffendes. Wiesbaden: Gabler.

Tilstra, A. H., Seepersad, C. C., & Wood, K. L. (2012). A high-definition design structure matrix (HDDSM) for the quantitative assessment of product architecture. Journal of Engineering Design, 23(10-11), 767–789. doi:10.1080/09544828.2012.706748

Tuot, K. (2015). Process-driven document analysis and understanding. München: Dr. Hut.

Ulrich, C. M. (2015). Auswirkungen der kundenbezogenen Produktindividualisierung auf den Entwicklungsprozess technischer Produkte (Master Thesis). Technical University of Munich, München.

Ulrich, K. T. (1995). The role of product architecture in the manufacturing firm. Research Policy, 24(3), 419–440. doi:10.1016/0048-7333(94)00775-3

Ulrich, K. T., & Eppinger, S. D. (2004). Product design and development (3rd ed.). Boston: McGraw-Hill.

Ulrich, K. T., & Seering, W. P. (1990). Function sharing in mechanical design. Design Studies, 11(4), 223–234. doi:10.1016/0142-694X(90)90041-A

van Beek, T. J., & Tomiyama, T. (2008). Connecting Views in Mechatronic Systems Design, a Function Modeling Approach. In International Conference on Mechatronic and Embedded Systems and Applications (MESA'2008) (pp. 164–169). Piscataway: IEEE. doi:10.1109/MESA.2008.4735676

VDI 2206 (2004). Design methodology for mechatronic systems. Berlin: Beuth.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). Fault Tree Handbook. NUREG-0492. Washington D.C.: U.S. Nuclear Regulatory Commission.

Vesely, W. E., Stamatelatos, M. G., Dugan, J., Fragola, J., Minarick, J., & Railsback, J. (2002). Fault Tree Handbook with Aerospace Applications. Washington D.C.: NASA.

Vogel-Heuser, B., Folmer, J., Aicher, T., Mund, J., & Rehberger, S. (2015). Coupling simulation and model checking to examine selected mechanical constraints of automated production systems. In IEEE (Ed.), 13th International Conference on Industrial Informatics (INDIN) (pp. 37–42). Piscataway: IEEE. doi:10.1109/INDIN.2015.7281707

Walcher, D. (2007). Der Ideenwettbewerb als Methode der aktiven Kundenintegration: Theorie, empirische Analyse und Implikationen für den Innovationsprozess. Wiesbaden: Deutscher Universitätsverlag.

Walker, W. E., Harremoës, P., Rotmans, J., van der Sluijs, Jeroen P., van Asselt, M., Janssen, P., & Krayer von Krauss, M. P. (2003). Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-Based Decision Support. Integrated Assessment, 4(1), 5–17. doi:10.1076/iaij.4.1.5.16466

Wang, J., & Ruxton, T. (1997). A Review of Safety Analysis Methods Applied to the Design Process. Journal of Engineering Design, 8(2), 131–152. doi:10.1080/09544829708907957

Weber, C. (2005). CPM/PDD–an extended theoretical approach to modelling products and product development processes. In H. Bley, H. Jansen, F.-L. Krause, & M. Shpitalni (Eds.), Proceedings of the 2nd German-Israeli Symposium on Advances in Methods and Systems for Development of Products and Processes (pp. 159–179). Stuttgart: Fraunhofer-IRG.

Weilkiens, T. (2007). Systems engineering with SysML/UML: Modeling, analysis, design. The OMG press. Burlington: Morgan Kaufmann.

Werdich, M. (2011). FMEA - Einführung und Moderation: Durch systematische Entwicklung zur übersichtlichen Risikominimierung (inkl. Methoden im Umfeld) (1st ed.). Wiesbaden: Springer.

Wickel, M. C., & Lindemann, U. (2015). How to build up an Engineering Change dependency model based on past change data? In T. R. Browning, S. D. Eppinger, D. M. Schmidt, & U. Lindemann (Eds.), Modeling and managing complex systems. Proceedings of the 17th International DSM Conference (pp. 221–231). München: Carl Hanser.

Wolf, M. (2014). Integration von Fehleranalyse- und Qualitätsmanagement Methoden in die Strukturmodellierung (Bachelor Thesis). Technical University of Munich, München.

Wölkl, S., & Shea, K. (2009). A Computational Product Model for Conceptual Design Using SysML. In American Society of Mechanical Engineers (ASME) (Ed.), ASME 2009 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (pp. 635–645). doi:10.1115/DETC2009-87239

Wright, I. C. (1997). A review of research into engineering change management: Implications for product design. Design Studies, 18(1), 33–42. doi:10.1016/S0142-694X(96)00029-4

Würtenberger, J., Kloberdanz, H., Lotz, J., & Ahsen, A. von (2014). Application of the FMEA During the Product Development Process - Dependencies Between Level of Information and Quality of Result. In D. Marjanović, M. Storga, N. Pavković, & N. Bojcetić (Eds.), Proceedings of the DESIGN 2014 13th International Design Conference (pp. 417–426). Glasgow: Design Society.

Xiang, J., Yanoo, K., Maeno, Y., & Tadano, K. (2011, January). Automatic Synthesis of Static Fault Trees from System Models. In 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement (pp. 127–136). Piscataway: IEEE. doi:10.1109/SSIRI.2011.32

Zwicky, F. (1966). Entdecken, Erfinden, Forschen im morphologischen Weltbild: Droemer/Knaur.

9. Appendix

This appendix provides further information on the studies and support methods presented in this thesis. It includes details of the questionnaire survey and focus-interviews conducted in chapter 3. Moreover, details on the construction of the ESMK knowledge framework and a description of all ESMK methods is given. In addition, the evaluation questionnaires are provided.

9.1 Details of the Questionnaire Survey on UDC Impacts

This section provides details of the questionnaire survey presented in Section 3.2. They originate from the connected student project (Ulrich, 2015) and the prior publication (Roth et al., 2016). To prevent potential bias, the questions and transcripts of interviews as well as the questionnaire are provided in their original German form and are not translated.

9.1.1 Semi-structured Interview Guideline of the Qualitative Exploration

The semi-structured guideline used within the qualitative interviews consited of the following ten question items (Ulrich, 2015):

Interviewleitfaden

- *In welchem Bereich arbeiten Sie? Wie lange sind Sie dort bereits tätig?*
- *In wie fern ist Ihre Arbeit mit einzelnen Phasen der Produktentwicklung verknüpft?*
- *Welche Aspekte der Anforderungen werden von der kundenindividuellen Produktentwicklung beeinflusst und inwiefern?*
- *Sehen Sie Auswirkungen der kundenbezogenen Produktindividualisierung im Bereich der Konzeption eines Produktes? Wenn ja wo genau?*
- *Sind Ihrer Meinung nach Bereiche beim Produktentwurf durch kundenspezifische Individualisierung betroffen? Wenn ja, welche?*
- *Welcher Zusammenhang besteht zwischen der Entwicklung eines kundenindividuellen Produktes und dem Prozess der Ausarbeitung?*
- *Wo sehen Sie Auswirkungen und neuartige Anforderungen der individuellen Produktgestaltung durch den Kunden auf die Systemintegration? Erläutern Sie bitte.*
- *Neben der eben besprochenen inhaltlichen Planung der Entwicklung und Konstruktion gibt es als Rahmenbedingungen ebenso die zeitliche/terminliche Planung sowie die Kostenplanung (Target Costing) der Produktentwicklung. Welchen Einfluss der Produktindividualisierung durch den Kunden sehen Sie dort?*
- *Welche neuen Herausforderungen sehen Sie für das Risikomanagement bei der Produktentwicklung im Zusammenhang mit „offener Produktindividualisierung“?*
- *Wie wird Ihrer Meinung nach das Konfigurationsmanagement durch die kundenbezogene Produktindividualisierung beeinflusst?*

9.1.2 Transcripts of the Semi-structured Interviews

The semi-structured interviews were conducted by the involved student, recorded on audio file, and transcribed afterwards. In the following, the transcripts of the interviews in their original language are provided (Ulrich, 2015):

Transcript of Interview I (2015/06/22)
Attendees: Consultant (E1), Interviewer (I)

Description of E1:
E1 works as consultant since ten years. He is involved in projects, which address all phases of the product life cycle, starting from concept development up to sales and distribution. He mainly is involved in business-to-business relationships in the automobile and plant industry as well as in process engineering. His focus there is the product design and innovation management.

Interview:
I: In welchem Bereich sind Sie genau tätig?
E1: Ich bin in einer Unternehmensberatung tätig, die Unternehmen hilft, Produkte zu entwickeln. Man könnte es auch als Business Development bezeichnen. Also nicht als knallharte Produktentwicklung. Also die Phasen davor, wie müssen Produkte definiert werden und wie müssen diese aussehen, damit dann am Ende damit Geschäft gemacht werden kann.
I: Und wie lange sind Sie dort schon tätig?
E1: Seit 10 Jahren.
I: Das heißt also bei Ihrer Arbeit sind Sie in allen Phasen der Produktentwicklung (PE) tätig?
E1: Nicht in allen Phasen. Als Berater bin ich natürlich involviert bis zur Markteinführung. Aber der Fokus liegt auf der Arbeit bis das Lastenheft erstellt worden ist. Erst wird das Lastenheft definiert und dann fängt irgendein CAD-Zeichner an, die Konstruktion festzulegen. Wir machen aus den schwammigen Kundenanforderungen ein knallhartes Lastenheft und dann geht es über zur PE. Bis dahin bin ich immer dabei.
I: Dann können wir zum Thema Anforderungen in Bezug auf das Lastenheft kommen. Im Fall der eben besprochenen Kundenindividualisierung, z.B. im dem Projekt „InnoCyFer“ mit Bosch Siemens Hausgeräte (BSH), was ändert sich Ihrer Meinung nach in Bezug auf die Anforderungen? Was wird vielleicht einfacher, was wird komplizierter? Inwiefern gibt es dort neue Herausforderungen auf die Anforderungen bezogen?
E1: Jetzt ist es so, wenn BSH in einem Szenario, in dem es diese kundenindividualisierte Produkte anbieten will, entspricht das in dem Fall ungefähr den Herausforderungen, die bei Mass Customization aufgestellt worden sind. Da gab es einen Arbeitskreis vor etwa zehn Jahren, den Herr Moser und der Herr Piller am Lehrstuhl in Reichwald durchgeführt haben. Da gab es ein Projekt mit 15 Industriepartnern über 2 Jahre. Dort wurden monatliche Workshops durchgeführt, wo genau diese Fragen besprochen worden sind. Wenn Sie jetzt zum Beispiel fragen, welche Herausforderungen es gibt, um kundenindividualisierte Produkte herstellen zu können, dann gibt es das erste Thema: Sie brauchen ein funktionsfähiges Frontend, also einen Konfigurator, dann brauchen Sie dahinter einen Modulbaukasten, der da liegt, weil Sie können nicht alle Produkte mit 3D-Druck-Technik herstellen.
I: Ja genau, aber da sind Sie ja eher im Bereich der Konzeption und beim Entwurf.
E1: Das müssen Sie halt von Anfang an mit in Ihre Überlegungen einbeziehen.
I: Ja genau das ist der erste Schritt, bei dem das alles vorberietet wird.
E1: Sie können nicht sagen, wir machen hier ein kundenindividualisiertes Produkt, ohne dass sie sich im Vorfeld überlegen, aus welchen Modulen dieses Produkt bestehen kann. Außer Sie haben ein reines kundenindividualisiertes Produkt, wo Ihre Fertigungstechnologie, und jetzt kommen wir zum nächsten Punkt,

Sie brauchen also eine modulfähige Fertigungstechnologie oder eine die gar keine Module nötig hat, also wie eine 3D-Druck Technologie. Also das wäre eine nächste Herausforderung, das heißt ihr Produkt muss über Module oder 3D-Druckverfahren herstellbar sein. Was zum Beispiel bei vielen Produkten extrem schwierig wird das zu tun. Es entstehen ja dann geraume Kosten, wenn Sie so was machen wollen in Ihrem Fertigungsprozess. Dann haben Sie das ganze Logistikproblem, denn dann müssen Sie ja die ganzen Module vorrätig haben, Sie müssen die fertigen oder Sie brauchen eine Zuliefererstruktur hinter dem Modul. Das kann ja beliebig aufwendig und komplex werden. Da gibt es ja dieses Beispiel vom neuen Audi, da gibt es 10^32 verschiedene Ausführungen.

I: Varianten in diesem Fall.

E1: Ja genau. Und das ergibt sich im Fall einer Kaffeemaschine auch, wenn Sie Änderungen zulassen.

I: In diesem Fall gibt es da sogar unendlich viele Varianten.

E1: Genau.

I: Deswegen hatte ich zur Vorbereitung auch nochmal die Merkmale der Anforderungsliste zur Verfügung gestellt. Könnten Sie da vielleicht sagen, was Sie hauptsächlich als problematisch ansehen auf diese wirklich kundeninduzierte individuelle Produktentwicklung.

E1: Fangen wir mal früher an: Sie brauchen überhaupt einen Kunden der das Bedürfnis hat und die Zahlungsbereitschaft für dieses Preisprämium mitbringt. Denn Sie werden dieses Produkt niemals zu dem Preis herstellen können, zu dem Sie ein nicht individualisiertes Produkt herstellen. D.h. Sie brauchen einen Kunden, der das gerne möchte, dass es individualisiert ist und der bereit ist dafür Geld zu bezahlen. Ich würde sagen in 99.8% aller Fälle ist das nicht gegeben, da die Kunden sagen, wenn die Kaffeemaschine das Zweifache kostet, nur weil der Knopf anders platziert ist oder die Farbe anders ist, das bin ich nicht bereit zu zahlen. Weil Sie müssen sich ja überlegen, das Thema das in der Autoindustrie abläuft, ist ja eigentlich nicht Individualisierung sondern Massenproduktion in Variantenbauweise. Das ist ja was anderes. D.h. sicherlich kann man sagen, es gibt es Firmen wie Dacia, da gibt es keine Varianten, deswegen können die auch Kosten raus nehmen, weil sie diese Variantenvielfalt nicht haben und sie können dann Autos auch auf Halde produzieren und Sie kaufen die dann einfach ab, egal welche Ausstattungsmerkmal sie haben. Dadurch können Sie den Preis billiger machen. Der Kunde muss bereit sein ein Preisprämium zu zahlen und er muss das Bedürfnis haben, dass etwas individualisiert ist. Und das müssen Sie unterteilen in Bedürfnisse in zwei Punkten. Auf der einen Seite haben Sie das Thema, ob das überhaupt ein funktionales Bedürfnis ist, wie z.B. ein Rollstuhlfahrer, der größere Knöpfe benötigt, weil er irgendwie Schwierigkeiten hat den Arm zu heben, d.h. dann ist es was Funktionales.

I: Das ist aber der andere Teil des Projektes. Nur um auf dem richtigen Fokus zu bleiben, bei mir geht es ja wirklich rein um die Produktentwicklung an sich. Wie man die Kunden zum Kauf bewegt, ist für mich nebensächlich.

E1: Genau, aber wenn Sie über Erfolgsfaktoren reden, dann ist das für mich einer der zentralen Punkte, dass sie überhaupt Kunden haben, die das Bedürfnis haben und zum andern bereit sind, das zu bezahlen.

I: Ja genau. Ich gehe jetzt aber mal davon aus, die Kunden gibt es, die existieren. Und ich interessiere mich im speziellen dafür welche neuen Anforderungen gibt es für die Produktentwicklung. Und da im speziellen, da Sie dort Experte sind, bei der Erstellung des Lastenhefts.

E1: Genau, also wenn Sie das Lastenheft anschauen wollen. Das Lastenheft muss natürlich individualisiert hergestellt werden. Aber dazu brauchen Sie natürlich eine ganz andere Art des Produktentwicklungsprozesses.

I: Genau, was ändert sich Ihrer Meinung nach da?

E1: Sie brauchen, dadurch das Sie ein Toolkit haben, wo die Produkte im Vorfeld definiert werden von den Menschen, die diese Produkte haben wollen, müssen Sie diese Informationen von dem Toolkit in den Produktionsprozess einfließen lassen. Und jetzt kommen wir wieder zu dem Punkt, ist Ihr Produkt denn schon fertig entwickelt, an der Stelle wenn der Kunde es haben will, oder muss da noch entwickelt werden? Also das halte ich für Unsinn. Es wird niemals ein Produkt erst entwickelt in Ihrem Konsumgüterbereich, wenn der Kunde auf den Knopf drückt, ich will JETZT das Produkt haben. Das ist Quatsch.

I: Nein, also es kann nicht über jedes fertige Produkt nochmal ein Entwickler drüber schauen. Es muss schon insofern vordefiniert sein.

E1: Genau, die Art der Produktion gibt´s schon. Z. B. im Anlagenbau, wenn die BASF ein neues Chemiewerk baut, dann müsste das erst entwickelt werden, auch wenn die Firma die das macht, die Rohre im Vorfeld schon hat, aber dann geht die Entwicklung erst los, wenn die BASF das erst haben. Aber das ist ja nicht Ihr Thema. Wir reden ja hier über Kaffeemaschinen.

I: Ja genau als Beispiel. Nur als Beispiel.

E1: Ja genau. Die Kaffeemaschine wird nicht erst dann entwickelt, wenn der Kunde sie haben will. D.h. Sie müssen das Toolkit und die einzelnen Formen vorentwickelt haben. Für den Fall, dass der Kunde jetzt dieses oder jenes Produkt haben möchte. D.h. diese möglichen Lastenhefte, die jedes mögliche Produkt haben könnte, müssen vordefiniert sein. Also Sie können nicht sagen, ich warte mal wie das Lastenheft aussieht. Sie können doch kein Toolkit bauen in dem so viele Freiheitsgrade drin sind, dass ein Produkt rauskommt, bei dem Sie gar nicht wissen, wie Sie es machen wollen.

I: Das ist ja genau die Frage. Wenn Sie sagen so viele Freiheitsgrade, dann muss man fragen: Die Sicherheit, die Ergonomie z. B. ist das alles erfüllt?

E1: Das muss man alles vorher definiert haben. D.h. am Ende ist in Ihre Art ein Produkt zu entwickeln identisch, mit der Art ein normales Produkt zu entwickeln, nur Sie müssen das ALLES im Vorfeld berücksichtigt haben. D.h. Sie müssen sich selbstverständlich vorher überlegt haben, wie jede einzelne Ausführung aussieht und müssen für jede einzelne Ausführung eine Sicherheitsprüfung durchgeführt haben. Also wir reden ja über eine Kaffeemaschine. Denn was kostet eine Kaffeemaschine? Selbst wenn sie individualisiert ist kostet, sie 1000 €. Sie können doch nicht für ein Produkt was 1000 € kostet nicht erst wenn der Kunde auf den Knopf drückt: Toolkit ich möchte jetzt, dass das so aussieht auf den Knopf drückt, dann entsteht ein Lastenheft für die Produktion, also ein Anforderungsheft. Da können Sie doch nicht, wenn´s dann in der Produktion durchgeführt wird, dann können Sie sich ja nicht erst überlegen, ist es zertifiziert, ist es sicher, funktioniert es überhaupt? Das können Sie nicht erst machen, das muss alles vorher definiert sein. Deswegen sind ja all diese Firmen Konkurs gegangen, weil ja dieser Prozess extrem komplex ist. In ihrem Beispiel gibt es meiner Meinung nach kein individualisiertes Lastenheft. Die Individualisierung im Lastenheft ist schon vorgedacht. (…)

Wenn ich in meinem Konfigurator die und die Teile zusammenbaue, dann sieht das Produkt so aus und dann erfüllt es deswegen die Sicherheitsanforderungen.

I: Also das muss alles vorher definiert sein und das ist hoch komplex.

E1: Ja genau. Weil sonst können Sie das ja gar nicht herstellen. Der Roboter muss das ja vorher wissen, wie er das Produkt herstellt.

I: Ja genau. Aber um jetzt den Punkt der Anforderungsklärung abzuschließen, können Sie denn sagen, weil Sie ja vorher meinten, das wird alles hoch komplex, bei welchem Punkt der Anforderungen sehen Sie die größten Veränderungen, bzw. die größten Herausforderungen.

E1: Mir ist nicht ganz klar, was Sie mit den Merkmalen der Anforderungsliste meinen? Was bedeutet denn Sicherheit in der Anforderungsliste?

I: Welche Merkmale muss das Produkt erfüllen, um sicher zu sein für den Endverbraucher. Die Merkmale sind natürlich alle miteinander verknüpft. Z. B. auch mit dem Material usw.

E1: Ihnen geht es doch um das Thema wie das Lastenheft aussehen muss oder meinen Sie wie das Produkt aussehen muss?

I: Mir geht es darum, generell bei der Anforderungsbestimmung, was ja durch das Lastenheft ausgeführt wird. Mein Thema zielt darauf ab, was ändert sich bei der Aufstellung des Lastenheftes, warum? Wo sehen Sie Schwierigkeiten?

E1: Also das ist ja mein Punkt. Wenn Sie es konservativ machen, brauchen Sie für alle individualisierten Ausführungen ein individualisiertes Lastenheft. Das müssen Sie im Vorfeld darstellen. Ob Sie das jedes Mal alles ausformulieren ist ja eine andere Frage, aber Sie müssen sich halt überlegen, wenn jetzt der runde Schalter und der eckige Schalter zusammen kommen, was bedeutet das jetzt für mein Lastenheft. Da muss ja dann drin stehen, die Maschine hat die und jene Schalter und diese Verkabelung. Das muss ja alles vorhanden sein. Sonst können sie das Produkt ja gar nicht individualisiert herstellen, außer sie haben in Ihrem System eine Intelligenz drin, nur ich glaube das ist so weit weg von der Realisierung das wird nicht funktionieren.

(irrelevant explanations of the basic topic)

E1: Da Sie diese unterschiedlichen Lastenhefte alle auf einer Produktionsanlage durchführen müssen, müssen die dahinter liegenden Differenzen durch eine modulare Architektur abbildbar sein. D.H. das Produkt muss in irgendeiner Art und Weise Modular aufgebaut sein, oder durch ein 3D individualisierbares Herstellungsverfahren herstellbar sein. Das ist eine Herausforderung. Die nächste Herausforderung ist das ganze Logistikkonzept. Denn Sie müssen sich ja überlegen, für jede unterschiedliche Ausprägung brauchen Sie natürlich unterschiedliche Teile. Im Gegensatz dazu, wenn Sie die Kaffeemaschine in Rot oder Blau anbieten, dann haben Sie zwei unterschiedliche Gehäuse. Wenn Sie das beliebig groß aufbauen, erhalten Sie zehntausende Einzelteile. Diese zehntausende Einzelteile können Sie natürlich nicht erst bestellen, wenn der Kunde den Bestellvorgang auslöst. (…) Dadurch dass das alles vorrätig sein muss, sind da enorme Kapitalkosten gebunden.

I: Also ist hier auch der Kostenpunkt ausschlaggebend.

E1: Ja genau. Sie haben hier natürlich enorme Kapitalkosten die in dem Fall an Material gebunden sind.
Also das Logistikkonzept ist extrem aufwändig, dann brauchen Sie den Konfigurator, der ist extrem aufwendig, dann müssen Sie diese Lastenhefte im Vorfeld alle definiert haben, was extrem aufwendig ist. Und Sie brauchen eine modulare Architektur in der auch alle Lastenhefte abbildbar sind, um das halt herstellen zu können. Das sind für mich eigentlich die Entscheidenden Punkte.

I: Ok, danke schön. Jetzt haben Sie ja gesagt, dass Hauptfokus Ihrer Arbeit die Erstellung des Lastenhefts ist. Können Sie denn zu den nächsten Schritten der Produktentwicklung, wenn Sie sich das V-Modell anschauen, Konstruktion oder zum Entwurf oder Ausarbeitung auch noch etwas sagen?

E1: Also die Frage ist ja, ob das V-Modell zu dem was ich Ihnen gesagt habe überhaupt passt, da das V-Modell gelaufen ist, bevor der Kunde irgendetwas auslöst.

I: Ja genau, also die zeitliche Abfolge ändert sich komplett.

E1: Genau, das Entwickeln des Produktes ist ja im Prinzip fertig.

I: Aber mal ganz abgesehen davon, wann oder ob das in der ursprünglichen Art des V-Modells abläuft, ganz egal davon abgesehen wann das abläuft ist trotzdem meine Frage wo Sie neue Anforderungen an die Konzeption, an den Produktentwurf etc. sehen.

E1: Da sie nicht mehr nur ein Produkt vorentwickeln, müssen Sie sich auf die Modularisierung der Komponenten einstellen und verstehen wie das alles miteinander zusammenhakt. Das ist für mich die größte Herausforderung.

I: Das ist dann wieder das Thema Komplexität.
Mit der Systemintegration haben Sie eher weniger zu tun?

E1: Ja damit hab ich weniger zu tun.

I: Ok, das ist ja die inhaltliche Planung, was wir grade besprochen haben. Daneben gibt es ja auch noch zeitliche und terminliche Planung und die Kostenplanung bezogen auf Projektkosten, Herstellungskosten usw. Also es geht wieder darum, welche neuen Anforderungen oder in wie fern wird das beeinflusst durch eine kundenindividuelle Produktherstellung?

E1: Wie ich schon gesagt hatte dadurch, dass Sie enorme Mengen an Material vorhalten müssen, Sie müssen das Toolkit programmieren und unterhalten, Sie brauchen Systemadministratoren. Das sind halt höhere Kosten. D.h. Ihr Produkt selber muss halt zu höheren Kosten verkauft werden. Denn es wird sicherlich niemals so billig sein wie ein Produkt von der Stange. Am Ende ist das Produkt selber deutlich teurer. Das hat jetzt aber nichts mit der Entwicklung des Produktes an sich zu tun.

I: *(the question is repeated on request of the interviewee)*

E1: Naja, das Produkt muss ja vorentwickelt werden wie jedes andere Produkt auch, und dabei muss halt berücksichtigt werden, dass Sie halt ganz verschiedene Systeme vorentwickeln. D.h. Sie müssen sich verschiedene Lastenhefte vorher überlegen. Dadurch brauchen Sie länger, dadurch brauchen Sie mehr Kapital. Was wahrscheinlich noch ganz interessant ist, Sie müssen sich hier (hinter einzelne Lastenhefte) Wahrscheinlichkeiten dahinter schreiben. (..) D.h. Sie müssen halt vorher überlegen, wie hoch wird die Wahrscheinlichkeit sein, dass ein Kunde ein spezielles Produkt haben will oder wie hoch ist die Wahrscheinlichkeit für ein Produkt mit diesen Ausprägungen. (…) Ah, guter Punkt. Sie müssen sich auch überlegen wie die Preisstruktur ihrer Produkte ist, die es dann hinten ausspuckt. Sie müssen sich im Vorfeld überlegen wie viele Leute kaufen welches Produkt, wie häufig wird das passieren? Wie hoch sind die einzelnen Produktionskosten, die Lagerkosten für die einzelnen Teile und daraus haben Sie dann ein individualisiertes Pricing-Modell entwickelt. Wenn Sie das wollen, Sie müssen das nicht, würde ich aber dringend raten.

I: Dann gibt es als Übergruppe bei der Produktentwicklung noch das Risikomanagement. Sehen Sie da irgendwelche neuen Anforderungen?

E1: Sie müssen sich halt überlegen, wenn sie das Lastenheft anlegen ist das ja alles für verschiedene Produkte und Sie müssen diese Produkte ja alle vorher getestet haben. Die Funktion des Produktes, die Sicherheit des Produktes, die Langlebigkeit, dann IT-System, alles was dahinter steckt. Das müssen Sie halt im Vorfeld alles genau überlegen. Sie brauchen eben bei jedem einzelnen Lastenheft diese Risikoabschätzungen und das ist ein enormer Aufwand.

I: Also sehen sie diese Abschätzungen im Vorhinein wie Sicherheit und Funktion und Langlebigkeit hatten Sie glaub ich noch gesagt, als neue Herausforderungen.

E1: Ja genau. Da sie das ja nicht nur für eine Ausführung machen müssen, sondern für alle.
Dazu könne Sie sich vielleicht auch nochmal zum Thema Homologation einlesen.
(discussion of moose test)
Wenn ein Produkt aus Einzelteilen besteht und jedes Einzelteil eine perfekte Homologation hat, heißt das immer noch nicht, dass es insgesamt hinterher in jeder Ausstattungsvariante perfekt funktioniert. Das herauszufinden ist extrem kompliziert. Dafür gibt es ja auch diesen EMV-Test, dieser Elektromagnetischer-Verträglichkeits-Test. (…)

I: Das hängt auch wieder mit dem Thema der Funktionsfähigkeit zusammen und wahrscheinlich den Kosten.

E1: Ja genau.

I: Generell gibt es bei der Produktentwicklung auch noch das Thema Konfigurationsmanagement. (Vorlesen der Definition) Wie wird dieses durch die kundenbezogene Produktindividualisierung beeinflusst?

E1: Also, dass das Produkt was hinten raus kommt immer die gleichen Eigenschaften besitzt und die gleichen Qualitätsansprüche hat, z. B. Ja, das ist natürlich ein ganz wichtiger Punkt, (Beispiele Adidas und 121 time etc.) dass man nur spezielle Kombinationen designen konnte. Und zwar nicht aufgrund von Sicherheit oder Funktionalitätssicherstellung, sondern aufgrund von Markenimageverletzungen. (…) Das ist das, was beim

Konfigurationsmanagement hinten stattfinden sollte. Dass die Leute das eben nicht so zusammenstellen, dass es unsinnig ist.
(further discussions of the production process – not relevant in the context of this thesis)

Transcript of Interview II (2015/06/24)
Attendees: Interim manager (E2), Interviewer (I)

Description of E2:

E2 is currently applied as interim manager due to his large experience. He moreover supports a startup in the field of sensors as mentor. His experience ranges from robotics to chip development. In this fields, he was involved in product development and production in the context of individual customer needs.

Interview:
I: Da Sie ja im ersten Teil der Systementwicklung nicht wirklich integriert sind, möchte ich einfach mal durchsprechen, z.B. bei der Ausarbeitung. Was würden Sie sagen, wenn Sie sich diesen kundenindividuellen Prozess verstellen, wo ist mehr Aufwand, wo sind da Änderungen speziell im Entwicklungsprozess zu erwarten?
E2: Also, was stark zunehmen wird ist die Kommunikation mit dem Kunden. Das muss ja auf einer Basis passieren, wo man sich irgendwie versteht. Verstehen jetzt im Sinne von die richtigen Themen richtig rüber bringen. Weil man redet oft im technischen Bereich aneinander vorbei. Der eine versteht dieses, der andere versteht jenes, da ist die Präzision der Aussagen gefragt. Ist dieses grün wirklich grün oder ist dunkelgrün oder hellgrün, verstehen Sie sowas in der Richtung. Dass man sich wirklich eine Präzision angewöhnt oder eine systematische Durchtaktung des ganzen Themas. Das erfordert sehr gut struktureierte Projektvorgehensweise. Also, wo man sagt mit Meilensteinen oder auch mit Projektpunkten muss da sehr sorgfältig umgegangen werden, sonst geht das am Ende schief. Dann wird der Kunde sagen, ich habe etwas grün Gestreiftes bestellt, aber etwas blau Kariertes bekommen. Also auch eine psychologische Komponente wenn man in den Mass-Market geht, um zu verstehen, was der Kunde wirklich will…
I: Wenn man jetzt z.B. bei der Chipherstellung so ein Toolkit vorstellen würde, da könnte ja der Kunde seine Anforderungen persönlich eingeben. Dann wäre ja quasi da diese Kommunikation gegeben. Zumindest, dass der Kunde da seinen Input gibt und klar macht, ich möchte dies und jenes. Ich weiß nicht, welche Vorgaben der Kunde bei der Chipherstellung macht, aber dass da der Kunde seine Anforderungen klar macht.
E2: Also, das ging meistens so: Man kommt mit einem Portfolio zum Kunden und sagt das kann man zurzeit, das bieten wir dir an. Wenn man das so und so konfiguriert, dann kann das Produkt dieses und jenes leisten. Dann kommt der Kunde mit seinen Wünschen daher und sagt ich möchte aber. Meistens passt es aber nicht und der Kunde möchte mehr haben, dann kann es technisch noch nicht geleistet werden. Es muss also nachentwickelt werden für technische Teile, die einfach noch nicht existent sind, oder wir könnten, aber für unseren Kunden ist das viel zu teuer, was meistens der Fall ist. D.h. die Individualisierungen die kosten immer Geld, was man ja natürlich jetzt entsprechend vorhalten muss. Das ist im Fertigungsprozess aber natürlich auch im Konstruktionsprozess der Fall, weil Dinge ja neu konstruiert werden müssen. Sie müssen jedes Mal die Konstruktionsanforderungen machen.
I: Ja, mit diesem Projekt, dem „InnoCyFer“ soll das wirklich in der Art geschehen, dass diese Konstruktion durch dieses intelligente bionische System berechnet wird, dass nicht nach jeder Eigenkonstruktion durch den Kunden noch einmal ein Konstrukteur drüber schauen muss. Nehmen wir jetzt mal den Bereich des Kaffeevollautomaten, da würde der Preis ja ins utopische schießen, wenn bei jedem Vollautomaten noch einmal ein Konstrukteur drüber schauen würde.

E2: Dann ist zunächst einmal die übergeordnete Konstruktionsleistung maßgebend, nämlich das System aufzubauen, indem sich der Kunde bewegen darf, bewegen kann. Der kann ja nicht willkürlich operieren, sondern der hat ja seine Raumbedingungen und innerhalb dieser Raumbedingungen kann er sich dann beliebig austoben, wenn er will. Die Frage ist, natürlich kann ein solches System einigermaßen aufgebaut werden und kann es alle Eventualitäten abfangen? Kaffeemaschine, denken wir mal wieder an die Farbe. Man hat silbergrau, statt weiß glänzend. Jetzt sag ich mal die Oberfläche kann nicht weiß glänzend sein, weil aufgrund des Fertigungsverfahrens kann es nicht glänzend sein. Damit ist es eine Einschränkung. Z.B. das Gehäuse kann nicht 5 Kubikmeter groß sein oder 2 mm^2 groß sein, sondern es muss bestimmte Größenverhältnisse haben, und solche Geschichten. Es müssen Borderlines da sein in jeder Hinsicht. Und der Kern grundsätzlich, das hatten Sie ja am Anfang gesagt, die grundsätzliche Mechanik bei so einer Kaffeemaschine sollte nach Möglichkeit auch nicht verändert werden. D.H. das muss irgendwie rein passen, das muss verankert werden, das muss einen Wassertank haben oder was auch immer. Da ist es oftmals schwierig die Grenzen da so sinnvoll festzulegen, dass da auch jemand anderes, der jetzt nicht Konstrukteur einer Kaffeemaschine ist, etwas damit anfangen kann. Das ist die eine Seite. Das ist eher eine technische Machbarkeit, kann ich konstruieren, so dass es feld-, wald- und wiesentauglich ist, sag ich mal. Die andere Seite ist natürlich ist da Bedarf dafür da? (…)

I: Das ist eine Sache, der Bedarf ist eher Thema vom Marketing. Wo findet man Kundengruppen, die das wünschen?

E2: (…) Der Kunde muss mittlerweile immer mehr selber machen. Dann kann man ein Stück weiter gehen und tut dem Kunden einen Teil der Konstruktionsleistung übertragen. Das kann sehr positiv sein.

I: Wo zum Beispiel? Oder sehen Sie, dass in irgendeinem der Konstruktionsschritte oder beim Systementwurf oder bei der Systemintegration Arbeit abgenommen wird oder sich dieses positiv verändert für den Konstrukteur? Oder wo könnten Schwierigkeiten, wenn wir jetzt z.B. beim Planen und Klären der Aufgabe sind, auftreten. Wo sehen Sie, dass durch den Zusatz, dass eben noch diese Variable X dabei ist durch den Kunden, die unvorhersehbar ist, wo sehen Sie da Veränderungen an den Anforderungen?

E2: Jetzt kehr ich einfach mal mein Arbeitssicherheitsthema raus. Wenn der Kunde die Maschine herstellt, die ist dann aber nicht notwendigerweise so aufgeschlagen, dass er nach der Maschinenrichtlinie fertigt. D.h. er muss die ganzen gesetzlichen Vorgaben kennen und einhalten. Auch wenn es nur für ihn eine Maschine ist. Sprich, wenn ich, nachdem er es nicht kann, muss trotzdem der Hersteller, d.h. der der das verkauft, das individuell prüfen. Und das ist ein gnadenloser Aufwand. Oder man engt das sehr stark ein. In dem Fall sind wir aber heute schon, wie gesagt beim Beispiel BMW, da sind alle Teile schon spezifiziert.

I: Vorher schon vorentwickelt.

E2: D.h. egal wie ich die konfiguriere, ich mein da gibt´s auch Einschränkungen, ich kann auch nicht alles konfigurieren. Aber die sind dann schon festgelegt. Ich habe bestimmte Freiheitsgrade in denen ich mich bewegen kann als Kunde und dann kann ich bestellen. Da bin ich aber sicher, dass das fertige Produkt, also das fertige Auto, gesetzeskonform hergestellt ist. Das ist eines der Themen. Das andere ist natürlich man kommt von hinten vom Herstellverfahren. Es können natürlich nur Herstellverfahren zur Anwendung kommen, die so eine Individualisierung zulassen. (…) Für Gehäuse könnte ich mir das relativ schnell vorstellen, solange sie aus Kunststoff sind, dann nehme ich den 3D-Drucker und lasse das drucken.

I: Oder Metalle mit Lasersintern. Würden Sie sagen, dass das z.B. schon die Konzeption einschränkt?

E2: Ja, auf jeden Fall, denn es muss ja bezahlbar bleiben. Ich kann so eine Individualisierung oder eine Kundeneinbeziehung nur dann machen, wenn es sich dann auch rechnet für den Kunden. (…) Es wird kommen, durch Kataloge, wo der Kunde sich dann das Produkt zusammenstellen kann.

(The difference between mass customization and UDC is clarified and the focus is shifted to product development.)

I: Aber nochmal auf das Thema Arbeitssicherheit zu kommen. Das ist ein sehr interessantes Thema. Gerade auch wahrscheinlich hinten bei der Systemintegration, beim Test.

E2: Einmal das, weil das muss ja individuell dann gemacht werden, ja. Also wenn das Gehäuse ein konstruktiver Teil einer Kaffeemaschine ist, dann muss das sicher sein. Da darf kein heißes Wasser auslaufen oder sonst was. Das muss dann individuell geprüft werden und das ist dann gleich ein Aufwand ohne Ende. Außer Sie bringen das wieder ganz nach vorne in den ganzen Konstruktionsprozess rein und geben dem Prozess als solchen die Borderlines mit. Er darf Wandstärke nicht unter ein Limit unterschreiten oder sonstiges. Damit haben Sie das ganze Vorschriftenwerk letztendlich abzubilden in dieses Toolset, dass sie dem Kunden zur Verfügung stellen und der kann sich dann, wenn es dann noch möglich ist, in diesem Toolset einigermaßen frei bewegen. Das wird die Hauptaufgabe sein, eines Herstellers, dieses Toolset dann entsprechend zu gestalten und zu konfigurieren. Und der Kunde nimmt das und macht dann noch die Ausprägungen. Macht dann noch ein Ohr hier hin oder einen Haken oder Henkel oder sonst irgendwas. Wenn er das will. Das muss kundenfreundlich sein, das muss schnell anwendbar sein und wie gesagt, das muss im Zweifelsfall auch eine Online-Hilfe haben, um zu sagen, ist das eigentlich noch möglich. Man lagert einen bestimmten Teil der Konstruktion aus, aber sage ich mal mehr, die Design bestimmenden Themen. Die funktionalen, da sehe ich noch viel mehr Probleme. Also wenn Sie z.B. am Pumpenmotor einer Kaffeemaschine was ändern wollen. (…)

I: Aber auch da, um jetzt nochmal auf den Prozess zurück zu kommen. Z.B. beim Thema Arbeitssicherheit. Auf welche Schritte wirkt sich das hierbei Ihrer Meinung besonders aus?

E2: Auf jeden.

I: Also auf jeden der Schritte?

E2: Man muss, genauso wie die Qualität muss man auch die Sicherheit ein designen. Also, d.h. es muss schon im vordersten Bereich mit vorgesehen werden und berücksichtigt werden.

I: Also es zieht sich Ihrer Meinung nach durch den kompletten Prozess?

E2: Also bei elektrischen Geräten müssen Sie elektrische Richtlinien beachten und das müssen Sie vorne schon mit betrachten, die Isolationsabstände und die richtigen Steckverbindungen müssen Sie schon bei der Konstruktion berücksichtigen. Das kann man dann nicht reinprüfen, sondern das ist ein Konstruktionsmerkmal. D.h. es muss eine Begrenzung geben der Variabilität der Konstruktion.

I: Und eben hatten Sie noch in einem Nebensatz erwähnt, das Thema Qualität?

E2: Ja, Qualität, das ist ein ganz dehnbarer Begriff. Viele verstehen da die Dauerfestigkeit drunter. D.h. wie lange hält so ein Teil. Das ist auch ein Konstruktionsmerkmal. (…)

(The interviewer summarizes the findings. Safety and quality are important topics as they are involved in the whole task clarification and concept design.)

I: Wenn wir uns jetzt hier (am Produktenwicklungsprozess) entlanghangeln, würde Ihnen dazu noch etwas einfallen, zum Thema Lastenheft, Konzeption, Entwurf … also was quasi noch ein wichtiger Aspekt ist, der sich bei der Produktentwicklung ausweiten würde, oder verändern würde, dadurch dass die Produkte individuell gestaltet werden können?

E2: Vielleicht! Nehmen wir mal an, das Produkt wird irgendwann mal auf den Müll geworfen.

I: Also Thema Recycling.

E2: Genau. Wie kann das recycelt werden? Wie kann das wieder dem Stoffkreislauf zurückgeführt werden? Das ist auch wieder ganz vorne zu sehen, denn in der Auswahl der Stoffe bin ich dann auch wieder eingeschränkt und muss dann entsprechend berücksichtigen, je nach Verfahren, die ich dann anwenden will. Das sind so Themen.

(The focus of the interviewee is shifted back to product development aspects.)

E2: Also so gesehen würde ich zunächst einmal sagen, es ist ein Riesenaufwand die Möglichkeiten des Kunden so zu begrenzen, dass er sinnvoll arbeiten kann, also ihm eine Systemumgebung so zurecht zu schnitzen, jetzt nicht im Sinne von Tooling, sondern einfach die Grenzen aufzeigen, wie weit kann er denn gehen.

Dann hätten wir das erstmal fixiert und alle Eventualitäten, die einem Kunden so einfallen könnten, die muss man berücksichtigen. Und das nächste ist dann, nachdem der Kunden sowas realisiert hat, dass man das ganze Ding bewertet, über die ganzen Kriterien die wir grad noch genannt haben. Also Maschinenrichtlinien oder… also wie gesagt.

I: Also die Bewertung auf Sicherheit und Qualität?

E2: Da das Einzelprodukte sind, muss ich das dann immer machen. D.h. da steigt der Aufwand mengenmäßig ganz gewaltig an. Und ich hab nicht nur ein Produkt, sondern viele Produkte. Und viele Produkte heißt auch viel Arbeit. Und das kann ich auch kaum standardisieren. Da ich jedes Produkt halt einfach einzeln anschauen muss und bewerten muss und dann auch zurückgeben muss, wenn es nicht den Anforderungen entspricht.

I: Also die Bewertung des Ganzen. Aber jetzt hatten Sie ja gesagt, die ganzen Faktoren müssen bewertet werden, aber welche Faktoren sehen Sie da als Schwerpunkt? Jetzt hatten wir ja schon Qualität und Sicherheit.

E2: Ja, gehen wir mal vom Idealfall aus. Da wäre alles in die Systemumgebung gepackt. Da kommt der Kunde gar nicht aus, irgendwas zu machen was nicht Systemkonform ist. Sei es Fertigbarkeit, sei es Rechtssicherheit, sei es Qualität etc. Das ist alles definiert und bewegt sich nur noch in diesem Rahmen. Dann brauche ich die Kontrolle auch nicht mehr. Wenn ich das sicherstellen kann, dann ist es einfach automatisch durchlaufen. Dann macht der Kunde sein Design und das läuft wie von selber. Wenn das nicht der Fall ist, und das wird sehr lange nicht der Fall sein, meines Erachtens, würde es einen Riesenaufwand darstellen, solche Grenzen aufzustellen. Alle Eventualitäten abzufedern. Also muss ich eine nachfolgende Prüfung machen.

I: Also sehen Sie beim Systemtest, Integrationstest einen westlich höheren Aufwand?

E2: Je mehr Freiheiten ich dem Kunden lasse, desto aufwändiger wird das Ganze. (…)

I: (…) Klar steigt die Komplexität, aber die Schwierigkeiten die man hat, ob man jetzt einen Kuli herstellt oder eine Kaffeemaschine… durch die Individualisierung, die Faktoren die da betroffen sind ja immer noch die Gleichen. D.h. nur bei der Kaffeemaschine sind sie viel viel größer ausgeprägt als wenn ich sage, ok ich habe jetzt hier diesen Kugelschreiber…

E2: Ich vermute halt, dass das alles exponentiell steigt. So dass das erstmal absurd wird.

I: Das auf jeden Fall. Nur ich sag mal die Faktoren, die es betrifft, die man bedenken muss, das sind ähnliche oder gleiche wahrscheinlich.

E2: Wahrscheinlich ja.

I: Das ist einfach das wo ich hin möchte, also welche Faktoren sind das, die man bedenken soll.

(Summary of the named aspects through the interviewer)

I: Betrachtet man die Systemintegration. Da gibt es ja am Ende auch noch den Akzeptanztest.

E2: Der entfällt, denn der Kunde hat das ja für sich gemacht.

I: Der entfällt? Also könnte man hier sagen, dass es sogar dann einen positiven Effekt gibt.

E2: Die Marktthematik verschiebt sich. Ich muss nicht mehr schauen, dass ich das Ding los werde, sonders das ist individuell geschnitzt und das ist hier bereits entschieden. (…)

I: Das könnte man dann im Zuge der Produktindividualisierung als geringeren Aufwand betrachten, weil dieser Test so gut wie weg fällt.

E2: Ja, das ist die Frage wie sich der Aufwand hier verteilt. Also wenn ich jetzt Kaffeemaschinen verkaufe, dann habe ich 10 Sorten im Markt, 10 verschiedene. Und ich hab 100.000 im Markt (*verkauft*) dann muss ich 100.000 Mal das (*Akzeptanztest*) machen statt 10 Mal als Aufwand jetzt. Und das fällt natürlich weg.

I: Aber trotzdem hat man insgesamt mehr Aufwand?

E2: Also der steigt schon gewaltig (*in Bezug auf die Festlegung der Rahmenbedingungen*). Und vor allen Dingen man verlagert den Aufwand in Richtung Kunde.
I: Und Sie meinten gerade noch in diesem Fall beim Komponententest, beim Integrationstest.
E2: Da kommt´s dazu ja. Sowas muss ich ja immer fürs Einzelprodukt machen. Da kann man viel standardisieren, so ist es nicht, aber das ist trotzdem aufwändiger, wenn …
I: Klar, wenn man individuelle Teile mit drin hat.
E2: Damit hängt das Ganze schon sehr stark vom Produkt ab. Wenn das Produkt wenig komplex ist, dann kann ich mir sowas schon vorstellen.
I: Klar, je komplexer das Produkt, desto mehr steigt der Aufwand. Die Frage ist eben an welcher Stelle. Da hatten Sie ja gerade gesagt, gerade am Anfang beim Systementwurf oder bei der Systemintegration beim Komponententest und Integrationstest.
E2: Da wird der Aufwand dann gewaltig steigen ja.
I: Und warum steigt der Aufwand Ihrer Meinung nach da gewaltig?
E2: Einfach die Menge. Also um die gleiche Anzahl von Produkten in den Markt zu bringen, muss ich sie in dem einen Fall nur einmal machen, wenn ich 10.000 Stück habe, oder 10.000 Mal. Ganz linear geht's nicht, denn ich kann auch Rationalisierungsaufgaben bei den 10.000 anbringen. Das ist wirklich deutlich mehr, als wenn ich nur einmal eine Typenprüfung mache. Also wenn ich Schrauben z.B. herstelle, Schrauben sind Massenware. Das spuckt die Maschine einfach aus, tonnenweise. Aber wenn ich jetzt meine individuelle Schraube gestalten möchte, dann muss ich die erstmal prüfen, hält die auch die Festigkeit z.B. oder sowas. Natürlich kann ich da wieder meine Grenzen festlegen, aber so richtig sicher bin ich dann doch nicht. Wenn es Dinge sind, die nicht so relevant sind, wie mein Kugelschreiber oder Ihr Kugelschreiber, dann kann man sagen ok, dann sind diese Typenprüfungen nicht so relevant.
I: Aber trotzdem sollte er mir jetzt auch nicht in der Hand zerbrechen und mir in den Finger schneiden.
E2: Aber da kann man ja wieder sagen, mit einer bestimmten Wandstärke bei diesem Material usw.
(The interview closes with a summary of the findings of the interviewer)

Transcript of Interview III (2015/07/02)
Attendees: Consultant and product manager (E3), Consultant and project manager (E4), Interviewer (I)

Description of E3:

E3 is employed in the field of consulting since one year. He mainly is involved in customer service and software product and project management. While his position has interfaces to all phases of the product development, his focus is the system design stage and its interfaces.

Description of E4:

E4 also is since about one year consultant. He works in the field of idea management as project manager. He is involved in all phases of the product development, but mainly in the requirements analysis and identification of customer needs.

Interview:
I: Wir können direkt in die Anforderungsanalyse einsteigen. Mein Ziel ist es, da einfach rauszufinden, was ist die Meinung der Experten, was ändert sich da bei der Anforderungsanalyse, wenn man solche kundenindividuellen Produkte hat, wo der Kunde wirklich frei Teile verändern kann.
E3: Also, was ich auf jeden Fall bei uns immer ein wichtiger Punkt ist sind Zeit und Kosten was immer zusammen spielt. Also was auch immer man individuell macht kostet natürlich viel Geld. (*short irrelevant*

aspects) Je individueller, desto mehr Kommunikationsaufwand, mehr Programmierungsaufwand. Also unsere Abteilungen Programmierung, Design, Projektmanagement, Sales und Campaining. Die müssen wir halt immer alle abholen, d.h. es ist ein riesiger Kommunikationsaufwand erstmal. Die einen, die müssen es verwenden am Ende, für die muss die User-Experience stimmen, für die anderen muss das Programmieren… idealerweise wollen wir nichts entwickeln was wir nicht in unsere Basisversion aufnehmen können. D.h. man muss es verkaufen können auch klar. Genau und Design muss auch vor allem auch im Hinblick auf die User-Experience mit einbezogen werden. D.h. bei allem was individuell ist, ist ein riesen Kommunikationsaufwand. Und was ändert sich noch an den Anforderungen? Also bei uns macht´s nur Sinn was individuell zu entwickeln, was wir eigentlich weiterentwickeln können. Also was wir auch aufnehmen können in den Standard und auch wiederverwerten können. Also Recycling ist glaube ich ganz wichtig.

I: Also bei diesem „InnoCyFer" Projekt ist da auch das Ziel, also einmal, natürlich wird da das „Best of" dann wahrscheinlich auch als Serie entwickelt, aber trotzdem kann da jeder Kunde… natürlich wird der Preis auch etwas höher werden für diese individuellen Produkte… aber dass da durchaus jeder Kunde sagen kann, ok ich bin bereit ein Preisprämium zu bezahlen für das Produkt, dafür hat jeder Kunde die Möglichkeit sein individuelles Produkt zu erstellen durch dieses Toolkit eben.

E3: Was wir auch viel sehen, bei individualisierten Produkten ist, dass die Instanthaltung wahnsinnig schwierig ist, weil, man muss immer jemanden haben. Idealerweise hat man den, der es entwickelt hat, der es dann auch instand halten soll. Wenn der zufällig grad nicht da ist oder vielleicht gar nicht mehr Unternehmen ist, weil es sind ja ältere Plattformen, dann ist es wahnsinnig schwierig, dass man da jemand anderen hat, der sich da rein denkt.

E4: Es ist quasi das Risiko erhöht sich, weil, wenn ich letztendlich nur eine endliche Anzahl von Modulen habe, um das Produkt für den Kunden zusammen zu bauen, dann habe ich auch ein endliches Risiko. Dann muss ich auch nur eine endliche Anzahl von Ersatzteilen vorbereiten, ja. Und wenn ich jetzt eben individuell was mache, dann ist das nicht so leicht das eben mal nach zu fertigen, wenn individuell was kaputt geht z.B.

E3: Was auch noch ein Punkt ist finde ich, wenn man dann… die Kompatibilität mit anderen Produkten, wenn man dann… bei der Kaffeemaschine wärs jetzt, wenn ich mir noch einen Milchaufschäumer dazu kaufen will, dass der dann irgendwie dazu passt, wenn ich den unabhängig davon kaufe. Oder bei unserer Software, jetzt ein Beispiel. Wenn ich jetzt eine App da anbinden will, dann ist es da wieder schwierig, dass die Schnittstellen aufeinander passen.

I: Ja das ist ein guter Punkt.

E4: Ich weiß nicht inwiefern das in den Prozess reinspielt, aber wenn ich eine nicht standardisierte Mühle in eine Kaffeemaschine baue, dann kann ich auch schlecht die allgemein zertifizieren lassen. Also es geht so um CE-Kennzeichnung zum Beispiel. Das weiß ich jetzt auch aus dem InnoCyFer Projekt, da ging es nämlich darum, dass die Kunden gerne Mahlwerke individualisieren wollten. Ist aber schwierig, weil da ist Elektronik drin und sobald da Elektronik drin ist muss ich es irgendwie abnehmen lassen vom TÜV.

I: Das ist ja dann auch quasi vorher schon noch beim Klären der Anforderungen. Wenn man sich das Produkt eben so anschaut, es muss natürlich einen fixen Bereich als Kern geben, den der Kunde nicht anrühren darf. Das ist dann gerade am Anfang von so einem Projekt gerade alles was mit der Elektronik verknüpft ist.

E3: Und was noch ein Punkt ist, vielleicht… hier steht Transport, das haben wir nicht. Aber wir müssen es ja irgendwie verkaufen. D.h. je weiter das Produkt weg vom Standard ist, desto schwieriger ist es, dass man einfach mal dem Kunden sagt, hey wir verkaufen das. Weil im Endeffekt, wenn ein Kunde zu uns kommt, dann können wir sagen, ja wir haben eine Software und wir können daraus dies und jenes machen. Und wenn wir am Anfang noch nicht wissen, was der Kunde eigentlich haben will, dann ist es ganz schwierig auf den zuzugehen und zu sagen, ja wir haben eigentlich genau das, was du brauchst, weil wir machen ja theoretisch alles möglich in dem

Sinne. Das ist bei der Kaffeemaschine jetzt einfach, was eine Kaffeemaschine ist. ist am Ende wahrscheinlich, aber wer weiß, vielleicht macht sich dann irgendjemand da irgendwie eine Saftmaschine draus oder so. Das ist schwierig, dass man noch die Zielgruppe hat am Ende.

I: Ja und wenn ich da grad nochmal auf dieses Zertifizierungsthema eingehen darf, das kann man ja eigentlich schon auch gut in den Prozess einordnen. Weil Sie meinten, dass Sie das nicht so genau wissen. Das ist ja dann eher bei der Systemintegration, nehme ich mal an, diese Systemtests.

E4: Das könnte man jetzt vielleicht umformulieren, dass man vielleicht sagt, die einzelnen Phasen des Produktentwicklungsprozesses, die greifen viel stärker ineinander. Also ich kann jetzt nicht tatsächlich die Phasen nacheinander ablaufen, sondern ich muss schon in der Anforderungsanalyse berücksichtigen, dass ich später in dieses Problem laufen könnte.

I: Ja man kann es nicht mehr so schön Schritt für Schritt im V-Modell ablaufen.

E4: Natürlich kann ich das machen, ich kann vorher die Anforderungen erheben usw. und wenn ich dann aber hinterher feststelle, oh, das geht ja gar nicht, da muss ich jetzt jedes Produkt einzeln vom TÜV abnehmen lassen. Das sind ja Kosten, dann ist es halt zu spät. Also ich muss ja hier viel ganzheitlicher denken.

I: Also zum Thema Anforderungen habe ich mir jetzt schon viele nützliche Stichpunkte machen können. Fällt ihnen da noch etwas zum weiteren Verlauf im V-Modell ein. Wenn wir das jetzt einfach mal abgehen würden, Schritt für Schritt, oder würden Sie sagen, dass Sie eher im Anforderungsbereich da mehr tätig sind und zu den anderen Punkten nicht wirklich Aussagen tätigen könnt.

E3: Da kann ich auf jeden Fall noch bis zum Konzipieren gehen. Also weil wir zum einen die Software für unsere Kunden konzipieren und zum anderen, weil es glaube ich ganz schwierig ist, wenn die Entwickler selber ihre Konzepte erstellen, weil die den Kunden weniger im Blick haben.

Es ist ganz wichtig, dass die Struktur, also der Software, z. B. vorher definiert wird. Weil sonst können halt irgendwann Probleme aufkommen, dass die falschen Daten an den falschen Werten hängen. Dann was auch immer ganz wichtig ist, dass man halt intern alles abholt was es schon gibt sozusagen. Also bei der Kaffeemaschine wäre es wahrscheinlich eher das Problem, was es am Markt schon gibt. Genau, was ich dann glaube, was auch noch ganz wichtig ist, dass es ein 100 Prozent modular aufgebautes Produkt ist.

E4: Natürlich muss eine viel bessere Kommunikation zum Kunden stattfinden, wenn der öffentlich quasi Vorschläge machen kann auf einer Plattform. Das hat nicht unbedingt was mit dem internen Prozess zu tun, aber wenn du auf einer Plattform entwickelst, entwickelst du ein neues Produkt, eine Idee oder was und da reicht der Kunde ja Vorschläge ein und ist dann vielleicht auch sauer, wenn sein Vorschlag nicht akzeptiert wird. Und das muss ich natürlich auch vorbereiten.

I: Klar, wenn dann die Rückmeldung von der Community oder Plattform oder wie auch die Rückmeldung kommt…

E4: In Form eines Shit-Storms *(laughing)*

I: Ja, ich kann mir das auch so vorstellen, ich weiß nicht, ob das schon so durchführbar ist, aber, dass der Kunde da wirklich seine Kaffeemaschine konzipiert und dann ein total abstruses Gehäuse eben und dass da im Hintergrund irgendwelche Berechnungen ausspucken, oh das ist so nicht ausführbar, das würde so nicht halten oder… so könnte ich mir das auch vorstellen, dass der Kunde einfach enttäuscht ist und sagt, ja ok, dann kann ich mir ja … ja, irgendwie diese Enttäuschung abfangen ja.

E3: Ja was bei uns auch irgendwie … wenn die Inhalte vorher noch nicht definiert sind. Also ich weiß nicht wie man das bei der Kaffeemaschine sehen könnte. Aber wenn wir jetzt eine Plattform erstellen sozusagen und der Kunde sagt, er hätte gerne eine Plattform, die soll das und das können, und dann am Ende kommen erst die…, also klar haben wir dann schon Design Mock-up und so weiter und so fort, aber der Kunde benutzt sie dann wirklich erst am Ende. Und dann fallen ihnen 1000 Sachen auf, die sie vielleicht doch anders haben wollten.

I: Das ist ja dann im Bereich des Akzeptanztests hier.

E4: Also es ist halt schwieriger diese, also es gibt immer bei einem individualisierten Produkt so eine Gap zwischen Erwartungen und was ich mit dem Produkt tatsächlich anfangen kann. Und ich glaube je individualisierter das Produkt ist, desto größer kann diese Lücke werden. Eigentlich sollte sie ja schmaler werden.

I: Also, Sie meinen sogar, dass dann sozusagen beim Akzeptanztest am Ende nochmal ein Mehraufwand durchaus auftreten könnte, weil dann der Kunde merkt, dadurch dass er das Produkt selber erstellt hat…"oh das habe ich nicht bedacht". Ok.

E3: Weil er ja auch vieles gar nicht wissen kann, theoretisch. Weil ich mein es gibt Menschen, die beschäftigen sich ein Leben lang damit sozusagen, die Kaffeemaschine zu entwickeln und wenn ich das jetzt selber mache, klar kann ich mir denken, dass ich, weiß ich nicht… einen Milchaufschäumer und eine Kaffeemühle haben will, aber vielleicht denke ich nicht dran, dass ich mir auch gerne mal heißes Wasser für meinen Tee runter lasse.

I: Ja, oder es ja natürlich wirklich auch sein kann, dass er sich das so erstellt und im Nachhinein überlegt, was Sie vorhin auch gesagt haben, ich möchte dann das Produkt noch dran setzten und das ist dann nicht möglich dadurch das es individualisiert ist.

E3: Genau, und deshalb ist es glaube ich ganz wichtig, dass man den Prozess so gestaltet, dass die Benutzer immer wieder darauf hingewiesen werden, was bedeutet … dass man ihm entlang des Prozesses quasi immer wieder Erfahrungen mitgibt. Okay, weißt du jetzt übrigens, wenn du das anklickst oder dieses Modul noch haben willst, dann wird es am Ende so und so aussehen und vielleicht kannst du dann das und das nicht machen. So dass man dann immer wieder die Informationen mitgibt, was bedeutet das, was ich da jetzt genau mache. Was sind die Erfahrungswerte der anderen Leute.

I: Ja, das würde ja bedeuten, dass man einen Teil des Akzeptanztests am Ende schon vorzieht.

E4: Erstens das und zweitens was da auch noch so ein bisschen mit reinspielt ist noch ein ganz anderer Faktor, nämlich dass man den Nutzer viel stärker anlernen muss, je mehr er selber am Produkt machen kann. Ja, weil das Kaufen, das erfordert kein Anlernen. Weil, wenn er tatsächlich in die Entwicklung eingreift, was er ja über das Toolkit machen soll, dann muss man ihn halt auch anlernen.

(*not relevant information of the InnoCyFer project.)*

E3: Ich sehe als nächsten Punkt das Ausarbeiten. Da können wahnsinnig viel unvorhersehbare Fehler auftreten. Dadurch, dass man es neu gemacht hat, oder dass es so zusammen gestellt wird, wie es der Kunde zu der Zeit haben will und noch nie vorher getestet hat, können da 1000 Probleme auftreten, die man nicht vorhersehen kann. Also das ist auch ein wahnsinnig großes Risiko was man nicht einschätzen kann, was aber hinzukommt. Normalerweise, wenn man Produkte hat, dann weiß man schon die typischen Wehwehchen sozusagen. Oder was die Kunden normalerweise reklamieren. Aber wenn ich dieses Produkt noch nie vorher ausgeliefert hab in dem Sinne, dann ist es halt wahnsinnig schwierig, dass man dann das Risiko abschätzen kann, was da jetzt zurückkommen kann.

I: Ja, das ist quasi ja der Übergang vom Ausarbeiten zum Komponententest.

E3: Oder dass du einfach hier einen Mehraufwand hast.

I: Ja, oder dass man wahrscheinlich, wenn ich das jetzt richtig verstehe, man arbeitet das aus, testet das, dann kommen die Fehler, dass man da viel öfter diese Schleife durchlaufen muss.

E3: Und das einfach der Aufwand größer wird pro Schleife sozusagen.

E4: Also entweder man dreht halt sehr viele Schleifen, die andere Möglichkeit ist, dass man sag ich mal, den Raum, in dem sich der Kunde frei bewegen kann, so gut definiert, dass am Ende nur Sachen raus kommen können, die man auch fertigen kann. Und allein diese Komplexität, dass man alle Eventualitäten abdeckt, dass kostet halt sehr viel.

E3: Das ist ja eigentlich Ziel des ganzen oder? Das soll ja idealerweise 100 prozentig individualisierbar sein.

E4: Beim Toolkit wäre es so, dass alles was ich mit dem Toolkit irgendwie machen kann, kann ich auch produzieren. Bei uns heißt das, der Kunde bekommt tatsächlich einen Konfigurator, wo er sich dann eine Software zusammen klickt und die funktioniert dann auch. Ohne dass noch einmal ein Entwickler dran war.

E3: Genau, aber bei uns gibt es das halt auch, dass man sagt, ok, wir haben unsere Basis und jetzt will aber jemand auf einmal was total abgespacetes, was wir noch nie zuvor hatten. Dann sagen wir, ja klar, machen wir. Und dann machst du es natürlich und das zahlt der Kunde auch, aber es ist wahnsinnig schwierig erstens den Aufwand wirklich vorher abzuschätzen und zweitens mit den Problemen danach umzugehen.

E4: Genau, der Testaufwand steigt.

I: Und das vorherige Abklären ist ja wieder mehr am Anfang vom Systementwurf. Dass man sich wirklich vorher komplett, wie Sie gesagt haben, alle Eventualitäten vorher überlegt.

E3: Das versucht man, aber grad bei der Softwareentwicklung ist das nicht möglich, dass du wirklich vorher weißt, wie du es machst, wie lange es dauert, wie viel es kostet und was dann noch alles damit zusammen spielen wird.

I: Und Sie hatten eben noch gesagt mehr Testaufwand? Also wo sehen Sie das besonders?

E3: Ich glaube, dass das bei Komponenten und Akzeptanz am größten ist.

I: Könnten Sie nochmal erläutern warum?

E3: Naja, sagen wir mal System- und Integrationstest, das kann man vorher alles relativ gut abschätzen, aber ob der Entwurf wie ich ihn gemacht habe dann wirklich umsetzbar ist, also da geht es ja wirklich um die technische Machbarkeit dann. Und das ist glaube ich wirklich das schwierige, weil man diesen Code nicht wirklich vorher planen kann, ohne ihn zu schreiben. Es ist Trial & Error. Man probiert es, also man überlegt sich eine Lösung und dann am Ende sieht man ob es dann klappt oder nicht.

I: Dann haben Sie wahrscheinlich schon Erfahrungswerte und man kann sich überlegen, ob das funktioniert.

E3: Genau, aber speziell wenn du dann neue Module bastelst, die du vorher nie hattest, dann probierst du natürlich und klar aufgrund deiner Erfahrungen machst du es am besten, aber es kann immer sein, dass man da Kleinigkeiten übersieht und dann wird's schwierig. Und Akzeptanz ist halt wirklich, dass halt der Kunde drauf schaut und es wirklich verwendet, ob dann da nicht auch noch Sachen auf einen zukommen, die vielleicht der Entwickler nicht bedacht hat. Weil der nicht mit dem Kunden gesprochen hat. Weil da ist meistens ja noch einer dazwischen sozusagen.

I: Ja, und dann einmal hat der Kunde ein Produkt mit dem er nicht zufrieden ist, oder man hat diesen Mehraufwand, dass man das nochmal ausbessern muss, um einen zufriedenen Kunden zu haben ja. (…)

E3: Es gibt natürlich auch so modulare Software, die du dann zusammen klicken kannst und dann kriegst du die einfach, aber das ist dann im Endeffekt auch ein Standardprodukt, dann mit ein paar Variablen. Aber wenn du es wirklich individualisiert haben willst…

I: Dann wäre das dann wahrscheinlich so, dass man wirklich seine Module hat und dann noch einen Freitext hat, so welche Sonderfunktionen wünsche ich. Und dann müsste das ja auch automatisiert irgendwie umgesetzt werden können.

E3: Genau, so weit sind wir noch nicht. Kann alles noch kommen, das wäre die Idealvorstellung. (*Lachen*)

I: Ja, sehr schön, eigentlich sind wir dann schon den Entwicklungsprozess abgegangen, wenn ich das so sehe. Sie hatten vorhin noch angesprochen, weil das war ja jetzt alles quasi die inhaltliche Planung, die wir so betrachtet haben. Daneben gibt es ja auch noch die Kostenplanung und die zeitliche/terminliche Planung.

Können Sie dazu noch etwas sagen, also was da der Mehraufwand oder der Einfluss der Individualisierung in der Produktentwicklung ist?

E3: Dass man es überhaupt nicht vorhersehen kann. Also, man kann es immer abschätzen, man kann Zeit abschätzen, man kann Kosten abschätzen, aber man weiß im Endeffekt nie, ob man es wirklich schafft.

I: Und können sich die beiden auch gegenseitig beeinflussen. Also dadurch, dass man die zeitliche Planung nicht einhält?

E3: Also, das ist bei uns eins und eins dasselbe, weil wir haben in dem Sinne kein Materialaufwand, sondern wir haben unsere Entwickler, die programmieren und die Ihre Mann-Tage haben sozusagen, deshalb geht das bei uns Hand in Hand.

I: Würde sich die Kosten- oder die Zeitplanung oder beides zusammen verändern, dadurch, dass man weiß wir haben jetzt immer noch eine unbekannte Komponente, die da rein spielen kann in unseren Entwicklungsprozess? Dass man das irgendwie anders durchführen müsste?

E3: Am besten keine Deadline haben. (*laughing*) Aber bei uns ist es halt oft so, dass wir ein Go-Life haben sozusagen und das wird vorher kommuniziert und ehrlich gesagt wirkt es sich dann auf die Qualität aus. Wenn man es dann sozusagen erzwingt, dass man zur rechten Zeit fertig wird, weil dann und dann der Liefertermin ist. Dann macht man natürlich so gut es geht bis dahin, aber es wirkt sich dann auf die Qualität aus. (31:10)

E4: Also, es hat auf jeden Fall Auswirkungen. Es lässt sich nicht mehr so gut planen welches Produkt jetzt individuell Zeitplanung braucht und ich kann nicht sagen jedes Produkt braucht drei Tage, sondern das hängt dann vom Produkt ab. Es ist dann auch schwieriger die Produkte zu priorisieren, welches wird als erstes gefertigt. Wenn ich immer dieselbe Zeit hab und dasselbe Produkt, dann ist es ja egal. Aber jetzt kann ich sagen dieses Produkt braucht 20 Tage, das andere braucht vielleicht einen Tag. Welches mach ich als erstes?

E3: Vielleicht braucht dann auch das, was dann nur einen Tag dauern sollte 5 Tage und das andere am Ende nur 3. Also es ist wahnsinnig schwierig voraus zu planen. Genau, was mein Kollege sagt, diese parallelen Produkte, man weiß dann auch nie wann die Ressourcen komplett gekillt sind, weil man es eben vorher nicht abschätzen kann. Ja, Kosten ist in dem Sinne auch schwierig, weil man kann ja nicht zu dem Kunden sagen es kostet so viel. Also könnte man theoretisch schon, aber wer kauft es, wenn du sagst, wir schauen halt wie viel Aufwand es ist und dann zahlst du.

I: Man muss, wenn der Kunde auf den Bestellknopf drückt….

E3: … dann muss man es zu dem Preis machen. Man ist dann preisgebunden in dem Sinne, was sich dann auch auf die Rentabilität auswirken kann. Weil, wenn der Kunde es dann für 5000 Euro kauft und am Ende sitzen 3 Entwickler für 3 Wochen dran, dann wird's schwierig.

I: Jetzt hätte ich einfach nochmal ganz allgemein die Frage, wir sind jetzt sehr an diesem V-Modell, was ich vorgegeben habe entlanggegangen, vielleicht habt ihr ja auch eine andere Vorgehensweise bei eurer Produktentwicklung. Würde euch dann sonst noch irgendein Punkt einfallen, der nach Ihrer Meinung noch wichtig ist, der vielleicht nicht drin vorkommt, worauf sich diese individuelle Produktentwicklung auswirken würde?

E3: Ich weiß nicht, was alles in diesem Planen und Klären der Aufgabe drin ist, weil das ist für mich so: Ok wir bauen ein neues Produkt und dann ist ein riesen Punkt mit dem wir uns erstmal beschäftigen, ok was haben wir schon, was wollen unsere Kunden, was gibt es für Erfahrungen die wir haben, was gibt es am Markt? Ja, so diese ganze Analyse der Anforderungen.

I: Ja, genau: Planen und Klären der Aufgabe, ein wesentlicher Bestandteil davon ist das Aufstellen der Anforderungsliste.

E3: Und die dann aber basierend auf… also erstmal diese ganzen Informationen sammeln.

E4: Also für mich gibt es eigentlich 3 große Punkte. Je mehr ich an den Kunden abgebe in der Produktentwicklung, desto mehr Aufwand habe ich ihn anzulernen, das hatte ich ja vorhin schon mal gesagt. Dann, desto mehr Kommunikationsaufwand und Abstimmungsaufwand habe ich und ich muss ihm auch mit meiner Erfahrung zur Seite stehen. Also, ich weiß nicht wie man das bezeichnen kann, Betreuungsaufwand oder so.

E3: Erwartungsmanagement ist das ehrlich gesagt, weil am Ende gibt es wahrscheinlich immer eine Lücke zwischen dem was der Kunde erwartet und dem was er bekommt…. Oder so ein kontinuierliches Erwartungsmanagement brauchst du eigentlich.

I: Ok, über den ganzen Prozess?

E3: Über den ganzen Prozess, weil dann muss man auch irgendwie definieren, ok, wann ist es jetzt berechtigt, dass er sagt, ok, das ist jetzt nicht so wie ich mir das vorgestellt habe, oder ist es unberechtigt, dass man sagt, aber du hast ja auf bestellen geklickt und das sah ja da schon so aus. Hättest du wissen müssen oder können, ich weiß nicht. Es muss halt auch irgendwie definiert sein, was ist eine Reklamation, was ist Zusatz, den man bestellt sozusagen.

I: Das man hinten quasi auch noch Definitionen aufstellen muss, dass dann… bessern wir nach.

E3: Also genau, dieser Akzeptanztest wird da wahrscheinlich ein ganzes Stück größer.

I: Und was Sie auch gesagt haben (*an B gereichtet*) mit Ihren 3 Punkten, also erstmal dieses Anlernen. Wenn ich mir jetzt so überlege, also das könnte ich jetzt nirgends in den normalen Produktentwicklungsprozess einordnen, das ist ja auch nochmal ein ganz neuer Punkt, der dann da aufkommt, eigentlich.

E4: Also, wenn man so von der Dienstleistungstheorie kommt, dann gibt es Dienstleistungen wo der Kunde nur konsumiert und es gibt Dienstleistungen, wo der Kunde mit kreiert oder mit erstellt. Und das ist ja hier dann auch so. Und je mehr eben der Kunde mit erstellen muss, desto mehr muss man ihn anlernen. Aber das ist halt, dass er nicht irgendetwas bekommt, also was man sagt, das hat eventuell noch Auswirkungen. Also Beispiel, beim Friseur muss ich mich nur hinsetzen und dann muss ich halt kurz noch irgendwie spezifizieren, will ich kurz oder die Farbe.

I: Genau, das ist dann Punkt eins, Klären der Aufgabe.

E4: Aber ich meine Bildung ist auch eine Dienstleistung und wenn ich da keinen Input bringe, dann kann die nie funktionieren. Und dann muss ich halt auch wissen, wie ich lerne.

I: Ja, das ist ein sehr guter Punkt.

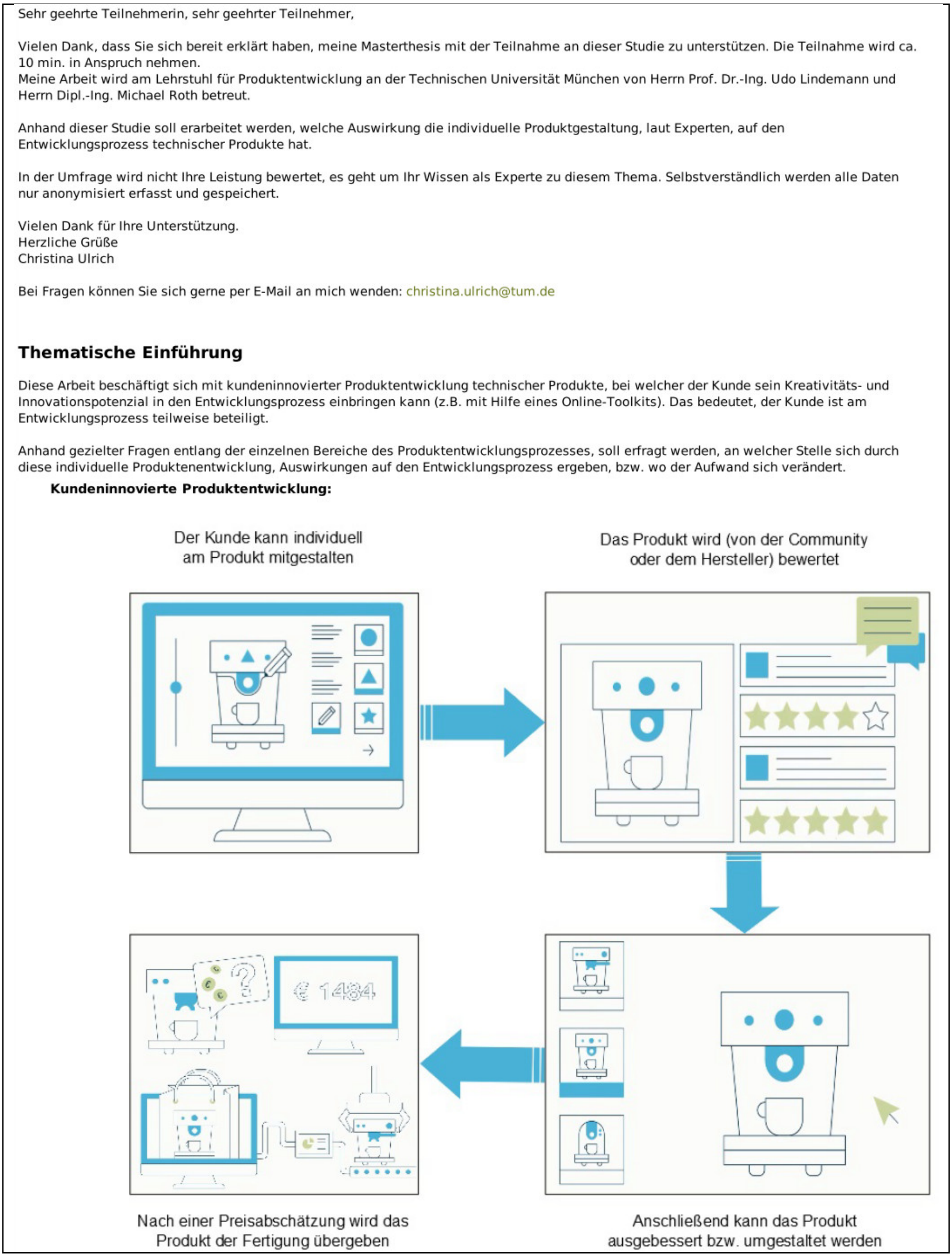
E3: Das ist ja auch bei Anforderungen, der Gebrauch, das spielt ja wahrscheinlich auch noch mit rein oder?

E4: Ja.

(Short discussion of the required services for individual products and summary of the findings through the interviewer)

9.1.3 Questionnarie of the Qualitative Exploration

As described in Subsection 3.2.1, the questionnaire of the qualitative exploration was hosted on the web portal “umfrageonline.com” starting from 6thAugust 2015 for eight weeks. It consists of a general introduction and the 18 question items shown in the following (Ulrich, 2015):



Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,

Vielen Dank, dass Sie sich bereit erklärt haben, meine Masterthesis mit der Teilnahme an dieser Studie zu unterstützen. Die Teilnahme wird ca. 10 min. in Anspruch nehmen.
Meine Arbeit wird am Lehrstuhl für Produktentwicklung an der Technischen Universität München von Herrn Prof. Dr.-Ing. Udo Lindemann und Herrn Dipl.-Ing. Michael Roth betreut.

Anhand dieser Studie soll erarbeitet werden, welche Auswirkung die individuelle Produktgestaltung, laut Experten, auf den Entwicklungsprozess technischer Produkte hat.

In der Umfrage wird nicht Ihre Leistung bewertet, es geht um Ihr Wissen als Experte zu diesem Thema. Selbstverständlich werden alle Daten nur anonymisiert erfasst und gespeichert.

Vielen Dank für Ihre Unterstützung.
Herzliche Grüße
Christina Ulrich

Bei Fragen können Sie sich gerne per E-Mail an mich wenden: christina.ulrich@tum.de

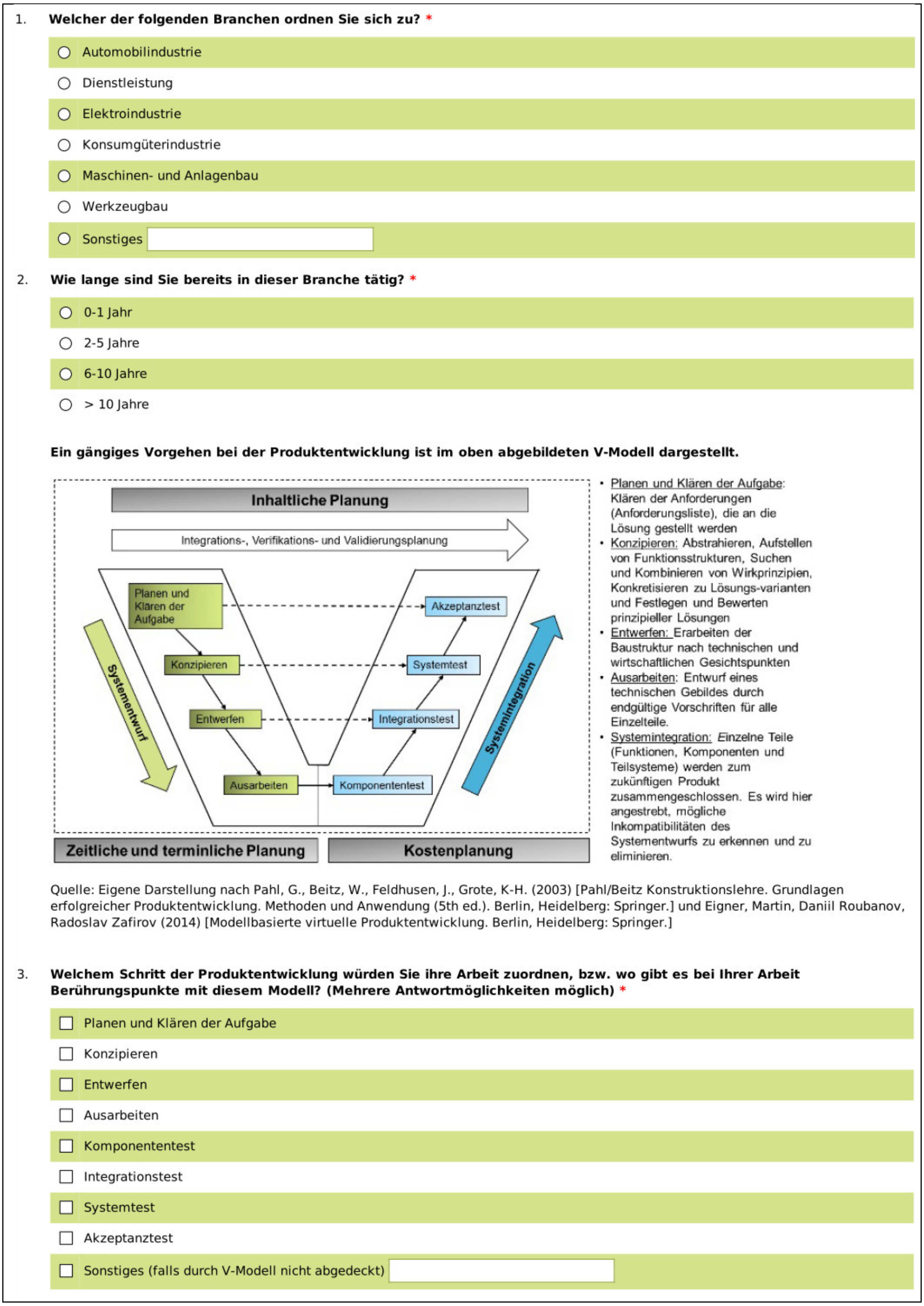
Thematische Einführung

Diese Arbeit beschäftigt sich mit kundeninnovierter Produktentwicklung technischer Produkte, bei welcher der Kunde sein Kreativitäts- und Innovationspotenzial in den Entwicklungsprozess einbringen kann (z.B. mit Hilfe eines Online-Toolkits). Das bedeutet, der Kunde ist am Entwicklungsprozess teilweise beteiligt.

Anhand gezielter Fragen entlang der einzelnen Bereiche des Produktentwicklungsprozesses, soll erfragt werden, an welcher Stelle sich durch diese individuelle Produktenentwicklung, Auswirkungen auf den Entwicklungsprozess ergeben, bzw. wo der Aufwand sich verändert.

Kundeninnovierte Produktentwicklung:

Der Kunde kann individuell am Produkt mitgestalten
Das Produkt wird (von der Community oder dem Hersteller) bewertet
€ 1484
Nach einer Preisabschätzung wird das Produkt der Fertigung übergeben
Anschließend kann das Produkt ausgebessert bzw. umgestaltet werden



1. **Welcher der folgenden Branchen ordnen Sie sich zu? ***

○ Automobilindustrie

○ Dienstleistung

○ Elektroindustrie

○ Konsumgüterindustrie

○ Maschinen- und Anlagenbau

○ Werkzeugbau

○ Sonstiges

2. **Wie lange sind Sie bereits in dieser Branche tätig? ***

○ 0-1 Jahr

○ 2-5 Jahre

○ 6-10 Jahre

○ > 10 Jahre

Ein gängiges Vorgehen bei der Produktentwicklung ist im oben abgebildeten V-Modell dargestellt.

- Planen und Klären der Aufgabe: Klären der Anforderungen (Anforderungsliste), die an die Lösung gestellt werden
- Konzipieren: Abstrahieren, Aufstellen von Funktionsstrukturen, Suchen und Kombinieren von Wirkprinzipien, Konkretisieren zu Lösungs-varianten und Festlegen und Bewerten prinzipieller Lösungen
- Entwerfen: Erarbeiten der Baustruktur nach technischen und wirtschaftlichen Gesichtspunkten
- Ausarbeiten: Entwurf eines technischen Gebildes durch endgültige Vorschriften für alle Einzelteile.
- Systemintegration: Einzelne Teile (Funktionen, Komponenten und Teilsysteme) werden zum zukünftigen Produkt zusammengeschlossen. Es wird hier angestrebt, mögliche Inkompatibilitäten des Systementwurfs zu erkennen und zu eliminieren.

Quelle: Eigene Darstellung nach Pahl, G., Beitz, W., Feldhusen, J., Grote, K-H. (2003) [Pahl/Beitz Konstruktionslehre. Grundlagen erfolgreicher Produktentwicklung. Methoden und Anwendung (5th ed.). Berlin, Heidelberg: Springer.] und Eigner, Martin, Daniil Roubanov, Radoslav Zafirov (2014) [Modellbasierte virtuelle Produktentwicklung. Berlin, Heidelberg: Springer.]

3. **Welchem Schritt der Produktentwicklung würden Sie ihre Arbeit zuordnen, bzw. wo gibt es bei Ihrer Arbeit Berührungspunkte mit diesem Modell? (Mehrere Antwortmöglichkeiten möglich) ***

□ Planen und Klären der Aufgabe

□ Konzipieren

□ Entwerfen

□ Ausarbeiten

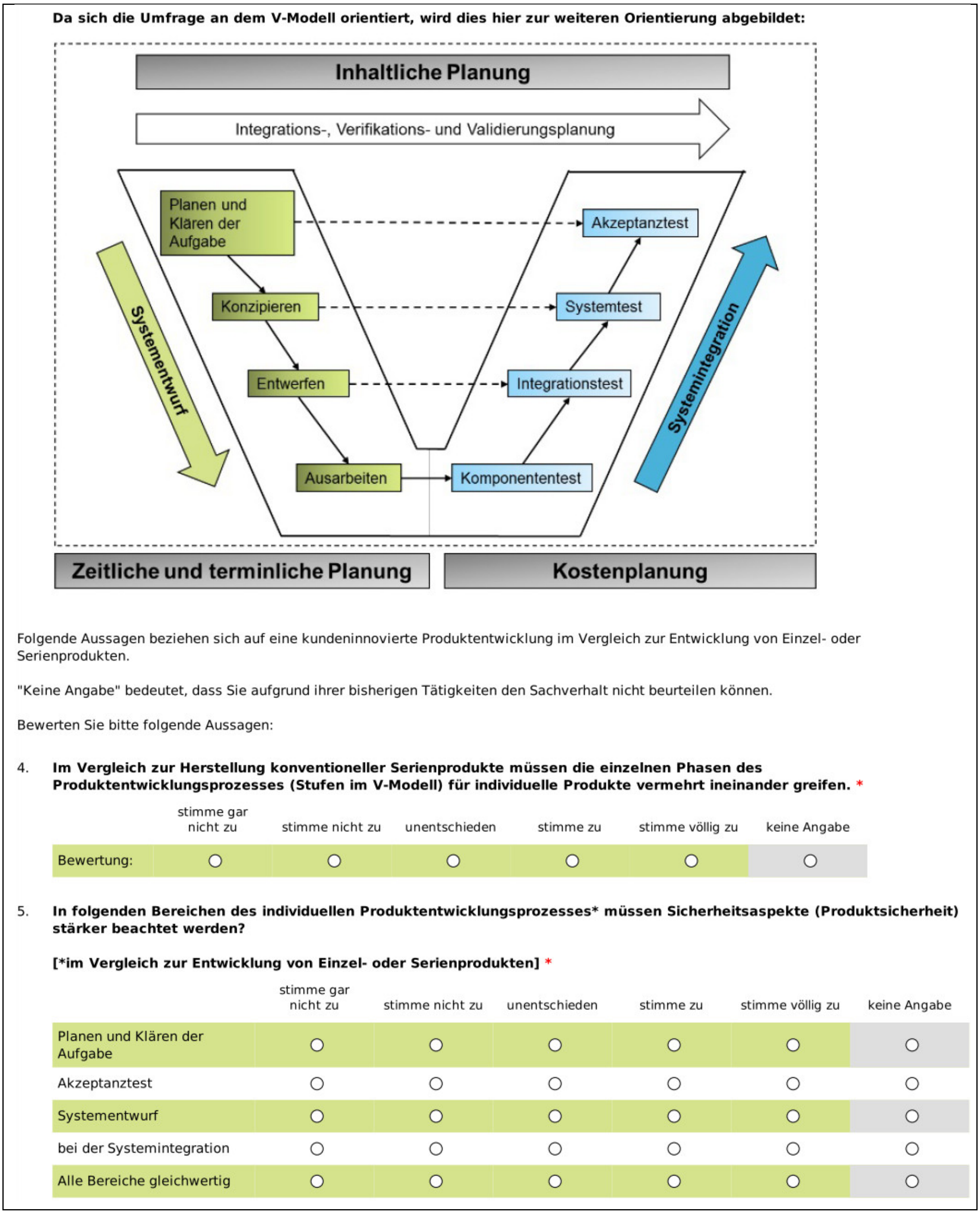
□ Komponententest

□ Integrationstest

□ Systemtest

□ Akzeptanztest

□ Sonstiges (falls durch V-Modell nicht abgedeckt)



Da sich die Umfrage an dem V-Modell orientiert, wird dies hier zur weiteren Orientierung abgebildet:

Folgende Aussagen beziehen sich auf eine kundeninnovierte Produktentwicklung im Vergleich zur Entwicklung von Einzel- oder Serienprodukten.

"Keine Angabe" bedeutet, dass Sie aufgrund ihrer bisherigen Tätigkeiten den Sachverhalt nicht beurteilen können.

Bewerten Sie bitte folgende Aussagen:

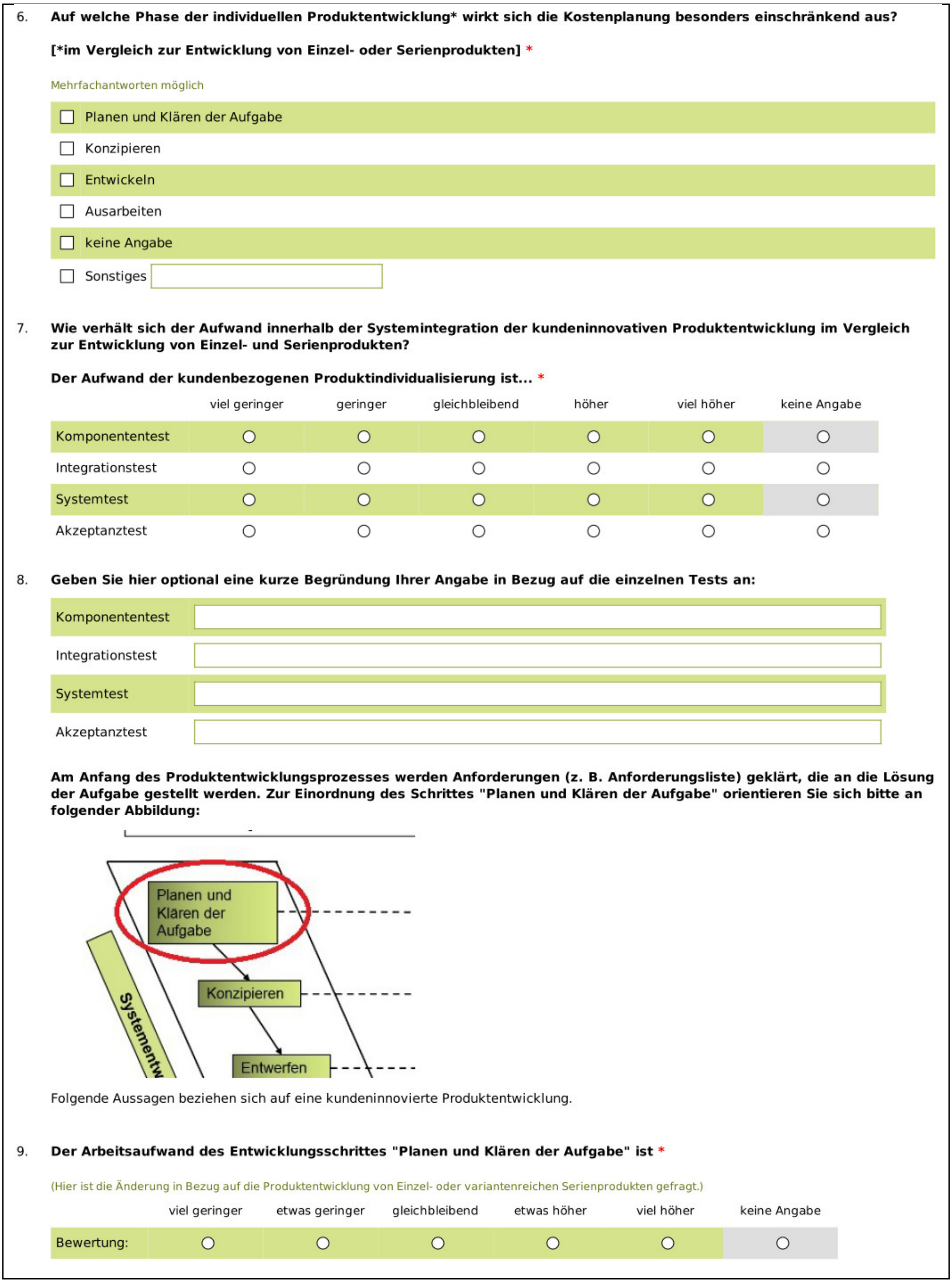
4. **Im Vergleich zur Herstellung konventioneller Serienprodukte müssen die einzelnen Phasen des Produktentwicklungsprozesses (Stufen im V-Modell) für individuelle Produkte vermehrt ineinander greifen.** *

	stimme gar nicht zu	stimme nicht zu	unentschieden	stimme zu	stimme völlig zu	keine Angabe
Bewertung:	○	○	○	○	○	○

5. **In folgenden Bereichen des individuellen Produktentwicklungsprozesses* müssen Sicherheitsaspekte (Produktsicherheit) stärker beachtet werden?**

[*im Vergleich zur Entwicklung von Einzel- oder Serienprodukten] *

	stimme gar nicht zu	stimme nicht zu	unentschieden	stimme zu	stimme völlig zu	keine Angabe
Planen und Klären der Aufgabe	○	○	○	○	○	○
Akzeptanztest	○	○	○	○	○	○
Systementwurf	○	○	○	○	○	○
bei der Systemintegration	○	○	○	○	○	○
Alle Bereiche gleichwertig	○	○	○	○	○	○



6. **Auf welche Phase der individuellen Produktentwicklung* wirkt sich die Kostenplanung besonders einschränkend aus?**

[*im Vergleich zur Entwicklung von Einzel- oder Serienprodukten] *

Mehrfachantworten möglich

- ☐ Planen und Klären der Aufgabe
- ☐ Konzipieren
- ☐ Entwickeln
- ☐ Ausarbeiten
- ☐ keine Angabe
- ☐ Sonstiges ________

7. **Wie verhält sich der Aufwand innerhalb der Systemintegration der kundeninnovativen Produktentwicklung im Vergleich zur Entwicklung von Einzel- und Serienprodukten?**

Der Aufwand der kundenbezogenen Produktindividualisierung ist... *

	viel geringer	geringer	gleichbleibend	höher	viel höher	keine Angabe
Komponententest	○	○	○	○	○	○
Integrationstest	○	○	○	○	○	○
Systemtest	○	○	○	○	○	○
Akzeptanztest	○	○	○	○	○	○

8. **Geben Sie hier optional eine kurze Begründung Ihrer Angabe in Bezug auf die einzelnen Tests an:**

Komponententest	
Integrationstest	
Systemtest	
Akzeptanztest	

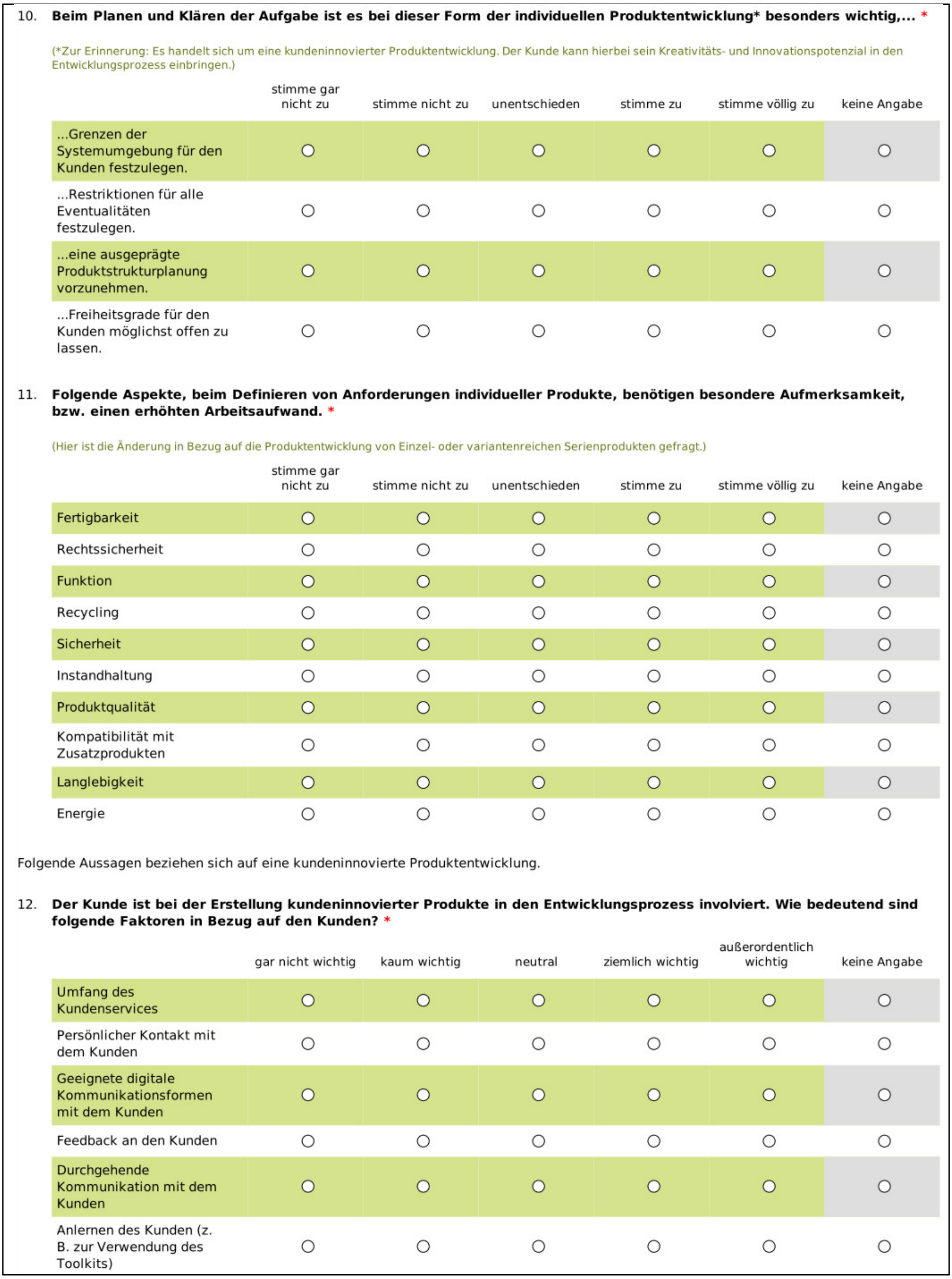
Am Anfang des Produktentwicklungsprozesses werden Anforderungen (z. B. Anforderungsliste) geklärt, die an die Lösung der Aufgabe gestellt werden. Zur Einordnung des Schrittes "Planen und Klären der Aufgabe" orientieren Sie sich bitte an folgender Abbildung:

Folgende Aussagen beziehen sich auf eine kundeninnovierte Produktentwicklung.

9. **Der Arbeitsaufwand des Entwicklungsschrittes "Planen und Klären der Aufgabe" ist** *

(Hier ist die Änderung in Bezug auf die Produktentwicklung von Einzel- oder variantenreichen Serienprodukten gefragt.)

	viel geringer	etwas geringer	gleichbleibend	etwas höher	viel höher	keine Angabe
Bewertung:	○	○	○	○	○	○



10. **Beim Planen und Klären der Aufgabe ist es bei dieser Form der individuellen Produktentwicklung* besonders wichtig,...** *

(*Zur Erinnerung: Es handelt sich um eine kundeninnovierter Produktentwicklung. Der Kunde kann hierbei sein Kreativitäts- und Innovationspotenzial in den Entwicklungsprozess einbringen.)

	stimme gar nicht zu	stimme nicht zu	unentschieden	stimme zu	stimme völlig zu	keine Angabe
...Grenzen der Systemumgebung für den Kunden festzulegen.	○	○	○	○	○	○
...Restriktionen für alle Eventualitäten festzulegen.	○	○	○	○	○	○
...eine ausgeprägte Produktstrukturplanung vorzunehmen.	○	○	○	○	○	○
...Freiheitsgrade für den Kunden möglichst offen zu lassen.	○	○	○	○	○	○

11. **Folgende Aspekte, beim Definieren von Anforderungen individueller Produkte, benötigen besondere Aufmerksamkeit, bzw. einen erhöhten Arbeitsaufwand.** *

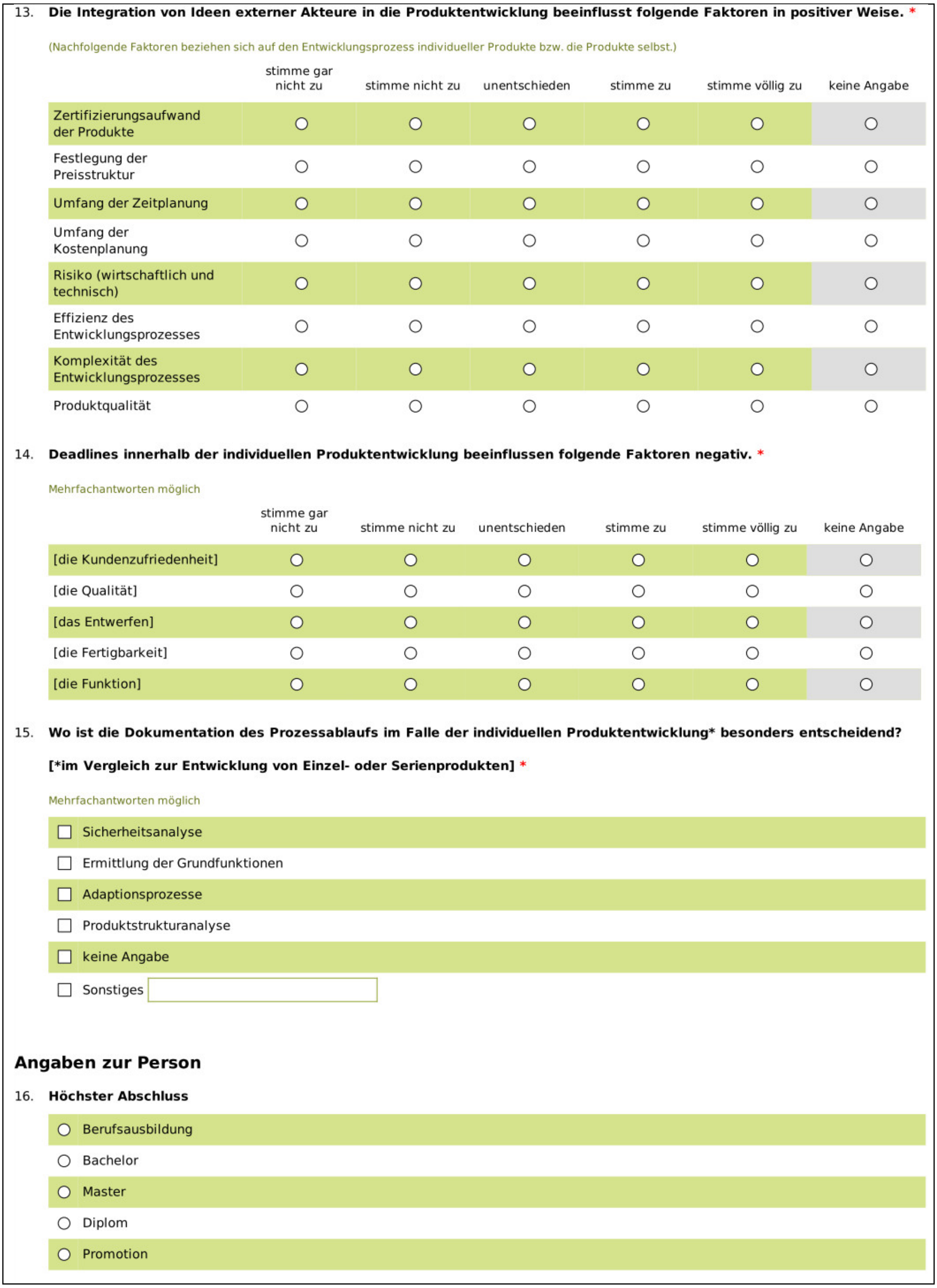
(Hier ist die Änderung in Bezug auf die Produktentwicklung von Einzel- oder variantenreichen Serienprodukten gefragt.)

	stimme gar nicht zu	stimme nicht zu	unentschieden	stimme zu	stimme völlig zu	keine Angabe
Fertigbarkeit	○	○	○	○	○	○
Rechtssicherheit	○	○	○	○	○	○
Funktion	○	○	○	○	○	○
Recycling	○	○	○	○	○	○
Sicherheit	○	○	○	○	○	○
Instandhaltung	○	○	○	○	○	○
Produktqualität	○	○	○	○	○	○
Kompatibilität mit Zusatzprodukten	○	○	○	○	○	○
Langlebigkeit	○	○	○	○	○	○
Energie	○	○	○	○	○	○

Folgende Aussagen beziehen sich auf eine kundeninnovierte Produktentwicklung.

12. **Der Kunde ist bei der Erstellung kundeninnovierter Produkte in den Entwicklungsprozess involviert. Wie bedeutend sind folgende Faktoren in Bezug auf den Kunden?** *

	gar nicht wichtig	kaum wichtig	neutral	ziemlich wichtig	außerordentlich wichtig	keine Angabe
Umfang des Kundenservices	○	○	○	○	○	○
Persönlicher Kontakt mit dem Kunden	○	○	○	○	○	○
Geeignete digitale Kommunikationsformen mit dem Kunden	○	○	○	○	○	○
Feedback an den Kunden	○	○	○	○	○	○
Durchgehende Kommunikation mit dem Kunden	○	○	○	○	○	○
Anlernen des Kunden (z. B. zur Verwendung des Toolkits)	○	○	○	○	○	○



13. **Die Integration von Ideen externer Akteure in die Produktentwicklung beeinflusst folgende Faktoren in positiver Weise.** *

(Nachfolgende Faktoren beziehen sich auf den Entwicklungsprozess individueller Produkte bzw. die Produkte selbst.)

	stimme gar nicht zu	stimme nicht zu	unentschieden	stimme zu	stimme völlig zu	keine Angabe
Zertifizierungsaufwand der Produkte	○	○	○	○	○	○
Festlegung der Preisstruktur	○	○	○	○	○	○
Umfang der Zeitplanung	○	○	○	○	○	○
Umfang der Kostenplanung	○	○	○	○	○	○
Risiko (wirtschaftlich und technisch)	○	○	○	○	○	○
Effizienz des Entwicklungsprozesses	○	○	○	○	○	○
Komplexität des Entwicklungsprozesses	○	○	○	○	○	○
Produktqualität	○	○	○	○	○	○

14. **Deadlines innerhalb der individuellen Produktentwicklung beeinflussen folgende Faktoren negativ.** *

Mehrfachantworten möglich

	stimme gar nicht zu	stimme nicht zu	unentschieden	stimme zu	stimme völlig zu	keine Angabe
[die Kundenzufriedenheit]	○	○	○	○	○	○
[die Qualität]	○	○	○	○	○	○
[das Entwerfen]	○	○	○	○	○	○
[die Fertigbarkeit]	○	○	○	○	○	○
[die Funktion]	○	○	○	○	○	○

15. **Wo ist die Dokumentation des Prozessablaufs im Falle der individuellen Produktentwicklung* besonders entscheidend?**

[*im Vergleich zur Entwicklung von Einzel- oder Serienprodukten] *

Mehrfachantworten möglich

□ Sicherheitsanalyse

□ Ermittlung der Grundfunktionen

□ Adaptionsprozesse

□ Produktstrukturanalyse

□ keine Angabe

□ Sonstiges ______

Angaben zur Person

16. **Höchster Abschluss**

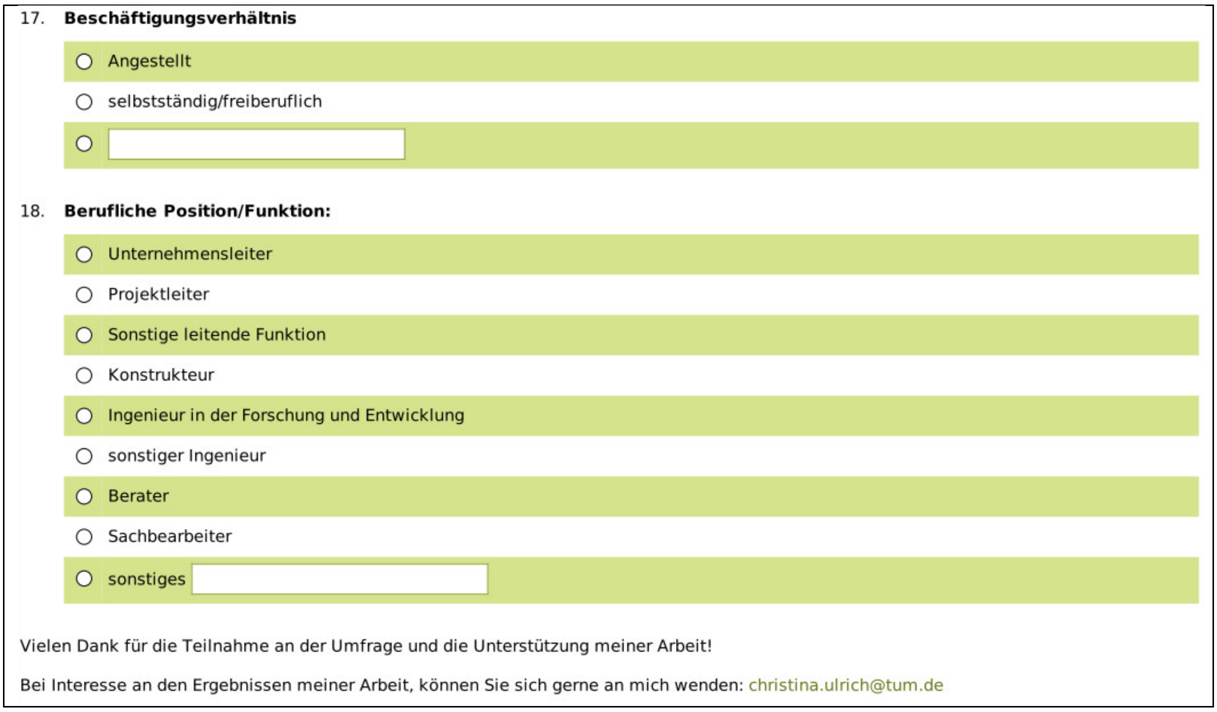
○ Berufsausbildung

○ Bachelor

○ Master

○ Diplom

○ Promotion



17. **Beschäftigungsverhältnis**

○ Angestellt

○ selbstständig/freiberuflich

○

18. **Berufliche Position/Funktion:**

○ Unternehmensleiter

○ Projektleiter

○ Sonstige leitende Funktion

○ Konstrukteur

○ Ingenieur in der Forschung und Entwicklung

○ sonstiger Ingenieur

○ Berater

○ Sachbearbeiter

○ sonstiges

Vielen Dank für die Teilnahme an der Umfrage und die Unterstützung meiner Arbeit!

Bei Interesse an den Ergebnissen meiner Arbeit, können Sie sich gerne an mich wenden: christina.ulrich@tum.de

9.1.4 Statistical Results of the Questionnaire Survey

The statistical analysis of the questionnaire survey results is shown in the following (Roth et al., 2016; Ulrich, 2015):

												95% confid. interval	
hyp	**item**	**dependent variable**	**topic**	**N**	**mean**	**std. deviation**	**mean std.error**	**t**	**df**	**sig. (2-tailed)**	**mean difference**	**lower**	**upper**
H1	4	interconnection & integration	integration	40	3.4750	1.15442	.18253	2.602	39	0.013	0.47500	0.1058	0.8442
H2	5	safety efforts	task clarification	37	3.7838	1.03105	.16950	4.624	36	0.000	0.78378	0.4400	1.1276
			system design	35	3.3143	1.13167	.19129	1.643	34	0.110	0.31429	-0.0745	0.7030
			system integration	35	3.8286	1.07062	.18097	4.579	34	0.000	0.82857	0.4608	1.1963
			validation	35	3.8571	1.00419	.16974	5.050	34	0.000	0.85714	0.5122	1.2021
			equal in all phases	21	3.0000	1.09545	.23905	0.000	20	1.000	0.00000	-0.4986	0.4986
H3	9	task clarification efforts	task clarification	33	3.7576	1.11888	.19477	3.890	32	0.000	0.75758	0.3608	1.1543
H4	10	need for restrictions	system boundaries	32	4.0938	1.02735	.18161	6.022	31	0.000	1.09375	0.7234	1.4641
			extensive product structure planning	32	3.6875	0.93109	.16460	4.177	31	0.000	0.68750	0.3518	1.0232
			restrictions covering all possibilities	31	3.3871	1.28264	.23037	1.680	30	0.103	0.38710	-0.0834	0.8576
			maximal degrees of freedom	33	3.3333	1.33853	.23301	1.431	32	0.162	0.33333	-0.1413	0.8080
H6	7	testing efforts	component tests	36	3.5000	0.84515	.14086	3.550	35	0.001	0.50000	0.2140	0.7860
			integration tests	36	3.8611	0.79831	.13305	6.472	35	0.000	0.86111	0.5910	1.1312
			system tests	36	3.7222	0.74108	.12351	5.847	35	0.000	0.72222	0.4715	0.9730
			validation	32	3.1563	1.08090	.19108	0.818	31	0.420	0.15625	-0.2335	0.5460
H7	12	need for user involvement	digital user communication	32	4.1563	0.88388	.15625	7.400	31	0.000	1.15625	0.8376	1.4749
			extent of user service	31	3.7419	0.85509	.15358	4.831	30	0.000	0.74194	0.4283	1.0556
			continuous communication	32	4.0938	0.92838	.16412	6.664	31	0.000	1.09375	0.7590	1.4285
			feedback to users	31	4.2258	0.71692	.12876	9.520	30	0.000	1.22581	0.9628	1.4888
			training of users	32	3.5313	0.91526	.16180	3.283	31	0.003	0.53125	0.2013	0.8612
			personal user communication	32	3.7813	1.00753	.17811	4.386	31	0.000	0.78125	0.4180	1.1445

												95% confid. interval	
hyp	item	dependent variable	topic	N	mean	std. deviation	mean std.error	t	df	sig. (2-tailed)	mean difference	lower	upper
H8	13	benefit for general aspects	price structure	33	3.1212	1.11124	.19344	0.627	32	0.535	0.12121	-0.2728	0.5152
			complexity	32	2.1563	1.19432	.21113	-3.996	31	0.000	-0.84375	-1.2743	-0.4132
			pricing	32	2.5313	.98323	.17381	-2.697	31	0.011	-0.46875	-0.8232	-0.1143
			risk	33	2.6667	1.13652	.19784	-1.685	32	0.102	-0.33333	-0.7363	0.0697
			certification	33	2.0606	1.11634	.19433	-4.834	32	0.000	-0.93939	-1.3352	-0.5436
			scheduling	32	2.3750	1.03954	.18377	-3.401	31	0.002	-0.62500	-0.9998	-0.2502
			efficiency	32	2.5000	1.21814	.21534	-2.322	31	0.027	-0.50000	-0.9392	-0.0608
			quality	33	2.9697	1.01504	.17670	-0.171	32	0.865	-0.03030	-0.3902	0.3296
H9	15	importance for documentation	safety	n.a.									
			basic function’s elicitation										
			adaption processes										
			product structure analysis										
			none										

9.2 Details of the Interviews on UDC’s Impact on Safety Analysis

This section provides details of the focus-interviews presented in Section 3.3. They originate from the connected student project (Gehrlicher, 2014) and the prior publication (Roth et al., 2015). To prevent potential bias, the questions and protocols of the interviews are provided in their original German form and are not translated.

9.2.1 Semi-structured Interview Guideline of the Focus-Interviews

The semi-structured guideline used within the qualitative interviews consited of the following 17 question items (Gehrlicher, 2014):

Interviewleitfaden

Standardbauteile/ Module:

- *Welchen prozentualen Anteil an Standardprodukten?*
- *Was sind das für Standardprodukte?*
- *Zulassung und Zertifizierung der Standardbauteile?*
- *Einzelzulassung für jedes Einzelteil?*
- *Ablauf einer Risiko- und Gefährdungsanalyse der Standardbauteile?*
- *Prüfer intern oder extern?*
- *Umgang mit Kombi von Standardbauteilen und deren Schnittstellen?*

Individuelle Produkte:

- *Umgang mit individuellen Produkten?*
- *Wie viel Prozent wird komplett neu entwickelt?*
- *Erneute Risiko- und Gefährdungsanalyse für das gesamte Endprodukt?*
- *Gibt es immer neue Komplettabnahmen oder nur zusätzliche Einzelabnahmen?*
- *Umgang mit der Schnittstelle zweier Standartbauteile?*

Strategie zur wiederholten Nutzung:

- *Wiederholte Wissensnutzung vorhanden?*
- *Methode der wiederholten Nutzung von Ergebnissen früher Risiko und Gefährdungsanalysen?*
- *Dokumentation oder/und Erfahrungswissen?*

Individualisierung:

- *Welche neuen Herausforderungen sehen Sie für das Risikomanagement bei der Produktentwicklung im Zusammenhang mit „offener Produktindividualisierung“?*
- *Wie wird Ihrer Meinung nach das Konfigurationsmanagement durch die kundenbezogene Produktindividualisierung beeinflusst?*

9.2.2 Minutes of the Semi-structured Focus-Interviews

The semi-structured focus-interviews were conducted by the involved student and logged by an assistant. In the following, the minutes of the interviews in their original language are provided (Gehrlicher, 2014):

Minutes of Interview I (2014/07/04)

Attendees: Senior engineer (E1), Interviewer (I)

Description of company and E1:

The interviewee is a very experienced engineer of a company following an engineer-to-order concept. He possesses more than 20 years of experience and is deeply involved in safety assurance and norming committees.

Interview:

Genereller Umgang:

In welche Abteilung wird Risiko- und Gefährdungsanalyse durchgeführt?

- *70 Teams*
- *FMEA aber kein System Engineering*

In welchen Entwicklungsschritt ist eine Risiko- und Gefährdungsanalyse eingebunden?

- *Problematik: Komponentenspezialist vs. Systemspezialist*

Nur in Form von FMEA oder andere Methoden zur Risiko- und Gefährdungsanalyse?

- *FMEA immer*
- *ob Risikoanalyse ist fraglich*
- *oft aus Erfahrung regelbasiert*
- *FMECA*
- *EBA*

FMEA Typ?

- *Prozess bis System FMEA*

Software für Methoden vorhanden?

- *Ja , FaultTtree+*

Standardelemente/ Module:

Ablauf einer Risiko- und Gefährdungsanalyse der Standardbauteile?

- *Systeme werden für Einsatz geplant (Strecken)*
- *Auslegung mit Sicherheit, nach Normen*
- *Sicherheitsmaßnahmen: Einzelausfall darf keinen Einfluss*
- *Geschachtelt von unten*

Prüfer für Produktzulassung intern oder extern?

- *Elektrik von TÜV*
- *Mechanik: Homologiert durch einen Fahrzeugbauer im Test*

Sind die einzelnen verbauten Standardkomponenten schon vorzertifiziert und haben bereits eine Risiko- und Gefährdungsanalyse durchlaufen?

- *System muss geforderte RB enthalten*
- *System FMEA*
- *Auch auf Komponenten Ebene finden FMEAs statt*
- *3 Verfahren des Risikos: Regelbasiertes Vorgehen, Risikoanalyse, Referenzbasiert*

Individuelle Produkte:
Wie viel Prozent wird komplett neu entwickelt?

- *70% bis 80% sind Standard*
- *Verpackung und Kombinationen sind individuell*

Gibt es immer neue Komplettabnahmen mit Risiko- und Gefährdungsanalyse oder nur zusätzliche Einzelabnahmen, der individuellen Produkten mit einer Risiko- und Gefährdungsanalyse?

- *Neuabnahme ist trotzdem erforderlich*
- *Wenn Zertifikate vorhanden sind, ist eine Gesamtabnahme leichter*
- *Bei Neuentwicklungen wird auch der Entwicklungsprozess beurteilt*

Wie geht man diesbezüglich mit den Schnittstellen zu den Standardkomponenten um?

- *Kombinationen und Schnittstellen werden nochmal genau überprüft (FMEA, Auswirkungsanalyse)*
- *Auch Standardstrategien*

Strategie zur wiederholten Nutzung:
Wiederholte Wissensnutzung vorhanden? (ähnliches Produkt-> keine erneute Risiko- und Gefährdungsanalyse)

- *Wiederverwendung von Excel -Tabellen schwierig*

Methode der wiederholten Nutzung von Ergebnissen früher Risiko und Gefährdungsanalysen?

- *Ziel: Modellbasiertes System mit Variantenmanagement*

Dokumentation oder/und Erfahrungswissen?

- *Bisher hauptsächlich Expertenbasiert*
- *Hoher Nutzen für Risiko- und Gefährdungsanalyse vorhanden*

Deutlich kleineres Risiko, Fehlervermeidung?

- *Erwartungen von weniger Aufwand und größerer Sicherheit*

Minutes of Interview II (2014/08/11)
Attendees: Senior engineer (E2), Interviewer (I)

Description of company and E2:
The interviewee is a very experienced engineer of a company being both, engineer-to-odder OEM and first tier supplier.

Interview:
Genereller Umgang:
In welche Abteilung wird Risiko- und Gefährdungsanalyse durchgeführt?

- *Technische Konstruktion*

Standardelemente/ Module:
Im Anschluss Zulassung und Zertifizierung dieser Standardbauteil?

- *Alle CE Siegel*

Prüfer für Produktzulassung intern oder extern?

- *Je nach Größe der Anlage*
- *Je nachdem wer die Inbetriebnahme absolviert*
- *Mehr als zwei Sicherheitskomponenten: TÜV intern: befähigte Personen*

Sind die einzelnen verbauten Standardkomponenten schon vorzertifiziert und haben bereits eine Risiko- und Gefährdungsanalyse durchlaufen?

- *Alles mit CE Siegel vorzertifiziert*
- *Standardkomponenten vorhanden*
- *Alle Standardkomponenten haben einen Risiko- und Gefährdungsanalyse bereits durchlaufen*

Individuelle Produkte:

Wie viel Prozent wird komplett neu entwickelt?

- *30% bis 40%*

Gibt es immer neue Komplettabnahmen mit Risiko- und Gefährdungsanalyse oder nur zusätzliche Einzelabnahmen, der individuellen Produkten mit einer Risiko- und Gefährdungsanalyse?

- *Sowohl Komplettabnahmen als auch Einzelabnahmen*
- *Je nachdem wer die Inbetriebnahme durchführt: Verkauf von Einzelkomponenten, komplette Inbetriebnahme, Teilinbetriebnahme*

Wie geht man diesbezüglich mit den Schnittstellen zu den Standardkomponenten um?

- *Schnittstellen werden immer erneut geprüft*

Strategie zur wiederholten Nutzung:

Wiederholte Wissensnutzung vorhanden? (ähnliches Produkt-> keine erneute Risiko- und Gefährdungsanalyse)

- *Bisher Expertenwissen*
- *Wiederholte Wissensnutzung vorhanden, aber ausbaufähig*

Methode der wiederholten Nutzung von Ergebnissen früher Risiko und Gefährdungsanalysen?

- *Erfahrungswissen*
- *Expertenwissen*

Dokumentation oder/und Erfahrungswissen?

- *Keine Dokumentation*
- *hoher Nutzen für Risiko- und Gefährdungsanalyse vorhanden*

Deutlich kleineres Risiko, Fehlervermeidung ?

- *Notwendig für die Zertifizierung*
- *Nicht anders möglich*

Transcript of Interview III (2014/09/24)

Attendees: Safety engineer (E3), Interviewer (I)

Description of company and E3:

The interviewee is an experienced engineer of a company acting as OEM of mass products with high variance. He is the responsible expert for the safety analysis and approval of one class of products.

Interview:

Genereller Umgang:

In welche Abteilung wird Risiko- und Gefährdungsanalyse durchgeführt?

- *Qualitätssicherung*
- *Nach Richtlinien und Normen*

In welchen Entwicklungsschritt ist eine Risiko- und Gefährdungsanalyse eingebunden?

- *Von Anfang an*

Nur in Form von FMEA oder andere Methoden zur Risiko- und Gefährdungsanalyse?

- *Ausgehen von Normen*
- *Nach Normen sind prinzipiell alle Risiken (bekannten) abgesichert*
- *Durchgehend jede Anforderung*
- *Checkliste*
- *Vermutungswirkung: man kann nie ausschließen, dass was passiert*

FMEA Typ?

- *Prozess, Konstruktion und System FMEA*
- *FMEA mit nicht normativen Risiken: Risiken sind zwar in der Norm festgehalten, aber stellen dennoch ein Risiko dar*

Software für Methoden vorhanden?

- *Ja , QM Software*

Standardelemente/ Module:

Ablauf einer Risiko- und Gefährdungsanalyse der Standardbauteile?

- *Ausgehend von Normen*
- *Checklisten*

Prüfer für Produktzulassung intern oder extern?

Intern über Abteilung (befugt Person)

- *CB-Report*
- *Auditbericht*
- *VDE: Überprüfung der Protokolle*
- *VDE: Plausibilitätscheck*

Sind die einzelnen verbauten Standardkomponenten schon vorzertifiziert und haben bereits eine Risiko- und Gefährdungsanalyse durchlaufen?

- *Zukaufsteile durch Hersteller*
- *Sicherheitskritische Bauteile werden explizit aufgelistet*
- *Einbaubedingungen werden in jedem Gerät neu geprüft*

Variantenreiche Serienprodukte:

Wird nur an einer Variante aus einer Produktlinie eine Risiko- und Gefährdungsanalyse durchgeführt oder na allen Varianten?

- *Regelmäßiges aktualisieren des Reports*
- *Alle Änderung VDE melden*
- *Zulassung im Report von Typen: in einem Report werden die unterschiedlichen Varianten einer Serie aufgelistet*
- *Entscheidungen durch Einschätzungen*

Strategie zur wiederholten Nutzung:

Wiederholte Wissensnutzung vorhanden? (ähnliches Produkt-> keine erneute Risiko- und Gefährdungsanalyse)

- *Nicht normative Risiken werden meist wieder verwendet*
- *Erfahrungswissen*

Methode der wiederholten Nutzung von Ergebnissen früher Risiko und Gefährdungsanalysen?

- *Dokumentation oder/und Erfahrungswissen?*

- *Größtes Problem: Dokumentation*
- *Erziehungsarbeit in der Entwicklung ist gefragt*
- *Nicht normative Risiken werden immer dokumentiert, zu Rate gezogen*
- *hoher Nutzen für Risiko- und Gefährdungsanalyse vorhanden*

9.3 Details of the ESMK Knowledge Framework

This section provides details of the ESMK knowledge framework defined in Section 4.2. This includes the evaluation of ECM methods and an overview of nodes and edges used in the framework.

9.3.1 Evaluation of ECM Methods

The ESMK knowledge framework is developed based on a review on existing ECM methods, which is partially published (Roth et al., 2016). In the following, the detailed evaluation of these methods is provided:

title	authors	year	components	flows	functions	fault	processes	comp. properties	design parameters	requirements	abstract objects	information	individuals/resources	DSM/DMM	CPM	C&CM	Monte Carlo simulation	propagation tree	QFD	Bayesian networks	FBS	function propagation method	heuristics	others	own
supporting the management of the engineering change process through a cross-domain traceability model	Ahmad	2010	x		x		x		x	x					x										
an MDM-based approach to manage engineering change processes across domains of the design process	Ahmad, Wynn, Clarkson	2009	x		x				x	x				x	x										
information models used to manage engineering change: a review of literature 2005-2010	Ahmad, Wynn, Clarkson	2011	x		x		x		x	x					x										
change propagation in complex design: predicting detailed change cases with multi-levelled product models	Ariyo	2007	x											x	x										
tolerance margins as constraining factors of changes in complex products	Ariyo, Eckert, Clarkson	2004	x											x	x										
on the use of functions, behaviour and structural relations as cues for engineering change prediction	Ariyo, Eckert, Clarkson	2006	x		x										x						x				
predicting change propagation on different levels of granularity: an algorithmic view	Ariyo, Keller, Eckert, Clarkson	2007	x											x	x			x							
DSM based approach for managing requirements, rules and design parameters in knowledge based design process	Bhaskara	2010	x				x		x			x		x											
matrix-based change management: a case study in a construction project	Chen, Li	2010					x						x	x											
predicting change propagation in complex design	Clarkson, Simons, Eckert	2004	x											x	x										
impact of architecture types and degree of modularity on change propagation indices	Colombo, Cascini, de Weck,	2015	x											x			(x)								

title	authors	year	components	flows	functions	fault	processes	comp. properties	design parameters	requirements	abstract objects	information	individuals/resources	DSM/DMM	CPM	C&CM	Monte Carlo simulation	propagation tree	QFD	Bayesian networks	FBS	function propagation method	heuristics	others	own
on the role of DSM in designing systems and products for changeability	de Weck	2007	x											x											
a functional analysis of change propagation	Flanagan, Eckert, Smith, Eger, Clarkson	2003	x		x									x								x			
classifying components based on change propagation potential	Grinnell, Schmidt, Austin	2012	x											x											
FBS linkage model – towards an integrated engineering change prediction and analysis method	Hamraz, Caldwell, Clarkson	2012	x		x		x		x												x				
a matrix-calculation-based algorithm for numerical change propagation analysis	Hamraz, Caldwell, Clarkson	2013	x											x	x										
a multidomain engineering change propagation model to support uncertainty reduction and risk management in design	Hamraz, Caldwell, Clarkson	2012	x		x					x				x	x						x				
requirements-based development of an improved engineering change management method	Hamraz, Caldwell, Wynn, Clarkson	2013	x		x									x	x						x				
industrial evaluation of FBS linkage – a method to support engineering change management	Hamraz, Clarkson	2015	x		x									x	x						x				
a model-based approach to support the management of engineering change	Jarratt	2004	x											x	x										
the benefits of predicting change in complex products: application areas of a DSM-based prediction tool	Jarratt, Eckert, Clarkson	2004	x											x	x										
product architecture and the propagation of engineering change	Jarratt, Eckert, Clarkson, Schwankl	2002	x												x										
predicting change propagation: algorithms, representations, software tools	Keller	2007	x				x							x											
product models in design: a combined use of two models to assess change risks	Keller, Alink, Pfeifer, Eckert, Clarkson, Albers	2007	x											x	x	x									
heuristics for change prediction	Keller, Eckert, Clarkson	2006	x											x	x								x		
using an engineering change methodology to support conceptual design	Keller, Eckert, Clarkson	2009	x												x										
visualising change propagation	Keller, Eger, Eckert, Clarkson	2005	x											x	x			x							
managing change propagation in the development of complex products	Koh	2010	x					x		x			x	x	x				x		x				
using a matrix-based approach to model change propagation	Koh, Caldwell, Clarkson	2009	x					x		x				x	x			x							
a technique to assess the changeability of complex engineering systems	Koh, Caldwell, Clarkson	2013	x											x	x										

title	authors	year	components	flows	functions	fault	processes	comp. properties	design parameters	requirements	abstract objects	information	individuals/resources	DSM/DMM	CPM	C&CM	Monte Carlo simulation	propagation tree	QFD	Bayesian networks	FBS	function propagation method	heuristics	others	own
a modeling method to manage change propagation	Koh, Clarkson	2009	x					x		x			x	x	x			x							
using engineering change forecast to prioritise component modularisation	Koh, Förg, Kreimeyer, Lienkamp	2015	x							x				x											
component classification: a change perspective	Koh, Keller, Eckert, Clarkson	2007	x											x	x										
change propagation modelling to support the selection of solutions in incremental change	Koh, Keller, Eckert, Clarkson	2009	x					x		x					x	x			x						
influence of feature change propagation on product attributes in concept selection	Koh, Keller, Eckert, Clarkson	2008	x					x		x				x	x			x							
a Bayesian network approach to improve change propagation analysis	Lee, Hong	2015	x											x	x					x					
an analytic network process approach to measuring design change impacts in modular products	Lee, Seol, Sung, Hong, Park	2010	x																						x
identification of clusters and interfaces for supporting the implementation of change requests	Li, Chen	2014	x		x									x											
path-based and pattern-based approaches for change management	Li, Rajinia	2010									x			x											
simulating progressive iteration, rework and change propagation to prioritise design tasks	Maier, Wynn, Biedermann, Lindemann, Clarkson	2014	x				x						x	x			x							x	
supporting the modification process of products through a change management tool	Malatesta, Raffaeli, Mengoni, Germani	2013	x					(x)							x										
dependency identification for engineering change management (ECM): an example of computer-aided design (CAD)-based approach	Masmoudi, Leclaire, Zolghadri, Haddar	2015							x																x
taking into account the change of geometry in system simulation processes	Mauser, Breitsprecher, Hasse, Wartzack	2015			x					x						x									
predicting requirement change propagation, using higher order design structure matrices: an industry case study	Morkos, Shankar, Summers	2012								x				x											
investigation of system sensitivity to propagated configuration faults	Nagel, Stone, Greer, McAdams	2009		x	x	x																		x	
evaluating the risk of change propagation	Oduncuoglu, Thomson,	2011	x		(x)				(x)	(x)				x	x										
functional structure based change assessment in product design	Oizumi, Aoyama	2012	x		x				x					x					x						
multilayer network model for analysis and management of change propagation	Pasqual, de Weck	2011	x				x						x	x											

title	authors	year	components	flows	functions	fault	processes	comp. properties	design parameters	requirements	abstract objects	information	individuals/resources	DSM/DMM	CPM	C&CM	Monte Carlo simulation	propagation tree	QFD	Bayesian networks	FBS	function propagation method	heuristics	others	own
multilayer network model for analysis and management of change propagation	Pasqual, de Weck	2012	x										x	x	x										
development of a multilayer change propagation tool for modular products	Raffaeli, Germani, Graziosi, Mandorli	2007	x					x										x							x
controlling product related engineering changes in the aircraft industry	Riviere, Féru, Tollenaere	2003								(x)	(x)		(x)												x
simulation of product change effects based on design structure and domain mapping matrices	Schneider, Schlick, Röwenstrunk, Mütze-Niewöhner	2012	x				x		x					x											
can change prediction help prioritise redesign work in future engineering systems?	Wynn, Caldwell, Clarkson	2010	x				(x)							x	x		x	x							

9.3.2 Nodes and Edges of the ESMK Knowledge Framework

The ESMK knowledge framework defined and implemented using the software Soley (see Subsection 5.1.2). The graph-based model mainly consists of the following classes of nodes and attributes:

node class	attribute	description
all nodes	name (string)	name of the node
	id (string)	identifier of the node
	level (int)	hierarchical decomposition level of the node
	abstraction_ok (int)	marker for the abstraction level within the analyses
boolean_gate (extends failure)	property_type (string)	type of gate (AND or OR)
component	part_identification_number (string)	part identification number of the component
	document (string)	number of the component documents
	is_customizable (boolean)	marker if component is offered for UDC
	is_fixed (boolean)	marker if component is defined as fixed/standard
	UDC_demand (double)	value to assess the UDC demand of a component
	is_customized (boolean)	marker if component is customized in the toolkit
	connectivity_no (int)	number of connected components
	safety_req_no (int)	number of connected safety requirements
	hazard_no (int)	number of connected hazards
	safety_level1 (double)	safety-relevance value (level 1)
	safety_level2 (double)	safety-relevance value (level 2)
	safety_level3 (double)	safety-relevance value (level 3)
	geoDistance (double)	geometrical distance in the MBHPA's propagation tree
	weightedDistance (double)	weighted distance to compute the MBHPA's propagation tree
	resp_department (string)	information on responsible departments
	proc_document (string)	document describing the validation procedure

node class	attribute	description
failure	isTopEvent (boolean)	marker if the failure is considered as top event
	isBasicEvent (boolean)	marker if the failure is considered as basic event
	distance (int)	distance of the failure in the fault tree
	occurrence (int)	occurrence of the failure in minimal cut sets
	severity (int)	combined severity of the failure
	origin_id (string)	id of the origin of the fault
faultcollection (extends failure)	none	
flow	flow_type (flowtype)	type of flow (predefined types e.g. energy, information, etc.)
	is_harmful (boolean)	marker if flow has potential of harm
FMEArow	componentName (string)	name of the component causing the failure mode
	componentID (string)	id of the component causing the failure mode
	SupportColumnParameter (string)	auxiliary information (parameters of the component)
	SupportColumnOutflow (string)	auxiliary information (output flows of the component)
	SupportColumnInflow (string)	auxiliary information (input flows of the component)
	SupportColumnFunction (string)	auxiliary information (functions of the component)
	FailureEffectGlobal (string)	top events affected by the considered failure mode
	FailureEffectLocal (string)	failures directly affected by the considered failure mode
	FailureModeName (string)	name of the considered failure mode
	FailureModeID (string)	id of the considered failure mode
	FailureModeOrigin (string)	possible origins of the considered failure mode
	FailureModeAvoidance (string)	avoidance measures/safety functions preventing the failure mode
	TracedTopFault (string)	traces from the considered failure mode to the affected top events
	severity (int)	severity of the considered failure mode
	occurrence (int)	occurrence of the considered failure mode
	detection (int)	detection of the considered failure mode
hazard	weight (double)	hazard weight
minimalCutSet	none	
modelingErrorNode	property_error_type (string)	type of the identified modeling error
	concerned_nodes (string)	nodes involved in the modeling error
	detailed_error_description (string)	detailed description of the identified modeling error
product_function	safetyFunction (boolean)	marker if the function is a safety function
	is_harmful (boolean)	marker if the function is potentially harmful
requirement	req_ref_number (string)	reference number of the requirement
	req_source (string)	source document of the requirement
	req_document (string)	specification document of the requirement
	weight (double)	weight of the requirement
	req_target (target)	target of the requirement (required in evaluation case III)
	req_status (status)	status of the requirement (required in evaluation case III)
	req_productfamily (productFamily)	addressed product family of the requirement (required in evaluation case III)
	req_implemented (boolean)	marker if the requirement is already implemented (required in evaluation case III)
safety_requirement (extends requirement)	none	
safetyMeasure (extends component)	effectiveness (string)	effectiveness of the safety measure (used in the model-based hazard analysis)
	reliability (double)	reliability of the safety measure (used in the model-based hazard analysis)
useCase	isMisuse (boolean)	marker if the use case is a misuse case (used in the model-based hazard analysis)
validationProcedure	proc_source (string)	source document of the validation procedure
	proc_document (string)	document describing the validation procedure

The graph-based model moreover primarily consists of the following classes of edges and attributes:

edge class	connects	description	attributes
addresses	safety_requirement - hazard	edge to establish a connection from requirements to their considered hazards	
all edges	all nodes		name (string)
areIncontact	component - component	edge to model geometrical component contacts	
bears	flow - hazard	edge to model the hazardous effects of flows	
causes	component - failure	edge to map components and their failures	
causes	useCase - failure	edge to connect misuse cases to their corresponding failure	
contains	component - component	edge to model hierarchical component decomposition	
contributes	product_function - product_function	edge to model hierarchical function decomposition	
effects	product_function - flow	edge to model the effect of functions on flows	
flowConnection	component - component	edge to create the flow-based component structure (consolidates input and output edges	type (flowtype)
fulfills	component - product_function	edge to model how components realize functions	
has_output	component - flow	edge to model flow relations between components	
influences	flow - product function	edge to model the effect of flows on functions	
is_in	failure - minimalCutSet	edge to allocate failures to minimal cut sets	
is_input	flow - component	edge to model flow relations between components	
mayCause	failure - failure	edge to establish a fault tree	
mightPropagate	component - component	edge to model identified propagations (MBHPA)	type (string)
			origin (string)
			weight (double)
			occurrence (int)
ModelingErrorEdge	ModelingErrorNode - all nodes	edge to allocate the identified modeling error in the graph	
prevents	product_function - hazard	edge to map safety functions with their addressed hazards	
refines	requirement - requirement	edge to model hierarchical requirement decomposition	
represents	failure - hazard	edge to translate hazards to top event failures	
satisfies	component - requirements	edge setting up the link between components and requirements	
verifies	validationProcedure - requirement	edge to map requirements with their corresponding validation procedure	

9.4 Descriptions of ESMK Methods

The ESMK introduced in Section 4.3 provides a set of twelve support methods and tools. Within those, eight methods represent the core contribution of the ESMK. In the following for these core methods, a description according to the scheme provided by Lindemann (2009, pp. 61–62) is given:

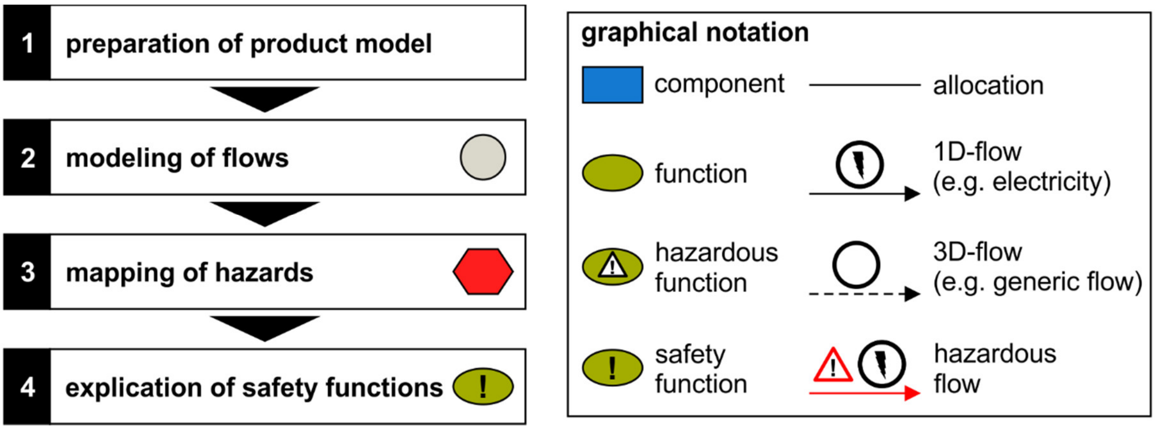
Method to Explicate Safety Functions

ESMK phase: II Feature Analysis

supported task: explicate safety functions

purpose:	**situation:**	**effect:**
• make implicit safety knowledge explicit • explicate and model safety in early stages of design • integrate safety aspects in models	• existing gap between design and safety • make safety knowledge accessible for multiple persons • required product model integrating safety and design aspects • large amount of implicit safety knowledge	• modeled and defined safety functions • "safe" functional structure on all decomposition levels • extended understanding of safety functions

approach:



1 preparation of product model

2 modeling of flows

3 mapping of hazards

4 explication of safety functions

graphical notation

🟦 component

allocation

function

1D-flow (e.g. electricity)

hazardous function

3D-flow (e.g. generic flow)

safety function

hazardous flow

tools/methods:

- existing norms and standards to identify hazards e.g. checklists, Preliminary Hazard Analysis, etc.
- product architecture models

remarks:

- flows represent the origin of hazards
- flows are modeled as 1D- or 3D flows
- it is suggested to model user contact as an abstract flow
- to model large systems tool support is recommended
- safety functions can be active or passive

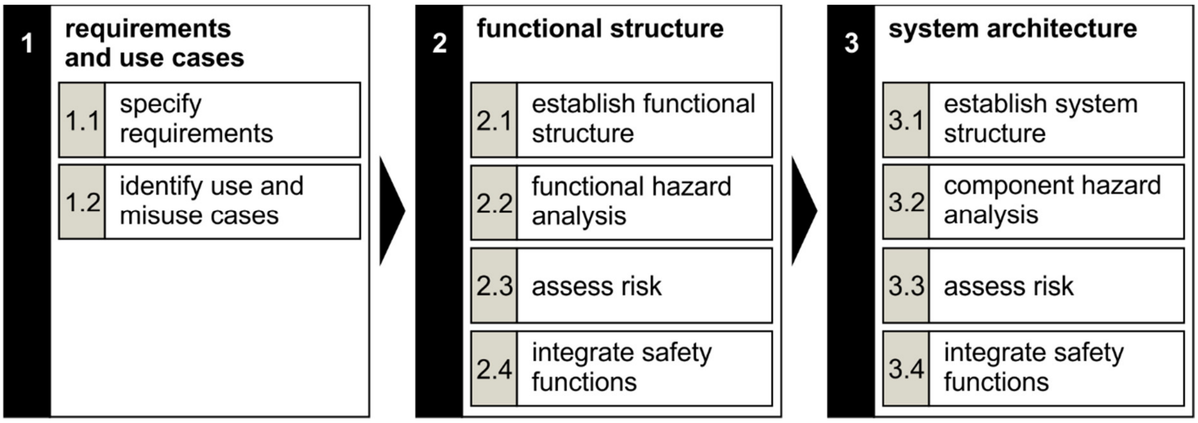
Model-based Hazard Analysis

ESMK phase: II Feature Analysis

supported task: identify hazards and failures

purpose:	situation:	effect:
• identify possible failures and hazards • consider misuse cases and resulting hazards • support a hazard-oriented system development	• required detailed model-based hazard analysis • important role of user interaction • continuous integration of hazard analysis in the design process is required	• knowledge of occurring hazards • modeled hazards and countermeasures • modeled misuse cases and resulting hazards • continuous model-based hazard analysis

approach:


1
requirements and use cases
1.1 specify requirements
1.2 identify use and misuse cases
2
functional structure
2.1 establish functional structure
2.2 functional hazard analysis
2.3 assess risk
2.4 integrate safety functions
3
system architecture
3.1 establish system structure
3.2 component hazard analysis
3.3 assess risk
3.4 integrate safety functions

tools/methods:

- “hazard analysis” SysML-profile
- SysML modeling support
- existing product models

remarks:

- independent of any particular hazard analysis method
- deductive and inductive techniques are applicable
- the SysML-profile can be expanded and adapted to specific tasks of safety analysis
- level of abstraction is variable through functional decomposition

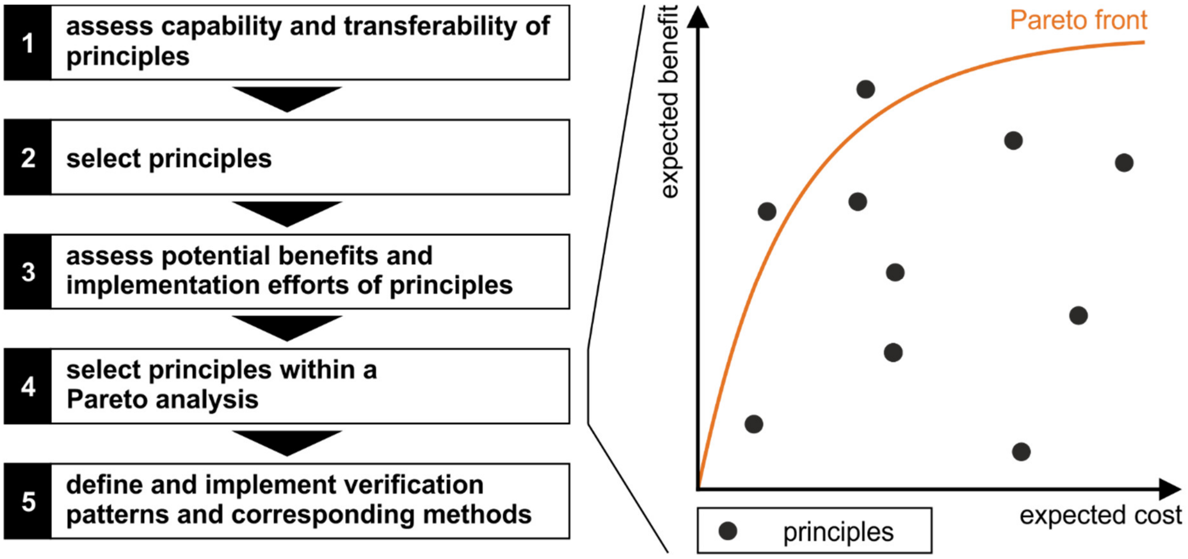
Pattern-based Model Verification

ESMK phase: II Feature Analysis

supported task: verify the product model

purpose:	**situation:**	**effect:**
• identify and eliminate modeling errors • reduce the impact of uncertainties on the model quality	• for large and complex models affected by uncertainty • model complexity too large for manual analysis • models of different sources are integrated • ensure conformity of model changes	• automated model analysis based on verification patterns • identification of invalid model patterns

approach:



1 assess capability and transferability of principles

2 select principles

3 assess potential benefits and implementation efforts of principles

4 select principles within a Pareto analysis

5 define and implement verification patterns and corresponding methods

tools/methods:

- product architecture model
- principle/pattern library
- software support for graph handling

remarks:

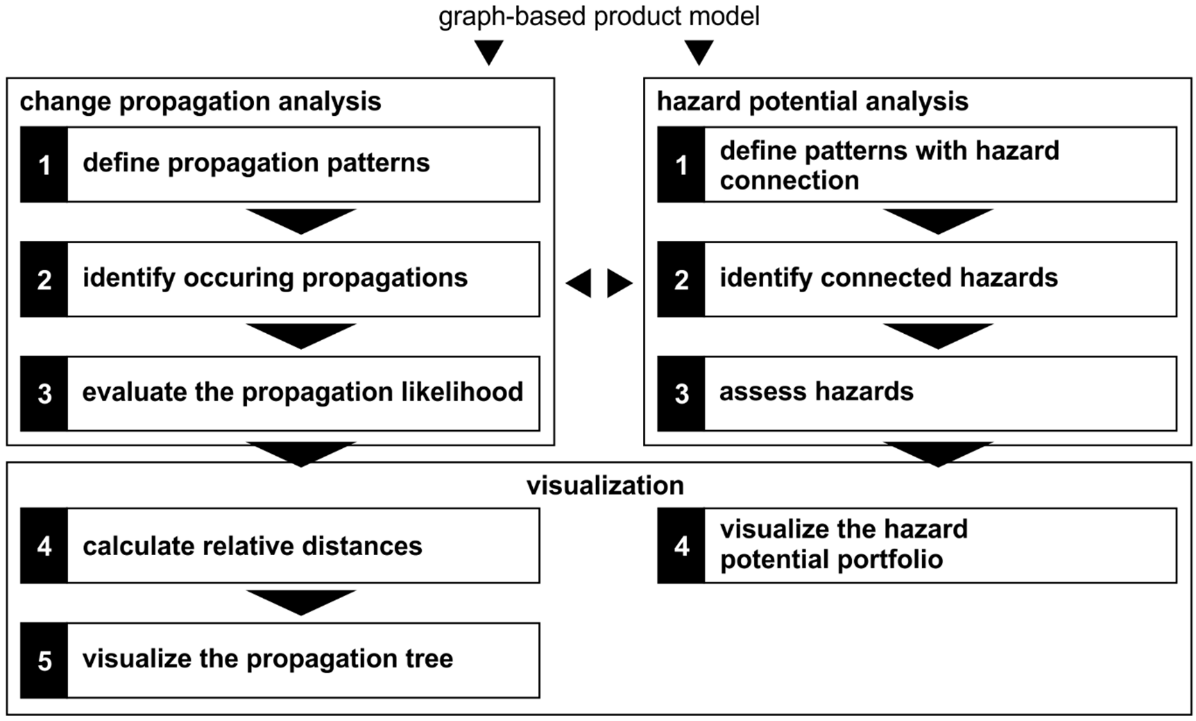
- applicability of patterns strongly depends on the specific model
- some patterns can be used for automatic repair of model errors as well

Model-based Hazard and Propagation Assessment (MBHPA)

ESMK phase: III Propagation Analysis
supported task: identify propagation effects

purpose:	**situation:**	**effect:**
• identify potential propagation effects of changes • establish link between change propagations and their hazard impacts • evaluate the effects of changes	• consider propagations from a worst-case perspective • limited expert knowledge on potential change propagations	• identified propagations effects • modeled propagation effects form a worst-case perspective • knowledge of the hazard potential of components

approach:


graph-based product model
change propagation analysis
1 define propagation patterns
2 identify occuring propagations
3 evaluate the propagation likelihood
hazard potential analysis
1 define patterns with hazard connection
2 identify connected hazards
3 assess hazards
visualization
4 calculate relative distances
5 visualize the propagation tree
4 visualize the hazard potential portfolio

tools/methods:

- product architecture model
- patterns of potential propagations and their likelihood
- weights of hazards
- software support for graph handling

remarks:

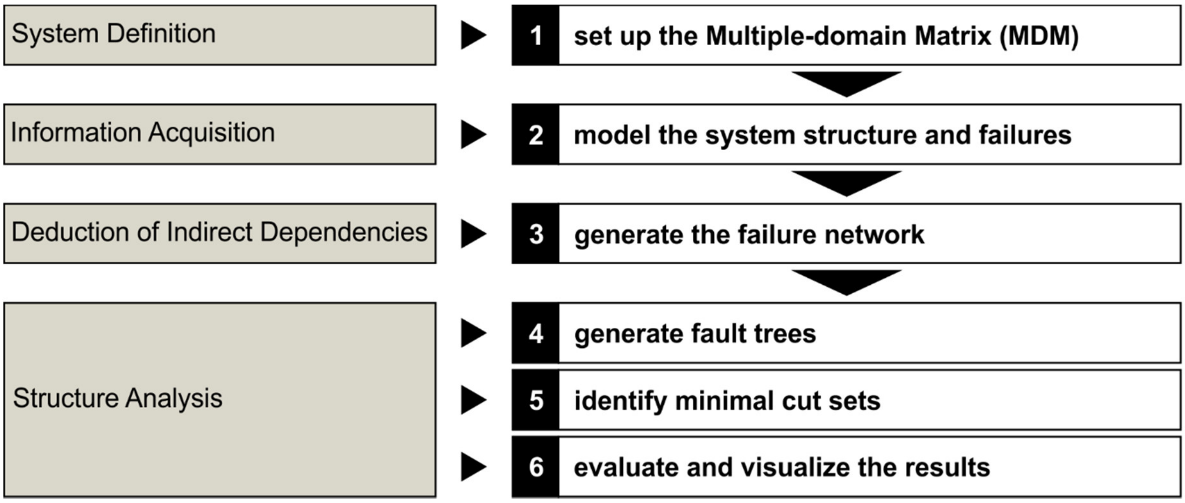
- analysis results depend on the product model
- propagation patterns can be defined on different abstraction levels
- propagation patterns and likelihoods depend on actual product and situation

Matrix-based Multi-hierarchy Fault Tree Generation and Evaluation (MHFTA)

ESMK phase: III Propagation Analysis
supported task: conduct preliminary FTA & FMEA

purpose:	**situation:**	**effect:**
• conduct preliminary FTA from a worst-case perspective • reduce manual efforts for FTAs	• preliminary FTA is required for a large and complex system • comparison of failure propagations in different architectures • evaluate the safety impact of occurring failures	• modeled fault trees • qualitative evaluation of fault trees • identified critical failures

approach:


System Definition
1 set up the Multiple-domain Matrix (MDM)
Information Acquisition
2 model the system structure and failures
Deduction of Indirect Dependencies
3 generate the failure network
Structure Analysis
4 generate fault trees
5 identify minimal cut sets
6 evaluate and visualize the results

tools/methods:

- modeled product architectures (incl. hierarchy)
- modeled propagations
- matrix-calculation support
- Hauptmanns‘ algorithm (Hauptmanns et al., 2004)

remarks:

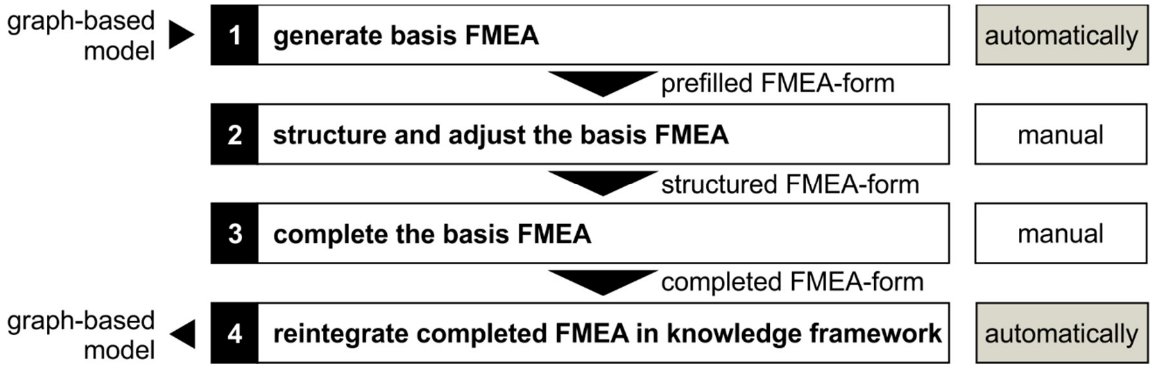
- too detailed models can reduce the quality of the results
- modeling redundancies remains manual
- different abstraction levels of modeled failures helps to adjust efforts

Model-based Preliminary FMEA

ESMK phase: III Propagation Analysis
supported task: conduct preliminary FTA & FMEA

purpose:	**situation:**	**effect:**
• prepare and prefill a FMEA-form • reduce manual efforts for FMEA	• manual FMEA preparations have to be reduced • worst-case perspective for the FMEA is required • completeness of the FMEA needs to be improved	• consolidated and structured information on occurring failure modes • overview of potential failure mode effects • support completeness of the FMEA

approach:

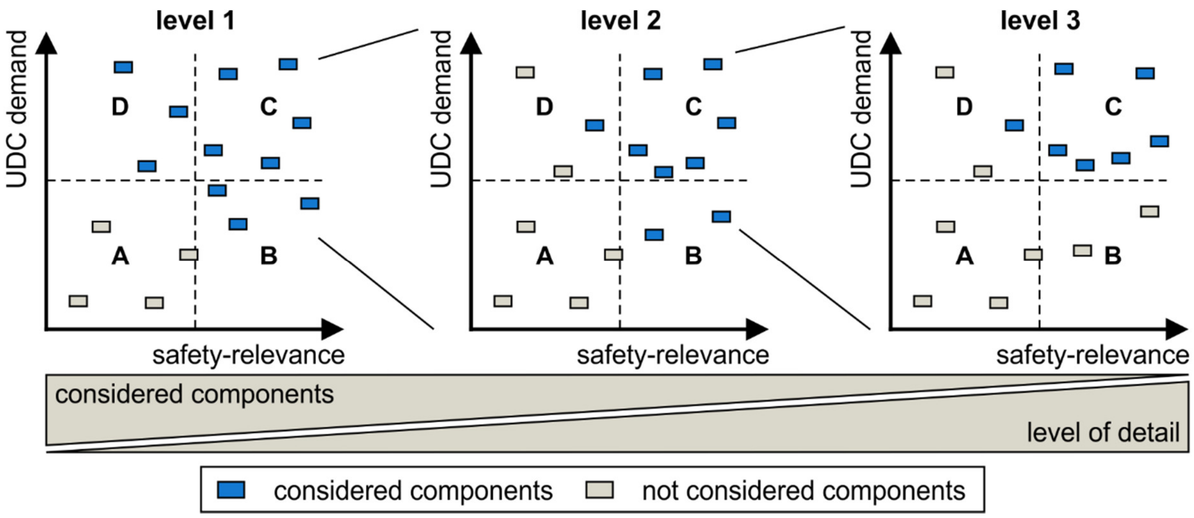


tools/methods:

- product architecture model
- modeled propagations and fault trees
- software support for graph handling

remarks:

- the preliminary FMEA can be conducted on different system decomposition levels
- the completion of the FEMA remains a manual task
- the reintegration of the manual adaptions is essential for efficiency and reuse

<table>
<tr><th colspan="3">UDC Safety-relevance Portfolio</th></tr>
<tr><td colspan="3"><b>ESMK phase:</b> III Propagation Analysis
<b>supported task:</b> assess elements</td></tr>
<tr><td><b>purpose:</b>
• evaluate the safety-relevance of components
• visualize the trade-off between UDC demands and safety-relevance</td><td><b>situation:</b>
• identification of UDC options
• balancing UDC options and safety aspects
• evaluate the suitability of different system concepts</td><td><b>effect:</b>
• assessment of components representing their safety-relevance
• guidance to handle the trade-offs between safety and UDC</td></tr>
<tr><td colspan="3"><b>approach:</b>


level 1
level 2
level 3
UDC demand
safety-relevance
A
B
C
D
considered components
level of detail
considered components
not considered components

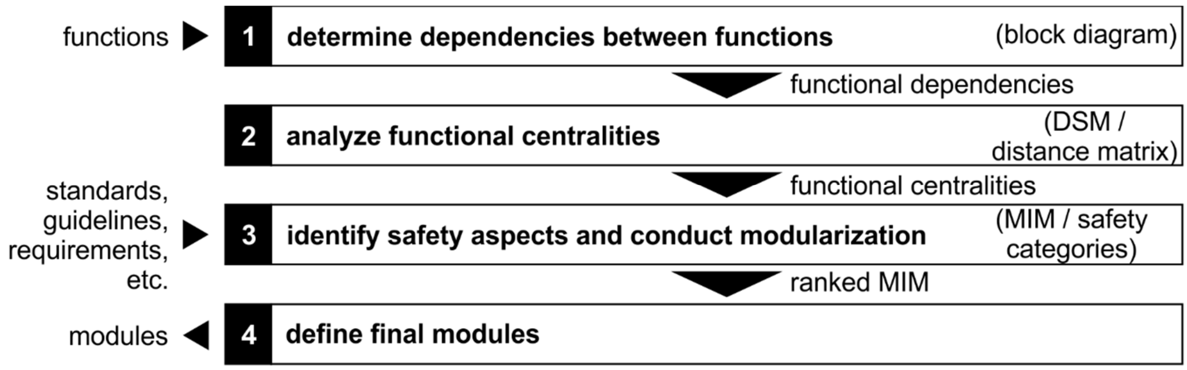
</td></tr>
<tr><td colspan="3"><b>tools/methods:</b>
• product architecture model
• modeled propagations and fault trees
• UDC demands</td></tr>
<tr><td colspan="3"><b>remarks:</b>
• assessment levels need to be adapted depending on specific product and situation
• iterative procedure helps to handle complexity</td></tr>
</table>

Safety-oriented Modular Function Deployment (sMFD)

ESMK phase: III Propagation Analysis
supported task: improve product architecture

purpose:	**situation:**	**effect:**
• improve product architecture from a safety perspective • achieve product architectures which reduce safety efforts	• improvement of existing products from safety perspective • safety efforts for modular product portfolios need to be reduced • establishment of flexible modules, which are decoupled from safety aspects	• safety-oriented module concept • clusters of elements with similar safety restrictions • modules decoupled from safety aspects

approach:


functions
1 determine dependencies between functions
(block diagram)
functional dependencies
2 analyze functional centralities
(DSM / distance matrix)
functional centralities
standards, guidelines, requirements, etc.
3 identify safety aspects and conduct modularization
(MIM / safety categories)
ranked MIM
modules
4 define final modules

tools/methods:

- product architecture model
- explicit safety knowledge (i.e. safety requirements)
- matrix calculation software support

Remarks:

- resulting modules need to be balanced with modules from other modularization drivers
- safety categories depend on specific situation and product
- modules with too much elements of high safety-relevance can lead to unmanageable complexity

9.5 The Hazard Analysis SysML-Profile

The following quick reference provides an overview of the stereotypes of the Hazard Analysis SysML-profile used in the model-based hazard analysis. It originates from the connected student project (Müller, 2015) and the prior publication (Müller et al., 2016) and introduces the stereotypes, explains their usage, and lists the connected relations and tagged values:

Hazard

description	existing hazards in the system model
meta-class	*SysML::Block*
relations	
↔*derivedHzd*	derivation association to one or more *Blocks* (subsystems, components, etc.) in the BDD
↔ *cause*	cause relation to a further *Hazard* in the BDD
→ *trigger*	is triggered by relation to a *Hazard Cause* in the BDD
← *cause*	causes relation to the *Hazard Effects* in the BDD
tagged values	
severity s	severity of the potential damage enumeration: *catastrophic, critical, minor, negligible*
probability p	probability of transition from hazard to mishap enumeration: *common, probable, occasionally, remote, improbable*
risk index RI	criticality of hazard derived from a risk matrix enumeration: *safety-critical, not safety-critical*

Hazard Cause

description	Potential cause of a *Hazard*
meta-class	*SysML::Block*
relations	
← *trigger*	triggering relation to a *Hazard* in the BDD

Hazard Effect

description	Potential effect of a *Hazard*
meta-class	*SysML::Block*
relations	
→ *cause*	is caused by relation to a *Hazard* in the BDD

Malfunction

description	failure of a function; used for execution failure and value failure
meta-class	*SysML::Action*
relations	
→ *cause*	is-caused-by relation to the failure cause like *Misuse* or other input parameters in the ACT
→ *derivedFct*	derivation association to the related *Action* in the ACT
↔ *cause*	cause relation to a further *Malfunction* in the ACT
←	relation to the end node in the ACT if the failure causes an abort
→ *prevent*	is prevented by relation to the associated *Safety Function*

Misuse

description	Not intended, improper and hence potentially hazardous use of the system
meta-class	*SysML::UseCase*
relations	
→ *derivedMisuse*	derivation association to the related *Use Case* in the UC relation to actor in UC
← *cause*	input parameter of a *Malfunction*
← *cause*	cause-relationship to a *Hazard* in the BDD

Safety Function

description	prevention or mitigation measure to avoid or reduce the effects of a *Malfunction*
meta-class	*SysML::Action*
relations	
← *prevent*	prevents relation to the associated *Malfunction*

Safety Measure

description	prevention or mitigation measure to avoid or reduce the effects on component level
meta-class	*SysML::Block*
relations	
← *prevent*	prevention relation to the corresponding *Hazard* in the BDD
tagged values	
efficiency e	efficiency of the *Safety Measure* enumeration: *prevention, mitigation*
costs c	costs to integrate the *Safety Measure* enumeration: *high, medium, low*
reliability r	reliability of the component, which implements the *Safety Measure* enumeration: *float*

Safety Requirement

description	requirements concerning the system safety; distinguished from general and functional requirements by unique identifier and textual description
meta-class	*SysML::Requirement*
relations	
↔ *deriveReqt*	derivation association of top-level *Requirements* to detailed lower-level *Requirements* in the REQ
→ *refine*	refinement association between *Requirement* and *Use Case* in the REQ
tagged values	
source	origin of the *Safety Requirement* including the reference to norms or standards

9.6 The 121 Principles for the Pattern-based Model Verification

The following table provides an overview of the 121 principles for the pattern-based model verification. It originates from the connected student project (Schürmann, 2016) and describes the exemplarily applicability of each pattern as well as its origin.

no.	principle	group	exemplary applicability	references
1	finite nature of the velocity of light	physics	incorporation of signaling delays	Oppen & Melchert (2005), Hahn (2007)
2	three dimensions of space	physics	necessity of three information to determine positions in space	Oppen & Melchert (2005), Hahn (2007)
3	differential dependency location - velocity-acceleration	physics	consistency of states	Oppen & Melchert (2005), Hahn (2007)
4	Newton's first law: bodies maintain their state (velocity), if no external force is applied	physics	consistency of force and velocities	Oppen & Melchert (2005), Hahn (2007)
5	law of gravitation: masses attract each other	physics	usable for planetary systems	Oppen & Melchert (2005), Hahn (2007)
6	law of conservation of energy	physics	consistency of flow transformations	Oppen & Melchert (2005), Hahn (2007)
7	no perpetuum mobile exists	physics	losses within energy transformations	Oppen & Melchert (2005), Hahn (2007)
8	conservation of momentum	physics	consistency of collisions	Oppen & Melchert (2005), Hahn (2007)
9	the mass point of rigid bodies remains fixed	physics	consistency of mass inertias	Oppen & Melchert (2005), Hahn (2007)
10	gases can be compressed	physics	verify thermodynamic models	Oppen & Melchert (2005), Hahn (2007)
11	absolute zero is -273,16°C (0K)	physics	cooling of ideal gases	Oppen & Melchert (2005), Hahn (2007)
12	thermal expansion (with exceptions)	physics	warming leads to increased volume	Oppen & Melchert (2005), Hahn (2007)
13	3 aggregate conditions	physics	consistency of material flows	Oppen & Melchert (2005)
14	use of energy despite constant temperature at phase transition	physics	consistency of phase transitions	Oppen & Melchert (2005), Hahn (2007)
15	regelation of ice	physics	when ice is modeled	Oppen & Melchert (2005)

no.	principle	group	exemplary applicability	references
16	heat transfer occurs between bodies of different temperatures	physics	consistency of heat flows	Oppen & Melchert (2005)
17	first law of thermodynamics (similar to law of conservation of energy)	physics	consistency of flow transformations	Oppen & Melchert (2005), Hahn (2007)
18	second law of thermodynamics: the sum of entropies increases	physics	consistency of the direction of flow transformations	Oppen & Melchert (2005), Hahn (2007)
19	entropy cannot be destroyed	physics	consistency of the direction of flow transformations	Oppen & Melchert (2005), Hahn (2007)
20	Bernoulli's principle (conservation of energy in fluid dynamics)	physics	transformations and consistency of fluid flows	Oppen & Melchert (2005), Hahn (2007)
21	random movement of atoms	physics	for atomic models	Oppen & Melchert (2005)
22	viscosity of fluids	physics	inconsistency of fluid flows	Oppen & Melchert (2005), Hahn (2007)
23	Doppler effect	physics	for acoustical models	Oppen & Melchert (2005), Hahn (2007)
24	electrical fields	physics	direction of flow of electric charges, necessity of isolation	Oppen & Melchert (2005), Hahn (2007)
25	magnetic fields	physics	direction of magnetic flows	Oppen & Melchert (2005), Hahn (2007)
26	Lorentz force	physics	consistency of EMFs and forces	Oppen & Melchert (2005), Hahn (2007)
27	Coulomb's law	physics	consistency of EMFs and forces	Oppen & Melchert (2005), Hahn (2007)
28	induction results from changed magnetic fields	physics	consistency of electromagnetic transformations	Oppen & Melchert (2005), Hahn (2007)
29	polarization of conductors in electrical fields	physics	direction of magnetic flows	Oppen & Melchert (2005)
30	electromagnetic waves are independent of the medium	physics	consistency of electromagnetic waves	Oppen & Melchert (2005), Hahn (2007)
31	electromagnetic waves spread with the speed of light	physics	limited or no delays for flows	Oppen & Melchert (2005), Hahn (2007)
32	absorption of electromagnetic waves	physics	consistency of shielding in models	Oppen & Melchert (2005), Hahn (2007)
33	refraction of light	physics	when prisms are modeled	Oppen & Melchert (2005), Hahn (2007)
34	diffraction of light	physics	consistency of optical models	Oppen & Melchert (2005), Hahn (2007)
35	reflection	physics	consistency of optical models	Oppen & Melchert (2005), Hahn (2007)
36	coherence of waves	physics	for optical measurement models	Oppen & Melchert (2005), Hahn (2007)
37	photoelectric effect	physics	when optical active materials are modeled	Oppen & Melchert (2005), Hahn (2007)
38	wave-particle duality	physics	when systems are modeled on particle level	Oppen & Melchert (2005), Hahn (2007)
39	element-specific color spectrums	physics	for models on atomic level	Oppen & Melchert (2005)
40	Bohr model (1st postulate: electron shells)	physics	for models on atomic level	Oppen & Melchert (2005)
41	Bohr model (2nd postulate: electron transition)	physics	for models on atomic level	Oppen & Melchert (2005)

no.	principle	group	exemplary applicability	references
42	Bohr model (3rd postulate: spin and frequency)	physics	for models on atomic level	Oppen & Melchert (2005)
43	tunnel effect	physics	for models on atomic level	Oppen & Melchert (2005)
44	transformation chains	physics	for models considering nuclear decay	Oppen & Melchert (2005)
45	ionizing radiation	physics	for models considering nuclear radiation	Oppen & Melchert (2005)
46	intermolecular forces	physics	for models on atomic level	Oppen & Melchert (2005)
47	semiconductors	physics	for models considering integrated circuits, consistency of transformations	Oppen & Melchert (2005)
48	mean	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
49	median	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
50	mode value	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
51	midrange	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
52	expected value	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
53	minimum	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
54	maximum	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
55	range	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
56	variance	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
57	standard deviation	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
58	coefficient of variation	statistics	identification of conspicuous elements	Tiemann (2013)
59	z-transform	statistics	identification of conspicuous elements	Tiemann (2013)
60	two dimensional contingency table	statistics	identification of conspicuous elements	Fahrmeir et al. (2011)
61	box plots	statistics	identification of conspicuous elements	Tiemann (2013)
62	trend adjustments	statistics	prevent misinterpretations	Tiemann (2013)
63	correlation	statistics	identification of non-conformant elements	Tiemann (2013), Kreyszig (1988)
64	contingencies	statistics	identification of non-conformant elements	Tiemann (2013)
65	regressions	statistics	identification of non-conformant elements	Tiemann (2013), Kreyszig (1988)
66	chi-squared test	statistics	identification of non-conformant elements	Tiemann (2013), Kreyszig (1988)
67	mediation	statistics	identification of non-conformant elements	Durst (1991)
68	moderation	statistics	identification of non-conformant elements	Durst (1991)
69	normal distribution	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)

no.	principle	group	exemplary applicability	references
70	t-distribution	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
71	chi-squared distribution	statistics	identification of conspicuous elements	Kreyszig (1988)
72	Bernoulli distribution	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
73	binominal distributions	statistics	identification of conspicuous elements	Tiemann (2013), Kreyszig (1988)
74	sign test	statistics	identification of non-conformant elements	Kreyszig (1988)
75	t-test	statistics	identification of non-conformant elements	Tiemann (2013)
76	test for randomness	statistics	identification of non-conformant elements	Kreyszig (1988)
77	ranking test	statistics	identification of non-conformant elements	Kreyszig (1988)
78	minimax theorem	statistics (game theory)	identification of non-conformant elements	Kreyszig (1988)
79	Bayes' theorem	statistics (game theory)	identification of non-conformant elements	Kreyszig (1988)
80	exhaustive search	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
81	trial-and-error	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
82	hill-climbing algorithm	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
83	Lin Kerningham algorithm	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
84	Brent's method	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
85	simplex algorithm	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
86	greedy algorithm	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
87	A* algorithm	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
88	simulated annealing	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
89	Tabu search	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
90	evolutionary algorithms	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
91	neural networks	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
92	fuzzy logics	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
93	co-evolutionary approach	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
94	multicriteria decision-making	heuristics	identification of non-conformant elements	Michalewicz & Fogel (2004)
95	algebras of propositions	logics	identification of logical chains and violations in the model	Barnes & Mack (1975)
96	truth in the propositional calculus	logics	consistency of implementations and states	Barnes & Mack (1975), Barwise & Keisler (1977)

no.	principle	group	exemplary applicability	references
97	soundness theorem	logics	test on validity of model elements	Barnes & Mack (1975), Barwise & Keisler (1977)
98	consistency theorem	logics	basic rule for models	Barnes & Mack (1975), Barwise & Keisler (1977)
99	truth functions	logics	analyze reuse of elements and identify inconsistencies in sequences	Barnes & Mack (1975)
100	decidability	logics	identify endless loops in the model	Barnes & Mack (1975)
101	predicate calculus	logics	consistency of sub models	Barnes & Mack (1975)
102	identity	logics	identify duplicates	Barnes & Mack (1975), Barwise & Keisler (1977)
103	completeness	logics	consistency of sub models	Barnes & Mack (1975), Barwise & Keisler (1977)
104	axiom of extension	logics	comparison of patterns, identification of duplicates	Barnes & Mack (1975)
105	axiom schema of subset	logics	identification of non-conformant elements	Barnes & Mack (1975)
106	axiom of pairing	logics	limited usability, but useful for models with uniqueness requirements	Barnes & Mack (1975)
107	axiom of union	logics	identification of non-conformant elements in the hierarchical decomposition	Barnes & Mack (1975)
108	axiom of power set	logics	identification of non-conformant elements in the hierarchical decomposition	Barnes & Mack (1975)
109	axiom of infinity	logics	might be useful in mathematical models	Barnes & Mack (1975)
110	axiom of choice	logics	might be useful in mathematical models	Barnes & Mack (1975)
111	axiom schema of replacement	logics	useful in specific models	Barnes & Mack (1975)
112	axiom schema of restriction	logics	basic rule for models	Barnes & Mack (1975)
113	isolated nodes: no isolated nodes should exist	model-specific rules	identify not connected nodes	definition of the ESMK knowledge framework
114	conformity of edges: no violation of predefined interfaces	model-specific rules	identify edges violating the meta-model	definition of the ESMK knowledge framework
115	catch hazards	model-specific rules	identify missing safety functions	definition of the ESMK knowledge framework
116	hierarchical component decomposition	model-specific rules	identify missing composition edges	definition of the ESMK knowledge framework
117	uniqueness of assembly groups	model-specific rules	identify duplicates in the hierarchical decomposition	definition of the ESMK knowledge framework

no.	principle	group	exemplary applicability	references
118	requirements trace	model-specific rules	identify missing edges in the requirements trace	definition of the ESMK knowledge framework
119	hierarchical function decomposition	model-specific rules	identify missing composition edges	definition of the ESMK knowledge framework
120	hierarchical requirement decomposition	model-specific rules	identify missing composition edges	definition of the ESMK knowledge framework
121	inheritance of contacts and flows	model-specific rules	identify missing connections, identify non-conformant decompositions	definition of the ESMK knowledge framework

9.7 Details of the Evaluation

This section provides details of the evaluation of the ESMK. This includes the structured questionnaires used to evaluate the core contributions of the ESMK.

9.7.1 Evaluation Questionnaire of the MBHPA

The following table provides an overview of the questionnaire used to evaluate the MBHPA and the resulting ratings and comments.

Questionnaire to evaluate the MBHPA, filled 2016/02/03	not agree	partially not agree	neutral	partially agree	agree
I) efficiency					
The MBHPA can be applied in an appropriate time				*x*	
The MBHPA reduces the time needed to conduct the propagation assessment of User-driven Customizations compared to the current practice.			*x*		
The MBHPA reduces the manual efforts needed to conduct the propagation analysis of User-driven Customizations compared to the current practice.	*x*				
The MBHPA reduces the experience required to conduct the propagation analysis of User-driven Customizations compared to the current practice.				*x*	
The savings in terms of time and efforts are greater than the one-time implementation efforts to set up the underlying model.	*x*				
The estimated time savings for each individual product are: *additional 20-30%*					
Further comments: *problems may occur, when engineers blindly trust the results*					
II) safety awareness and preparation					
The MBHPA increases the awareness for the technical effects of User-driven Customizations.				*x*	
The MBHPA increases the awareness for the safety impact of User-driven Customizations.			*x*		
The MBHPA facilitates the safety-oriented preparation of products for UDC.				*x*	
The MBHPA facilitates the evaluation of safety aspects in the case of User-driven Customizations.		*x*			
Further comments: *The MBHPA especially might also be useful in the internal change management to increase awareness for safety aspects there as well.*					

Questionnaire to evaluate the MBHPA, filled 2016/02/03	not agree	partially not agree	neutral	partially agree	agree
III) propagation analysis / quality					
The MBHPA allows identifying potential effects of User-driven Customizations at an early stage.				*x*	
The MBHPA allows evaluating potential effects of User-driven Customizations at an early stage.		*x*			
The MBHPA identifies all potential hazards (assuming a sufficient model quality)		*x*			
The MBHPA identifies not enough potential hazards (assuming a sufficient model quality)			*x*		
The MBHPA identifies too many potential hazards (assuming a sufficient model quality)				*x*	
The MBHPA improves the traceability of the evaluation of potential effects of User-driven Customizations.					*x*
Further comments: *The MBHPA might not be able to identify all potential hazards, as the model might be too abstract.*					
IV) documentation and applicability					
The MBHPA improves the transparency of the analysis and evaluation of potential effects of User-driven Customizations.				*x*	
The MBHPA facilitates the documentation of propagation analyses.				*x*	
The MBHPA reduces the complexity data to a manually processable level.		*x*			
The MBHPA visualizes the potential effects of User-driven Customizations in a way, which allows a fast comprehension.				*x*	
The MBHPA visualizes the hazard potentials of User-driven Customizations in a way, which allows a fast comprehension.			*x*		
V) additional remarks					
Advantages of the MBHPA are especially: *good overview of dependencies between components and hazards*					
Disadvantages of the MBHPA are especially: *limited value, if model is too abstract and large efforts to create a detailed model*					

9.7.2 Evaluation Questionnaire of the MHFTA and model-based FMEA

The following table provides an overview of the questionnaire used to evaluate the MHFTA and the resulting ratings and comments.

Questionnaire to evaluate the MHFTA, filled 2016/05/10	not agree	partially not agree	neutral	partially agree	agree
I) efficiency					
The MHFTA reduces the time needed to conduct the failure analysis of User-driven Customizations compared to the current practice.	*x*				
The MHFTA reduces the manual efforts needed to conduct the failure analysis of User-driven Customizations compared to the current practice.	*x*				
The MHFTA reduces the experience required to conduct the failure analysis of User-driven Customizations compared to the current practice.				*x*	
The MHFTA facilitates the reuse and the handling of minor changes			*x*		
The MHFTA provides a good basis for a faster manual failure analysis	*x*				

Questionnaire to evaluate the MHFTA, filled 2016/05/10	not agree	partially not agree	neutral	partially agree	agree
Further comments: *The MHFTA provides valuable support in the design phase and for designers. However, for the final analysis experience and manual analysis are irreplaceable. Especially exceptional cases and removed branches of the tree have to be reconsidered.*					
II) failure analysis / quality					
The MHFTA allows identifying potential failure causes at an early stage without comprehensive analyses.				*x*	*(x)*
The MHFTA identifies all potential failure causes (assuming a sufficient model quality)	*x*				
The MHFTA identifies not enough potential failure causes (assuming a sufficient model quality)	*x*				
The MHFTA identifies too many potential failure causes (assuming a sufficient model quality)					*x*
Further comments: *Especially for designers, an improved identification of failure causes is expected. However, there is the danger of seeing the wood for the trees.*					

The following table provides an overview of the questionnaire used to evaluate the model-based FMEA and the resulting ratings and comments.

Questionnaire to evaluate the model-based FMEA, filled 2016/05/10	not agree	partially not agree	neutral	partially agree	agree
I) efficiency					
The model-based FMEA reduces the time needed to conduct the failure analysis of User-driven Customizations compared to the current practice.	*x*				
The model-based FMEA reduces the manual efforts needed to conduct the failure analysis of User-driven Customizations compared to the current practice.				*x*	
The model-based FMEA reduces the experience required to conduct the failure analysis of User-driven Customizations compared to the current practice.				*x*	
The model-based FMEA facilitates the reuse and the handling of minor changes				*x*	
The model-based FMEA provides a good basis for a faster manual failure analysis	*x*				
Further comments: *Manual work in total might not be reduced due to the one-time implementation efforts. However, the manual work to create the FMEA will be reduced. At the current stage, manual analyses are mandatory and cannot be replaced.*					
II) failure analysis / quality					
The model-based FMEA allows identifying potential failure causes at an early stage without comprehensive analyses.				*x*	
The model-based FMEA identifies all potential failure causes (assuming a sufficient model quality)	*x*				
The model-based FMEA identifies not enough potential failure causes (assuming a sufficient model quality)	*x*				
The model-based FMEA identifies too many potential failure causes (assuming a sufficient model quality)					*x*
Further comments: *Especially for designers, an improved identification of failure causes is expected. Value is expected, when safety functions are directly assigned to the components in the CAD tool.*					

10. List of Dissertations

Lehrstuhl für Produktentwicklung
Technische Universität München, Boltzmannstraße 15, 85748 Garching

Dissertations under supervision of:

- Prof. Dr.-Ing. W. Rodenacker,
- Prof. Dr.-Ing. K. Ehrlenspiel, and
- Prof. Dr.-Ing. U. Lindemann

D1 COLLIN, H.:
Entwicklung eines Einwalzenkalanders nach einer systematischen Konstruktionsmethode. München: TU, Diss. 1969.

D2 OTT, J.:
Untersuchungen und Vorrichtungen zum Offen-End-Spinnen.
München: TU, Diss. 1971.

D3 STEINWACHS, H.:
Informationsgewinnung an bandförmigen Produkten für die Konstruktion der Produktmaschine.
München: TU, Diss. 1971.

D4 SCHMETTOW, D.:
Entwicklung eines Rehabilitationsgerätes für Schwerstkörperbehinderte.
München: TU, Diss. 1972.

D5 LUBITZSCH, W.:
Die Entwicklung eines Maschinensystems zur Verarbeitung von chemischen Endlosfasern.
München: TU, Diss. 1974.

D6 SCHEITENBERGER, H.:
Entwurf und Optimierung eines Getriebesystems für einen Rotationsquerschneider mit allgemeingültigen Methoden.
München: TU, Diss. 1974.

D7 BAUMGARTH, R.:
Die Vereinfachung von Geräten zur Konstanthaltung physikalischer Größen.
München: TU, Diss. 1976.

D8 MAUDERER, E.:
Beitrag zum konstruktionsmethodischen Vorgehen durchgeführt am Beispiel eines Hochleistungsschalter-Antriebs.
München: TU, Diss. 1976.

D9 SCHÄFER, J.:
Die Anwendung des methodischen Konstruierens auf verfahrenstechnische Aufgabenstellungen.
München: TU, Diss. 1977.

D10 WEBER, J.:
Extruder mit Feststoffpumpe – Ein Beitrag zum Methodischen Konstruieren.
München: TU, Diss. 1978.

D11 HEISIG, R.:
Längencodierer mit Hilfsbewegung.
München: TU, Diss. 1979.

D12 KIEWERT, A.:
Systematische Erarbeitung von Hilfsmitteln zum kostenarmen Konstruieren.
München: TU, Diss. 1979.

D13 LINDEMANN, U.:
Systemtechnische Betrachtung des Konstruktionsprozesses unter besonderer Berücksichtigung der Herstellkostenbeeinflussung beim Festlegen der Gestalt.
Düsseldorf: VDI-Verlag 1980. (Fortschritt-Berichte der VDI-Zeitschriften Reihe 1, Nr. 60).
Zugl. München: TU, Diss. 1980.

D14 NJOYA, G.:
Untersuchungen zur Kinematik im Wälzlager bei synchron umlaufenden Innen- und Außenringen.
Hannover: Universität, Diss. 1980.

D15 HENKEL, G.:
Theoretische und experimentelle Untersuchungen ebener konzentrisch gewellter Kreisringmembranen.
Hannover: Universität, Diss. 1980.

D16 BALKEN, J.:
Systematische Entwicklung von Gleichlaufgelenken.
München: TU, Diss. 1981.

D17 PETRA, H.:
Systematik, Erweiterung und Einschränkung von Lastausgleichslösungen für Standgetriebe mit zwei Leistungswegen – Ein Beitrag zum methodischen Konstruieren.
München: TU, Diss. 1981.

D18 BAUMANN, G.:
Ein Kosteninformationssystem für die Gestaltungsphase im Betriebsmittelbau.
München: TU, Diss. 1982.

D19 FISCHER, D.:
Kostenanalyse von Stirnzahnrädern. Erarbeitung und Vergleich von Hilfsmitteln zur Kostenfrüherkennung.
München: TU, Diss. 1983.

D20 AUGUSTIN, W.:
Sicherheitstechnik und Konstruktionsmethodiken – Sicherheitsgerechtes Konstruieren.
Dortmund: Bundesanstalt für Arbeitsschutz 1985. Zugl. München: TU, Diss. 1984.

D21 RUTZ, A.:
Konstruieren als gedanklicher Prozess.
München: TU, Diss. 1985.

D22 SAUERMANN, H. J.:
Eine Produktkostenplanung für Unternehmen des Maschinenbaues.
München: TU, Diss. 1986.

D23 HAFNER, J.:
Entscheidungshilfen für das kostengünstige Konstruieren von Schweiß- und Gussgehäusen.
München: TU, Diss. 1987.

D24 JOHN, T.:
Systematische Entwicklung von homokinetischen Wellenkupplungen.
München: TU, Diss. 1987.

D25 FIGEL, K.:
Optimieren beim Konstruieren.
München: Hanser 1988. Zugl. München: TU, Diss. 1988 u. d. T.: Figel, K.: Integration automatisierter Optimierungsverfahren in den rechnerunterstützten Konstruktionsprozess.

Reihe Konstruktionstechnik München

D26 TROPSCHUH, P. F.:
Rechnerunterstützung für das Projektieren mit Hilfe eines wissensbasierten Systems.
München: Hanser 1989. (Konstruktionstechnik München, Band 1). Zugl. München: TU, Diss. 1988 u. d. T.: Tropschuh, P. F.: Rechnerunterstützung für das Projektieren am Beispiel Schiffsgetriebe.

D27 PICKEL, H.:
Kostenmodelle als Hilfsmittel zum Kostengünstigen Konstruieren.
München: Hanser 1989. (Konstruktionstechnik München, Band 2). Zugl. München: TU, Diss. 1988.

D28 KITTSTEINER, H.-J.:
Die Auswahl und Gestaltung von kostengünstigen Welle-Nabe-Verbindungen.
München: Hanser 1990. (Konstruktionstechnik München, Band 3). Zugl. München: TU, Diss. 1989.

D29 HILLEBRAND, A.:
Ein Kosteninformationssystem für die Neukonstruktion mit der Möglichkeit zum Anschluss an ein CAD-System.
München: Hanser 1991. (Konstruktionstechnik München, Band 4). Zugl. München: TU, Diss. 1990.

D30 DYLLA, N.:
Denk- und Handlungsabläufe beim Konstruieren.
München: Hanser 1991. (Konstruktionstechnik München, Band 5). Zugl. München: TU, Diss. 1990.

D31 MÜLLER, R.
Datenbankgestützte Teileverwaltung und Wiederholteilsuche.
München: Hanser 1991. (Konstruktionstechnik München, Band 6). Zugl. München: TU, Diss. 1990.

D32 NEESE, J.:
Methodik einer wissensbasierten Schadenanalyse am Beispiel Wälzlagerungen.
München: Hanser 1991. (Konstruktionstechnik München, Band 7). Zugl. München: TU, Diss. 1991.

D33 SCHAAL, S.:
Integrierte Wissensverarbeitung mit CAD – Am Beispiel der konstruktionsbegleitenden Kalkulation.
München: Hanser 1992. (Konstruktionstechnik München, Band 8). Zugl. München: TU, Diss. 1991.

D34 BRAUNSPERGER, M.:
Qualitätssicherung im Entwicklungsablauf – Konzept einer präventiven Qualitätssicherung für die Automobilindustrie.
München: Hanser 1993. (Konstruktionstechnik München, Band 9). Zugl. München: TU, Diss. 1992.

D35 FEICHTER, E.:
Systematischer Entwicklungsprozess am Beispiel von elastischen Radialversatzkupplungen.
München: Hanser 1994. (Konstruktionstechnik München, Band 10). Zugl. München: TU, Diss. 1992.

D36 WEINBRENNER, V.:
Produktlogik als Hilfsmittel zum Automatisieren von Varianten- und Anpassungskonstruktionen.
München: Hanser 1994. (Konstruktionstechnik München, Band 11). Zugl. München: TU, Diss. 1993.

D37 WACH, J. J.:
Problemspezifische Hilfsmittel für die Integrierte Produktentwicklung.
München: Hanser 1994. (Konstruktionstechnik München, Band 12). Zugl. München: TU, Diss. 1993.

D38 LENK, E.:
Zur Problematik der technischen Bewertung.
München: Hanser 1994. (Konstruktionstechnik München, Band 13). Zugl. München: TU, Diss. 1993.

D39 STUFFER, R.:
Planung und Steuerung der Integrierten Produktentwicklung.
München: Hanser 1994. (Konstruktionstechnik München, Band 14). Zugl. München: TU, Diss. 1993.

D40 SCHIEBELER, R.:
Kostengünstig Konstruieren mit einer rechnergestützten Konstruktionsberatung.
München: Hanser 1994. (Konstruktionstechnik München, Band 15). Zugl. München: TU, Diss. 1993.

D41 BRUCKNER, J.:
Kostengünstige Wärmebehandlung durch Entscheidungsunterstützung in Konstruktion und Härterei.
München: Hanser 1994. (Konstruktionstechnik München, Band 16). Zugl. München: TU, Diss. 1993.

D42 WELLNIAK, R.:
Das Produktmodell im rechnerintegrierten Konstruktionsarbeitsplatz.
München: Hanser 1994. (Konstruktionstechnik München, Band 17). Zugl. München: TU, Diss. 1994.

D43 SCHLÜTER, A.:
Gestaltung von Schnappverbindungen für montagegerechte Produkte.
München: Hanser 1994. (Konstruktionstechnik München, Band 18). Zugl. München: TU, Diss. 1994.

D44 WOLFRAM, M.:
Feature-basiertes Konstruieren und Kalkulieren.
München: Hanser 1994. (Konstruktionstechnik München, Band 19). Zugl. München: TU, Diss. 1994.

D45 STOLZ, P.:
Aufbau technischer Informationssysteme in Konstruktion und Entwicklung am Beispiel eines elektronischen Zeichnungsarchives.
München: Hanser 1994. (Konstruktionstechnik München, Band 20). Zugl. München: TU, Diss. 1994.

D46 STOLL, G.:
Montagegerechte Produkte mit feature-basiertem CAD.
München: Hanser 1994. (Konstruktionstechnik München, Band 21). Zugl. München: TU, Diss. 1994.

D47 STEINER, J. M.:
Rechnergestütztes Kostensenken im praktischen Einsatz.
Aachen: Shaker 1996. (Konstruktionstechnik München, Band 22). Zugl. München: TU, Diss. 1995.

D48 HUBER, T.:
Senken von Montagezeiten und -kosten im Getriebebau.
München: Hanser 1995. (Konstruktionstechnik München, Band 23). Zugl. München: TU, Diss. 1995.

D49 DANNER, S.:
Ganzheitliches Anforderungsmanagement für marktorientierte Entwicklungsprozesse.
Aachen: Shaker 1996. (Konstruktionstechnik München, Band 24). Zugl. München: TU, Diss. 1996.

D50 MERAT, P.:
Rechnergestützte Auftragsabwicklung an einem Praxisbeispiel.
Aachen: Shaker 1996. (Konstruktionstechnik München, Band 25). Zugl. München: TU, Diss. 1996 u. d. T.: MERAT, P.: Rechnergestütztes Produktleitsystem

D51 AMBROSY, S.:
Methoden und Werkzeuge für die integrierte Produktentwicklung.
Aachen: Shaker 1997. (Konstruktionstechnik München, Band 26). Zugl. München: TU, Diss. 1996.

D52 GIAPOULIS, A.:
Modelle für effektive Konstruktionsprozesse.
Aachen: Shaker 1998. (Konstruktionstechnik München, Band 27). Zugl. München: TU, Diss. 1996.

D53 STEINMEIER, E.:
Realisierung eines systemtechnischen Produktmodells – Einsatz in der Pkw-Entwicklung
Aachen: Shaker 1998. (Konstruktionstechnik München, Band 28). Zugl. München: TU, Diss. 1998.

D54 KLEEDÖRFER, R.:
Prozess- und Änderungsmanagement der Integrierten Produktentwicklung.
Aachen: Shaker 1998. (Konstruktionstechnik München, Band 29). Zugl. München: TU, Diss. 1998.

D55 GÜNTHER, J.:
Individuelle Einflüsse auf den Konstruktionsprozess.
Aachen: Shaker 1998. (Konstruktionstechnik München, Band 30). Zugl. München: TU, Diss. 1998.

D56 BIERSACK, H.:
Methode für Krafteinleitungsstellenkonstruktion in Blechstrukturen.
München: TU, Diss. 1998.

D57 IRLINGER, R.:
Methoden und Werkzeuge zur nachvollziehbaren Dokumentation in der Produktentwicklung.
Aachen: Shaker 1998. (Konstruktionstechnik München, Band 31). Zugl. München: TU, Diss. 1999.

D58 EILETZ, R.:
Zielkonfliktmanagement bei der Entwicklung komplexer Produkte – am Bsp. PKW-Entwicklung.
Aachen: Shaker 1999. (Konstruktionstechnik München, Band 32). Zugl. München: TU, Diss. 1999.

D59 STÖSSER, R.:
Zielkostenmanagement in integrierten Produkterstellungsprozessen.
Aachen: Shaker 1999. (Konstruktionstechnik München, Band 33). Zugl. München: TU, Diss. 1999.

D60 PHLEPS, U.:
Recyclinggerechte Produktdefinition – Methodische Unterstützung für Upgrading und Verwertung.
Aachen: Shaker 1999. (Konstruktionstechnik München, Band 34). Zugl. München: TU, Diss. 1999.

D61 BERNARD, R.:
Early Evaluation of Product Properties within the Integrated Product Development.
Aachen: Shaker 1999. (Konstruktionstechnik München, Band 35). Zugl. München: TU, Diss. 1999.

D62 ZANKER, W.:
Situative Anpassung und Neukombination von Entwicklungsmethoden.
Aachen: Shaker 1999. (Konstruktionstechnik München, Band 36). Zugl. München: TU, Diss. 1999.

Reihe Produktentwicklung München

D63 ALLMANSBERGER, G.:
Erweiterung der Konstruktionsmethodik zur Unterstützung von Änderungsprozessen in der Produktentwicklung.
München: Dr. Hut 2001. (Produktentwicklung München, Band 37). Zugl. München: TU, Diss. 2000.

D64 ASSMANN, G.:
Gestaltung von Änderungsprozessen in der Produktentwicklung.
München: Utz 2000. (Produktentwicklung München, Band 38). Zugl. München: TU, Diss. 2000.

D65 BICHLMAIER, C.:
Methoden zur flexiblen Gestaltung von integrierten Entwicklungsprozessen.
München: Utz 2000. (Produktentwicklung München, Band 39). Zugl. München: TU, Diss. 2000.

D66 DEMERS, M. T.
Methoden zur dynamischen Planung und Steuerung von Produktentwicklungsprozessen.
München: Dr. Hut 2000. (Produktentwicklung München, Band 40). Zugl. München: TU, Diss. 2000.

D67 STETTER, R.:
Method Implementation in Integrated Product Development.
München: Dr. Hut 2000. (Produktentwicklung München, Band 41). Zugl. München: TU, Diss. 2000.

D68 VIERTLBÖCK, M.:
Modell der Methoden- und Hilfsmitteleinführung im Bereich der Produktentwicklung.
München: Dr. Hut 2000. (Produktentwicklung München, Band 42). Zugl. München: TU, Diss. 2000.

D69 COLLIN, H.:
Management von Produkt-Informationen in kleinen und mittelständischen Unternehmen.
München: Dr. Hut 2001. (Produktentwicklung München, Band 43). Zugl. München: TU, Diss. 2001.

D70 REISCHL, C.:
Simulation von Produktkosten in der Entwicklungsphase.
München: Dr. Hut 2001. (Produktentwicklung München, Band 44). Zugl. München: TU, Diss. 2001.

D71 GAUL, H.-D.:
Verteilte Produktentwicklung - Perspektiven und Modell zur Optimierung.
München: Dr. Hut 2001. (Produktentwicklung München, Band 45). Zugl. München: TU, Diss. 2001.

D72 GIERHARDT, H.:
Global verteilte Produktentwicklungsprojekte – Ein Vorgehensmodell auf der operativen Ebene.
München: Dr. Hut 2002. (Produktentwicklung München, Band 46). Zugl. München: TU, Diss. 2001.

D73 SCHOEN, S.:
Gestaltung und Unterstützung von Community of Practice.
München: Utz 2000. (Produktentwicklung München, Band 47). Zugl. München: TU, Diss. 2000.

D74 BENDER, B.:
Zielorientiertes Kooperationsmanagement.
München: Dr. Hut 2001. (Produktentwicklung München, Band 48). Zugl. München: TU, Diss. 2001.

D75 SCHWANKL, L.:
Analyse und Dokumentation in den frühen Phasen der Produktentwicklung.
München: Dr. Hut 2002. (Produktentwicklung München, Band 49). Zugl. München: TU, Diss. 2002.

D76 WULF, J.:
Elementarmethoden zur Lösungssuche.
München: Dr. Hut 2002. (Produktentwicklung München, Band 50). Zugl. München: TU, Diss. 2002.

D77 MÖRTL, M.:
Entwicklungsmanagement für langlebige, upgradinggerechte Produkte.
München: Dr. Hut 2002. (Produktentwicklung München, Band 51). Zugl. München: TU, Diss. 2002.

D78 GERST, M.:
Strategische Produktentscheidungen in der integrierten Produktentwicklung.
München: Dr. Hut 2002. (Produktentwicklung München, Band 52). Zugl. München: TU, Diss. 2002.

D79 AMFT, M.:
Phasenübergreifende bidirektionale Integration von Gestaltung und Berechnung.
München: Dr. Hut 2003. (Produktentwicklung München, Band 53). Zugl. München: TU, Diss. 2002.

D80 FÖRSTER, M.:
Variantenmanagement nach Fusionen in Unternehmen des Anlagen- und Maschinenbaus.
München: TU, Diss. 2003.

D81 GRAMANN, J.:
Problemmodelle und Bionik als Methode.
München: Dr. Hut 2004. (Produktentwicklung München, Band 55). Zugl. München: TU, Diss. 2004.

D82 PULM, U.:
Eine systemtheoretische Betrachtung der Produktentwicklung.
München: Dr. Hut 2004. (Produktentwicklung München, Band 56). Zugl. München: TU, Diss. 2004.

D83 HUTTERER, P.:
Reflexive Dialoge und Denkbausteine für die methodische Produktentwicklung.
München: Dr. Hut 2005. (Produktentwicklung München, Band 57). Zugl. München: TU, Diss. 2005.

D84 FUCHS, D.:
Konstruktionsprinzipien für die Problemanalyse in der Produktentwicklung.
München: Dr. Hut 2006. (Produktentwicklung München, Band 58). Zugl. München: TU, Diss. 2005.

D85 PACHE, M.:
Sketching for Conceptual Design.
München: Dr. Hut 2005. (Produktentwicklung München, Band 59). Zugl. München: TU, Diss. 2005.

D86 BRAUN, T.:
Methodische Unterstützung der strategischen Produktplanung in einem mittelständisch geprägten Umfeld.
München: Dr. Hut 2005. (Produktentwicklung München, Band 60). Zugl. München: TU, Diss. 2005.

D87 JUNG, C.:
Anforderungsklärung in interdisziplinärer Entwicklungsumgebung.
München: Dr. Hut 2006. (Produktentwicklung München, Band 61). Zugl. München: TU, Diss. 2006.

D88 HEßLING, T.:
Einführung der Integrierten Produktpolitik in kleinen und mittelständischen Unternehmen.
München: Dr. Hut 2006. (Produktentwicklung München, Band 62). Zugl. München: TU, Diss. 2006.

D89 STRICKER, H.:
Bionik in der Produktentwicklung unter der Berücksichtigung menschlichen Verhaltens.
München: Dr. Hut 2006. (Produktentwicklung München, Band 63). Zugl. München: TU, Diss. 2006.

D90 NIßL, A.:
Modell zur Integration der Zielkostenverfolgung in den Produktentwicklungsprozess.
München: Dr. Hut 2006. (Produktentwicklung München, Band 64). Zugl. München: TU, Diss. 2006.

D91 MÜLLER, F.:
Intuitive digitale Geometriemodellierung in frühen Entwicklungsphasen.
München: Dr. Hut 2007. (Produktentwicklung München, Band 65). Zugl. München: TU, Diss. 2006.

D92 ERDELL, E.:
Methodenanwendung in der Hochbauplanung – Ergebnisse einer Schwachstellenanalyse.
München: Dr. Hut 2006. (Produktentwicklung München, Band 66). Zugl. München: TU, Diss. 2006.

D93 GAHR, A.:
Pfadkostenrechnung individualisierter Produkte.
München: Dr. Hut 2006. (Produktentwicklung München, Band 67). Zugl. München: TU, Diss. 2006.

D94 RENNER, I.:
Methodische Unterstützung funktionsorientierter Baukastenentwicklung am Beispiel Automobil.
München: Dr. Hut 2007 (Reihe Produktentwicklung) Zugl. München: TU, Diss. 2007.

D95 PONN, J.:
Situative Unterstützung der methodischen Konzeptentwicklung technischer Produkte.
München: Dr. Hut 2007 (Reihe Produktentwicklung) Zugl. München: TU, Diss. 2007.

D96 HERFELD, U.:
Matrix-basierte Verknüpfung von Komponenten und Funktionen zur Integration von Konstruktion und numerischer Simulation.
München: Dr. Hut 2007. (Produktentwicklung München, Band 70). Zugl. München: TU, Diss. 2007.

D97 SCHNEIDER, S.:
Model for the evaluation of engineering design methods.
München: Dr. Hut 2008 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2007.

D98 FELGEN, L.:
Systemorientierte Qualitätssicherung für mechatronische Produkte.
München: Dr. Hut 2007 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2007.

D99 GRIEB, J.:
Auswahl von Werkzeugen und Methoden für verteilte Produktentwicklungsprozesse.
München: Dr. Hut 2007 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2007.

D100 MAURER, M.:
Structural Awareness in Complex Product Design.
München: Dr. Hut 2007 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2007.

D101 BAUMBERGER, C.:
Methoden zur kundenspezifischen Produktdefinition bei individualisierten Produkten.
München: Dr. Hut 2007 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2007.

D102 KEIJZER, W.:
Wandlungsfähigkeit von Entwicklungsnetzwerken – ein Modell am Beispiel der Automobilindustrie.
München: Dr. Hut 2007 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2007.

D103 LORENZ, M.:
Handling of Strategic Uncertainties in Integrated Product Development.
München: Dr. Hut 2009 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2008.

D104 KREIMEYER, M.:
Structural Measurement System for Engineering Design Processes.
München: Dr. Hut 2010 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2009.

D105 DIEHL, H.:
Systemorientierte Visualisierung disziplinübergreifender Entwicklungsabhängigkeiten mechatronischer Automobilsysteme.
München: Dr. Hut 2009 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2009.

D106 DICK, B.:
Untersuchung und Modell zur Beschreibung des Einsatzes bildlicher Produktmodelle durch Entwicklerteams in der Lösungssuche.
München: Dr. Hut 2009 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2009.

D107 GAAG, A.:
Entwicklung einer Ontologie zur funktionsorientierten Lösungssuche in der Produktentwicklung.
München: Dr. Hut 2010 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2010.

D108 ZIRKLER, S.:
Transdisziplinäres Zielkostenmanagement komplexer mechatronischer Produkte.
München: Dr. Hut 2010 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2010.

D109 LAUER, W.:
Integrative Dokumenten- und Prozessbeschreibung in dynamischen Produktentwicklungsprozessen.
München: Dr. Hut 2010 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2010.

D110 MEIWALD, T.:
Konzepte zum Schutz vor Produktpiraterie und unerwünschtem Know-how-Abfluss.
München: Dr. Hut 2011 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2011.

D111 ROELOFSEN, J.:
Situationsspezifische Planung von Produktentwicklungsprozessen.
München: Dr. Hut 2011 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2011.

D112 PETERMANN, M.:
Schutz von Technologiewissen in der Investitionsgüterindustrie.
München: Dr. Hut 2011 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2011.

D113 GORBEA, C.:
Vehicle Architecture and Lifecycle Cost Analysis in a New Age of Architectural Competition.
München: Dr. Hut 2011 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2011.

D114 FILOUS, M.:
Lizenzierungsgerechte Produktentwicklung – Ein Leitfaden zur Integration lizenzierungsrelevanter Aktivitäten in Produktentstehungsprozessen des Maschinen- und Anlagenbaus.
München: Dr. Hut 2011 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2011.

D115 ANTON, T.:
Entwicklungs- und Einführungsmethodik für das Projektierungswerkzeug Pneumatiksimulation.
München: Dr. Hut 2011 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2011.

D116 KESPER, H.:
Gestaltung von Produktvariantenspektren mittels matrixbasierter Methoden.
München: Dr. Hut 2012 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2012.

D117 KIRSCHNER, R.:
Methodische Offene Produktentwicklung.
München: TU, Diss. 2012.

D118 HEPPERLE, C.:
Planung lebenszyklusgerechter Leistungsbündel.
München: Dr. Hut 2013 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2013.

D119 HELLENBRAND, D.:
Transdisziplinäre Planung und Synchronisation mechatronischer Produktentwicklungsprozesse.
München: Dr. Hut 2013 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2013.

D120 EBERL, T.:
Charakterisierung und Gestaltung des Fahr-Erlebens der Längsführung von Elektrofahrzeugen.
München: TU, Diss. 2014.

D121 KAIN, A.:
Methodik zur Umsetzung der Offenen Produktentwicklung.
München: Dr. Hut 2014 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D122 ILIE, D.:
Systematisiertes Ziele- und Anforderungsmanagement in der Fahrzeugentwicklung.
München: Dr. Hut 2013 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2013.

D123 HELTEN, K.:
Einführung von Lean Development in mittelständische Unternehmen - Beschreibung, Erklärungsansatz und Handlungsempfehlungen.
München: Dr. Hut 2015 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D124 SCHRÖER, B.:
Lösungskomponente Mensch. Nutzerseitige Handlungsmöglichkeiten als Bausteine für die kreative Entwicklung von Interaktionslösungen.
München: TU, Diss. 2014.

D125 KORTLER, S.:
Absicherung von Eigenschaften komplexer und variantenreicher Produkte in der Produktentwicklung.
München: Dr. Hut 2014 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D126 KOHN, A.:
Entwicklung einer Wissensbasis für die Arbeit mit Produktmodellen.
München: Dr. Hut 2014 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D127 FRANKE, S.:
Strategieorientierte Vorentwicklung komplexer Produkte – Prozesse und Methoden zur zielgerichteten Komponentenentwicklung am Beispiel Pkw.
Göttingen: Cuvillier, E 2014. Zugl. München: TU, Diss. 2014.

D128 HOOSHMAND, A.:
Solving Engineering Design Problems through a Combination of Generative Grammars and Simulations.
München: Dr. Hut 2014 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D129 KISSEL, M.:
Mustererkennung in komplexen Produktportfolios.
München: TU, Diss. 2014.

D130 NIES, B.:
Nutzungsgerechte Dimensionierung des elektrischen Antriebssystems für Plug-In Hybride.
München: TU, Diss. 2014.

D131 KIRNER, K.:
Zusammenhang zwischen Leistung in der Produktentwicklung und Variantenmanagement – Einflussmodell und Analysemethode.
München: Dr. Hut 2014 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D132 BIEDERMANN, W.:
A minimal set of network metrics for analysing mechatronic product concepts.
München: TU, Diss. 2015.

D133 SCHENKL, S.:
Wissensorientierte Entwicklung von Produkt-Service-Systemen.
München: TU, Diss. 2015.

D134 SCHRIEVERHOFF, P.:
Valuation of Adaptability in System Architecture.
München: Dr. Hut 2015 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2014.

D135 METZLER, T.:
Models and Methods for the Systematic Integration of Cognitive Functions into Product Concepts.
München: Dr. Hut 2016 (Reihe Produktentwicklung).

D136 DEUBZER, F.:
A Method for Product Architecture Management in Early Phases of Product Development.
München: TU, Diss. 2016.

D137 SCHÖTTL, F.:
Komplexität in sozio-technischen Systemen - Methodik für die komplexitätsgerechte Systemgestaltung in der Automobilproduktion.
München: Dr. Hut 2016 (Reihe Produktentwicklung).

D138 BRANDT, L. S.:
Architekturgesteuerte Elektrik/Elektronik Baukastenentwicklung im Automobil
München: TU, Diss. 2017.

D139 BAUER, W.:
Planung und Entwicklung änderungsrobuster Plattformarchitekturen
München: Dr. Hut 2016 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2016.

D140 ELEZI, F.:
Supporting the Design of Management Control Systems In Engineering Companies from Management Cybernetics Perspective
München: TU, Diss. 2015.

D141 BEHNCKE, F. G. H.:
Beschaffungsgerechte Produktentwicklung – Abstimmung von Produktarchitektur und Liefernetzwerk in frühen Phasen der Entwicklung
TU München: 2015. (als Dissertation eingereicht)

D142 ÖLMEZ, M.:
Individuelle Unterstützung von Entscheidungsprozessen bei der Entwicklung innovativer Produkte.
München: Dr. Hut 2017 (Reihe Produktentwicklung).

D143 SAUCKEN, C. C. V.:
Entwicklerzentrierte Hilfsmittel zum Gestalten von Nutzererlebnissen.
München: Dr. Hut 2017 (Reihe Produktentwicklung).

D144 KASPEREK, D.:
Structure-based System Dynamics Analysis of Engineering Design Processes
München: TU, Diss. 2016.

D145 Langer, S. F.:
Kritische Änderungen in der Produktentwicklung – Analyse und Maßnahmenableitung
München: Dr. Hut 2017 (Reihe Produktentwicklung).

D146 Herberg, A. P.:
Planung und Entwicklung multifunktionaler Kernmodule in komplexen Systemarchitekturen und –portfolios – Methodik zur Einnahme einer konsequent modulzentrierten Perspektive
TU München: 2016. (als Dissertation eingereicht)

D147 Hashemi Farzaneh, H.:
Bio-inspired design: Ideation in collaboration between mechanical engineers and biologists
München: TU, Diss. 2017.

D148 Helms, M. K.:
Biologische Publikationen als Ideengeber für das Lösen technischer Probleme in der Bionik
München: TU, Diss. 2017.

D149 Gürtler, M. R.:
Situational Open Innovation – Enabling Boundary-Spanning Collaboration in Small and Medium-sized Enterprises
München: TU, Diss. 2016.

D150 Wickel, M. C.:
Änderungen besser managen – Eine datenbasierte Methodik zur Analyse technischer Änderungen
München: TU, Diss. 2017.

D151 Daniilidis, C.:
Planungsleitfaden für die systematische Analyse und Verbesserung von Produktarchitekturen
München: TU, Diss. 2017.

D152 Michailidou, I.:
Design the experience first: A scenario-based methodology for the design of complex, tangible consumer products
München: TU, Diss. 2017.

D153 Schmidt, D.M.:
Increasing Customer Acceptance in Planning Product-Service Systems
München: Dr. Hut 2017 (Reihe Produktentwicklung). Zugl. München: TU, Diss. 2017.

D154 Roth, M.:
Efficient Safety Method Kit for User-driven Customization
München: Dr. Hut 2017 (Reihe Produktentwicklung).

D155 Plötner, M.:
Integriertes Vorgehen zur selbstindividualisierungsgerechten Produktstrukturplanung
TU München: 2017. (als Dissertation eingereicht)

D156 Herbst, L.-M.:
Entwicklung einer Methodik zur Ermittlung raumfunktionaler Kundenanforderungen in der Automobilentwicklung
München: Dr. Hut 2017 (Reihe Produktentwicklung).

D157 Kammerl, D. M. A.:
Modellbasierte Planung von Produkt-Service-Systemen
TU München: 2017. (als Dissertation eingereicht)

D158 Münzberg, C. H. W.:
Krisen in der Produktentwicklung und ihre operative Bewältigung
TU München: 2017. (als Dissertation eingereicht)

D159 Heimberger, N.:
Strukturbasierte Koordinationsplanung in komplexen Entwicklungsprojekten
TU München: 2017. (als Dissertation eingereicht)