INTERNATIONAL DESIGN CONFERENCE - DESIGN 2016
Dubrovnik - Croatia, May 16 - 19, 2016.

A METHOD TO EXPLICATE SAFETY FUNCTIONS

M. Roth, C. Muenzberg and U. Lindemann

Keywords: safety analysis, modelling, functional modelling, TRIZ

1. Introduction

Current markets put companies under pressure to offer even more variants and individual products. Simultaneously the complexity of these products is increasing [Piller 2006], [Lindemann et al. 2008]. But also safety aspects are gaining more and more importance and safety regulations are getting stricter (e.g. ISO 26262) [Leveson 2012]. The combination of all these trends causes increasing efforts to successfully run through the processes of safety analysis and approval for each new developed variant or individual adaption [Roth et al. 2015]. At the current stage safety analyses are mainly done review-based with focus on late stages of design. This might lead to late and expensive changes and rework cycles [Sierla et al. 2012]. Thus, recent publications demand for a consideration of safety aspects starting from the early stages of the design process [Sierla et al. 2012], [Leveson 2012], [Berres and Schumann 2014a]. Other studies show that this strategy is not sufficiently implemented in industrial application [Berres and Schumann 2014a], [Roth et al. 2015]. Especially gaps between the fields of safety and design and a need for the explication of safety knowledge are identified [Biehl et al. 2010], [Jensen and Tumer 2013], [Berres and Schumann 2014a], [Roth et al. 2015]. Overcoming these challenges in early design stages can help to reduce the overall efforts and handle the increasing complexity.
Therefore this paper develops a method to explicate and model safety in early stages of design. It integrates safety considerations in modelling methods applied during these stages. It also supports them by introducing an extended understanding of safety functions. It aims to close the gap between designers and safety engineers and to contribute to the successful shift of safety considerations to early stages.
In the following we discuss and define the key terms of safety and highlight current practices and challenges in this field. We then introduce the main basic product models in early stages of design and present existing extensions addressing safety aspects. Based on this, the requirements on an improved method are derived and our improved method is presented. Each modelling step is deduced and explained in detail. The applicability of the method is tested in an industrial case. Finally the paper concludes and gives an outlook on further research.

2. Background

This chapter introduces the key terms of safety and highlights the connected challenges. An overview of product modelling methods is then given before their extensions, which include safety considerations, are presented.

2.1 Key terms and definitions

To understand the addressed challenges and the developed method it is necessary to provide a common understanding. Therefore the following paragraphs introduce and define the terms of "safety", "mishap" and "hazard".

2.1.1 Safety

Depending on the background multiple interpretations of the term "safety" exist. To make safety knowledge explicit it is first of all important to understand what safety is.

According to the widely spread MIL-STD-882E, 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" [DoD 2012]. This definition is consistent with Leveson who considers safety as "freedom of accidents" [Leveson 2012].

Yet, considering safety from application perspective, the total freedom cannot be achieved. This aspect is considered by Neudörfer. According to him, safety is an immaterial system property. It describes that in the expected product life cycle hazards are limited to an acceptable risk [Neudörfer 2014]. This thought is shared by Jensen and Tumer who also define safety as system property which is measured by the relative difficulty for safety constraints to be violated [Jensen and Tumer 2013].

These definitions are not contradictory but focus on different aspects. This paper uses the definition of Jensen and Tumer, as it considers the remaining risks and establishes the link to safety requirements.

2.1.2 Mishap/Accident

The previously described safety tries to avoid or exclude specific situations. Aligning with the definition of safety, e.g. the MIL-STD-882E calls an event or series of events that results in the consequences precluded in the definition of safety a mishap [DoD 2012]. Accident is defined as "undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, etc.)" [Leveson 2012]. As both definitions are consistent, the terms of mishap and accident can be treated as synonyms. In this paper the term mishap will be used.

2.1.3 Hazard

The system state or set of conditions that will result in an accident [a mishap] is called hazard [Leveson 2012]. Consistent with this, the MIL-STD-882E emphasizes the potential nature of this state [DoD 2012]. Also Neudörfer includes this potential aspect and defines a hazard as potential state which includes a latent or virulent material or energetic potential which, when freed, can lead to an accident [Neudörfer 2014]. As this paper focusses on abstract modelling in early phases, this definition is most suitable and will be used in the following.

2.2 Practices and challenges in safety engineering

For the safety analysis of products various methods are applied. Recent studies identified that the Fault Tree Analysis (FTA), the Failure Mode and Effect Analysis (FMEA) and the Preliminary System Safety Analysis (PSSA) are most common [Berres et al. 2014b], [Roth et al. 2015]. However, especially the FTA and FMEA are often performed review-based [Jensen and Tumer 2013] and in late stages only [Cuenot et al. 2014].

However, as mentioned in section 1, many researchers, e.g. [Leveson 2012], [Sierla et al. 2012], demand for an early integration of safety considerations in the design process to cope with increasing complexity and requirements. This can reduce rework cost and late changes. Especially in the context of increasing customization, a suitable preparation and efficient analysis of safety gains in importance [Roth et al. 2015]. To achieve this, it is important to integrate safety considerations in early stages. However, a gap is identified between the domains of safety engineering and system design [Biehl et al. 2010]. Other studies confirm this and especially point out the need to explicit safety knowledge [Jensen and Tumer 2013], [Roth et al. 2015].

In summary, the two major challenges in safety are to achieve an early integration and to explicit safety knowledge. To achieve this, safety considerations should be integrated in methods used in early design stages in a way which helps to make the connected safety knowledge explicit.

2.3 Functional and structural modelling in early design stages

A key method of early design stages is the description and formulation of an abstract problem and its decomposition. One of the most important methods in these early design stages are functional or structural models [Pahl et al. 2007], [Lindemann 2009].

Therefore various modelling methods are established. In their core they all use an abstract description of functions and their interrelations to draft a solution concept. These functional structures occur with minor variations in all basic works on engineering design (e.g. [Ulrich and Eppinger 2004], [Pahl et al. 2007], [Lindemann 2009]). The main variation lies in the type and detail level of interrelations. For example, it is suggested to model the functional structure by using flows of material, energy and information [Pahl et al. 2007].
Also TRIZ uses similar methods to model abstract problems. From structural perspective TRIZ Function Analysis describes the functional behaviour of a technical system. Based on the identification of all relevant components (Component Analysis) and their interaction in the sense of physical contact (Interaction Analysis) the functional model (Functional Modelling) is build [Münzberg et al. 2014]. A problem-specific model can be derived with the help of TRIZ Substance-Field-Analysis (Su-Field Analysis). The resulting models describe single problem situations (e.g. harmful functions or insufficient/excessive functions). Generic solutions for these problems are proposed by 76 Standard Inventive Solutions [Altshuller 2004], [Belski 2007]. Both approaches use fields as representation of interaction between system elements. These fields have a wider scope than in classical physics. Valid fields are Mechanical, Acoustic, Thermal, CHemical, Electric, and Magnetic, Intermolecular, and Biological fields abbreviated with MATChEMIB [Belski 2007].
As alternative to the flow- or field-based interrelations, Lindemann picks up the idea of Terninko et al. [1998] and suggests a relation oriented modelling approach. Instead of flows, this method models supportive relations and causalities [Lindemann 2009].
Extending classical engineering design, in systems engineering the most common modelling method is the Systems Modeling Language (SysML). It is a graphical modelling language and allows to specify, analyse, design, verify and validate complex systems. It aims to improve development, communication and information management. Similar to the previously described methods, it distinguishes structural and behavioural diagrams. Structural aspects are mainly modelled in block diagrams. Behavioural aspects are modelled mainly by activity, sequence and state machine diagrams. Between the model elements, transitions, allocations and flows can be modelled [Weilkiens 2007], [Friedenthal et al. 2015].

2.4 Models explicating safety aspects

Building on the previously described basic modelling methods, some approaches help to make safety aspects explicit in early design phases.
The mentioned relation oriented functional modelling distinguishes between harmful and useful functions. It is usually applied during the problem formulation. There it helps to identify all relevant functions, useful and harmful, in a structured way by providing standard questions [Terninko et al. 1998], [Lindemann 2009]. This method inherently models safety functions: functions which inhibit harmful functions could be considered safety functions. However, harmful functions are defined in a wide scope. They do not have a necessary link to hazards as they can also represent e.g. inefficiencies. Moreover, the link to structural models and a decomposition of safety functions is difficult to model.
Also the TRIZ models have extensions or features which help to consider safety aspects: Using the Su-Field Analysis, it is possible to systematically identify and analyse possible failures [Belski et al. 2013]. In their approach Belski et al. point out, the major advantage: the MATChEMIB fields cover most phenomena [Belski et al. 2013]. Thus, these fields help to achieve completeness and identify all possible failures. However, following their approach, it is necessary to add auxiliary fields to the model in order to identify all possible failures [Belski et al. 2013]. Thus, this approach successfully makes failure and safety knowledge explicit in a systematic and very complete way.
The advantages and value of Su-Field Analysis is also acknowledged by other researchers. E.g. Regazzoni and Russo propose a methodology to improve and simplify FMEAs by the application of the Su-Field Analysis [Regazzoni and Russo 2011]. They identify critical situations (similar to mishap) and model these in substance-field models. These models are then used to derive preventive or corrective measures, which can be seen as safety measures.
Developed for complex systems, also SysML has extensions which address safety issues. E.g. Biggs et al. extend the standard SysML to model safety and design information conjointly [Biggs et al. 2014]. Their profile SafeML increases the traceability and consistency between both aspects. They model

design information with standard SysML and introduce seven elements to model the safety information in block definition diagrams. This includes hazards and possible transitions to mishap as well as measures to detect and prevent those [Biggs et al. 2014]. The SafeML thus, is a powerful tool to model structural safety aspects. Yet, it does not consider the functional architecture and requires a detailed model. Furthermore, it requires formal SysML modelling and does not provide systematic modelling support. Also Jensen and Tumer use SysML to model safety in early design [Jensen and Tumer 2013]. They introduce the concept of safety functions which prevent the transition from hazard to mishap. These functions are derived from hazards and consist of control structures (sensors, controllers, actuators and the process). However, this structure leads to the constraint that a safety function is not decomposable. Also low level functional failures cannot be mapped to these safety functions. But to support the systematic modelling, they provide a 6-step support process for safety centric design [Jensen and Tumer 2013].
In summary, some existing methods provide simple modelling but lack of sufficient and simple explication of safety aspects and the linkage of structural and functional domain. Other methods provide extensive modelling of safety aspects but require detailed models and focus on active safety functions only. A modelling method which combines early design phase models with a complete modelling of safety functions is missing in the state of the art.

3. Approach to explicate safety functions

In the previous sections existent methods to explicit safety in product models were introduced. We highlighted their strengths and weaknesses and derived a need for further improvement of these existing methodologies. Based on this, we adapted existing methods to develop our approach. In the following, we first introduce our methodology including the requirements on our approach. Then, the approach and made adaptions are explained step by step.

3.1 Methodology

To develop the approach we consolidated the works discussed in section 2 to derive major requirements on an approach explicating safety. This resulted in the following core and optional requirements:

- Safety aspects have to be modelled starting from the early phases of design [Biehl et al. 2010], [Sierla et al. 2012], [Berres and Schumann 2014a]. Therefore, it is important to integrate safety aspects in methods applied to early design stages. This results in the requirement: "Safety aspects shall be included in functional and structural modelling."
- Between designers and safety engineers is a gap in the understanding of safety aspects and the connected knowledge [Roth et al. 2015]. The modelling of safety functions helps to arise awareness for all safety aspects and helps to define safe concepts. This results in the requirement: "Safety functions shall be explicated in functional modelling."
- The product architecture includes the allocation of functional and structural architecture [Ulrich 1995]. Failures (causes of mishap) occur on structural level [Jensen and Tumer 2013]. Both aspects result in the requirement: "The link of components to hazards and safety functions shall be modelled."
- Additionally system modelling is strongly influenced by uncertainties [Boardman and Sauser 2006]. Therefore, an optimal modelling approach helps to minimize them and to eliminate model failures. This results in the optional requirement: "Impact of uncertainties shall be reduced."

Based on these four requirements, we evaluated the models and methods introduced in section 2. The most suitable approaches we identified and selected are the relation oriented function structure [Terninko et al. 1998], [Lindemann 2009] and the modelling of safety functions [Jensen and Tumer 2013]. However, to completely satisfy the requirements both approaches have been combined and further adapted.
The development of the resulting approach was conducted on two models: An abstract model of a hand mixer and a partial model of a fully automated coffee machine. Then the approach was applied and tested with the full model of the coffee machine, which will be described in section 4 in detail. The graphical notation and models were implemented using Soley Desk (www.soley-technology.com).

3.2 Solution approach

In the following, the resulting solution approach is presented. First, an overview is given and the term safety function is redefined. Then each of the five steps is derived and explained in detail.

3.2.1 Overview and definitions

As one main objective of the approach is to make safety functions explicit, it is necessary to first define what a safety function is. Thereby we build on the interpretation of Jensen [Jensen and Tumer 2013] but extend and adapt it in two aspects. Those aspects aim to ensure the link to components and low level failures and to also cover passive safety measures. This results in the following definition of safety functions:

- Safety functions either prevent the system's transition from hazard to mishap or maintain the current system state (in compliance with [Jensen and Tumer 2013]).
- Safety functions can be decomposed.
- Safety functions can manifest in multiple components, with multiple principles and as passive features or active control structures.

Building on this understanding of safety functions, the approach comprises five steps (see Figure 1): (I) preparation of the product model, (II) modelling of flows, (III) mapping of hazards, (IV) elicitation of safety functions and (V) verification of the model. In the following each step is explained and reasoned. For the models, we use the notation also indicated in Figure 1.

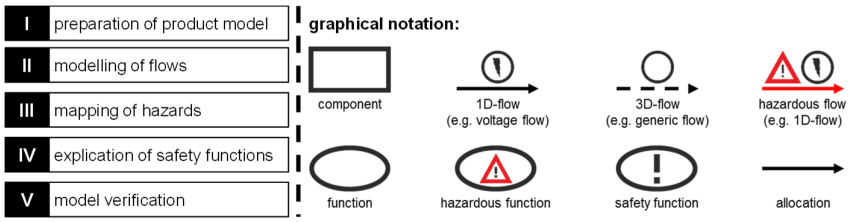

Figure 1. Modelling steps (left) and model notations (right)

3.2.2 Step I: Preparation of product model

The first step of the modelling approach prepares the required data and product models. This includes all basic tasks of system modelling. I.e. to define scope, systems boundaries and analysis granularity.
Following the basic definition [Ulrich 1995], [Göpfert 2009], the product architecture includes both, the functional and structural decomposition as well as their linkage. For the modelling approach, both structures should be decomposed and modelled up to the chosen level of granularity. Various support is available therefore (e.g. in the basic works [Ulrich and Eppinger 2004], [Pahl et al. 2007], [Haberfellner 2012]). At this point the procedure slightly differs from the TRIZ Functional Modelling as the component and functional structures are modelled simultaneously.
To explain the approach in each step of the approach the example of a hand mixer is used. In Figure 2 this exemplary product is shown. The figure also depicts excerpts of both structures and indicates the system boundaries of the example used in the following.

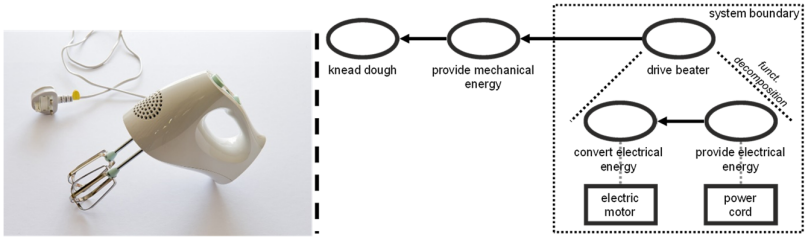

Figure 2. Example hand mixer (left) and its functional & structural model

Besides the product models also relevant safety data needs to be acquired in this step. According to the definition of safety given in section 2.1.1, transitions to mishap have to be avoided. Therefore, possible

hazards have to be identified and collected. Existing norms and standards provide support (e.g. checklists) for this task. For example, ISO 12100 provides an extensive list of existing hazards. Often also internal hazard checklists exist in companies which are constantly updated and adapted. The hazards relevant for the hand mixer example can be extracted e.g. from the norm EN 60335. To supplement these standards other support methods exist: The Preliminary Hazard Analysis [Roland and Moriarty 1990] for example helps to systematically identify relevant hazards of the considered system.

3.2.3 Step II: Modelling of flows

Complementing the product architecture the second step of the approach models interactions between components through flows. This has two reasons: First, failures in a product occur on component level [Jensen and Tumer 2013]. As failures are the relevant threat to safety, the component level is the major focus when explicating safety. Second, risks occur on interactions of components or of components with the environment [Ghemraoui et al. 2009]. Therefore it is stated, that interactions of fields and substances help to systematically identify all possible failures [Belski et al. 2013].
Extending the Su-Field perspective and to better model complex mechatronic systems, the approach integrates the concept of energy, material and information flow [Pahl et al. 2007] and the principle of substances and fields [Belski 2007]. The approach thus allows to model two types of flows:

- 1D-flows (energy/material/information) corresponding to "substances" which are bound to a local interaction. Examples of this type of flow are electrical control signals or mechanical torque on a shaft.
- 3D-flows model flows which spread more or less freely. They correspond to the fields of the Su-Field Analysis. Thus, the "MATChEMIB"-phenomena support to distinguish the two types of flow and their modelling.

In summary, the major task of this step is to systematically analyse components on their interactions and to model those as 1D- and 3D-flows. Thus, it is important to also include all interactions with the environment. Especially 3D-flows like heat or electromagnetic fields play an important role for safety.
The modelling of flows of the hand mixer example results in the model shown in Figure 3. There, the previously described 3D interactions with the environment can also be seen.

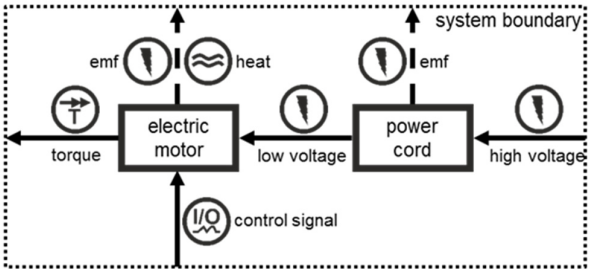

Figure 3. Structural model of the hand mixer with 1D and 3D-flows

Once the flows are modelled, they can be transferred to the functional structure when needed. This can easily be achieved via the allocation of functions to components. However, if done in graphical form this can significantly reduce the clarity of the visualization.

3.2.4 Step III: Mapping of hazards

As stated in the previous step, risks occur on interactions, which therefore help to systematically identify possible failures [Ghemraoui et al. 2009], [Belski et al. 2013]. Thus, this step analyses the modelled flows in detail. Each flow is examined on its risks (i.e. hazards) by comparison with the collected possible hazards. If the flow bears a hazard, this hazard is added to the model. At this point it is important to note, that of course a flow can bear multiple hazards, but that it is also possible that it bears no hazard at all. For the hand mixer example, Figure 4 visualizes the identified hazards.
Via the allocation of functions to components described in the previous step, potential hazardous functions can be identified. A hazardous function is a function which, if executed, directly or indirectly

can lead to a mishap. These functions are assigned to the corresponding regular functions and temporarily added to the functional structure. This temporal assignment can also be seen in Figure 4.

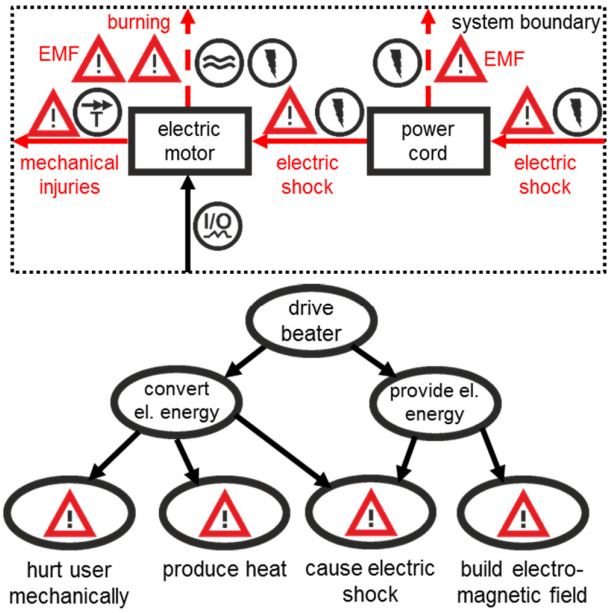

Figure 4. Hazards allocated to flows in the structural model (top) and hazardous functions allocated in the functional structure (bottom)

3.2.5 Step IV: Explication of safety functions

Building up on the identified hazards, the fourth step makes the safety functions explicit. Systematically for each hazardous function at least one safety function has to be defined, which prevents the transformation from hazard to mishap. These safety functions have to be allocated on the same decomposition level as the corresponding hazardous function and should be linked to the hazard they address. Once this is done, the hazardous functions can be removed from the functional structure as they now represent redundant information. The resulting functional structure is visualized in Figure 5.
With defined safety functions, their allocation to the structural elements remains. Based on the hazards and flows, safety functions are assigned to their realizing components. It is important to note that a safety function can be very generic. For example to avoid the hazard electric shock, the safety function "isolate current" can be defined. This function can in return be realized simultaneously by multiple components within the product. But also different safety functions can be used. For the electric shock, for example prevent contact could be an additional safety function reducing the connected risk. This underlines the need for a definition of safety functions, which allows their composition.

3.2.6 Step V: Model verification

With the modelled safety functions from step IV, the initial goal of the approach of explicating and integrating safety in early modelling is achieved. However, modelling is strongly influenced by uncertainties and inconsistencies [Boardman and Sauser 2006]. Therefore, the final step aims to prevent the model-"hazard" of wrong assessment due to model failures. It tries to identify and eliminate inconsistencies in by applying pattern-based rules. For the elicitation of safety functions, we suggest the following rules:

- Global safety: All hazards identified in the model should be connected to a safety function preventing them from transition to mishap.
- Local safety: Either the components connected to a hazardous flow have to fulfil at least one safety function addressing that hazard or one of the components connected to the flow has to fulfil a safety function which minimizes the risk of the hazardous flow.

Extending these patterns, depending on the specific application, further rules may apply. Generic examples are the continuity of flows or the conservation-of-energy principle.

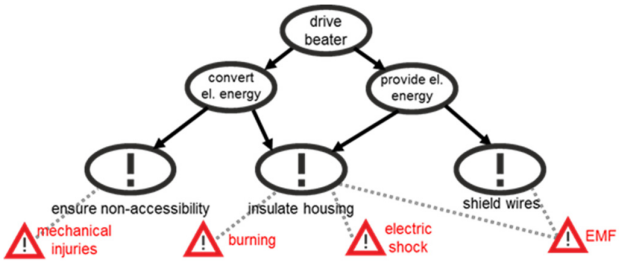

Figure 5. Safety functions in the functional structure with corresponding hazards

4. Application

To validate the developed modelling method, it was applied to model the functional structure of a fully automated coffee machine.

4.1 Application of the approach

The preparation (step 1) consolidated the Bill of Material with it's over 1000 components to a suitable level of abstraction with 84 components or assemblies. They realize the 53 functions (total decomposition tree) of the coffee machine. Moreover, based on the experience of the industrial partner and based on relevant norms and standards, 16 hazards were identified.

In step II, the flows between components are identified. We chose a medium abstraction level and modelled 16 flows. The focus was laid on material flows and e.g. information flows were condensed to "control signal". The model thus mainly consists of 1D-flows, and few 3D-flows (e.g. heat and emf).

In step III the hazards were assigned to flows ad hazardous functions were derived. By that, within the 53 product functions, 46 with hazardous potential were identified.

For those hazardous functions, step IV defines 20 safety functions and assigns them to components. These 20 functions include many functions which in the functional decomposition are assigned to multiple parent functions. They are thus also assigned to various components. For example, the function "avoid contamination of beverage with hazardous material" has to be assigned to all components involved in the brewing process and the delivery of the coffee.

The modelled safety functions were verified using the previously introduced local and global safety patterns and also the continuity of flows was checked to improve the model quality.

When safety functions which are assigned to multiple regular functions are split to unique instances, the lowest level of our functional decomposition includes 64 branches. It is illustrated in Figure 6.

4.2 Discussion of the application

The results of this previously described application of the approach were discussed with a safety expert and a designer of the coffee machine company. Also the results were compared to a functional modelling conducted with a prior model of the coffee machine.

First of all, the requirements formulated in section 3.1 are all satisfied. The approach supports the modelling and explication of safety functions/aspects in models of early design phases and it links safety aspects to both, functional and structural models. Furthermore, the discussion with the experts clearly identified the following advantages of the methodology.

It helps to improve the completeness of the model by explicating many safety aspects. For example some hazards are usually not considered by the designers and the safety expert reported that he had to remind the designers in some cases that e.g. the housing will heat up and this has to be considered during the design.

Also advantageous is that the safety functions are integrated in the regular functional decomposition. Previously, the functional decomposition modelled safety functions under a separate main function. The developed approach systematically integrates the safety functions into the functional decomposition.

This combines both, safety and design aspects. This makes safety functions explicit to designers. But also reusability considerations are simplified: The functional decomposition includes only branches which are "safe" as they include all relevant safety functions in the tree.

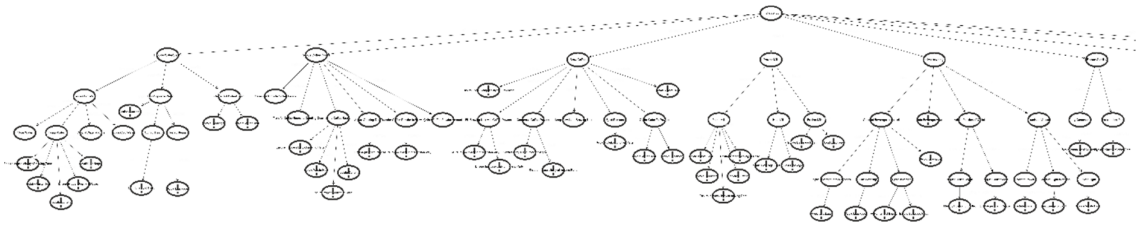

Figure 6. Functional structure (extract) of coffee machine with explicated safety functions

5. Outlook and conclusions

This paper introduces a modelling method which helps to explicit safety knowledge and model safety functions. It therefore unites existing methods and improves the concept of safety functions hand in hand with a simple modelling method.

The major advantages of the method identified during the application and development are:

- It is tool independent and builds on established modelling methods.
- It introduces an extended concept of safety functions which not only is limited to active safety measures.
- It improves the completeness of the product model through its systematic nature.
- It makes safety aspects explicit and integrates them in product models.

With these benefits our method contributes to a shift of safety considerations to early phases and helps to bridge the gap between safety experts and product designers.

Yet, it is not able to fully solve the connected problems. While it can help to increase the awareness for safety functions in early stages it does not provide quantitative results or specific safety analyses and needs to be complemented by suitable further methods. However, the modelled safety functions and their completeness provide a valuable input for these methods.

Yet, the improved completeness goes on the cost of increased efforts. This contradicts the need for improved efficiency. Still, for a small number of system elements the method easily can be performed manually. Yet, to be efficient on larger systems, suitable tool support needs to be developed.

The extended definition of safety functions allows an abstract and complete modelling. But information on the realization of this safety function is not included in the model. Yet, to profit in later stages, the early consideration has to be transformed to later phases. Support to concretize these abstract representation and to realize them (e.g. active vs. passive) therefore needs to be researched.

Furthermore, a full traceability needs to be achieved and thus it is necessary to include the relevant safety functions in other development methods. For example, it has to be researched how these functions (i.e. safety functions with multiple allocations) shall be considered during modularization or QFDs.

References

Altshuller, G., "And suddenly the inventor appeared - TRIZ, the theory of inventive problem solving", Technical Innovation Center, Worcester, 2004.

Belski, A., Belski, I., Chong, T. T., Kwok, R., "Application of substance-field analysis for failure analysis", Proceedings of the 13th ETRIA World TRIZ Future Conference 2013, Aoussat, A., Cavallucci, D., Trela, M., Duflou, J. (eds.), Arts Et Metiers ParisTech, Paris, France, 2013, pp. 483–490.

Belski, I., "Improve your thinking - Substance-field analysis", TRIZ4U, Melbourne, 2007.

Berres, A., Schumann, H., "Closing the safety process gap: Early integration of safety", Maurer, M. S., Schulze, S.-O. (eds.), Tag des Systems Engineering, München, Hanser, Carl, 2014a, pp. 143–152.

Berres, A., Schumann, H., Spangenberg, H., "European survey on safety methods application in aeronautic systems engineering", ESREL Conference 2014. Worclaw, Poland, 14.09.-18.09.2014, 2014b.

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

Biggs, G., Sakamoto, T., Kotoku, T., "A profile and tool for modelling safety information with design information in SysML", Software & Systems Modeling, 2014, pp. 1–32.
Boardman, J., Sauser, B., "System of Systems – the meaning of of", International Conference on System of Systems Engineering 2006, IEE/SMC (ed.), IEEE, Piscataway, 2006, pp. 118–123.
Cuenot, P., Ainhauser, C., Adler, N., Otten, S., Meurville, F., "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, 05.02-07.02.2014, 2014.
DoD, "MIL-STD-882E: DoD Standard Practice for System Safety", 2012.
Friedenthal, S., Moore, A., Steiner, R., "A practical guide to SysML - The systems modeling language", Elsevier/Morgan Kaufmann, Waltham, MA, 2015.
Ghemraoui, R., Mathieu, L., Tricot, N., "Design method for systematic safety integration", CIRP Annals - Manufacturing Technology, Vol.58, No.1, 2009, pp. 161–164.
Göpfert, J., "Modulare Produktentwicklung - Zur gemeinsamen Gestaltung von Technik und Organisation; Theorie, Methodik, Gestaltung", Books on Demand, Norderstedt, 2009.
Haberfellner, R., "Systems Engineering - Grundlagen und Anwendung", Orell Füssli, Zürich, 2012.
Jensen, D. C., Tumer, I. Y., "Modeling and Analysis of Safety in Early Design", 2013 Conference on Systems Engineering Research, Vol.16, 2013, pp. 824–833.
Leveson, N., "Engineering a safer world - Systems thinking applied to safety", The MIT Press, Cambridge, Mass., 2012.
Lindemann, U., "Methodische Entwicklung technischer Produkte - Methoden flexibel und situationsgerecht anwenden", Springer, Berlin, 2009.
Lindemann, U., Maurer, M. S., Braun, T., "Structural Complexity Management", Springer, Berlin, 2008.
Münzberg, C., Hammer, J., Brehm, A., Lindemann, U., "Further Development of TRIZ Function Analysis based on Applications in Projects", Proceedings of the DESIGN 2014 13th International Design Conference, Marjanović, D., Štorga, M., Pavković, N., Bojčetić, N. (eds.), Design Society, Glasgow, 2014, pp. 333–342.
Neudörfer, A., "Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG-Maschinenrichtlinie", Springer, Berlin, 2014.
Pahl, G., Beitz, W., Feldhusen, J., Grote, K.-H., "Engineering Design", Springer, London, 2007.
Piller, F. T., "Mass customization - Ein wettbewerbsstrategisches Konzept im Informationszeitalter", Deutscher Universitätsverlag, Wiesbaden, 2006.
Regazzoni, D., Russo, D., "TRIZ tools to enhance risk management", Procedia Engineering, Vol.9, 2011, pp. 40–51.
Roland, H. E., Moriarty, B. (eds.), "System Safety Engineering and Management", Hoboken, NJ, USA: John Wiley & Sons Inc, 1990.
Roth, M., Gehrlicher, S., Lindemann, U., "Safety of Individual Products - Perspectives in the Context of Current Practices and Challenges", Design Organisation and Management, Weber, C., Husung, S., Cascini, G., Cantamessa, M., Marjanovic, D., Bordegoni, M. (eds.), Design Society, Glasgow, 2015, pp. 113–122.
Sierla, S., Tumer, I. Y., Papakonstantinou, N., Koskinen, K., Jensen, D., "Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework", Mechatronics, Vol.22, No.2, 2012, pp. 137–151.
Terninko, J., Zusman, A., Zlotin, B., "Systematic innovation - An introduction to TRIZ ; (theory of inventive problem solving)", St. Lucie Press, Boca Raton, 1998.
Ulrich, K. T., "The role of product architecture in the manufacturing firm", Research Policy, Vol.24, No.3, 1995, pp. 419–440.
Ulrich, K. T., Eppinger, S. D., "Product design and development", McGraw-Hill/Irwin, Boston, 2004.
Weilkiens, T., "Systems engineering with SysML/UML - Modeling, analysis, design", Morgan Kaufmann, Burlington, 2007.

Michael Roth, Dipl.-Ing. M.Sc.
Technical University of Munich, Institute of Product Development
Boltzmannstr. 15, 85748 Garching, Germany
Email: michael.roth@pe.mw.tum.de