The Efficient Safety Concept of the SpeedE Steer-By-Wire System

Christoph **Gillen**, Lars **Hesse**, Matthias **Lammermann**
Forschungsgesellschaft Kraftfahrwesen mbH Aachen, Aachen, Germany

Summary

The Institute for Automotive Engineering (ika) at RWTH Aachen University is developing the research vehicle SpeedE together with its partners. The innovative vehicle concept possesses a wheel-individual steer-by-system controlled by sidesticks. A functional safety concept has been developed which reduces the number of required redundancies compared to known safety concepts to a minimum in order to increase the cost efficiency of such steering systems. This text gives an overview of the identified key factors in the development processes which support the derivation of more efficient safety concepts.

1 Introduction

The research vehicle SpeedE has been developed by the Institute of Automotive Engineering (ika) at RWTH Aachen University since 2011. By putting innovative features of electric vehicles into focus of the design process, the prototype shall display the advantages of this vehicle type beyond zero emission driving. For ika and its partners like Forschungsgesellschaft Kraftfahrwesen mbH Aachen (fka) it is a platform to show new ideas for systems and components, independent of any car manufacturer. The revolutionary design has been developed in cooperation between ika and the School of Design of Pforzheim University. Financial support for this project is offered by the foundation Hans Hermann Voss-Stiftung.

Fig. 1: Research vehicle SpeedE with front suspension and steering actuators

Beside the propulsion which is realized by two wheel-individual electric motors on the rear axle, one of the main topics of research in this context is the innovative steering system. The steer-by-wire system comes with one steering actuator per steered wheel on the front axle allowing large wheel-individual steering angles. The steering wheel as input unit of conventional steering systems is replaced by two sidesticks placed left and right of the driver's seat. In contrast to aircrafts, where fly-by-wire architectures are commonly used, pure steer-by-wire systems without a mechanical fallback layer have never been established in passenger cars, although these systems come with a number of advantages. Legitimately the end customer expects a steering system that is as safe as conventional steering systems, i.e. insensitive to faults of for example power supply. Safety concepts developed based on aviation standards like triple redundancy [5] have turned out to be too expensive for the price sensitive car industry.

For the SpeedE steer-by-wire system a safety concept has been developed which is safe based on the current status of analysis and realized as efficient as possible. The following text overviews the main ideas of the safety concept and describes the process steps supporting the derivation of efficient safety concepts.

2 Efficient Safety Concepts

Functional safety concepts for steering systems of passenger cars are developed based on the functional safety standard ISO 26262. The standard is the adaption of IEC 61508 which defines Functional Safety for electric and electronic systems in a generic, i.e. industry independent way. Effective safety concepts ensure the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems" [2]. Effectiveness can therefore be named as the basic requirement of all functional safety concepts. As described in chapter 1, the automotive industry in particular has high demands regarding product costs, size, weight and reliability. In addition increasingly short development cycles and product diversity request robust and reusable development results including safety concepts. Thus functional safety concepts do not only have to be effective, but efficient, using available resources in the most effective way in order to meet automotive industry's demands.

The functional safety concept is typically handled as an extension to the regular functionality of the system, resulting in multi-layer concepts [3] or component redundancy. Especially the latter one conflicts directly with the abovementioned requirements to keep costs, size and weight low. It is common understanding that domain-centered thinking in the product development has worked against these demands in the past, preventing to take advantage of the capabilities of other domain's components in order to avoid redundancies. Therefore cross-domain alternatives can be considered to be more efficient than domain-centered safety concepts. Safety concepts which are reusable across platforms and architectures reduce development efforts and support proven-in-use argumentations, increasing the efficiency of the concepts.

As pointed out in chapter 1 lacking efficiency of the safety concepts was one of the show-stoppers for introduction of steer-by-wire systems in passenger cars. Presenting a new concept for steer-by-wire the SpeedE steering system takes these demands into account and appears with an efficient functional safety concept. Four key factors for the development of efficient functional safety concepts could be identified during the development process and shall be described in the following.

2.1 Consistent Data Management

As described above an efficient safety concept uses its resources as effective as possible, leading to results which require a minimum of cost, size and weight and providing a maximum of reliability at the same time. In addition reusability and cross-domain approaches have been identified to support the efficiency of safety concepts. Increased efficiency of development products often comes along with increased system complexity which has to be absorbed by a more robust development process. ISO 26262 names a number of processes, which support during the development process. Mentioned in the standard, but not further specified is the consistency of the system information, safety concept and other available data. For an efficient, i.e. reusable cross-domain safety concept consistent data management has turned out to be one of the most important factors.

Making the step from a text and spreadsheet document based to a single source approach increases the manageability of the working data significantly. The single source approach can be handled in different ways: The integration in the requirement engineering tool chain is relatively simple, because no additional tool has to be used. One important factor on the other hand is the link between the different elements (functions, safety requirements, components etc.) and external documents like fault trees or other analysis results. Here other approaches have their strength especially model-based approaches. Several proprietary tools are available on the market. In order to reduce costs for additional tools and fit the data management in the existing tool environment, several manufacturers and suppliers decided to develop company internal solutions based on the Unified Markup Language (UML) [3].

In the development process of SpeedE steer-by-wire the latter approach is chosen. Providing an UML-based environment based on Enterprise Architect to develop models of the functional and technical architecture, the safety concept as well as the functional allocation, it is possible to store all data relevant for the safety concept in one single model file and show different views of the same system based on the chosen abstraction level. In this environment it is possible to visualize information flow, function allocation, links to external elements like fault trees and system requirements as well as safety concepts, including safety requirements and their structure. In addition it is possible to generate text documents from these models, examples are item definitions and safety concept documentation. Fig. 2 gives a visual impression of the available system views.

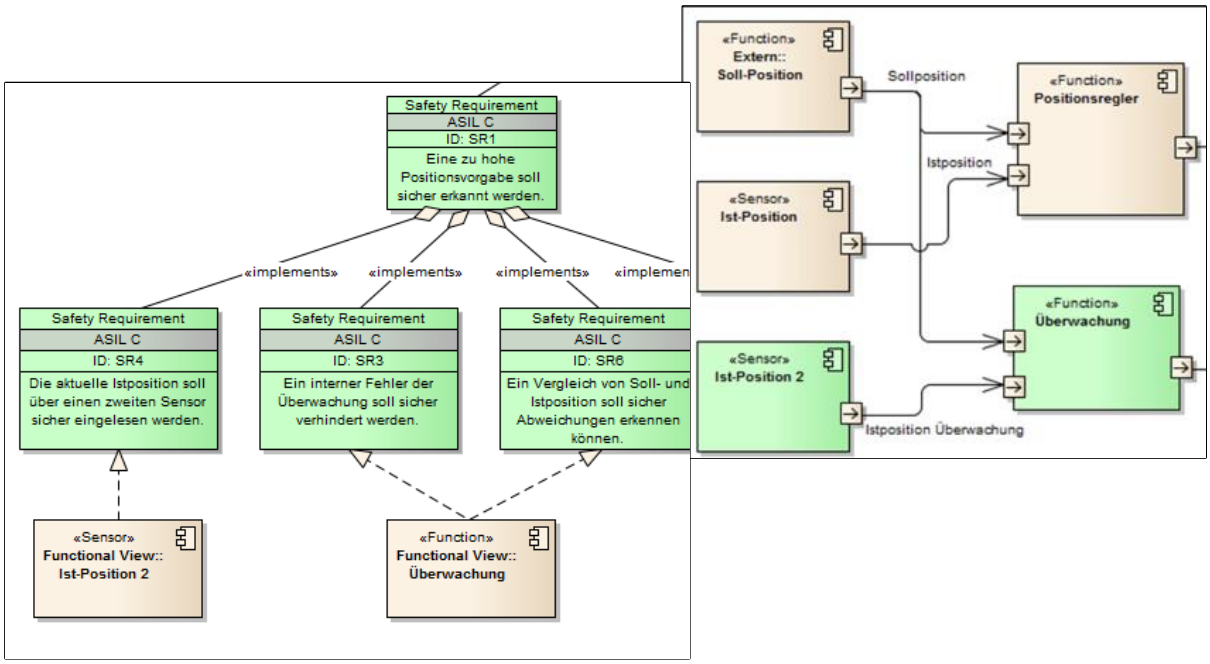

Fig. 2: Example diagrams of the UML environment

A similar approach which can be mentioned in this context is the Component Fault Tree (CFT) approach of Fraunhofer IESE which combines system, fault tree and safety concept modeling in one UML suite. [1]

2.2 Safety Goals

Basis and therefore essential part of the functional safety concept are the so called safety goals. Safety goals are abstract top-level safety requirements and a result of the Hazard Analysis and Risk Assessment (H&R) [2]. During H&R possible hazardous situations resulting from a malfunction of the analyzed system are identified and if safety critical classified by an Automotive Safety Integrity Level (ASIL) reaching from ASIL A (lowest) to ASIL D (highest). Hazardous situations which do not reach ASIL A do not require any additional measures except standard measures of quality management (QM). For each hazardous situation which has been rated ASIL A or higher, a safety goal has to be defined which prevents the hazardous situation to occur. It inherits the ASIL of the hazardous situation defining the recommended techniques and methods to ensure the integrity of the measures defined to reach the safety goal. From the safety goals as abstract top-level requirements safety requirements are derived, which define these measures on lower level. The sum of all safety requirements and their structure form the functional safety concept.

As described above, safety goals are the basis of the safety concept and their correct definition essential for the efficiency of the concept. Considering the function of a headlamp of a passenger car to be safety relevant under certain environmental conditions, the following safety goal could be defined:

A failure of the headlamp shall be prevented.

A safety concept reaching this safety goal might integrate a redundant lamp or a monitoring system for the deactivation function. Another option to define the safety goal could be:

A reduction of the illumination to an unsafe level shall be prevented.

The latter safety goal offers the possibility to make use of the second headlamp, the fog lamps etc. to prevent the hazardous situation to occur saving costs for a second lamp compared to the first example. This simple example shows that some safety goals lead to more efficient safety concepts than others. Therefore the correct definition of safety goals has been identified to be the second key factor in the definition of efficient safety concepts.

The safety goals of the SpeedE steer-by-wire system are defined based on parameters on vehicle level, i.e. for example based on the lateral displacement of the car and not based on the steering angle error. This offers a larger number of opportunities to reach the safety goal and does not limit the solution space needlessly.

	H 3	H 6	H 14	H 15	H 17	H 1	H 2	H 4	H 5	H 13	H 16
S 7	D	D	D	D	D	D	D	D	D	B	B
S 6	C	C	C	C	C	C	C	C	C	B	B
S 8	C	C	C	C	C	C	C	C	C	B	B
S 10	C	C	C	C	C	C	C	C	C	B	B
S 11	C	C	C	C	C	C	C	C	C	B	B
S 1	C	C	C	C	C	C	C	C	C	A	A
S 2	C	C	QM	QM	QM	QM	QM	QM	QM	QM	QM
S 12	B	B	B	B	B	B	B	B	B	A	A
S 3	A	A	A	A	A	A	A	A	A	QM	QM
S 4	A	A	A	A	A	A	A	A	A	QM	QM
S 5	A	A	A	A	A	A	A	A	A	QM	QM
S 13	A	A	A	A	A	A	A	A	A	QM	QM
S 9	QM	QM	A	A	A	QM	QM	QM	QM	QM	QM

Fig. 3: Heatmap of hazardous situation matrix

A safety goal can be assigned to multiple hazardous situations and inherit their highest ASIL. Thereby the number of safety goals can be reduced which can have positive effects on the development efforts of the safety concept as well as the manageability of the safety requirements. On the other hand the inheriting of the highest ASIL may lead to higher development efforts for hazardous situations with the same safety goal and lower ASIL rating. A heatmap of the hazardous situation matrix as shown in Fig. 3 can help to solve the trade-off between number of safety goals and assigned ASIL. The matrix shows the assigned ASIL for the combinations between possible hazards and situations. The colouring and sorting makes it easier to determine groups of hazardous situations and derive reasonable safety goals.

For the SpeedE steering system five safety goals were derived from the results of the Hazard Analysis and Risk Assessment shown in the matrix above (Fig. 3). All safety goals aim to keep the lateral displacement of the vehicle within an acceptable range.

2.3 Derivation of Safety Concept

With definition of the safety goals the basis of the functional safety concept is determined. Third identified key factor in the development of an efficient safety concept is the deductive derivation of safety requirements. Starting from the safety goals safety requirements have to be derived defining measures to fulfill the safety goals. The model-based approach from chapter 2.1 supports this task by depiction of the causal paths within the system. Starting from the negated safety goals as top event deductive analyses like fault tree analyses can be derived following the paths from the actuators where the hazard occurs to the possible causes within the system.

Measures need to be defined working against the violation of the safety goal in order to make sure that no single point or combination with latent fault leads to the occurrence of a critical hazard. The most efficient measures in this context are those which take effect as close to the top event as possible. Because of the nature of fault trees or comparable deductive analyses a measure covers more single point faults, the closer to the top event a measure affects. This is comparable to felling a tree: It is quite ineffective to fell a tree starting to cut down the leaves and the smallest branches. By cutting the branches close to the trunk, the goal is reached with fewer cuts although some of these cuts may require higher effort.

As one example in the SpeedE steer-by-wire system, faulty steering interventions caused by one of the steering actuators are compensated by counter-steering on the other steered wheel and torque-vectoring interventions on the rear axle. Although more complex on the functional side than a redundant steering actuator, this measure covers a large number of possible causes for this hazard and is thus situated close to the top event in the corresponding fault tree. The cross-domain nature (using the wheel-individual propulsion) makes this measure even more efficient, because expensive and bulky redundant actuators as known from other safety concepts for steer-by-wire systems are not required.

2.4 Early Verification

As described above, efficient safety concepts can be more complex than less efficient concepts. Among others the reasons can be found in the possible cross-domain nature and the efforts for single efficient measures. This shows that the most efficient solution is not necessarily the one that is the easiest one to develop. To make sure that the ideas of the safety concept are valid and as less development efforts are wasted as possible, early verification of the safety concept has been identified to be the fourth key factor for efficient safety concepts.

In the verification process several characteristics require special attention:

- Effectiveness
- Timing
- Energy supply
- Common causes
- Integrity of external systems/components

Beside the effectiveness of the measure to be verified, it has to be made sure that the measure can become effective in time. For electrical actuators and other electrical systems the topic of energy supply has to be verified, especially in the context of common cause analyses. Within safety concepts, particularly in those with cross-domain nature, it has to be made sure, that all external systems or components inheriting an ASIL can fulfill the integrity requirements.

In the example of the SpeedE steering system simulations have been made to make sure, that the measure described in chapter 2.3 physically has the potential to counteract faulty steering interventions and to estimate to which extent the measure is effective.

ay / vx	Δδ	0 m/s²	2 m/s²	4 m/s²	6 m/s²	8 m/s²
80 km/h	3.5°	235 ms	150 ms	60 ms	-	-
	2.5°	275 ms	195 ms	125 ms	60 ms	70 ms
160 km/h	3.5°	270 ms	190 ms	-	-	-
	2.5°	295 ms	225 ms	160 ms	80 ms	100 ms

Fig. 4: Simulation results of the reaction time for counter measures

Fig. 4 shows the simulation results for two steering angle errors (Δδ 2.5° and 3.5°) at different vehicle speeds and lateral accelerations. The time values indicate the time to detect the error and initiate the countermeasure, in this case the application of a

differential torque on the rear axle and a countersteering intervention on the other steered wheel. The results show that a steering angle error of 3.5° cannot be compensated under all conditions. The measure can be considered to be effective based on these results, but the limitation of the steering angle error to 2.5° and the timing constraints have to be considered in the safety concept.

3 Conclusion

Steer-by-wire systems come with a number of benefits compared to conventional steering systems in terms of functionality, package and weight. However these systems were never introduced in the market in a large scale. As one of the reasons, costs for the necessary safety measures can be identified. In order to increase the economical attractiveness of such systems it is possible to increase the efficiency of safety concepts without reduction of their effectiveness.

The measures described above show how the efficiency of safety concepts can be increased based on the experience of the SpeedE project. Main idea is to keep the solution space as wide as possible, not to miss efficient measures by a too limited focus in the early concept phase. Supported by a consistent data management and verification, efficient safety concepts can be derived. Applied to the example of SpeedE steer-by-wire these measures lead to a functional safety concept with an increased efficiency compared to concepts which work mainly on component redundancy as described for example in [4] and [5]. By making use of other existing components and systems with the potential to influence the yaw-moment of the vehicle, the number of redundancies can be limited and the appropriate demands in terms of costs, installation space, and weight are reduced.

4 References

[1] ALLMANN, C.; SCHÜSSLER, M.; LANDGRAF, J.
Forschungsprojekt e performance
Modularer Systembaukasten für elektrifizierte Fahrzeuge
Cuvillier Verlag, Göttingen, 2013

[2] International Organization of Standardization (ISO)
ISO 26262
Road Vehicles – Functional Safety
Switzerland, 2011

[3] Object Management Group (OMG)
OMG Unified Modeling Language (OMG UML)
Infrastructure, Version 2.4.1
OMG, 2011 (www.omg.org, 24.07.2014)

[4] WALLENTOWITZ, H.; REIF, K.
Handbuch Kraftfahrzeugelektronik
Grundlagen, Komponenten, Systeme, Anwendungen
Vieweg Verlag, Wiesbaden, 2006

[5] YEH, Y.C.
Triple-triple redundant 777 primary flight computer
Aerospace Applications Conference, 1996.
Proceedings IEEE, Aspen, 1996