SAFETY OF INDIVIDUAL PRODUCTS – PERSPECTIVES IN THE CONTEXT OF CURRENT PRACTICES AND CHALLENGES

Roth, Michael; Gehrlicher, Steffi; Lindemann, Udo
Technische Universität München, Germany

Abstract

The safety of products is one essential feature on the way to approval. Methods of safety analysis are applied to ensure this. Facing growing demand for individual products and stricter regulations, these analyses require increasing efforts. In mechanical and mechatronic engineering, these analyses in practice are dominated by traditional methods. Current research aims to improve and enhance this process of considering safety during all stages in design. However, these works mainly focus on software or embedded systems. Thus, this paper aims to understand the current practices and challenges in mechanical or mechatronic engineering. It examines existing approaches from literature and records the industrial practices within an interview study. Challenges in safety analysis are discussed with special focus on increasing variance and user innovation concepts. By that our paper contributes to a better understanding of current and upcoming challenges in the domain of mechanical and mechatronic engineering and identifies the needs and directions for further research.

Keywords: Safety Analysis, Safety Engineering, Design for X (DfX), Design methods

Contact:
Michael Roth
Technische Universität München
Institute of Product Development
Germany
michael.roth@pe.mw.tum.de

Please cite this paper as:
Surnames, Initials: *Title of paper*. In: Proceedings of the 20th International Conference on Engineering Design (ICED15), Vol. nn: Title of Volume, Milan, Italy, 27.-30.07.2015

1 INTRODUCTION

Customers' expectations and requirements, as well as their variance are steadily increasing. Thus, companies are under pressure to offer even more variants and individual products (Lindemann *et al.*, 2008; Piller, 2006). As a result we observe a hardly manageable amount of variants in the industry. In combination with stricter safety regulations this development causes immense efforts to successfully run through the process of safety analysis and approval for each new variant or individual adaption.
However, traditional methods of safety analysis strongly rely on the experience of expert analysts. These methods are mainly applied review-based and at the design validation stage only. This might lead to late and expensive changes and rework cycles (Sierla *et al.*, 2012; Jensen and Tumer, 2013).
Recent publications in the field of safety analysis postulate, that the consideration of safety aspects should be shifted to the early stages of the design process (Sierla *et al.*, 2012; Jensen and Tumer, 2013; Leveson, 2012). However, the literature and our own observations show that this strategy is not sufficiently implemented in industrial application.
As (Herfeld *et al.*, 2007) underline in their case study, a high number of variants drastically increases the complexity of product safety. In this context and if even approaches like user innovation (Hippel, 2001) are followed, the early integration of safety gets challenging. To handle this, it is necessary to improve the process and strategies of safety analysis.
Existing approaches in this field mainly focus on software or embedded systems. From our point of view, they do not sufficiently consider the challenges connected to product variance and individual products in mechanical and mechatronic engineering. Therefore this paper records the actual practices of safety analysis in mechanical and mechatronic engineering companies. Based on these practices and on existing research, the major challenges for safety analysis are identified. This is achieved by combining a literature review and an interview study. We thus contribute to the understanding of current and upcoming challenges of safety analysis in mechanical and mechatronic engineering and reveal the existing gaps between research and industrial application.
In the following, we first provide a brief overview of traditional methods of safety analysis. After that, the challenges of safety analysis within the process of engineering design are then pointed out. We moreover discuss existing approaches to overcome these hurdles. We then present the methodology and results of an interview study in which we identified current practices and challenges in industrial application. This paper then discusses the results in comparison to the findings of the literature review. Moreover, the impact of high variance and individual consumer products is discussed. The paper finally concludes and gives an outlook on further research.

2 SAFETY ANALYSIS METHODS AND APPLICATION

This section first provides an overview of traditional methods of safety analysis. It then identifies challenges of the safety analysis within the engineering design processes and presents existing approaches to solve these.

2.1 Traditional methods of safety analysis

The safety analysis within product development requires both, deductive and inductive approaches (Cuenot *et al.*, 2014). Traditional methods used therefore are the failure mode and effects analysis (FMEA) and the fault tree analysis (FTA). In the following, we introduce these methods, their extensions and give an overview of other established methods.

2.1.1 Fault tree analysis (FTA)

The FTA is a traditional, standardized and normed method which is applied to the safety analysis of products and systems (IEC, 2006b). Its main objective is to identify conditions which may cause or contribute to the occurrence of an undesired top event. The conditions and their propagation are modeled in a graphical form (IEC, 2006b; Majdara and Wakabayashi, 2009).
As the FTA has a deductive character, it first identifies the undesired top events. Starting from them, the analysis follows down the possible causes of each top event. By that, the tree structure is created. If multiple causes of one failure occur, their dependencies are modelled by Boolean logic gates. The FTA follows down the branches of the tree until basic events are reached. A basic event represents a

failure in a single component or element, which has no other causes (IEC, 2006b; Majdara and Wakabayashi, 2009).
Based on this representation, the contribution of all basic events to the top event can be determined by using analytical methods. Moreover, the combinations of failures which will cause the top event can be identified. These combinations are called cut sets. An additional advantage of the FTA is, that it is able to identify the impact of basic failures on multiple top events. This phenomena is called a common cause (IEC, 2006b; Majdara and Wakabayashi, 2009).
However, many researchers point out, that the high manual efforts and experience which are required to conduct the FTA are the most important limitations of this method (Sierla *et al.*, 2012; Majdara and Wakabayashi, 2009; Mhenni *et al.*, 2014). Moreover, a component-based FTA will never be able to ensure full system safety (Leveson, 2012). Nevertheless, a product which is compliant to industry safety standards (e.g. IEC61508) requires the successful application and documentation of the FTA during the product development (Cuenot *et al.*, 2014).

2.1.2 Failure mode and effects analysis (FMEA)

In comparison to the FTA, the FMEA has an inductive character. Its main objective is to identify and assess possible failure modes. The FMEA is also normed and standardized (IEC, 2006a). It can be applied in various phases of product design or on various abstraction levels. Common types are the functional or systems FMEA, the design FMEA or process FMEA (IEC, 2006a).
The FMEA mainly consists of five steps: preparation, failure analysis, risk assessment, calculation of the risk level and, if necessary, deduction of countermeasures. The failure analysis identifies potential failures in the product are determines failure modes. In the following step of risk assessment, the probability, severity and detection of failure modes is assessed. Based on that, the risk level is calculated and, if necessary, measures to reduce this value are deduced (IEC, 2006a; Ben-Daya, 2009).
Many variants of the FMEA occur. For example the inclusion of the criticality is very common and normed (FMECA) or instead of risk levels, a risk matrix is used (IEC, 2006a; Ben-Daya, 2009).
The FMEA thus is able, to analyse product safety and to support its improvement. Yet, it is not able to identify the previously mentioned common causes. Moreover research criticizes the high manual efforts and experience which are consumed (Jensen and Tumer, 2013; Maurer and Kesper, 2011). However, like the FTA, the FMEA is also a mandatory part for the compliance with many standards (Cuenot *et al.*, 2014).

2.1.3 Other methods of safety analysis

Besides FTA and FMEA many other methods exist. The preliminary hazard analysis (PHA) (Roland and Moriarty, 1990) for example is a suitable method for the early phases of design. Another method is the event tree analysis (ETA), which is the inductive counterpart of the FTA. And also the hazard and operability study (HAZOP), which analyses planned operations and identifies potential risks is a suitable method (Ericson, 2005). Nevertheless, these methods in general do only occur supplemented by other methods, especially FMEA and FTA.

2.2 Safety analysis in engineering design

Based on these traditional methods, the following sections describe the state of the art of safety analysis within engineering design. While the engineered technologies developed rapidly, the traditional methods made little progress (Leveson, 2012). This induces a need for methods and strategies which are adapted to the changed context. In the following, existing challenges are pointed out and we discuss published solution approaches.

2.2.1 Integration of engineering design and safety analysis

The traditional methods described above are applied in the process of engineering design. However, Jensen and Tumer (2013) point out, that the standard practices are mainly review-centred. This means, the designed product is reviewed from a panel of experts to ensure product safety. Also Cuenot *et al.* (2014) observe, that the safety evaluation currently is often performed at a late stage of design.
Yet, to fulfil the safety requirements at low efforts and costs, an early consideration of safety aspects in the development process is needed (Cuenot *et al.*, 2014; Biehl *et al.*, 2010; Sierla *et al.*, 2012). This early consideration of safety can reduce late changes and rework costs. As late changes can additionally induce new sources of failure, their propagation also has to be managed (Eckert *et al.*,

2004). Thus, the integration of safety analysis throughout the whole process of engineering design is an important success factor.
This integration arises many challenges. For example Biehl *et al.* (2010) identify a gap between the disciplines of safety engineering and system design. To successfully achieve an integration of safety analysis, this gap needs to be bridged.
Moreover many authors like Cuenot *et al.* (2014) and Herfeld *et al.* (2007) state, that the increasing size and complexity of products complicates the safety analysis. The growing amount of components and their complexity induces the risk of inconsistency, as the safety analysis and design of all these components have to be harmonized.
Finally, as mentioned above, the large manual efforts involved in methods of safety analysis act as another hurdle and might prevent the early integration of safety analysis in design (Maurer and Kesper, 2011).
The challenges for safety analysis within the process of engineering design identified from literature thus can be summarized to:

- early integration of safety aspects
- bridging the gap between disciplines
- improving efficiency

2.2.2 Approaches for a better integration of safety analysis

In literature few approaches facing the previously described challenges exist. The most basic approach is the safety-centric design process by Leveson (2012). The main intention is, to create a product design from the safe design space instead of analysing established designs and identifying their violations of safety requirements (Jensen and Tumer, 2013). Other works are mainly driven from the compliance with safety standards like IEC 61508 and thus try to enable a consistent model based process, which covers both, product design and safety analysis. Table 1 depicts the main works we identified and categorizes them according to which challenge they mainly address.

Table 1. Existing approaches to overcome the challenges of safety analysis within engineering design and the challenges they address

authors	addressed challenge			approach
	early integration	bridging gaps	efficiency	
Biehl *et al.*, 2010		X		automated translation of architetecture description language (ADL2) and safety analysis language (HIP-HOPS)
Cuenot *et al.*, 2014		X		extension of architecture language (ADL) to comply with safety analyses
Li, 2012			X	ontology to reuse FMEAs of components within a product
Höfig *et al.*, 2014			X	metamodel of FMEA to enable reuse of component FMEA and to avoid different interpretations
Jensen and Tumer, 2013	(X)	X		explicit modelling of safety (safety functions) in the early design process
Leveson, 2012	X			safety centric design process for an early integration of safety aspect into product design
Maurer and Kesper, 2011	(X)		X	FMEA enhanced by the usage of matrix-based methods and software support
Mhenni *et al.*, 2013		X	(X)	integration of safety analysis and formal verification methods in SysML at early design stages to enable qualitative assessments

Sierla *et al.*, 2012	X	X		Functional Failure Identification and Propagation Framework (FFIP) to integrate safety analysis in early design stages and to complement traditional methods

2.2.3 Limitations of existing work

Most of the existing research discussed in the previous section has its main origin in embedded systems or software design. In these domains the works mainly discuss single case studies or initial implementations. This arises the question, how companies, especially in mechanical or mechatronic engineering, handle the safety analyses in their daily product developments.
Moreover, Jiang *et al.* (2007) and Papakonstantinou *et al.* (2011) identify a growing amount of individual and customized products and point out the connected challenges for quality, validation and safety aspects. While Papakonstantinou *et al.* (2011) focus on the automated generation and validation of software instances, Jiang *et al.* (2007) propose a quality management system for individualized products. Yet, both do not focus on the role of safety within the design of customizable or individual products.
So the questions we address in this paper are, how companies in mechanical and mechatronic engineering consider safety aspects, how they handle the challenges of an integrated safety analysis in their daily business and how they cope with variant or individual products.

3 INTERVIEW STUDY ON SAFETY IN PRODUCT DESIGN APPLICATION

The literature discussed in previous sections provides a large bandwidth of methods and strategies to consider safety during the design process. In the following we present the interview study, which we conducted to compare these findings to the actual practices in the industry and to answer the research questions postulated above.

3.1 Methodology

For the interview study we contacted safety experts of various companies and selected a total of three interviewees. They cover large parts of the whole domain of mechatronic products: Two of them are from companies which produce customized and individual mechatronic products. Both companies with individual products follow engineer to order strategies. The first company acts as an original equipment manufacturer (oem) and first tier supplier. The second company acts as a first tier supplier and produces systems with high safety-relevance. The third interviewee is from a mass-producing company, which acts as oem in the consumer goods industry.
The companies are in the size between 4000 and 50000 employees. Our interview partners all are experts for product safety in their company and they are involved in safety analysis and approval activities. Our interview sample, thus allows us to capture the practical application of safety methods in both, the design of individual and mass products.
The interviews aim to identify the applied practices of considering safety during product design. Therefore, it is necessary to understand the product, its structure and the companies' design and safety processes. That is why the interviews are not limited to applied methods only and follow the 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

All interviews were held personally in a semi-structured form. This format aims to collect qualitative insights and not quantitative data. 15 central questions guided through the interview. These central questions build the framework of the interview. Depending on the situation additional and individual questions have been asked by the interviewer to support the interviewee and to guide him along the central questions.
To avoid reservations of the interviewees, the interviews were not recorded by audio or video devices. Therefore, the interviewer was assisted by a minute taker who noted down the answers. One interview took between one and two hours. Within that, the 15 central questions were clustered in the following three blocks:

The **first block** focuses on product structure and standardized products or modules. It captures the percentage of standardized components and their characteristics. For this type of components, the process and methods of safety analysis are addressed. Moreover, the strategies to conduct the safety analysis for combinations of standardized components are identified.
The **second block** addresses customized or individual components. Their percentage, the applied methods and processes are captured. Also for this group of components, the question is asked, how the interfaces to standardized components are handled during safety analysis.
The **third block** finally addressed the aspects of efficiency, documentation and reuse of analysis data.
An overview of these previously discussed blocks and their main aspects and the topics of the central questions can be found in Figure 1.

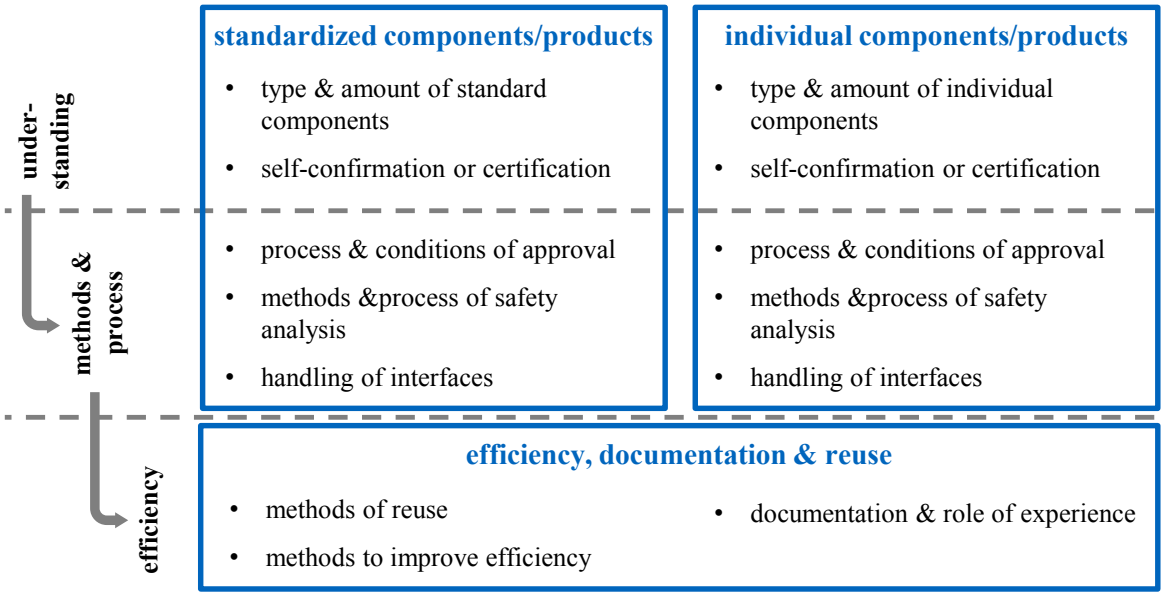

Figure 1. Aspects and Topics of the 15 central questions of the semi-structured interviews

3.2 Results of the interview study

The following sections present an outline of the interviews' results clustered according to the tree blocks of central aspects described in Figure 1.

3.2.1 Design and safety analysis of standardized products or modules

All interviewees try to design new products based on standardized components and strive to increase their percentage in the final product. Even the companies with engineer to order strategies have high percentages of 60% to 80% of standardized components or modules.
The basic safety strategy in all companies is to design the products according to norms and guidelines from the very beginning. This measure covers the known safety risks, but is not sufficient. To avoid remaining risks and hazards, all companies apply the traditional methods FMEA or FTA. They often adapt these methods to their specific requirements and in parts use tool support. The usage of these methods often even exceeds the mandatory extent.
The results governed by these methods are usually consolidated to a report. Based on this report, either the self-declaration on compliance or the external certification are conducted.
All companies moreover try to approve their standard components before they are integrated in a new product. This means, they all successfully passed a safety analysis before their integration. However, the strategies to handle the interfaces and combinations of standardized modules vary. The mass-producing company tries to cover different combinations of standard components in one approval. Thus, the final safety analysis and approval is conducted for a whole product line. The individual-producing companies instead mainly approve single products.
Yet, all companies try to approve as much as possible standard components in advance. When these components are integrated in a new product, the interfaces and surrounding conditions have to be tested on their compliance with the situation and conditions of the original safety analysis.

3.2.2 Design and safety analysis of standardized products or modules

For individual products or components, the process of safety analysis in general is the same as described above: The mass-producing company carries out the safety analysis of a whole product line in one process. The following paragraphs thus mainly focus on the individual-producing companies.
Custom or individual components usually cannot be analysed and approved in advance. Thus, according to the interviewees each individual component's safety has to be analysed. Therefore the interviewees denote, that the design according to guidelines and norms as the most important factor.
In the case of a product with individual components, the whole product and its remaining standard components have to be analysed and approved again. The interviewees mention, that only in some cases, if the individual amount does not exceed a critical level, a sole approval of the individual components can be sufficient. Still, the actual process of approval for individual products is similar to the process described in the section above.
Especially the expert from the company with safety-critical systems emphasizes the importance of an architecture which is tailored to system safety. Therefore the company invests in safety oriented architectures. However, according to the interviewee, the efforts still are not high enough.

3.2.3 Efficiency and reuse within safety analysis

As previous paragraphs show, the safety analyses of mass-products with high variance and the safety analyses of individual products are very similar. In both cases the interviewees emphasize the huge efforts which are connected to this process. Yet, the safety analysis efforts of mass-products can be distributed to large batch sizes. Instead, the individual producers are struggling with immense efforts which are required for each individual product. They especially mention, that as regulations and laws grow in number and complexity, the efforts for safety analysis and approval will increase even more.
Therefore, they try to increase the efficiency of their safety analyses. One strategy is the above mentioned higher percentage of standard components. Another strategy is to reuse findings of previous analyses. Moreover the companies try to improve the efficiency in their safety processes. They merely apply the research findings described in section 2 but focus on their own method improvements and adaptions. For example one company reduces the efforts needed to confirm the compatibility of standard components by applying different strategies. Depending on the situation and boundary conditions they apply one of the following three strategies to the safety analysis:

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

These strategies enable them to adjust the efforts needed for safety analysis and thus to reduce the efforts to a suitable amount.
According to the interviewee, the mass-producer is able to efficiently reuse pervious safety analyses or approvals during new developments. Even though short development cycles occur, the major changes of the product are known from the early phases of development. Yet he mentions, that often the documentation of previous analyses' results is not sufficiently done. Reasons therefore mostly are limited time and resources. This has the consequence, that even though the knowledge is reused, it happens mainly based on the individual experience and knowledge of the experts.
Also the interviewees from the individual-producing companies confirm, that findings from previous safety analyses are reused during the analysis of other individual products. However they also admit, that documentation is not done sufficiently and the reuse in their companies also mainly bases on individual experience. One of them moreover criticizes the used tools: According to him, the often used Microsoft Excel sheets do not support efficiency and reuse.

3.2.4 Challenges of the industrial application of safety analysis

In summary the challenges and approaches of all the interviewees are very similar. They all see both: the need for and the potential of improvement of the whole safety analysis process. However, they do not identify the challenges within the methods of safety analysis. Instead, they state, that the major challenges are located in the whole development process. The main areas of improvement are the following:

- early consideration of safety aspects in design (safety-oriented design)
- increased amount of standard components of modules

- better documentation of safety analyses' results and reduced experience focus
- efficient reuse of safety analyses through documentation and better support

3.3 Discussion

In the following we discuss the results of the interview study in comparison to the findings of the literature review. We moreover highlight the impact of these challenges in the context of an increasing amount of individual consumer products.

3.3.1 Findings of literature and interviews in comparison

The results of the interview study show, that the interviewees are all facing similar challenges and apply similar methods. Thus, we do not expect additional value of a larger sample and further interviews.

In the interviewees' companies traditional methods of safety analysis are commonly applied. However, the development usually is not safety-centric and the safety analysis is more or less conducted review-based. Same as in the state of science, the experts demand for an early integration of safety aspects and safety analyses in the design process. Model-based approaches are expected to improve this situation, but are not applied consequently yet.

Moreover, the interviewees all criticize the experience-based and inefficient use of safety analysis methods. They mainly demand for better documentation. While the results usually are documented in reports, the connected knowledge remains implicit expert knowledge. The better documentation could be achieved by model-based methods and especially in connection with formalized analyses. This non-sufficient documentation of knowledge seems to be the most important limitation of current safety analysis practice. Yet, this aspect is not in the focus of the approaches discussed in section 2.

Moreover the analysis shows, that according to the experts an increased amount of standard components can also improve the efficiency of safety analysis. This aspect is not addressed by the research discussed in the state of science. It exceeds the aspects of safety analysis and moreover emphasizes the dependency of safety analysis and product architecture. However, facing increasing demands of individual products, the sole standardization cannot be the solution. Thus, the challenge is to find the right balance of standardization and individual components and to consider safety aspects early during the definition of the product architecture.

Figure 2 contrasts the challenges identified in the literature review (section 2.2.1) with the challenges raised from the interview study. The aspects of early integration and improved efficiency are confirmed. While the gap between disciplines is not considered that relevant, the interviews point out the challenges of safety-oriented architectures and improved knowledge documentation.

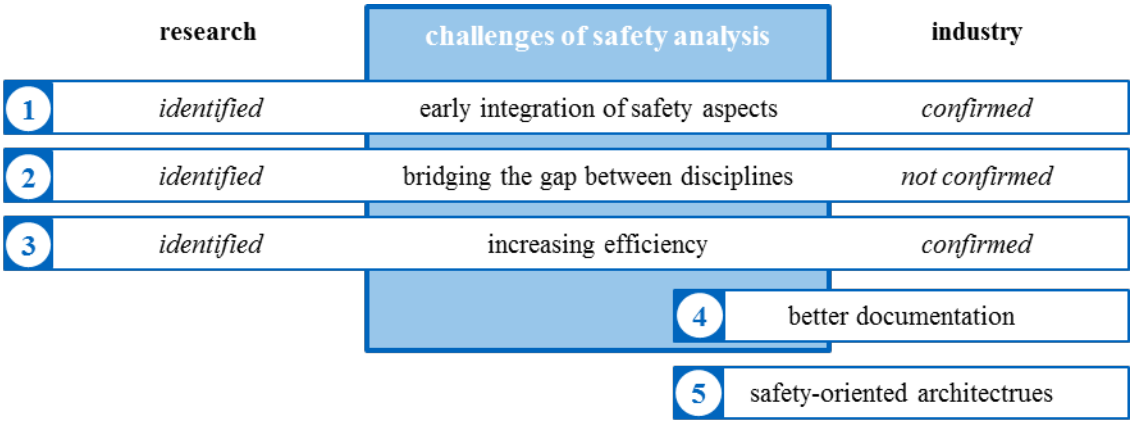

Figure 2. Challenges of safety analysis in research and industrial application

3.3.2 Challenges under the impact of individual products

The growing demand for individual mass products has a strong impact on the challenges identified in research and literature:

1. The literature review and interviews show, that the early integration of safety aspects in product design is complicated. However, to efficiently realize individual products, the individual variants should be generated as late as possible (Piller, 2006). The expected benefits of an early safety

analysis, thus can be diminished by propagation effects which are induced by individual changes. Moreover, a safety-centric design process is hardly possible, as the design space offered to the customer should not be limited too much in advance.

2. The bridging of the gap between disciplines in the current state is not an essential challenge. We pointed out the importance of an optimized architecture, but we do not expect a significant change of this challenge due to a switch to more individual products
3. Increasing the efficiency gets crucial. To realize individual products, the process of safety analysis and approval for each individual product has to be as efficient as possible. This will require a consistent strategy of reusing and harmonizing previous results of safety analyses. By that, the individual changes can be prepared from the perspective of safety analysis. In this context formal analysis methods can help to improve the efficiency. Without these measures, individual products might not be able to compete with mass products.
4. To achieve the effects described in the previous challenge, a better documentation of safety knowledge will be essential. Without this, a reuse of analyses is hardly possible.
5. A safety-oriented architectures and a higher standardization might cause conflicts with the increased demand for individual products. Thus, additional efforts should be invested in the optimal definition of product architecture and standard components. In that context, the early consideration of safety aspects as described in the first point is beneficial.

The effects for individual mass products will, from our point of view, be amplified by the trend of user innovated products (Hippel, 2001). Within this approach, the customers are enabled to design and innovate the products on their own. This can reduce the company's design efforts for individual products. Thus, the role of product architecture definition and product preparation gets more and more important. Also the safety analysis of the customer's individual designs will get challenging, but essential. As this contradicts the practical approach of designing the product from the beginning according to norms and guidelines, the design strategy of the companies will have to change.

4 CONCLUSIONS AND OUTLOOK

This paper discusses current practices and challenges of the safety analysis within the development of mechanical and mechatronic products. The literature review shows, that challenges are identified and solutions are developed. However, the industrial application recorded in an interview study does not confirm all of these challenges. The traditional methods FMEA and FTA are widely spread, but newer methods and strategies are mostly not in use.

Especially in the context of a growing amount of individual mass products, our paper identifies the most relevant fields of action, which in summary are:

- early integration of safety aspects in the product development process to define product architectures and standard components which simplify subsequent safety analyses
- improved efficiency and documentation of safety analyses to support the reuse of previous results

Even though, the interview results showed strong similarities between the different companies, the selection of interviewees from safety experts only limits the overall validity of the results. To comprehensively analyse the challenges of safety analysis additional interviews with expert designers have to be undertaken in order to integrate their perspective as well. Also the study presented in this paper can only capture the subjective challenges experienced by the safety experts. Challenges which are hidden to them have to be discovered by studies with another research methodology.

These findings arise many fields for further research: Methods and strategies to better integrate safety aspects in the design process have to be researched. I.e. in case of a switch to user innovated products, the whole design process has to be adapted. First considerations have been made in Holle and Lindemann (2014) who developed a framework to support the transfer of an existing product to a product suitable for user innovation. Our further research will find solutions how safety aspects can be integrated in such concepts.

Moreover, research has to find solutions, how the documentation and reuse of safety analyses can be improved in industrial application. As the interview shows, existing approaches are not yet applied in daily work.

Finally, a thoroughgoing concept will be needed, which supports all phases from the early consideration of safety to the final efficient safety analysis and consolidates all involved knowledge.

REFERENCES

Ben-Daya, M. (2009), "Failure Mode and Effect Analysis", in Ben-Daya, M., Duffuaa, S.O., Raouf, A., Knezevic, J. and Ait-Kadi, D. (Eds.), *Handbook of Maintenance Management and Engineering*, Springer London, London, pp. 75–90.

Biehl, M., Chen, D.-J. and Törngren, M. (2010), "Integrating safety analysis into the model-based development toolchain of automotive embedded systems", *LCTES*, pp. 125–132.

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

Eckert, C., Clarkson, P.J. and Zanker, W. (2004), "Change and customisation in complex engineering domains", *Research in Engineering Design*, Vol. 15 No. 1, pp. 1–21.

Ericson, C.A. (Ed.) (2005), *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, Inc, Hoboken, NJ, USA.

Herfeld, U., Fürst, F. and Braun, T. (2007), "Managing complexity in automotive safety development", in Lindemann, U., Danilovic, M., Deubzer, F., Maurer, M. and Kreimeyer, M. (Eds.), *Proceedings of the 9th International DSM Conference, München, 16.10. - 18.10.2007*, Shaker, Aachen, pp. 271–286.

Hippel, E. von (2001), "Perspektive: User toolkits for innovation", *Journal of Product Innovation Management*, Vol. 18 No. 4, pp. 247–257.

Höfig, K., Zeller, M. and Grunske, L. (2014), "metaFMEA-A Framework for Reusable FMEAs", in Ortmeier, F. and Rauzy, A. (Eds.), *Model-Based Safety and Assessment*, *Lecture Notes in Computer Science*, Vol. 8822, Springer International Publishing, pp. 110–122.

Holle, M. and Lindemann, U. (2014), *Design for Open Innovation (DfOI) – Product Structure Planning for Open Innovation Toolkits, International Conference on Industrial Engineering and Engineering Management*, Selangor.

IEC (2006a), *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)* No. 60812, 2nd ed., International Electrotechnical Commission, Geneva.

IEC (2006b), *Fault tree analysis (FTA)* No. 61025, 2nd ed., International Electrotechnical Commission, Geneva.

Jensen, D.C. and Tumer, I.Y. (2013), "Modeling and Analysis of Safety in Early Design", *2013 Conference on Systems Engineering Research*, Vol. 16, pp. 824–833.

Jiang, X., Liang, S., Ding, W. and Wang, W. (2007), "Research on Quality Management System for Individualized Customization Based-Customer Satisfaction", Jinan, China.

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

Li, G. (2012), "Ontology-Based Reuse of Failure Modes for FMEA: Methodology and Tool", Dallas, TX, USA.

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

Majdara, A. and Wakabayashi, T. (2009), "Component-based modeling of systems for automated fault tree generation", *Reliability Engineering & System Safety*, Vol. 94 No. 6, pp. 1076–1086.

Maurer, M. and Kesper, H. (2011), "eFMEA— Raising Efficiency of FMEA by Matrix-Based Function and Failure Networks", paper presented at 3rd International Conference on Research into Design, 10.01. - 12.01.2011, Bangalore.

Mhenni, F., Nga Nguyen, Kadima, H. and Choley, J. (2013), "Safety analysis integration in a SysML-based complex system design process", Orlando, FL.

Mhenni, F., Nguyen, N. and Choley, J.-Y. (2014), "Automatic fault tree generation from SysML system models", 08.07.-11.07.2014, Besacon.

Papakonstantinou, N., Sierla, S. and Koskinen, K. (2011), "Generating and validating product instances in IEC 61131–3 from feature models", Toulouse, France.

Piller, F.T. (2006), *Mass customization: Ein wettbewerbsstrategisches Konzept im Informationszeitalter,* 4th ed., Deutscher Universitätsverlag, Wiesbaden.

Roland, H.E. and Moriarty, B. (Eds.) (1990), *System Safety Engineering and Management*, John Wiley & Sons, Inc, Hoboken, NJ, USA.

Sierla, S., Tumer, I.Y., Papakonstantinou, N., Koskinen, K. and Jensen, D. (2012), "Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework", *Mechatronics*, Vol. 22 No. 2, pp. 137–151.

ACKNOWLEDGMENTS

We thank the German Federal Ministry for Economic Affairs and Energy for funding this work as part of the collaborative research project "InnoCyFer - Integrierte Gestaltung und Herstellung kundeninnovierter Produkte in Cyber-Physischen Fertigungssystemen".