Functional Safety – Dealing with Independency, Legal Framework Conditions and Liability Issues

By Martin Schmidt, Marcus Rau, Dr Ekkehard Helmig, Dr Bernhard Bauer

After 8 years of preliminary national and international work by the relevant standardization bodies, ISO 26262 (Volumes 1-9) has now been published. The motor vehicle industry is engaged in an intensive effort of implementing the resulting requirements for complementary development processes and the confirmation of safety-relevant products.

The generic cross-industry standard IEC 61508 uses the model of “equipment under control”. This means that the main focus is placed on equipment safety achieved by a specific control system. The limitation of the risk is based on specific safety functions. By contrast, ISO 26262 is based on the notion that vehicle safety is dependent upon the behaviour of the control system itself. Whereas IEC 61508 targets equipment produced in low volumes, ISO 26262 is oriented to the mass production of vehicles. The safety system must be validated prior to vehicles being put into circulation.[1]

A large number of experts are currently addressing this topic. The demand of the market for specialists in this field is extremely high at the moment and exceeds supply.

However, the focus is typically placed solely on the technical aspects of the new standard – often without sufficient consideration of accompanying norms or legal framework conditions.

This article provides an overview of the relevant legal environment as well as the current state of science and technology. In addition, it addresses topics which tend to be somewhat alien to developing engineers, such as independency in reviews and assessments. They are,

[1] ISO/FDIS 26262-10; 4.1 lit. b)

however, crucial for the legal classification of personal liability and the company's liability from the perspective of product liability, the producer's liability and contractual liability.

ISO 26262 on Functional Safety in passenger vehicles will be instrumental in determining the electrical and electronic architectures in this vehicle category in the future. It is highly relevant with respect to the implementation of requirements set out in European Regulation (EC) No 661/2009 according to which vehicle safety must be designed in line with the respective current state of science and technology.[2] Since the standard provides a framework for achieving Functional Safety when using complex electrical and electronic systems in motor vehicles ISO 26262, itself, is an element of the scientific and technological "state of the art".
Functional Safety is a property of these systems which can be assessed by using the methods of ISO 26262[3]. The assessment itself reduces risks but does not completely avoid them.

The standard calls for the integration of its requirements into the process of a quality management system based on ISO/TS 16949:2009. The implementation of the requirements set out in the standard substantially determines the responsibilities of the manufacturers of safety-relevant systems, particularly those of vehicle manufacturers, under civil and criminal law.
By requiring vehicle manufacturers and suppliers to enter into a mutual Development Interface Agreement (DIA) it forces them to establish and document in detail the safety activities in the concept phase, the development phase and the production phase.
ISO 26262 thus acquires enormous legal relevance for the relationship between the parties involved in the upstream value chain of the automotive industry with respect to contract and liability law.

Fundamentals of Liability– Product and Producer's Liability

To clarify the legal relevance of ISO 26262, the two legal spheres of "product liability" and "producer's liability" must be looked at.

Product liability – based on national and European product liability law – represents extra-contractual, statutory, *no-fault* liability (liability in tort) for faulty (sub-) products. It encompasses all cases in which a liability for faulty products must be assumed. It must be considered in this context that even a specification-conformant product may be "faulty". "The compensation obligation of the manufacturer is only excluded if the fault could not be detected based on the state of science and technology which existed at the time when the manufacturer put the product into circulation". (Section 1, Paragraph 2, Number 5, German Product Liability Act – PHG).

The producer's liability – here in particular with reference to Section 823, German Civil Code – BGB – describes extra-contractual, *fault-based* liability. The prerequisites for its application

[2] Official Journal of the European Union dated 31 July 2009, L 200/1
[3] ISO 26262-2; 6.4.5.6

are breach of duty + violation of a legal interest + damage + fault. As regards the aspect of breach of duty + fault, the issue of exercising "due care", e.g. with respect to the state of science and technology, is particularly relevant in this article.

The legal consequences of ISO 26262 do not result only from the application of a product that has been manufactured according to the processes set out in the standard. The standard itself claims to consider statutory provisions and requirements by government authorities. The user of the standard has to comply with legal requirements as early as in the concept phase, in the development phase and in production. The user's familiarity with the requirements is a prerequisite for such compliance.

Standards are not laws. The German Federal Court of Justice (BGH) ruled in its Airbag Judgment[4]: That safety measures are required which "according to the latest state of science and technology in existence at the time of putting the product into circulation are possible with respect to engineering design, and appear to be suitable and sufficient to prevent damage". Common industry practice expressly does not reflect the state of science and technology that exists "when based on validated technical [professional] knowledge of the relevant technical [professional] groups feasible solutions that can be put into practice are available". This can only be assumed to be the case when an alternative that delivers superior technical safety is ready for use in serial production.

The standard is based on the scientific finding that absolute safety is an unobtainable goal. The application of the standard is intended to serve the aim, and to demonstrate, that a safety system is free from unreasonable risks.[5] Courts accept this condition. However, they draw conclusions from this notion which are often overlooked, or at least are not implemented in many cases. In its Airbag ruling the Federal Court of Justice in Germany has established a clear line of reasoning:

"If hazards related to the use of a product cannot be avoided through engineering design measures according to the state of science and technology, or if engineering design measures would impose an unreasonable burden on the manufacturer and the product is allowed to be put into circulation despite the hazards emanating from it, then the manufacturer is principally required to warn the users of the product of the hazards which threaten from its intended use or likely misuse [and] which are not part of the generally existing knowledge of hazards possessed by the group of users".

This information duty set out in Section 5 e.g. of the German Equipment and Product Safety Act (GPSG) also encompasses the manufacturer's obligation to provide information established under tort law: The manufacturer has to inform the user of the vehicle about the residual risk of a driver assistance system in the operator's manual and may not conceal it by technical means (such as volatile memories) or cover it up. The information (§ 5 GPSG) has to be detailed enough for the vehicle user (i) to understand the risk, (ii) be able to evaluate the risk (iii), decide whether he/she is willing to assume the risk (iv) be able to develop

[4] Judgment dated 16 June 2009, VI ZR 107/08, Der Betrieb 2009, 1812; VersR 2009, 1125

[5] ISO 26262:19; 5.3.1: "Given that absolute safety is an unobtainable goal, safety cases can demonstrate that the system is free of unreasonable risk."

strategies in order to fend off the materialization of inherent hazards from him-/herself and innocent bystanders. This risk assessment from the user's perspective – the manufacturer's perspective is immaterial in this context – has to be determined, applied, implemented and, above all, documented in all phases with the appropriate criteria of the state of science and technology for all developments under the regime of ISO 26262.

Therefore, any future liability issue will be determined according to the objectivity, plausibility and integrity of all assessments and decisions made for the reasonableness of a risk decision both for the respective single product and, above all, for the compatibility with other systems ("freedom of interference").

State of Science and Technology / Legal Classification of ISO 26262

What does "state of science and technology" mean? Can it be equated to compliance with the relevant published standards (particularly ISO / IEC)?

No, not automatically: Standards may be obsolete and therefore no longer reflect the current state of technology. Manufacturers must fully use all technical and scientific findings which are accessible to them, *even if the known standards merely permit lower safety standards.*

Standards, however, form a *minimum standard* so that a product initially, from the average user's external perspective, creates the impression that it meets his/her safety expectations.

In an overall context, the state of science and technology is shaped by generally available (not necessarily new) technical findings and solutions – irrespective of whether they already represent common industry practice or where in the world they have been published. Under its obligation to exercise due care, it is the developing company's responsibility to apply the respective current state of science and technology during the course of the development.

Important factors to be considered with respect to the application of ISO 26262 are:

- If an E/E sub-system / a component is equipped with a safety-relevant functionality, then the currently available standards (or published drafts of standards) for Functional Safety must be applied or the minimum equivalent safety level achieved in an alternative manner.
- If the customer has not provided any technical safety specifications, then the supplier is by no means released from its obligation to exercise due to care. In other words the supplier is obligated to apply that which is possible to confirm safety-relevant functions and/or the sub-functions contained in the supplied part.

Now the question arises to what length a supplier has to go in order to determine the state of science and technology which is appropriate for the concrete application. The general rules are as follows:

- The hazard potential determines the extent of the effort to be made.
- A comparison with reference products available on the market is necessary.

- A comparison with known information for a potential confirmation must be performed.
- In case of new technologies and high risks in-house research and possibly the development of a proprietary and new state of science and technology (e.g. in the field of e-mobility) is inevitable.

With respect to ISO 26262, which is the subject of this article, the following applies in consideration of the legal environment:

- ISO 26262 is typically applied already in the contractual agreements of the vehicle manufacturers and TIER 1 suppliers. Therefore, its implementation is required for all current development projects of products at least in the defined scope of application. In addition (or, in case of appropriate supporting arguments, alternatively), the generic basic IEC 61508 standard may be applied in the commercial vehicle sector.

ISO 26262 = Vehicle Safety?

ISO 26262 is not an inherently closed system standard for the Functional Safety of E/E systems used in motor vehicles and the vehicles themselves. The equation:

“Compliance with the requirements of ISO 26262 = vehicle safety” is inappropriate. The requirements for “freedom of interference” and the unresolved issue of the driver’s distraction by too many assistance systems or the issue of the failure of just one sub-system and a resulting chain reaction affecting subsequent sub-systems and the ensuing limitation of the driver’s freedom of action alone are completely open at the moment.

ISO 26262 is a framework in the spirit of a guide (processes and methods) whose safety-relevant systems which are based on other technologies may be looked at. It contains:

- The automotive safety lifecycle including production
- The risk-oriented approach used in order to determine Safety Integrity Levels
- Requirements for the process-related verification, validation and confirmation of measures to confirm the achievement of the safety level and, as appropriate, to achieve a sufficient and acceptable level of safety
- Requirements for the determination and demonstration of an interface to assure a seamless and standard-conformant collaboration between the OEM and the suppliers

Environment Required for ISO 26262

The safety requirements of ISO 26262 only relate to E/E systems in the vehicle. In the hazards and risk analysis (H&R) all faults and problems with respect to functionality are considered but the standard does not set out requirements for other technologies (mechanical, hydraulic and pneumatic systems). Neither does it consider external influences acting on E/E systems such as hacking attacks via mobile data communications interfaces such as GPS, LTE, UMTS, GPRS and GSM and, furthermore, via the infotainment system on the vehicle's on-board network. Interferences such as vibrations, the operating environment in the vehicle, temperature, ambient influences, the driver's ability etc. are not covered any further in the E/E safety concept to be developed.

The standard makes no statements about the quality (absence of faults) of the components (sensors, chips, PCBs, micro-switches etc.) used in the systems. It predisposes the existence of a certified and effective QM system, for instance according to ISO/TS 16949:2009, for this purpose. ISO/TS 16949 is a quality management system which creates the conditions for the manufacture of fault-free products. It does not, however, assure the quality of the products themselves.

The activities according to ISO 26262 are an integral component of the overriding process-oriented approach of the quality management system according to ISO/TS 16949:2009, in particular chapter 7 (Product Realization). The processes of ISO/TS 16949 have to implement the activities of ISO 26262.

ISO 26262 extends the focus of ISO/TS 16949 from the responsibilities of the suppliers in the value chain (ISO/TS 16949 -02: "Interaction") in the spirit of fault avoidance and fault control [ISO/TS 16949 – Comment on 7.2.1] by the responsibility for validating the overall system of the OEM who is responsible for the safety of the whole vehicle.

Independency in Assessments and Audits

If the user looks at ISO 26262 in isolation from the rest of the world of standards, then the required independence of the reviewer, assessor and auditor seems to be clearly defined (Fig. 1 – Extract from ISO 26262-2 Table 1)

Confirmation measures	Degree of independency[a] applies to ASIL			
	A	B	C	D
Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates (see ISO 26262-8:2011, Clause 14) Independence with regard to the author of the argument	I0	I1	I2	I3
Confirmation review of the completeness of the safety case (see 6.5.3) Independence with regard to the authors of the safety case	I0	I1	I2	I3
Functional safety audit in accordance with 6.4.8 Independence with regard to the developers of the item and project management	—	I0	I1	I3
Functional safety assessment in accordance with 6.4.9 Independence with regard to the developers of the item and project management	—	I0	I2	I3

[a] The notations are defined as follows:

—: no requirement and no recommendation for or against regarding this confirmation measure;

I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person;

I1: the confirmation measure shall be performed, by a different person;

I2: the confirmation measure shall be performed, by a person from a different team i.e. not reporting to the same direct superior;

I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.

But how viable is this rating with respect to the state of science and technology? Typically, the proverbial rule “As long as no-one complains …” applies. This means that in the case of proper functionality of the product concerned, for instance with a Safety Integrity Level of ASIL D, the Functional Safety analysis by an individual from a different department or organisation without the requirement and documentation of that individual’s independence and expertise appears to be sufficient.

However, when looking at a possible product liability case (assumption: personal injury or death), various additional requirements emerge.

1. In a product liability case, the independence and expertise of the assessing and auditing parties are evaluated as part of the process of hearing evidence.

Factual independency only exists in the event that the analysing party is not dependent on the manufacturing company economically or in the context of labour law. In the case of company-internal analysing parties this must non-disputably be doubted. There are too many factors which may come into play: competitive pressures, cost interest, insufficient exchange of information prior to verification and validation, time pressures prior to SOP etc. In the event of damage, the evaluation during the ex-post review of the case is always crucial. Any judge and any prosecutor will look for arguments of how and why a subsequently detected problem could have been detected and avoided beforehand. The only protection against the finding of such arguments is provided by the determination of the planned and implemented independency in the analysis, the precise documentation of the decision parameters for the acceptance of a residual risk, the integrity of the risk weighing process and the precise risk description for the vehicle user from the anticipatory perspective of the risk and the probability of controlling the risk.

2. If, in addition, the expertise of the testing party is under investigation – and this must be assumed in a court case – then the serious aspect of the testing party's legal recognition additionally comes into play.

How is the level of expertise and independency of a conformity-assessing party according to the state of science and technology neutrally demonstrated internationally as a general rule (also in other technologies such as aerospace, automation technology, nuclear technology and rolling stock)? It is done through accreditations. According to ISO/IEC 17011 accreditation is the confirmation by a third party that formally expresses that a conformity-assessing body possesses the expertise to exercise certain conformity tasks. In Germany, the Deutsche Akkreditierungsstelle GmbH DAkkS has been exclusively responsible for all accreditations in this country since 01 January 2010. Currently, the German Federal Government has one third of the shareholdings in the DAkkS, one third is held by five German federal states and one third by The Bundesverband der Deutschen Industrie (Federation of German Industry - BDI).

For the conformity assessment of products, for testing bodies of ISO/IEC 17025 (optionally ISO/IEC 17020 for inspection bodies) the relevant international standard is valid – this also applies to Functional Safety. It provides the required basis for the acceptance of test reports / certification reports in the event of legal disputes[6]. They have a higher level of objectivity even though any expert opinion which has not been ordered by a court remains a "partisan opinion". An additional requirement is that the testing body is "unaffiliated", in other words that it is not a member of a common group of companies.

It is assumed that in the event of a court case the developing company, or the developer, are not released either with respect to product liability or the producer's liability and that no reversal of the burden of proof is possible if these framework conditions are disregarded. This means that courts do not accept any proof provided by organisational units that are dependent in the context of labour law or by third parties that do not possess Functional Safety accreditation as evidence of compliance with the state of science and technology.

[6] Alternative in the German legal sphere: publicly appointed and sworn experts by the court

With respect to exercising due care the “Assessment” portion of the Functional Safety product confirmation process being performed by testing parties that are accredited according to ISO/IEC 17025 and/or ISO/IEC 17020 and are not affiliated with the company whose product is under test is to be considered as reflecting the state of science and technology.

Conclusion – Current State

A comparison of the legal framework parameters and the state of science and technology, also in the realm of standardization, with current practice in the European automotive industry reveals that a lot has happened in the field of Functional Safety in recent years. Nevertheless, considerable efforts are typically still required to implement the current state of science and technology in the field of confirmation. However, awareness of the legal framework conditions, and the viability of confirmation according to the state of science and technology, is progressively moving forwards – nationally and internationally.

www.sgs-tuv-saar.com/fs

Authors:

Martin Schmidt

Is Head of Global Competence Center Functional Safety at SGS-TÜV GmbH – ein Unternehmen der SGS-Gruppe und des TÜV Saarland e.V., and co-initiator of the standardization work for ISO 26262

Marcus Rau

Is Head of of Training Functional Safety at SGS-TÜV GmbH, and SGS-TÜV delegate to the German Standardisation Committee for ISO 26262 as German working group to ISO TC22/SC3/WG16

Dr. Ekkehard Helmig

Is a freelance lawyer and notary focused on product liability, technical regulations in the automotive sector and their legal implementation

Dr. Bernhard Bauer

Is Acting Head of Electronics & IT of TÜV NORD Mobilität GmbH & Co. KG