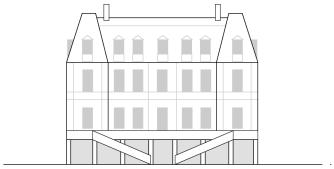

KANZLEI DR. ERBEN

Kanzlei Dr. Erben - Neuenheimer Landstr. 36 - D-69120 Heidelberg

Safety Designed Software Development:
Legal Aspects

1. Introduction

The use of software in automobiles increases rapidly.[1] As software – unless it is completely trivial – cannot be produced without faults, the number of software defects in electronic controller units (ECU) of the automobile increases as well, leading to malfunctions and failures of electronic systems.

Defects in safety relevant applications such as driver assistance systems (steering, brakes etc.) may have disastrous impacts on the OEM as well as on their suppliers: Defective products may not only cause personal deaths or injuries, but they may also result in recall actions, producing high costs and material damages of the reputation of – all – the companies involved. Since the risks arising from a legal conflict in connection with statutory or contractual liability are more than costly, the subject matter of safety designed software development should be treated with utmost attention.

In this lecture, we shall outline the potential warranty and liability risks under German law regarding defects in software, and we shall then present a composition of the necessary organizational and legal measures regarding the contractual and the project management, in order to prevent the realization of these risks to the extent possible.

2. Basic Legal Principles Regarding Defective Products

2.1 "Defect" in Terms of Law

The supplier is basically only liable to its customer or to any third party, in case its product contains a defect in terms of law. Therefore, the term "defect" is the central term within the framework of warranties and/or liabilities. In order to decide which measures must be taken to ensure that the development process of software and/or the resulting product does not contain a defect in terms of law, we shall first take a closer look on the legal definition of "defect".

2.1.1. Features Agreed on in the Contract as Defect

Where the parties have agreed on certain specifications of the contractual product, the product is defective in terms of law,

- if it does not comply with the specifications agreed between the parties;
- where there is nothing provided for in the contract, if the program does not contain such features necessary for the use of the program, which can generally be expected from a program falling into the category of the program agreed on in the contract; or
- if it does not contain such features, which the customer could have reasonably expected regarding the specific program or the agreements relating thereto;

Obviously, the customer will expect the program to have such features, which are expressly agreed on in the contract. As simple as this may sound, these expectations are often the basis for legal conflicts, since it is often unclear, what exactly the parties meant by certain wording and/or language in the contract in connection with the description of the program's specifications. If such questions are in dispute, the courts have to decide on the conflict in accordance with the common legal interpretation rules. This interpretation will, under German law, take into account the principles of good faith from an objective point of view, considering specific practices of the parties' profession.

Example: If it is agreed that "the software shall have appropriate response times", such response times are different regarding call center software or regarding software for the automotive industry, and they are also different depending on the scope of the specific task.

2.1.2 Features not expressly agreed on in the Contract as Defect

To the extent the parties have not expressly agreed on specific features in the contract, the software must contain such standard specifications, which can reasonably be expected by an average market participant.

What exactly such a participant is allowed to expect depends on the conceivable use of the program. Such use does not only contain the features the manufacturer intended, but also those functions which an average market participant usually expects from the product.

To comply with these possible expectations regarding Safety specific Defects:

- The program has to be designed and manufactured in accordance with the current standard of science and technique (= state-of-the-art techniques), as well as with the common use of the product usually applied by the relevant professions.[2]
- Furthermore, the software has to be as safe and secure as the customers (i.e. the public) can reasonably expect with respect to the program's common application areas.[3]

- In addition, the customer's expectations are legitimately influenced by the price range of the product. For example, a luxury car can be expected to have more safety-designed features than a lower middle class car. Or, another example, in the year 2000 the customer could, from a legal point of view, not have reasonably expected that a middle class car is equipped with an ABS-system.

Now we know what a "defect" is. So let us know deal with the question, in which cases the producer can be held liable for such a defect:

2.2 Liability Risks Arising from Defective Software

Under German law, two areas of liability risks have to be distinguished in connection with defective software. One arises from the **contractual** obligation vis-à-vis the contractual partner to deliver a non-defective product (contractual warranty and liability), and the other results from the **statutory** obligation to prevent the customer from damages to his property and from personal damages by distributing safe and secure products (so called "product liability" and "producer's liability").

2.2.1 Contractual Warranty and Liability

The German Civil Code[4] obliges the distributor to deliver non-defective products. If the product is not free of defects, the customer may, during the warranty period of two years, claim the remedy of the defect or the substitution of the defective product by a non-defective. The customer may exercise these rights regardless of whether the defect was caused by the distributor's fault or not.

However, if the defect was caused by the distributor's fault, the customer may additionally claim compensation for damages arising from the use or the uselessness of the defective product, such as damages to other objects, loss of profit, etc.

2.2.2 Statutory liability

Both legal concepts of statutory liability – product liability as well as producer's liability – are based on the idea that a producer, and, under certain conditions, also the distributor of a product shall advert damages from the property and the person of the product's user by making the product as safe as technically possible. The legal institution of "producer's liability" was developed by German courts as case law based on the statutory provisions relating to tortious liability, before the German Product Liability Act (PHG)[5] came into effect. The PHG states the legal framework for "product liability". Product liability and producer's liability coexist independently from another. The main difference between both institutions is that product liability applies regardless of whether the product user's damages were caused by the producer's fault or not (!).

Neither product nor producer's liability cover pecuniary losses. So they apply only for damages on products or injuries of persons, not for economical losses.

2.2.2.1 Product liability

Product liability applies in cases where a defect leads to damages, even if the manufacturer acts without any fault related thereto. The only exception from this liability applies, if the fault could not have been prevented even by using state-of-the-art technology at the time the product has been sold. As almost all faults are technically preventable, product liability will apply in almost all cases in which the product shows a defect. Therefore, from a legal point of view, product liability may only be avoided with respect to the end product by preventing defects in the course of the design and development process.

This is the reason why a safety designed development process shall be inevitably implemented into the organizational structure of any entity dealing with the design and development of products, including software, and, as we shall show, in particular with any entity dealing with the design and development of software in safety critical applications.

2.2.2.2 Producer's liability

Producer's liability means liability for defects caused by:

- the development and/or the design of the program (causing the occurrence of the defect to occur in each single exemplar of the series),
- the manufacturing the product (i.e. the defect can only be found in the products affected by the manufacturing error),
- or an incorrect instruction with respect to the product (i.e. the product itself is not defective, but the manual or user documentation leads to an incorrect application of the product). Please note that according to German jurisdiction software manuals are part of the product, which means that if the manual is defective, the software itself will be considered to be defective.

Since software defects are by nature defects in the development and/or design, the fulfilment of the organizational requirements of the producer/manufacturer in connection with the development and/or design process is the core instrument to prevent warranties and/or liability claims. Therefore, the non-compliance with safety oriented laws, statutes and/or technical standards is a clear fault in the development and/or design process of the software, regardless of whether this has been expressly agreed on in the contract or not.

2.3 Evidence rules

All these liability concepts (contractual warranty and liability, product liability and producer's liability) have one thing in common: A successful defense against claims for damages requires

the producer and/or distributor to be prepared to prove that he has undertaken everything possible to produce the relevant product without defects. This must be kept in mind, since many legal proceedings are decided on the basis of evidence rules. The loss of a lawsuit regarding claims for damages for defects in safety relevant applications can be crucial to the manufacturer.

2.3.1 Contractual Liability

For a successful assertion of contractual damage claims relating to defects in products, the claimant has basically only to expose and – in case of a contradiction of the opponent – to prove that his damage was caused by a defect of the relevant product and that the claimed defect has originated in the sphere of the contractual partner.

The contractual partner is only able to repel the claim if he can prove that the defect was not caused by his negligence. In case the manufacturer itself has distributed the product to the claimant, he has to prove that he has undertaken anything possible and reasonable to avoid the formation of defects during development, production and delivery of the product. This implies the application of quality assurance measures which match the current state-of-the-art methods and technologies.

If the product was not distributed by the manufacturer but by a (pre-)-supplier, the supplier has to prove that he has taken all possible and reasonable measures to detect the defect before delivery. Therefore, the supplier as well has to apply all state-of-the-art test procedures and logistics systems. All these quality assurance measures and their application have to be reasonably documented in case they need to be presented in a legal conflict.

2.3.2 Product Liability and Producer’s Liability

With respect to product liability and producer’s liability the burden of proof is similar as under contractual liability, since the customer usually is not in a position to analyze the design, development and production or distribution procedures of the manufacturer:

Once again, the customer has basically (only) to expose and to prove that his damage is a result of a defect in the product and that this defect has originated from the manufacturer’s sphere of responsibility. It is then the producer’s burden to disprove this allegation. Such allegation can only be successful if the producer maintains and controls the conformity with adequate quality assurance systems and the documentation of such measures.

Before taking a closer look at which quality assurance systems constitute an adequate safety orientated development process, let us deal with the question, of whether the compliance with applicable safety norms is sufficient to exclude the manufacturer´s liabilities.

3. Does compliance with applicable safety norms and/or state-of-the-art-techniques such as IEC 61508 result in an exemption from liability with respect to the producer and/or supplier?

It has already been stated that, on the one hand, the producer is obliged to comply with all applicable technical norms, as well as with all applicable laws or statutes regarding the fulfilment of such obligations, which apply in order to protect the safety and integrity of the general public. If he fails to do so, this would be a clear fault in the design and/or development process of the software.

On the other hand, however, the compliance with all applicable safety norms and/or state-of-the-art-techniques such as IEC 61508 does **not** result in an exemption from liability with respect to the producer and/or supplier. We would like to emphasize this point very clearly: The compliance with all applicable safety standards, for which IEC61508 – or depending on the product, similar product specific norms– , DIN, EN etc. are only examples, as well as with all applicable laws or statutes, in particular, without limitation, with the German Product Security Act (GPSG)[6], which determines the minimum standards the costumer is allowed to expect, is not sufficient to exclude or to limit any potential liabilities.

In practise, this means that the adherence with all these statutory laws and safety standards is not more than mere circumstantial evidence that the product complies with the state-of-the-art techniques.[7] If, however, the technical progress has already gone beyond these norms, or if the use of the product reveals new potential risks or dangers, the development and manufacturing process has to be adapted to the new requirements.[8] This means, that, in effect, the compliance with all applicable safety norms and/or state-of-the-art-techniques such as IEC 61508 may not even be sufficient to prove that the manufacturer is in fact faultless for any defects in the product.

4. Legal Measures for the Fulfilment of the Manufacturer's organizational and Due Diligence Obligations

What can, shall and/or must be done in terms of law to be as much on the safe side as possible? – The conclusion of the considerations so far is that one core instrument for a successful defence against contractual and statutory claims relating to product defects is a standardized project management which takes into account the necessary organizational and legal requirements and which has as its one goal of the design and development process: a "non-defective product".

4.1 Organizational Requirements

The goal: "non-defective product" is inseparably linked to the organization of the design and development, the production as well as the distribution process. It has to be ensured that this

process is organized in such a manner that all state-of-the-art measures and technologies are complied with. This requires, among other things, at least the following measures:

- Pre-supplier products have to be tested, unless the pre-supplier is able to prove that he has the relevant know-how to test the products itself and that he has in fact rendered all required tests.[9] However, the tests should, in any event, be carried through in-house, since nobody knows how far the literal sense of the concept “relevant know-how” might reach.

- The producer has, in addition, to monitor its products after the distribution, to be able to detect possible defects, which had been undetected during the development and manufacturing process.

- The development processes has to be structured with a clear phase scheme and milestones.

- The application of and the compliance with all these organizational measures have to be documented and stored so that they can be accessed and provided in the event of a legal conflict.

- Further – extremely important –: The development and production process has to comply with

    - all applicable statutory laws regarding the safety and integrity of the general public, including, without limitation, the German Product Security Act (GPSG), which determines the minimum safety standards the costumer can reasonably expect.

    - all technical standards and safety standards applicable at the time of delivery, such as IEC61508, DIN, EN.

    - with process maturity models[10], such as CMM, CMMI or SPICE the development has only to comply with to the extent contained in IEC 61508 or other applicable norms.

    We strongly advise to comply with all applicable safety norms and state-of-the art-techniques for another reason: It is a pre-condition for the producer to be able to prove that the designer and/or manufacturer or supplier has indeed complied with all applicable norms, and not only claims to have done so. Since, in the event of damages occurred, the German courts oblige the producer to exculpate itself from the assertion of negligent behaviour, as set out above,[11] the manufacturer is well-advised to implement and to control the adherence with a quality system, by which he can effectively prove that he has indeed complied with all applicable norms and standards in each process of the development and manufacturing of the software.

- When developing embedded systems, the manufacturer has to fulfil even further and additional requirements, since embedded systems are very complex, especially regarding the fact that software cannot be produced without faults.[12] This means that the project management must include and take into account the requirements for hardware and software in parallel environments with all necessary concepts for the design, implementation, testing, integration and simulation processes. Thus, an effective risk management, risk control procedures, as well as a configuration management are the minimum obligations the manufacturer has to comply with.

4.2 Requirements concerning Contractual Management

What needs to be done from a legal point of view regarding contractual management?

We strongly advise that any manufacturer of products in safety relevant applications set up an effective project as well as contractual management. This starts out with a clear contractual framework, including legal specifications of relevant terms for the development process, it includes clear and realizable specifications for the acceptance of the performances, including test specifications and acceptance criteria. It also includes a clear, realizable and verifiable process for change requests occurring during the development process. And, needless to say, it includes a clear specification of when which release of the product has been delivered, including a documentation of whether the delivery has occurred for testing purposes only or whether the release is the final, completely tested release, to go into production into serial products.

This means, that the contractual management shall be designed in such a manner that it defines a “legal environment”, in which product defects and discussions of whether a product defect has occurred are prevented to the extent possible. Phase building, clear, complete specifications, reasonable change request procedures and adherence to such agreed on procedures including the necessary control mechanisms, as well as all other quality control measures including criteria for tests and acceptance procedures are therefore only some of the inevitably necessary measures, which can help in achieving the goal of an appropriate project management – supported by an appropriate contractual management, to achieve the goal: “non-defective product”.

The contractual management shall comprise, among other things:

A clear specification of all relevant features of the program, of when which release of the product has been delivered, including a documentation of whether the delivery has occurred for testing purposes only or whether the release is the final, completely tested release, to go into production into serial products.

5. Summary

The implementation and application of procedures described in applicable safety standards, such as IEC61508, DIN, EN etc. are some of the minimum core conditions to prevent liability risks stated by German law in connection with defects of software caused by the software's design and/or development, production and distribution process.

Authors: *Dr. Meinhard Erben, Dr. Wolf Günther*
Attorneys-at-Law, Kanzlei Dr. Erben, Heidelberg
www.kanzlei-dr-erben.de

---

[1] Cf. *Schelling*/*Fetzer*/*Erben*, Software-Komponenten, Ein neuer Trend in der Automobilelektronik (= Software Components, a New Trend in Automotive Electronics), Automotive Electronics 2001, Special Release p. 1-2.
[2] BGHZ 80, 186 (BGH = German Federal Supreme Court).
[3] BGH VersR 1972, 559.
[4] Bürgerliches Gesetzbuch, BGB.
[5] Produkthaftungsgesetz, PHG.
[6] Geräte- und Produktsicherheitsgesetz, GPSG.
[7] Cf. *Amsler*/*Fetzer*/*Lederer*/*Erben*, Sicherheitsgerechte Entwicklungsprozesse (Safety-Designed Developing Processes), in Automotive Engineering Partners, 5/2004, p. 60-63.
[8] BGH NJW 1994, 3349; BGH NJW 1987, 372; BGHZ 80, 186.
[9] BGH NJW 1975, 1827.
[10] Cf. *Schelling*/*Fetzer*/*Erben*, Software-Komponenten, Ein neuer Trend in der Automobilelektronik (= Software Components, a New Trend in Automotive Electronics), Automotive Electronics 2001, Special Release p. 5-6.
[11] Cf. 2.3.
[12] Cf. *Amsler*/*Fetzer*/*Lederer*/*Erben*, Sicherheitsgerechte Entwicklungsprozesse (Safety-Designed Developing Processes), in Automotive Engineering Partners, 5/2004, p. 60-63.