ISO 26262 – Functional Safety in Personal Vehicles: Responsibilities and Liabilities of Functional Safety Managers

Dr. Ekkehard Helmig, Attorney-at-Law, Wiesbaden

Preface

ISO 26262 is a standard for the functional safety of vehicle systems which entered into force at the end of 2011 and aims at overall functional safety in vehicles. According to concept laid out therein, "Functional Safety Managers" (FSM) are responsible, on behalf of their company as well as personally, for making functional electrical and/or electronic safety-related items, such as airbags, driver assistance systems or lane departure warning systems, comply with the requirements of ISO 26262. The automotive industry deems this standard the state of the art of technology and engineering and considers it to be generally applicable within its sector.

I

Introduction to ISO 26262

The standard "Functional Safety – Road vehicles"[1] takes a process-oriented[2] approach to systematize a company's responsibilities with respect to the concept phase, development and production of electrical and/or electronic systems, taking into account statutory safety regulations, the latter, however, not being specified in the standard. In its capacity as technical standard it also sets out legal requirements regarding the producers' actions and thus constitutes a classical case of law and technology overlapping. To put it into technical terms: Technical standards and legal regulations form hybrid sources to technically and legally

[1] The extensive standard (counting more than 370 pages and only available in English) was drafted by the International Standard Organization in close cooperation with leading vehicle manufacturers and suppliers of safety-related systems. Even before entering into force, vehicle manufacturers had made it an integral part of contracts for the development and manufacturing of safety-related electrical and electronic systems. Helmig: "Fahrzeugsicherheit versus Fahrerverunsicherung – Kritische Überlegungen zur KVV und zur ISO 26262" (Vehicle safety vs. driver insecurity. Critical thoughts on design responsibility agreements and ISO 26262). In: PHi, 2010, p. 194 ff.; Helmig: "Functional Safety in accordance with ISO 26262 and product liability for No Trouble Found events", http://www.notar-helmig.de/de/publikationen.html. (The German original was published in PHi 2012, p. 32)

[2] The term "process" is used in a technical sense in this paper referring to the definition given by DIN EN ISO 9000:2005: "process is defined as 'set of interrelated or interacting activities which transforms inputs into outputs'".

evaluate current safety-related systems. In this context, standards and legal regulations can only be understood if looked at from an interdisciplinary angle. Therefore, ISO 26262 always serves as complementary yardstick to construe and evaluate technical products from the viewpoint of contract law and liability law; legislation only stipulates that a product shall be safe although it does not, and cannot, regulate in detail how technical safety is to be guaranteed.[3] Despite the standards' origins in private-law organizations there is a factual necessity to comply with them due to their importance and widespread application in practice.[4]

II

1.

Although there is no absolute safety with regard to technical products[5], established case-law of the German Federal Court of Justice (BGH) requires the manufacturer of a technical product to take all measures objectively necessary and reasonable in order to avoid danger or harm; he shall do so as early as during the concept and design phases. Required are those safety measures which are feasible in terms of engineering and which correspond to the state of the art of science and engineering at the time when the products are placed on the market.[6]

The notion of what is technically possible[7], coined by the BGH in this decision, refers to implementing all technically and economically reasonable measures to guarantee maximum safety and not to placing anything possible on the market without considering the risks. The application of technology has to be measurable by legal standards.

---

[3] The rules determined by the Economic Commission for Europe (ECE) based on the "Agreement Concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions", issued on March 20, 1958, and revised on October 16, 1995, are recommendations to the 47 member states of the Council of Europe as well as the 27 member states of the European Union that were transposed into national law respectively (currently about 126 rules). They are for the most part component-related. They do not constitute general safety requirements – not to mention the problems regarding their legislative legitimacy.

[4] Ensthaler/Müller/Synnatzschke: "Technologie- und technikorientiertes Unternehmensrecht" (Technology- and engineering-oriented corporate law), BB 2008, 2641.

[5] ISO 26262 (10-5.3.1) explicitly states: "Given that absolute safety is an unobtainable goal, safety cases can demonstrate that the system is free of unreasonable risk." The standard defines the term "unreasonable risk" (1.136) as follows: "Risk judged to be unacceptable in a certain context according to valid societal moral concepts."

[6] Ruling on June 16, 2009, VI ZR 107/08, VersR 2009, 1125, items 15 and 16.

[7] BGH, June 17, 2009, VI ZR 107/08, at the end of item 20 (listing further references).

2.

There have been attempts in the automotive industry to make these requirements less strict by referring to the "customs of the sector". As a consequence thereof, technical possibilities are praised in order to promote sales without visibly focusing on avoiding potential risks, which is what corresponds to the safety culture[8] as required by ISO 26262. Vehicles with complex electrical and electronic systems, manufactured by a multilayered supply chain comprising various suppliers, each of whom is specialized on different fields such as airbags or driver assistance systems, are not necessarily safe, much as the individual systems might be conducive to overall vehicle safety. Following the trend of the so called connected vehicle[9], where systems are operated anomalously via internet connections or infotainment systems (e.g. iphone, ipad, MP3 player) that are not vehicle-specific, particularly puts them at risk of malfunctioning. Malfunctions caused by influences of incompatible software which the system cannot process or by hack attacks occur ever more frequently.[10] This so called 'new vulnerability' is openly discussed in the USA as well as measures which have already been introduced by the National Highway Traffic Safety Administration (NHTSA) to counteract these tendencies.[11] These customs of the sector, which often lag behind the technical possibilities to avoid risks, are put to an end by the BGH's case-law. What appears perfectly logical to electronics engineers does not necessarily have to be logical to customers.[12]

III

The contents and system of ISO26262 can only be briefly described:

1.

ISO 26262 is targeted at achieving safety in vehicle items and hence encompasses[13] the entire safety lifecycle[14] of electrical and electronic safety-related systems in vehicles as a means to

---

8 ISO 26262-1:2011-1.107; ISO 26262-2:2011 – Annex B.

9 ADAC Motorwelt, no° 8, August 2012, p. 20.

10 In its "Comprehensive Experimental Analyses of Automotive Attack Surface" the Center for Automotive Embedded Systems Security (CAESS) has produced empirical evidence on the vulnerability of electrical systems, http://www.autosec.org/publications.html. Moreover: Handelsblatt-online on July 7, 2012: "Hacker greifen nach dem Steuer" (Hackers go for the steering wheel).

11 Automotive News on September 20, 2011, p. 11: "War with computer hackers hits the road".

12 In its issue of August 6, 2012, Automotive News featured the following comment: „Technology in automobiles is a great thing. But what is intuitive to the electronics engineers might not be intuitive to the customer".

13 ISO 26262-1:2011 -1.97

14 According to ISO26262, the safety lifecycle encompasses the concept phase, product development, production, service and decommissioning of a safety-related system.

avoid hazards. The safety lifecycle covers all safety activities during the concept phase, product development, production, operation, service and decommissioning.[15] However, the standard is a framework and as such intended to serve as a sample for safety-related systems which might be based on other technologies.

The standard's introduction states that "with the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures[16] and random hardware failures[17]." The standard's goal is to control this complexity and reduce residual risks, including potential hazards[18] and harms[19] thus arising, in order to achieve functional safety in a given system since, according to the standard, a vehicle's safety depends on the control systems' reactions[20] and not on the vehicle: An airbag only fulfils its function within the functional safety system if its release is only triggered by collision. This was the case for the above mentioned decision of the German Federal Court of Justice (BGH). Currently, however, recalls due to faulty airbags occur increasingly.[21]

ISO 26262 sets out a "concept of safety goals"[22] as well as a hierarchically classified "functional safety concept"[23] for each safety goal: (i) Hazard analyses and risk assessments identify potential hazards, the risk of which is to be reduced; (ii) A safety goal is formulated for each hazardous event taken into consideration; (iii) Each safety goal is assigned an Automotive Safety Integrity Level (ASIL)[24]; (iv) A functional safety concept describes a system's functionality

---

15 ISO 26262-2:2011 -5.2.1

16 ISO 26262-1:2011 -1.130

17 ISO 26262-1:2011 -1.92

18 ISO 26262-1:2011 -1.57

19 ISO 26262-1:2011 -1.56; ISO 26262-1:2011 -1.59

20 ISO 26262-1:2011 -4.1 lit. b).

21 See: http://www.auto-motor-und-sport.de/news/honda-airbag-rueckruf-1735547.html; http://www.auto-motor-und-sport.de/news/toyota-us-rueckruf-gelaendewagen-wegen-airbag-problemen-3675501.html; http://www.auto-motor-und-sport.de/news/ford-us-rueckruf-1-2-mio-pickups-mit-airbag-problem-3657395.html; http://www.autobild.de/artikel/rueckruf-honda-japan-usa-kanada--1124962.html;
Chrysler alone had to recall 745.000 vehicles due to defective airbags: "Chrysler is recalling certain model year 2002 and 2003 Jeep Liberty vehicles manufactured January 9, 2001, through March 28, 2003, and 2002 through 2004 Jeep Grand Cherokee vehicles manufactured February 13, 2001, through May 23, 2003. A component in the air bag control module may fail causing the front airbags, side curtain airbags, and/or seatbelt pretensioners to deploy inadvertently while the vehicle is being operated" (http://www-odi.nhtsa.dot.gov/recalls/latestRecalls.cfm).

22 Safety goals are the highest safety requirements for safety-related systems (ISO 26262-10:2012 -6.5.1). They are already determined during the concept phase.

23 ISO 26262-3:2011 -7.4.8 and 8.

24 ISO 26262-3:2011 -7; ISO 26262-8:2011 -4.3. The standard defines five ASIL with QM-ASIL being the lowest level, followed by ASIL A, ASIL B, ASIL C and finally ASIL D as highest safety-related level.

to achieve the safety goal; (v) A technical safety concept sets out how the functionality deriving from the functional safety concept is to be implemented in hardware and software; (vi) safety requirements for software and hardware describe those specific safety requirements which are to be part of the software and hardware design on the basis of the vehicle's overall safety functionality.

All processes and measures within and between the different levels of this classification are subject to continuous and documented confirmation measures[25] with increasing significance: The confirmation review[26] checks whether selected work products meet the requirements set out for a defined concept, product development or production process, either at the supplier's level or at supply chain level between two suppliers or ultimately at the vehicle manufacturer's level[27]. The functional safety audit evaluates the implementation of processes which are required for all safety activities. The functional safety assessment "evaluates the functional safety achieved by the item" at system level.[28]

2.

What appears to be the perfect, complete and self-controlling processes of a strict regime resulting in the assigned ASIL can lead to misunderstandings and, therefore, bears liability risks: According to the logic of ISO 26262, the functional safety of a given item does not constitute a product property in the sense that it will work in the vehicle. The item is only conceptually and generally suited to fulfill safety requirements in the vehicle if it has been designed, developed and produced according to the standard's processes. External conditions deriving from the vehicle itself (e.g. vibration, temperature, humidity, electro-magnetic influences etc.) or traffic are expressly not taken into account.[29] Therefore, functional safety is but a narrowly defined item feature which can be evaluated according to the standard's yardsticks by using the methods and instruments of the functional safety assessment (e.g. compatibility with other software contents in the vehicle[30]): The airbag is to be released at the time of the crash. The standard does not regulate whether the airbag will actually meet this requirement, i.e. perform

[25] ISO 26262-1:2011 -1.17 and ISO 26262-2:2011 -6.
[26] ISO 26262-1:2011 -1.18
[27] Whether intermediate or final products meet specified requirements is confirmed by verification processes (ISO 9000:2005 -3.8.4). Whether intermediate or final products meet the requirements of the next level in the supply chain is confirmed by validation (ISO 9000:2005 -3.8.5).
[28] ISO 26262-2:2011 -6.2; ISO 26262-10:2012 -5.2.2.
[29] ISO26262-2:2022 -1.
[30] So called freedom of interference.

its function.[31] Due to this self-limitation of ISO 26262 there is no equation of the kind that functional safety = vehicle safety.

3.

The evaluation of whether a hazardous event[32] might occur while or due to vehicle operation as well as the evaluation of its severity[33], its probability of exposure[34] and the hazardous event's controllability[35] through the driver and/or other persons at risk (for instance pedestrians) is based on selective assumptions and assessments. These selective assumptions are inevitably subjective and arbitrary compared to what the German Federal Court of Justice (BGH) demands. With regard to the respective safety goals for the driver's safety these assumptions can be correct, false or incomplete; the conclusions thus drawn about the safety measures, deriving from the assumptions themselves, have to be equally uncertain. For instance, the standard assumes the driver to be a "representative driver", meaning he is not tired, has average driving experience in areas not exactly characterized by light traffic and complies with traffic rules and due care requirements regarding other traffic participants.

a)

The system engineer makes precise assumptions about the driver's possible behavior in a likewise system-specific, yet arbitrary, hazardous event which are already included into the assumptions of the basic hazard analysis and the risk assessment[36] during the concept phase of a safety-related item; risk assessment is carried out to identify potential risks and define safety goals for the specified risks respectively. Reactions due to surrounding traffic or due to a safety-

[31] ISO 26262-2:2011 -6.4.5.6.

[32] ISO 26262-1:2011 -1.59

[33] ISO 26262-1:2011 -1.120

[34] ISO 26262-3:2011 -7

[35] According to ISO 26262-1:2011 1.19, controllability is "the ability to avoid a specified harm or damage through timely reactions of the persons involved". It is based on the estimated probability that the driver or other traffic participants will be capable of gaining sufficient control over the hazardous event, such that they can avoid potential harm. (ISO 26262-10:2012 -6.3). The safety validation (ISO 26262-4:2011 -9) evaluates the assumption of controllability in the hazard analysis and the risk assessment.

[36] New issues thus arise concerning the evaluation of whether a safety-related system corresponds to state-of-the-art science and technology as required by the BGH's airbag decision: The evaluation, already carried out in the concept phase, of whether a product meets these requirements does not depend on technical aspects alone. Where a product's safety or operation largely depends on human factors, such as the anticipated driving behavior, these state-of-the-art-requirements can only be satisfied if an interdisciplinary approach takes into account driver psychology and findings in the field of accident research. Very informative: Qureshi, "A Review of Accident Modelling Approaches for Complex Socio-Technical Systems", Australian Computer Society, 2007, http://crpit.com/confpapers/CRPITV86Qureshi.pdf.

related system's failure or malfunctioning (a damaged tire causes the tire pressure sensor to fail, which has direct impact on other engine control functions) can only be anticipated to a limited extent. The conclusions thus drawn as well as decisions based thereon regarding a safety-related item's final design are inevitably just as inexact. Studies have shown that driving behavior and drivers' attitudes towards safety-related systems differ immensely from each other and that reliable forecasts are not possible until established safety-related systems will have produced more empirical data.[37] ISO 26262 does not set out any system or process approach according to what German case-law stipulates, i.e. to apply the state-of-the-art-requirement regarding science, e.g. driver-related behavioral research and accident research, to state-of-the-art technology and engineering although doing so is the only way to develop a coherent safety concept.

b)

False assumptions and hence false conclusions regarding product realization, inevitable as they are, have an impact on the entire safety lifecycle and cannot be completely eliminated by means of confirmation reviews, functional safety audits or functional assessments because assumptions, for instance about driving behavior, can neither be confirmed nor refuted by these confirmation measures. A residual risk unavoidably remains to which is added further inevitable failure of software and hardware. A company that invokes its products' compliance with the technical requirements of ISO 26262 cannot claim that it places absolutely safe products on the market. This is why it has to call attention to residual risks. The description of these risks must be comprehensive, such that it enables the driver to recognize, understand and cope with them and to decide how he can avoid the risks for his own and other traffic participants' sake.[38]

IV

These weaknesses of the system cannot be avoided by ISO 26262 requiring a competence management[39], either: "The organization shall ensure that the persons involved in the execution of the safety lifecycle have a sufficient level of skills, competences and qualifications corresponding to their responsibilities" as well as the ability to assert their authority[40]. The persons in charge are the project manager[41], the safety manager[42], the person appointed to

[37] See: "Crash avoidance features reduce crashes…" (video), Highway Loss Data Institute news release, http://www.iihs.org/news/rss/pr070312.html.

[38] BGH decision on June 16, 2009 – VI ZR 107/08, VersR 2009, 1125; Section 6 (1) of the German Product Safety Act (ProdSG).

[39] ISO 26262-2:2011 -5.4.3.1 (Overall Safety Management).

[40] ISO 26262-2:2011 -5.4.2.1

[41] ISO 26262-2:2011 -6.4.2.2

carry out the functional safety audit[43], the person appointed to carry out the functional safety assessment[44] as well as the person appointed "to maintain the functional safety of the item after its release for production"[45]. Together they are responsible for all safety measures taken during development as well as any detected safety anomaly. As a consequence they have to determine redundant communication processes which are to be applied to the entire organization and notably fulfill the requirement of building on state-of-the-art science and engineering all the while documenting how this is achieved.[46] According to the standard, these persons are all equally responsible. Despite gradual differences with regard to decision making processes they can be called "Functional Safety Managers" (FSM).[47] First and foremost, they need to be independent. This requirement of independence implies certain forms of organization in a company.

The company must ensure the appointed FSM's independence, regardless of whether this person is an employee, a free lancer or an external consultant. This independence has to be part of the company's organization, needs to be documented and it must be possible to asses it in the course of management review.[48] Therefore, ISO 26262 obligatorily demands that "the organizations involved in the execution of the safety lifecycle shall have an operational quality management system complying with a quality management standard, such as ISO/TS 16949"[49], ISO 9000:2008, or equivalent. ISO/TS 16949 is a generally applied standard for quality management systems (QMS) in the international automotive industry, too. It is based on the international standard ISO 9001:2008 and includes additional requirements specific to the

---

[42] ISO 26262-2:2011 -6.4.2.4; according to ISO 26262-2:2011 -6.4.3.1 the "safety manager shall be responsible for the planning and coordination of the functional safety activities in the development phases of the safety lifecycle".

[43] ISO 26262-2:2011 6.4.8.2

[44] ISO 26262-2:2011 -6.4.9.3

[45] ISO 26262-2:2011 -7.4.2.1

[46] ISO 26262-2:2011 -5.4.2.3

[47] ISO 26262-1:2011 1.109: According to the standard's definition of the term, the safety manager is a "role filled by the person responsible for" the functional safety management (ISO 26262-2:2011) during the development phase.

[48] ISO/TS 16949:2009 -5.6

[49] ISO 26262-2:2011 -5.4.4.1. ISO/TS 16949:2009 is a binding Technical Specification for the international automotive industry; it Is based on the international standard for quality management systems, ISO 9001:2008, and includes additional requirements specific to the automotive industry. Both standards define the term organization as a company or facility responsible for the effectiveness of the management system so as to ensure functional safety or product quality. The term management, however, differs in its meanings: While ISO/TS 16949 defines it as business management in a hierarchically structured company, ISO 26262 generically uses the term to refer to the organization of the standard-specific processes during the safety lifecycle.

automotive industry.[50] ISO/TS 16949 is usually an integral part of contracts at all levels of the automotive supply chain. It determines essential requirements for the company's organization, management responsibilities, the provision of human and material resources as well as all fundamental processes during product realization.

ISO 26262 and the processes therein have to be understood as processes within an effective QMS framework that is in compliance with ISO/TS 16949, and need to be implemented accordingly. ISO 26262 does not name any processes which refer to, for instance, auditing the quality of parts and components of a safety-related system. Requirements of this nature go beyond the standard's application. They must be fulfilled by the QMS, which involves further requirements with regard to the entire customer communication process, identification of product-specific requirements as well as ensuring that all purchased parts and services are free from defects.[51] When dissecting ASIL according to different safety assessments, the guarantee that the components are free from defects is only based on the QMS.[52] Hence, ISO 26262 indirectly calls for an obligatory QMS, which is why QMS managers are at the same time always decision makers according to ISO 26262.

1.

The standard does not define the required independence of the safety managers. The "Final Draft" (FDIS) had determined the following with respect to the confirmation measures[53]: "The confirmation measures and the associated reviewer independence requirements are applied within the system safety process of an item in accordance with the highest ASIL level in the safety goals of the item under review. In order to ensure that these evaluations are conducted in an objective manner, confirmation measures can have additional criteria for the level of independence of the reviewer, auditors, or assessors." This crucial regulation has not been included into Part 10 of ISO 26262 (2012) anymore. Yet, the standard still states that the independence becomes all the more important the higher the ASIL level is.

In Part 2 of the standard ("Management of functional safety"), the idea behind the FSM's independence can be interpreted in that it requires the FSM, who confirms that a work product, including underlying assumptions and conclusions, corresponds to its assigned safety goal, to

[50] It was issued in close cooperation with the IATF (International Automotive Task Force) and sets out requirements for quality management systems and specific requirements for the application of ISO 9001:2008 to serial and spare parts production in the automotive industry. Moreover, it is complemented by so called Customer Specific Requirements (CSR) of individual international vehicle manufacturers.

[51] ISO/TS 16949 -7.4

[52] ISO 26262-10:2012 -11.3.6.2, table 4.

[53] ISO/DIS 26262-10 -5.1.3.2 „Level of independence for performing the confirmation measures".

not have participated in the work product's development or conception in order to ensure the most objective evaluation possible. With regard to the hazard analysis and the risk assessment, the item's developers, the project management and the authors of the work product are to be independent. The same "level of independency" is required for the confirmation review of the item integration and its testing plan, the validation plan and the safety analysis.[54]

2.

From a legislative and contractual viewpoint, this normative requirement of independence has legal quality with respect to what is required of a company's organization as well as the FSM personally. This requirement is not only targeted at generating or confirming technically correct work products based on objective evaluations. It is in particular intended to establish reliable communication between the parties involved in a safety-related system's development and production, i.e. supplier and manufacturer, as to whether statutory and agreed safety goals are being met. The addressee needs to be able to trust that statements and decisions based on this independence are reliable, accurate and faultless; this becomes all the more important considering that he will have only limited possibilities to check their being correct by carrying out verification and validation procedures if a product-specific supply chain consists of various suppliers. This is why ISO 26262 personifies this aspect by requiring that a person be appointed who shall be responsible for the contractual relationship between supplier and vehicle manufacturer.[55]

3.

The FSM's basis for decisions and his conclusions, which rely on independence, can be attributed to the company for the most part. According to ISO 26262, they represent the company's entire project-related level of know-how measured against state-of-the-art science and technology. By confirming compliance with ISO 26262, i.e. confirming that designated and agreed safety goals are being met through safety measures which have been determined and are applied to all processes, the company defines this know-how and pretends to have it. This know-how has to be documented, and thus be made an available resource, within the framework of a knowledge management which in turn is part of the overall technology management.[56]

---

[54] ISO 26262-2:2011 -6.4.7.1, table 1. The same requirements apply to the functioncal safety audit (ISO 26262-2:2011 -6.4.8) and the functional safety assessment (ISO 26262-2:2011 -6.4.9).

[55] ISO 26262-8:2011 -5.4.2.2 lit. e)

[56] Very detailed and to the point with respect to technology management: Müller in Ensthaler/Gesmann-Nuissl/Müller: "Technikrecht: Rechtliche Grundlagen des Technologie-

The FSM is always part of the knowledge management because he combines the company's entire knowledge in one function with direct external impact and because he represents this knowledge and is solely responsible for external communication about it: This applies to confirming that contractual obligations have been fulfilled as well as to giving rise to safety expectations regarding the operation of a safety-related item. The term knowledge describes a rather broad notion in this context: It encompasses any relevant information available to a company during the concept phase, development and production of a safety-related system. At the same time it also encompasses the electronic systems' "language" and their interaction. Communication within and between electronic components is based on flow-controlled data streams which are capable of modeling information or objects at the level of semantics, that is they can represent or trigger the technical processes for a safety-related system's intended functionality.[57] This information consists of datasets which are generated by the item and thus poses a challenge to knowledge management as generating and transferring this information is at the most triggered by a person but not deliberately controlled.[58] This information inevitably contains shortcomings arising in particular from the above mentioned arbitrarily selected assumptions and risk assessments of potential and probable failure of electronic components, i.e. failure which cannot be completely controlled. Testing software is of course subject to the same limited capacities.

4.

Ensuring the FSM's independence is a contractual obligation (Section 280 of the German Civil Code, BGB) throughout the entire supply chain. In my opinion, this does not only apply to the bilateral contractual relationships between suppliers and their customers at the next level of the supply chain or between an item manufacturer (Tier 1) and the vehicle manufacturer, but also entails protective consequences for the entire supply chain in which all actors depend and rely on each other. This is due to product responsibility according to the German Product Safety Act. Hence, ISO 26262 requires Development Interface Agreements (DIA)[59] as part of the safety plan; the DIA is to contractually determine each supplier's obligations as to their performance

managements" (technology law: the legal basis of technogoly management), Berlin/Heidelberg: Springer, 2012, p. 353 ff.

57 Müller in Ensthaler/Gesmann-Nuissl/Müller: "Technikrecht: Rechtliche Grundlagen des Technologie-managements" (technology law: the legal basis of technogoly management), Berlin/Heidelberg: Springer, 2012, p. 353 ff.

58 Ensthaler/Müller/Synnatzschke: „Technologie- und technikorientiertes Unternehmens-recht" (Technology- and engineering-oriented corporate law), BB 2008, 2643.

59 Sample in ISO 26262-8:2011, Annex B; ISO 26262-2:2011 -6.4.3.5 lit. f)

of the contract and their compliance with the item requirements of the vehicle manufacturer who is the last link of this chain of responsibility.[60]

5.

Primarily, the independence of FSM, i.e. persons making decisions, must be efficient. According to ISO 26262 they shall have the necessary authority, corresponding to their responsibilities, to maintain and monitor[61] the safety plan.[62] This requirement of the standard is contradictory: The company's management has to ensure the FSM's authority and implement control mechanisms thereto within the overall risk management system of the company (Section 91 (2) of the German Stock Corporation Act, AktG), the effectiveness of which, however, depends in turn on the FSM's professional competence and his authority to stand his ground in the face of opposing opinions. Therefore, the company management's release from primary liability by dint of appointing an FSM cannot be assumed just like that.

6.

As a consequence of this required authority and its realization, the FSM is inevitably confronted with conflicting goals at different levels which can only be addressed briefly in this paper. In the first instance, employing an FSM generates costs on the company's part, the efficiency of which is not directly measurable. Where the FSM is an employee, conflicts in terms of authority and responsibility can arise with his supervisor or, since the FSM's decisions apply across departments, with other departments of the company. The position as employee is compromising the strict and imperative independence according to ISO 26262. The measures taken and the decisions made by the FSM do not always have to be compatible with the company's interests, for instance if he dismisses results, does not give in to time pressure or insists on his decisions despite exceeding his budget.

7.

Moreover, the FSM is exposed to risks because he is personally responsible[63] for statements made concerning an item's safety as well as for misjudging aspects of the safety lifecycle[64]. He

[60] ISO 26262-8:2011 -5.

[61] ISO 26262-2:2011 -6.4.3.2 and 6.4.3.5

[62] ISO/TS 16949 -5.5.1.1 basically sets out the same form of authority when stipulating that personnel "responsible for conformity to product requirements shall have the authority to stop production to correct quality problems."

[63] Good overview on liability of employees who are responsible for quality management focusing on development activities: Dihlmann/Karcher/Schmidt/Gildeggen: „Die persönliche Haftung des Entwicklungsingenieurs für Produktfehler" (The development engineer's liability for defects), PHi 2012, p. 148 ff.

has to evaluate the results of a series of steps that have been taken beforehand and cannot audit every downstream activity in detail but rather needs to count on others for their work results to be reliable. Furthermore, it is not in his power to decide how the safety standards, maintained and confirmed by him, are used in contracts with other suppliers or vehicle manufacturers or how the vehicle manufacturer himself uses them in contracts with final customers. False, incomplete or exaggerated statements regarding the FSM-confirmed safety of an item and its interaction with other systems or the whole vehicle can lead to a defect according to Section 3 of the German Product Liability Act (ProdHaftG) on grounds of safety expectations not having been met; in this case the FSM has not had any influence on such statements.

The FSM is also responsible for consequences of false decisions made by his company, for example where risks are played down, in spite of a serious potential hazard, causing this risk to be assigned a lower ASIL than would actually be appropriate. It is a known fact that there are recurrent defects in vehicles' engine controls such as the following: The engine control fails at high speed and the emergency mode is activated. If the vehicle is driving on the left lane of a highway while the engine fails and needs to be maneuvered to the breakdown lane passing trucks which drive very closely to each other, the potential for an accident to occur is extremely high. Yet, this defect, the cause of which is allegedly unknown, is only assigned ASIL A and not ASIL D. There is no information on this in the operating manual. In the event of a liability trial, an independent FSM and his company will have to be ready to be asked how they justify trivializing this defect, especially if its cause is (allegedly) unknown but the vehicle is still put on the market.[65]

Besides corporate liability there is also the issue of the FSM's personal liability. The role of an FSM is for the most part comparable to that of a compliance-officer. Hence, there could be cases in which the FSM's position involves duties that could be relevant under German criminal law, comparable to what the German Federal Court of Justice (BGH) decided on compliance-officers.[66]

Therefore, the FSM needs special legal protection: From the viewpoint of labor law, a prohibition of discrimination due to any measures taken by the FSM has to be added to his employment contract. Moreover, the company has to indemnify him from all consequences following his actions, excluding cases of intent or gross negligence.

---

[64] ISO 26262-2:2011 -7.4.2.3

[65] The author has had experience with this kind of defect three times so far. This subject is discussed in internet chat rooms. The protocols of the diagnostic software do not provide any hint whatsoever as to what caused the failure to occur. The drivers thus remain guinea pigs for the vehicle manufacturer's – alleged – technical ignorance.

[66] BGH, July 17, 2009 – 5 StR 394/08.

In the event of the company going bankrupt, these protective measures in the employment contract are of no use to the FSM. Third parties can assert claim against him. This is why it is imperative that the FSM be included into the company's Public and Product Liability Insurance. Current insurance policies do not cover this aspect. Irrespective of the company, the FSM has to be exempt from the risk of costs potentially incurred due to civil or criminal legal defense by benefitting from legal protection insurance that can cover the costs; additionally, such insurance needs to remain in force even after the FSM might have left the company.

8.

The problem has become a practical one and is subject to intensive discussions without there being any clear, straight line to find a solution. In their presentation "A Critical View on 'Independence' in ISO 26262" at the 4th EUROFORUM conference on ISO 26262 in September 2012, Peter Grabs and Pierre Metz have indicated the problems arising from the standard's vague wording, the insecurities as to how the standard is to be dealt with on the whole and risks resulting thus. They describe the standard's inadequate definition of independence to the point – albeit not completely – with the following key words: "creates confusion; does not prevent economical [sic!] bias; does not prevent 'selective hiring'; neither addresses nor guarantees competence, can lead to arbitrary organizational changes" and "does not reflect psychology".

Grab and Metz propose an "objective" approach and state that "Independence merely is a method but not a goal". A process-oriented approach such as is set out by ISO/TS 16949 is the right path, but does not change the subjective quality of the FSM's independence in a legal sense at all since the term remains legally undefined.[67]

With regard to this individualization of liability for the company's actions concentrating on the persons of the FSM, the term independence, which does entail legal implications, is an alien element within ISO 26262. The strict, item-related and process-oriented standard cannot provide a specific process to define this independence in a legal sense because too many aspects of corporate law, labor law and insurance law are implied. Deleting the requirement of the FSM's independence might be recommendable for the standard's revision in 2014. Leaving it at the requirements of Chapter 6 of ISO/TS 16949 (Human resources) combined with determining the FSM's function during audits, reviews and assessments should be sufficient for the purposes of the standard.

[67] Conference documents of the 4th EUROFORUM Conference on ISO 26262 from September 12 to September 14, 2012. See Helmig: "Functional Safety in accordance with ISO 26262 and product liability for No Trouble Found events", http://www.notar-helmig.de/de/publikationen.html (The German original was published in PHi 2012, p. 32).

V

Technical standards, such as ISO 26262 for functional safety in personal vehicles, have direct legal relevance by being a basis to construe legal obligations within a sector such as the automotive industry.

What is technically possible can only be legally permissible if realizing the technically possible corresponds to statutory safety requirements, the latter always being part of safety goals which are determined by standards.

ISO 26262 is a process-oriented standard for the functional safety of safety-related systems standardizing a company's actions. It does not guarantee a vehicle's safety, but rather makes the vehicle controllable when it comes to anticipated hazards occurring under assumed conditions with respective probabilities of exposure.

ISO 26262 is by no means a detached standard. It can only be efficient within the framework of an effective quality management system.

The decision makers as envisioned by ISO 26262, i.e. Functional Safety Managers, are always managers within the quality management system and thus assume high personal responsibilities, just like quality managers. The imperatively required independence as set out by ISO 26262 necessitates protective measures through the company as well as labor law in terms of employment contracts.

Translated from German into English by Charlotte Kieslich