Functional Safety in accordance with ISO 26262 and product liability for No Trouble Found events

02/11/2012 by Dr. Ekkehard Helmig

The author is a lawyer and notary specialized in law governing the automotive supplier industry.
helmig@notar-helmig.de

ISO 26262 "Road vehicles -- Functional Safety" raises many issues regarding product liability, notably in cases of No Trouble Found. The processes of ISO 26262 in conjunction with ISO/TS 16949 always require adequate and extensive documentation. This documentation results in a significant simplification of the burden of proof in liability trials.

"The automobile is going to be reinvented. On-board computers will take over control in the cockpits: They will accelerate, slow down and overtake on their own." This is the future of driving as depicted by the newspaper Frankfurter Allgemeine Sonntagszeitung on January 8, 2012, in its preview of the Detroit Motor Show.[1] It quotes Daimler's head of development: "The autopilot could drive you to your holiday destination to Italy over night. You push "Brenner" and go to sleep."[2] Interconnected advanced driver assistance systems, traffic sign recognition, lane departure warning, electronic steering, tire pressure gauges, EPS, ESC, active roll stabilization systems, distance warning systems and drowsiness alert systems, to name but a few, complete – usually at extra charge – car manufacturers' and suppliers' offers of all-inclusive packages, primarily suggesting safety.

The downside does not play that big a role: What use is a lane departure warning if the public sector, in order to save costs, is decreasingly making use of road markings without which the system does not work?[3] What use is a Pre-Safe Brake, the radar of which only reacts to metal and edges but not to human bodies?[4] Scientific evidence shows that vehicles, not necessarily most modern ones, can be remote-controlled by hackers.[5] Drivers in deep sleep dreaming of their holidays in Italy do not fit into the mold of the international and still effective Vienna Convention on Road Traffic of 1968[6] which stipulates in Article 8(6.1) that: "A driver of a vehicle shall at all times minimize any activity other than driving", notably sleeping. And finally: too many safety features can overwhelm a driver, especially if one of the functions fails and the driver needs to handle the remaining ones to make the right decisions within seconds.[7]

---

[1] Frankfurter Allgemeine Sonntagszeitung (FAS), January 8, 2012, p. 27.

[2] Ibid.

[3] ADAC Motorwelt 12/2011, p. 50: Dangerous greed: The public sector is decreasingly making use of road markings for rural roads. This is an extremely dangerous practice: drivers lack orientation and modern lane departure warning systems are useless without road markings.

[4] "Ich bremse nicht für Tiere und Fußgänger". (I don't brake for animals or pedestrians), Frankfurter Allgemeine Zeitung-net, August 2, 2011. http://www.faz.net/aktuell/technik-motor/auto-verkehr/pre-safebremse-von-mercedes-ich-bremse-nichtfuer-tiere-und-fussgaenger-11106917.html.

[5] Automobildwoche, May 30, 2011. http://www.automobilwoche.de/apps/pbcs.dll/article?AID=2011110529981&NL=1. Hacking was possible via mobile phone, Bluetooth and a manipulated music file on a CD-ROM. The brakes as well as the engine control unit were rendered inoperative. Furthermore: Financial Times Deutschland, September 14, 2010, p. 1.

[6] http://en.wikipedia.org/wiki/Vienna_Convention_on_Road_Traffic

[7] Automotive News, November 14, 2010, p. 14.

The increased use of electronics in almost all vehicle systems as well as in their functions for driving behavior, including a connection to the internet, cannot be stopped. This increase also serves the vehicles' safety. But the complex technology of interconnected hard- and software and their functions combined in one electronic control unit poses currently uncontrolled risks; in particular, on grounds of a lack of standards for compatibility of software products by different manufacturers and increasing risks inherent in software from the internet that is not vehicle-specific, experts describe this phenomenon to the point by referring to it as "New Vulnerability".[8] Due to a primarily cost driven upgrading of vehicles with navigation and infotainment devices by different manufacturers, risks are accumulated as a result of driver distraction or complete loss of control over the vehicle caused by malware that uses its access to the system to exploit specific functions.[9]

Since 2008, if not earlier, the industry and its standard organizations have tried to gain control over the technological challenges they are faced with regarding interconnected safety systems and the interdependencies thereof by means of an international standard: ISO 26262 "Road vehicles – Functional Safety" is considered to be a generally appropriate tool to this end.[10] The standard's pretension to provide "functional safety" by dint of electronic safety-related systems establishes the safety requirements as defined by Section 3 of the German Product Liability Act (ProdHaftG) on a legal level; necessarily, the latter remain to a large extent unfulfilled by reason of the current lack of controllability, since, despite ISO 26262, there are no binding standards with regard to the overall safety architecture that would result from coordination among vehicle manufacturers or legislation.[11]

1 The content of ISO 26262

The standard cannot be described in its entirety in this article. The author focuses on those passages he deems to be the most relevant in terms of their legal significance. In order to be legally binding, standards must be agreed upon by contract. Apparently, almost all vehicle manufacturers have

---

[8] Automotive News, September 20, 2011, p. 28: "War with computer hackers hits the road". Recent attacks on thousands of computers with the so called DNSChanger worm demonstrate how deeply people mistrust internet security: in the second week of January 2012, the German Federal Office for Information Security (BSI) recommended to eliminate this malicious software by means of applying a testing software provided by BSI, Telekom and the Federal Criminal Police Office (BKA). However, according to a report by the journal *Focus* on January 13, 2012, internet users did not trust the software "dns-ok.de" as they feared their computers would get infected with the state trojan. http://www.focus.de/digital/internet/angst-vor-demstaatstrojaner-internetnutzer-trauendns-ok-de-nicht_aid_701936.html

[9] Especially in the USA warnings against driver distraction grow louder: „Chilling to watch, the video illustrates a major problem confronting the auto industry: driver distraction. Technology is pouring into cars. It has become a big selling point. But concerns about safety are escalating. Texting while driving is the current hot-button issue, but it represents only one of many alluring features that draw driver's attention away from the road."
Automotive News, May 3, 2010, p.3.

[10] As of this writing the standard is only available in English and not yet in its final version; however, the automotive industry already considers it to be a decisive standard. A German version is not expected. The first revision is expected for 2014.

[11] The EC-Regulation No 661/2009 of July 13, 2009, (OJ L 200/1, 31.7.2009) "concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor" requires the binding introduction of safety systems as precondition for type-approval. Yet, the Regulation does not state any provisions concerning requirements for these systems and their interdependencies, but it simply adopted what the industry already offers. Cf. Helmig, "Fahrzeugsicherheit versus Fahrerverunsicherung. Kritische Überlegungen zur KVV und zur ISO 26262" (Vehicle safety vs. driver uncertainty. Critical thoughts on KVV and ISO 26262). In: Phi 2010, p. 198 ff.

integrated ISO 26262 requirements for the development of new vehicles with safety-related systems into specifications and interface agreements as of 2011.[12]

The current version of ISO 26262 comprises 10 parts: Part 1: Vocabulary, providing the essential definitions. Part 2: Management of functional safety.[13] Part 3: Concept phase of an electronic system. Part 4: Product development at the system level. Part 5: Product development at the hardware level. Part 6: Product development at the software level. Part 7: Production and operation. Part 8: Supporting processes. Part 9: Automotive Safety Integrity Level (ASIL – Determination of safety categories assigned to safety goals after risk assessment for a representative sample of people from the target market[14]). Part 10: Guideline for understanding and application of ISO 26262.[15]

2 The goal of ISO 26262

ISO 26262 is considered to be a framework for future operation of safety-related electrical and/or electronic (E/E) systems in series production passenger cars with a maximum gross vehicle mass up to 3.500 kg.[16] Yet, the standard itself sets limits as to its application and thus its effectiveness for the safety of the vehicle in its entirety: „ISO 26262 addresses possible hazards by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems."[17]

It addresses possible hazards by malfunctioning behavior and/or interaction of the above stated systems.[18] The term "freedom of interference" describes the standard's requirement to prevent unintentional interaction of different software as well as negative mutual interference. The safety oriented processes stipulated by ISO 26262 are intended to avoid such hazards, if possible. The goal of the standard was appropriately phrased at the "Safetronic" conference in November 2011: It is crucial to identify the hazards a system can cause, to determine the associated risks and to demonstrably reduce them to an acceptable residual risk by taking appropriate countermeasures.[19] Functional Safety is therefore (merely) an approximation to the highest possible degree of preventing predictable, hence avoidable, risks.[20]

---

[12] However, as can be seen in practice, there still remains considerable uncertainty and vagueness as to the correct as well as the functional application of the standard. This applies in particular to the requirements' compatibility with other standards for vehicle electronics, such as Autosar or SPICE, and to the use of software of different provenance, such as specific software for selected control modules, vehicle manufacturers' or suppliers' embedded software and so called open software by different providers for electronic parts or components.

[13] The term "management" is a generic term for the application of the processes described in ISO 26262. It is not synonymous with management in terms of quality management systems as part of a company.

[14] ISO 26262:3-7.4.3.2

[15] In order to gain initial understanding of the extensive standard counting 370 pages, it is advisable to first read Part 10 and look up the terms' definitions in Part 1.

[16] In the terminology of European legislation this vehicle mass category corresponds to the vehicle categories M1 and N1 in accordance with the Directive 2007/46/EC relating to type-approval (OJ L 263/1, 9.10.2007).

[17] ISO 26262:2-1. While the term "safety" accordingly refers to the safe functioning of a system, physical "security", which prevents unauthorized access to application software, is not taken into account.

[18] ISO 26262:2-1. Suddenly occurring overvoltage resulting from the overall electric system of a vehicle is one of the major causes for system failure; afterwards, it is not possible to detect or reproduce the overvoltage's source.

[19] Trapp, Fraunhofer Institute for Experimental Software Engineering (ISES) in Kaiserslautern, presentation given at the "Safetronic" conference.

[20] ISO 26262 uses the term "unreasonable risk". 1.136; 26262:3-7.2.

Vehicle safety depends on the behavior of implemented control systems.[21] This is why ISO 26262 sets out a "concept of safety goals" as well as a "safety concept" in six steps: (1) Risk assessment and an analysis of possible harm and damage (hazards) are used to identify those harms requiring risk reduction; (2) For each hazard a safety goal has to be set; (3) Each safety goal is assigned a respective ASIL; (4) The functional safety concept thereby resulting describes how the safety goals can be reached (functionality); (5) The safety concept thus deriving describes how this functionality is to be implemented at the hard- and software levels; (6) Software safety requirements and hardware safety requirements determine system-related safety requirements which are to be implemented into the software and hardware designs.[22]

ISO 26262 sets out safety requirements based on assumptions

Every risk analysis and assessment for the dynamic environment of technical systems interacting in a vehicle in today's hectic transport is based on rather arbitrary assumptions concerning the conditions under which such risks exist. There always remains a situational residual risk due to the tremendously high number of unpredictable factors. The standard is based on the fact that absolute safety cannot be achieved for there is so absolute guarantee for software failure in electronic systems not to occur. According to ISO 26262, a "safety case" is given, where evidence based on assumptions can show that a system is free of "unreasonable risk" (rather: "intolerable").[23] It gives a completely vague definition of "unreasonable risk": „Risk judged to be unacceptable in a certain context according to valid societal moral concepts".[24]

The most important factors posing a threat to safety in this risk avoidance concept are the driver as well as other traffic participants. The determination of a safety case requires an evaluation of the controllability[25] of a given hazard, i.e. an estimation of the probability that the driver or other persons[26] potentially at risk are capable of gaining sufficient control over the hazardous event, such that they can avoid this specified harm. The standard calls this the "controllability"[27] by a "representative driver", meaning the driver is at an average age, not tired and in appropriate condition to drive, has average driving experience and complies with traffic rules and due care requirements regarding other traffic participants – hence, a species that could not possibly have been described more vaguely. The standard does not mention any decisive criteria as to how technicians are to implement those individual

[21] ISO 26262:10 -4.1 lit. b).

[22] ISO 26262:10 -4.1. lit. b).

[23] ISO 26262;10-5.3.1. Translations of the terms used in ISO 26262 often lead to inaccuracies, especially since the authors of the standard are not exclusively English native speakers. A literal translation of "safety case" into German could be misleading in that it implies a case of lacking safety, whereas ISO 26262 uses the term in a generic way to express that safety is given and proven. This is illustrated by the definition of the term (ISO 26262-1.106): "safety case: argument that the safety requirements for an item (System) are complete and satisfied by evidence compiled from work products of the safety activities during development" (i.e. from work results of the different conception processes).

[24] ISO 26262:1 -136.

[25] ISO 26262: 10-6.2: Controllability is defined as avoidance of a specified harm or damage by timely reaction of the person exposed to the risk.

[26] Stöhr: "Innocent bystanders". In: "Neminem laedere - Festschrift für Gerda Müller zum 65. Geburtstag" (Eds.: H.-P. Greiner, N. Gross, K. Nehm; A. Spickhoff), Köln 2009.

[27] The standard defines Controllability in ISO 26262-1.20 as "the ability to avoid a specified harm or damage through timely reactions of the persons involved, possibly with support from external measures."

assumptions to fully achieve the technical safety-related system requirements deriving from the challenges posed to the driver.[28]

The standard implies that by compliance with the designated processes therein for the concept, development and production phase, including the always required counterchecks, almost all causes of errors can be detected and minimized, such that the results confirm with a high probability that a tolerable risk can be defined which must be accepted. These results are verified and validated, thus supported by documentation, by means of Reviews (examination of the work products of the respective safety activities), Audits (application of the processes for functional safety) and Assessments (evaluation of the system at the vehicle level) of the above stated processes.[29]

According to the standard, Reviews and Audits shall not be carried out by those who evaluated whether the assumptions were correct. ISO 26262 requires these "Functional Safety Managers" be independent without naming sufficient conditions for this independence.[30] An employee in the position of Functional Safety Manager in a company is not independent, at least not if he were to make decisions that would be detrimental to his supervisor in terms of expertise or that would be contrary to cost objectives set by the management. External consultants, too, will scarcely be independent, if they have to fear for the next assignment in this branch that offers only limited business opportunities with a small number of clients. The independence required by ISO 26262, being essential for the justification of decisions about the conditions under which a tolerable risk is given and thus about the conditions for a saleable safety-related product, remains a legal fiction; the standard qualifies the legitimate safety expectations drivers have regarding the flawlessness of its results.[31]

ISO 26262 standards are but process standards

ISO 26262 is not a standard for manufacturing specific safety-related products. It explicitly does not address the actual performance and functionality of a safety-related system, for instance it does not guarantee that a lane departure warning system actually takes steps to ensure the vehicle stays in its lane. The standard describes but processes which, if complied with, applied and documented correctly,

---

[28] ISO 26262-3-Annex B 4 states: „The determination of the controllability class, for a given hazard, requires the estimation of the probability that the representative driver will be able to retain or regain control of the vehicle if a given hazard were to occur. This probability estimation involves the consideration of the likelihood that representative drivers will be able to retain or regain control of the vehicle if the hazard were to occur, or that individuals in the vicinity or the situation will contribute to the avoidance of the hazard by their actions. This consideration is based on assumptions about the control actions necessary by the individuals involved in the hazard scenario to retain or to regain control of the situation, as well as the representative driving behaviours of the drivers involved (which may be related to the target markets, individuals' age, eyehand coordination, driving experience, cultural background, etc.)."

[29] Verification as defined by ISO 9000:2005 3.8.4. is the confirmation that a work product fulfils the specifications agreed on, i.e. it fulfills its intended function at the supplier level. Validation as defined by ISO 9000:2005 3.8.5. gives an answer to the question whether the verified product fulfills its functionality at interfaces with other systems or components at the manufacturer level.

[30] In Germany the Functional Safety Manager will often have responsibilities comparable to compliance-officers, whose position involves duties relevant under the German criminal law. (German Federal Court of Justice (BGH) on July 17, 2009, 5 StR 394/08 –Compliance Officer).

[31] The independence could be ensured by certification in accordance with EC-Regulation No 765/2008 "setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93" (OJ L 218/30, 13.8.2008).

are to reduce the risks of a defectiveness intrinsic to electronic systems at the manufacturer's professional discretion. [32]

In order to do so the standard describes three tools: the "functional safety audit", which confirms the correct application of the processes described for the functional safety of a system; the "functional safety assessment", which confirms the steps decided upon for the concept, development and implementation of the system's design in order to guarantee that the system provides functional safety; the "confirmation reviews", which confirm that the "work products"[33] resulting from the different processes meet the goals set for the development life cycle.[34]

The processes described in ISO 26262 require to be linked with those for quality management in product realization in accordance with ISO/TS 16949:2009-7.[35] This obligatory integration is but marginally implied by the standard without setting out own requirements.

3 No Trouble Found (NTF), in search of the root cause

If an electronic safety system fails, the root cause cannot be detected, usually. In most cases, diagnostic systems are only capable of identifying a control unit in which an error has occurred. Errors that occur in volatile memory cannot be traced or reproduced at all. Neither the software's precise malfunctioning behavior that actually caused the failure (e.g. ionizing radiation, electromagnetic fields etc.), nor whether there are other causes, such as suddenly occurring, but not reproducible, overvoltage in the vehicle's overall electricity or non compatible software, can be detected afterwards. The effectiveness of testing software used in product development is limited to providing answers to designated test results. There is no testing software that could detect all possible error causes in another software by itself. Accordingly, diagnostic software used by automobile repair shops or implemented in the vehicle has limited capacity of doing so as well. Therefore, the driver, i.e. the party injured by failure of an electronic safety system, cannot provide the initial proof that is required in order to pursue a recourse claim against the vehicle manufacturer.[36]

The inability to detect errors when field failures occur as well as the deliberate or actual incapacity of reproducing errors or identifying root causes lead to annual warranty costs in the billions for the automotive industry. These costs will continue to rise in the course of the continually increasing use of electronics in vehicles. This is the reason why the German Association of the Automotive Industry (VDA)

---

[32] In Part 2 the standard refers to the compliance with and application and documentation of the processes as "Management of functional safety": "The key management tasks are to plan, coordinate and track the activities related to functional safety. These management tasks apply to all phases of the safety lifecycle" (ISO 26262:2-5.2.2).

[33] ISO 26262:8 -7.2 ff

[34] ISO 26262:10 -5.1.3.1

[35] ISO 26262 implies the integration of its processes into an effective quality management system, 2-5.3.2; 2-5.4.4.1; 8-5.4.2.1 (Note). For more details see Helmig, "Die ISO/TS 16949 steuert den Sachmangelregress in der automotiven Zulieferkette" (ISO/TS 16949 and its implications for recourse claims in the automotive supply chain on grounds of defect.), in: Phi 2001, p. 2 ff.

[36] Classic examples are the numerous cases in which airbags were triggered by error, as is also shown by the decision of the German Federal Court of Justice (BGH) on airbags, handed down on June 16, 2009. (VI ZR 107/07, VersR 2009, 1125); on this topic see Helmig, in: Phi 2009, p. 190 ff.; almost as frequently, cruise control systems fail and cannot be switched off, "Mercedes-Rückruf: Defekte Tempomaten" (Mercedes product recall: defective cruise control) Automobilwoche.de, April 13, 2011; Jaguar recall of 18.000 vehicles for a faulty cruise control software, Computerworld, October 24, 2001.

introduced the standard "Schadteilanalyse Feld" (field failure analysis) in 2009 as a tool to reduce these costs. In its introduction the standard states: The high amount of complaints from the field for which no errors can be detected constitutes an important spectrum of activity for the automotive industry. Complaints involving this kind of results are often either not dealt with any further or there is a lack of methodological approach to determine an error in a given product, process or system. In addition to warranty costs/ guarantee costs, which could often be avoided, components in which errors occur that cannot be reproduced generate high costs for logistics and analysis processes without there being any comparable economic benefit."[37]

The VDA standard thus defines the "NTF process" as follows: The process is used to find the causes for a problem that could not be identified in preceding analyses.[38] Where the NTF process has to be launched, at least one other VDA standard for avoiding errors as well as its verification method, for instance VDA 4.2 (Failure Mode and Effects Analysis, FMEA), have failed during product development: The VDA standard "Maturity Level Assurance for New Parts", as detailed methodological approach for planning quality in advance, is actually intended to avoid precisely those error causes during product development, which have to be determined by the NTF process after the field failure has occurred.[39]

4 ISO 26262 vs. VDA field failure analysis

The stringent and limited process oriented approach of ISO 26262 for concept, development and production phases of safety-related systems in vehicles is aimed at approving only those systems representing at the most not avoidable, yet acceptable risks; this pushes aside the interest to pursue recourse claims during an NTF process and reprioritizes extended root cause analysis. The VDA standard's concept is not adapted to the later published ISO 26262. ISO 26262 is itself not cut out to cover the increasing influence of, for instance, application software from the internet or to cover constantly modernized safety systems and electronic components, because there are no standards for this purpose (lacking "Control Flow Monitoring") and therefore every manufacturer develops individual apps, unknowing as to how they might interfere with or influence the other electronic systems in the vehicle due to their internet connection.[40]

Whoever invokes compliance with the processes of ISO 26262 carries the burden of proof for having satisfied all requirements the standard sets out. If this condition were given, there should be next to no NTF events from the field as the maturity level assurance has confirmed that a component was ready for

[37] VDA: "Das gemeinsame Qualitätsmanagement in der Lieferkette: Vermarktung und Kundenbetruung – Schadteilanalyse Feld" (Joint Quality Management in the Supply Chain: Marketing and Service), 1st edition 2009, ISSN 0943-4912. Daimler AG has applied this non-binding standard recommendation of the VDA to its own Werksnorm MBN 10448 (i.e. a corporate standard) which it has integrated into contracts with suppliers. In practice, however, the VDA standard's efficiency is diminished as its application is less intended to improve damage analysis in order to avoid errors and prevent accidents, but to establish a system to pursue recourse claims against suppliers. The cost driven priority is to reduce the number of defective parts that are returned from the field (so called reference market procedures). Analyzing root causes is neglected as a complaint only leads to the defective part being identified by the vehicle manufacturer. In practice, root causes, for which the vehicle manufacturer could be responsible or which result from the operating conditions under which the vehicle failed, are mostly not taken into consideration.

[38] VDA:"Schadteilanalyse Feld" (field failure analysis), p. 17.

[39] VDA: "Reifegradabsicherung für Neuteile". (Maturity Level Assurance for New Parts), 2nd revised edition, 2009. ISSN 0943-9412.

[40] Financial Times Deutschland, January 3, 2010, p. 4; Automobilwoche, February 21, 2011, p. 26.

series production. This holds true even more for the application of ISO 26262 because the Audits, Assessments and Reviews, which are intended for series production by the standard and carried out by independent experts, are interdependent in a way that is to rule out precisely the occurrence of not detectable errors and error causes.

Every NTF event that occurs anyhow (such as failing cruise control)[41] thus indicates a failure to comply with the processes or refutes the assumed quality and integrity of safety goals and the assessments thereto. Every NTF event that occurs anyhow refutes that the measures taken, based on the assumptions underlying the concept, development and production of a system, were sufficient to meet the safety goal assigned to a system to make it ready for series production while only posing a risk that is still tolerable. Until proven otherwise, every case of NTF declares the decision about a product being ready for series production as having been premature.[42]

5 "New vulnerability" due to documented processes

All processes in accordance with ISO 26262 have to be documented.[43] In case of liability or recourse claims ISO 26262 provides the guideline for the plaintiff's litigation. The plaintiff can identify the documentation based on the standard and, competently advised as to what the evidence is to proof, force the vehicle manufacturer to present the documentation in order to avoid a sentence due to discovery, the latter being inadmissible under German civil law. The procedural tools in this context arise from Sections 421 ff. of the German civil procedure code (ZPO). This also applies to pre-trial discovery in accordance with U.S. law, for which there are also possibilities within the scope of legal assistance in Germany.

The stringent processes of ISO 26262, oriented to the safety requirements of a product, establish a new vulnerability of the manufacturer of a safety-related system with respect to the evidence available. This is the price for giving rise to high safety expectations on the part of final customers by invoking compliance with the ISO 26262 processes; without these expectations the safety features would not be bought at extra charge, yet they get disappointed by the assumed non-compliance with ISO 26262 in cases of NTF. This, too, is taken into account by ISO 26262: As early as in the concept phase, legal requirements are just as important to be followed as technical requirements.[44] The same is required for an efficient quality management system.[45]

Cases of NTF are usually due to deliberate or ignored insufficiencies during the development process. Section 6 of the German Product Safety Act (ProdSG) stipulates that the manufacturer shall preventatively inform the customer about this and particularly about the fact that electronic systems can never be absolutely free of errors and as such represent potential hazards, including foreseeable misuse (Sections 2 (28)and 3 ProdSG). This is an explicit lesson learned from the BGH's airbag decision, also and especially if a safety-related system's saleability depends on the promises made with regard to safety, which necessarily conflicts with the manufacturer's obligation to inform customers about potential risks.

---

[41] Cf. footnote 36.

[42] This is a consequence of the BGH's decision on airbags (ibid. footnote 36); the BGH has stipulated that all required measures to avoid hazards shall be taken during the planning and concept phase.

[43] ISO 26262; 8-14.4.5.1; 10-9.4

[44] ISO 26262:3-5.2.

[45] ISO/TS 16949:2009 -1.1, note 2.

With respect to recourse claims the legal relationship between vehicle manufacturer and the suppliers of safety-related systems is essentially a matter of their processes being harmonized. ISO 26262 explicitly requires a Development Interface Agreement (DIA) determining responsibility interfaces (verification by the supplier, validation by the vehicle manufacturer). The responsibility for functional safety in a vehicle currently falls to numerous suppliers hardly cooperating with one another due to competition. The DIA's exactness, managed by the vehicle manufacturer including full documentation of all decisions made within the scope of Audits, Reviews and Assessments as well as Control Flow Monitoring at the interfaces, determines liability and the liability quotient. ISO 26262, by its very nature, provides all parties with evidence.

Translated from German into English by Charlotte Kieslich