

PREPARING THE FUTURE FOR FUNCTIONAL SAFETY OF AUTOMOTIVE E/E-SYSTEMS

Dr. Juergen Schwarz

Functional Safety & E/E-Processes, Daimler AG
Germany

Josef Buechl

System Safety, Audi AG
Germany

Paper Number 09-0445

ABSTRACT

The development of different sensor technologies and powerful signal processing procedures allows the automotive industry to develop new E/E-based safety systems, which may assist and protect drivers and also other traffic participants in very complex situations. The complexity of possible use cases for safety systems on the one hand generates on the other hand a variety of feasible safety concepts to prevent these systems from malfunctioning. But which safety concept is adequate for a specific safety system? It is not conceivable to standardize all possible safety concepts, but to give guidelines to the engineers of how to develop new safety concepts; the automotive industry has started to standardize the process of developing safety – related E/E systems. This paper gives insight into the ongoing standardisation work within ISO TC22/SC3/WG 16 functional safety and how companies have started to apply the draft standard and consequently how this standard may initiate the development of a new state of the art within the area of functional safety in the long term.

INTRODUCTION

Safety turns out to be one of the key issues of future automobile development. New functionality not only in the area of driver assistance but also in vehicle dynamics control as well as in active and passive safety systems increasingly touches the domain of safety engineering.

With the trend of increasing complexity, software content and mechatronic implementation, potentially there are increasing challenges from systematic faults and random hardware faults. When is a safety-related E/E-system reasonably well-engineered in order to avoid malfunctions? Being able to answer this question satisfactorily may help to accelerate market introduction of new safety technology. Standardisation has been started to give guidance to the automotive industry to maintain the very high safety level that has been reached within the last

years also for the coming generation of new safety systems. Currently in the state of a committee draft, the upcoming international standard ISO CD 26262 will summarise processes and methods that may help to establish comparable standards of processes within the entire automotive industry. As these standards cover the complete lifecycle of a vehicle it will take some time until the described procedures will have shown their effectiveness in daily work.

Standardization Effort on Functional Safety within the Automotive Industry

In contrast to other industries like aviation, rail or process industry, the topic of functional safety has only started to be discussed in detail a few years ago within the automotive industry. This can be explained by two main arguments. Firstly, the known risks based on failure mechanisms of cars are to a large extent still controllable by a driver. In most cases a driver can bring his car to a safe state by just stopping it. In contrast to that failures during a flight or a release of toxic material in a chemical plant normally lead directly to extremely risky situations. Secondly, the development process of the car industry allows an intensive testing phase with produced cars, before the product can be purchased by a customer. In contrast to that, a plane shouldn't have remaining critical faults already at the very first flight.

Nevertheless the development of new safety systems within automotive industry like active safety systems, driver assistance systems and currently the electrification of the powertrain, lead to new functionality, which is mainly based on E/E-systems. Failures in these systems may have also an impact on vehicle safety, as the competence of these systems is growing. Currently available standards on functional safety like IEC 61508 are not especially dedicated to the automotive industry. An application of the IEC 61508 within different companies would not lead to a harmonization of functional safety, as too many interpretations have to be made. But to reach a harmonized standard

with respect to functional safety should be the goal of normative work. Therefore a Working Group “Functional Safety” has been established within ISO TC22/SC3/WG16 to develop such a standard on functional safety for the automotive industry. 9 countries are actively involved in that working group, i.e. Belgium, Canada, France, Germany, Italy, Japan, Sweden, United Kingdom and USA. Currently a draft international standard ISO DIS 26262 is in preparation and may be expected to be published in Q3/2009.

For all companies not involved so far in that standardization, the publication of a DIS (draft international standard) gives the possibility to apply the standard and to give feedback to the working group via the national standardization bodies.

The Approach of ISO 26262

The standard ISO 26262 is divided into 9 volumes, describing the management of functional safety, core processes within product development as well as supporting processes and “ASIL”-oriented and safety-oriented analyses (see Figure 1). The term “ASIL” leads to the approach of that standard. The Automotive Safety Integrity Level (ASIL) is derived by doing hazard analysis and risk assessment. Right at the beginning of a development the intended functions are analyzed with respect to possible hazards. What may happen if malfunctions arise within different operational situations?

The estimation of risk, based on a combination of the probability of exposure, the possible controllability by a driver and the possible severity outcome of a critical event, leads to an ASIL, which will be given to a corresponding safety requirement that will be generated to avoid this risk.

There are four possible levels (A,B,C or D) of an ASIL to specify the requirements of this standard and safety measures for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level.

How to integrate a safety process into an installed E/E development process

As outlined above, the ASIL attribute is used to give guidance for choosing adequate methods, procedures, etc, within the necessary steps in an E/E development process, production and after sales in order to reach a certain level of integrity of the product.

Does the introduction of a process for functional safety change the complete E/E development? Certainly not. Currently used processes show, that cars are manufactured with a very high safety level. The standard ISO 26262 aims to give guidance for

complementing current processes, which are used for safety-related systems.

How to get started with ISO 26262

The main challenge is to get started with a new standard. Changing running processes during a development is very difficult in practice and cannot always be recommended.

Companies which have started to apply the ISO committee draft have experienced the challenge to implement the new requirements. Usually pilot projects are chosen to demonstrate the changes due to the ISO 26262. The experience shows that the tasks within a concept phase according to ISO 26262 are quite easy to be applied. Moreover we can already state that the tasks of doing hazard analysis and risk assessment as well as deriving functional safety concepts right at the beginning of a development are seen as very valuable tools to create stable safety concepts. A stable concept already designed in the concept phase is also seen to reduce potentially the effort of eliminating remaining faults in later phases.

More difficulties for implementing the ISO 26262 requirements arise within later development phases. Mainly due to the integration topics of a pilot project into an environment, that has not yet been developed to the same standard. In future car line projects many of these problems will be solved, because the aim is to have the complete car developed to the same standard. But still also a new car line is not completely a new car. There are still many basic systems that won't be changed from former car lines. And systems that are already installed in millions of cars showing, that they are proven in use should not be changed just for fulfilling a new standard. This problem has also been addressed within the ISO 26262. Systems that will be used without changes in following projects are still in line with the ISO 26262, if they have shown their integrity already in the fleet. That means that the full alignment to the ISO 26262 standard will take time until all E/E safety-related systems in a car will be developed accordingly. For the companies that are starting with implementing ISO26262 it is important to understand the guiding idea of this standard. Try to analyse the possible malfunctions of your system right at the beginning of a development, setup the corresponding safety requirements and make sure that these requirements are fulfilled during the development and following phases. And do not forget the good engineering judgement. As the experience of companies that have already started with applying the ISO 26262 draft version show, getting started with it will still afford many times the good engineering judgement to integrate the guiding idea of ISO 26262 into the currently used processes.

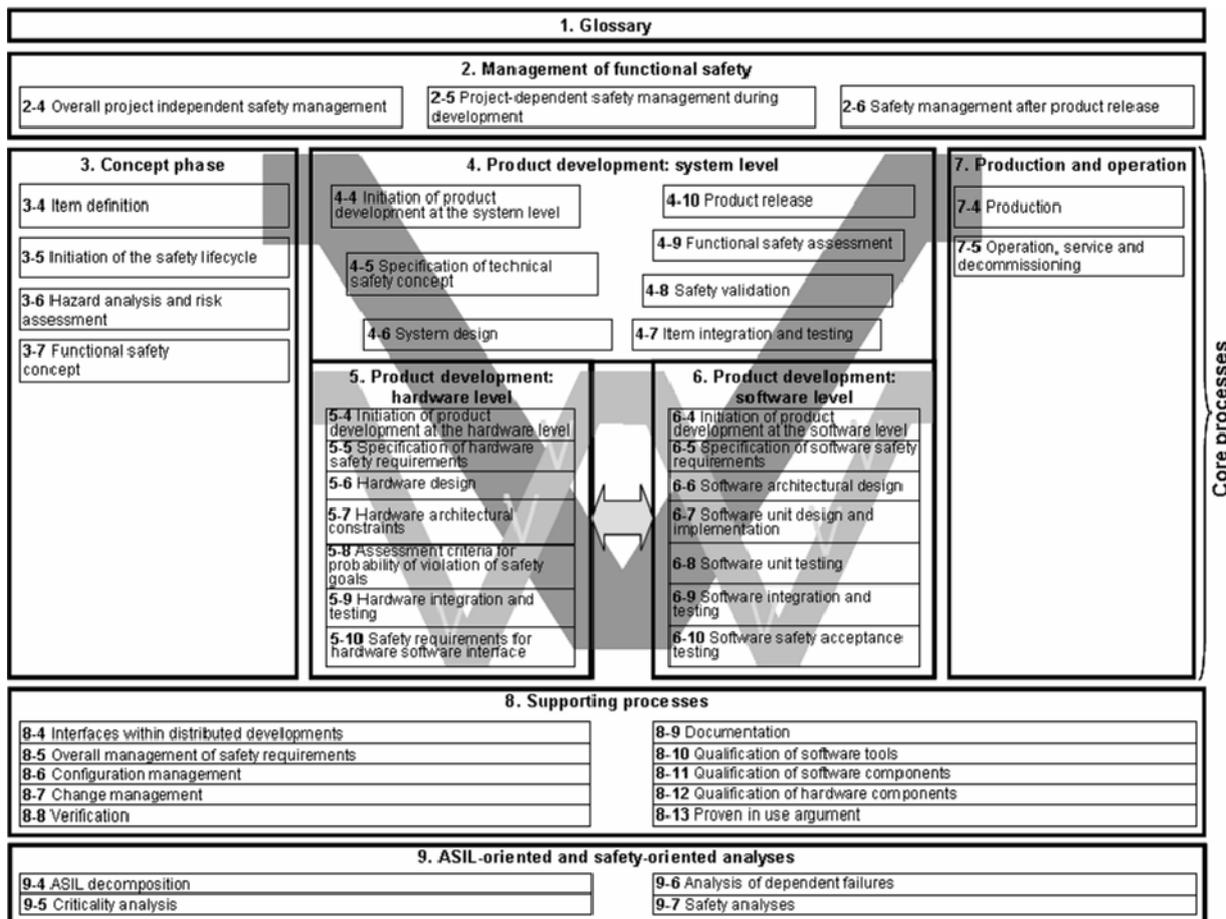


Figure 1. Overview of ISO 26262-1 to -9

CONCLUSIONS

With the upcoming publication of the automotive draft standard ISO DIS 26262, the automotive industry initiates the development of a new state of the art within the area of functional safety. Companies that have already experienced the application of preliminary draft versions within pilot projects can state the valuable benefit of using the described methods to systematically create safety concepts. As this standard is a process standard, it will take some time until this standard will be fully integrated into the existing E/E-processes. The combination of carry over systems and new systems will also imply that not all systems in a car line need to be developed according to the same standard. In case of constellations that are not explicitly described in the ISO 26262, it is important to understand the guiding idea of the standard and to use the good engineering judgement to steadily improve the processes used for safety-related E/E systems. If the ISO 26262 is understood as a means to improve functional safety and not as a burden in terms of a bundle of requirements that have to be fulfilled additionally, the benefit will be seen very soon.

Using the standard with the right attitude may lead the automotive industry to a new state of the art in the area of functional safety in the long term.