

Legal Aspects of Safety Designed Software Development, Especially under European Law

Authors: Dr. Meinhard Erben, Dr. Wolf Günther, Dr. Tobias Sedlmeier, Attorneys-at-Law

KANZLEI DR. ERBEN, Heidelberg, Germany

Dr. Dieter Lederer, Dr. Klaus-Jürgen Amsler

Vector Consulting GmbH, Stuttgart, Germany

Abstract: This lecture deals with the question what has to be done to prevent liability risks stated by European law. In particular, it deals with the question whether the compliance with state-of-the-art safety standards (such as IEC 61508) leads to an exemption from liability for producers and/or suppliers of software.

After having defined the terms “product liability” and “producer’s liability”, we shall point out the legal measures which are necessary for the fulfilment of the manufacturer’s organizational and due diligence obligations. Thereby, we shall come to the conclusion that the implementation and application of procedures described in applicable safety standards such as IEC 61508, EN etc. are only some of the minimum core conditions to prevent liability risks stated by European law in connection with defects of software caused by the software’s design, development, production and/or distribution process.

Keywords: Software development; product liability; producer’s liability; compliance with safety standards; IEC 61508

1. Introduction

The use of software in automobiles and other means of transportation increases rapidly.¹ As software – unless it is completely trivial – cannot be developed without defects, the number of software defects in electronic controller units (ECU) used in automobiles and other means of transportation 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 the suppliers: Defective software may not only cause personal deaths or injuries, but it may also result in recall actions, producing high costs and resulting in heavy burden on the image of all the companies involved. In Europe, product liability generally applies regardless of any fault of the manufacturer, with only one exception, i.e. if the relevant product’s defect was inevitable.

Due to these facts and since risks arising from a legal conflict in connection with statutory or contractual liability are more than costly, there can be no reasonable doubt that it is advisable to treat the subject of safety designed development processes with utmost care.

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

2. Basic Legal Principles Regarding Defective Software

2.1 “Defect” in Terms of Law

The supplier is basically only liable to its customers 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 software products resulting from this process do 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 software, the software is defective in terms of law:

- If it does not comply with the specifications agreed between the parties,
- – In case there is nothing provided for in the contract: If the software does not contain such features necessary for the use of the software that can generally be expected from a software falling into the same category as the software agreed on in the contract, or
- If it does not contain such features which the customer could have reasonably expected with respect to the specific software or with respect to the agreements relating thereto.

Obviously, the customer will expect the software 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 software'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 most European laws (e. g. 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 with respect to call center software or with respect to 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 a Defect

To the extent the parties have not expressly agreed on specific features in the contract, the software must – according to Article 6 of the European Directive 85/374 EEC – 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 software. 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 software 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 software'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-system⁴.

Now we know what a "defect" is. So let us now 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 European 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 Warranties and Liabilities

Under to the European Consumer Sales Directive 1999/44/EG, the distributor has to deliver non-defective products. In various EU member states, the tight rules of the Consumer Sales Directive have not only been implemented with respect to contracts with consumers, they have in fact also been implemented with regard to all other kinds of contracts. One provision of this Directive states that, if the product is not free of defects, the customer may claim the remedy of the defects or the substitution of the defective product by a non-defective product, both during the warranty period of two years. This warranty period of two years is mandatory with respect to contracts with consumers. Customers may exercise the before mentioned 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 customers may additionally claim compensation for damages caused by the use or the uselessness of the defective product, such as damages to objects other than the defective product, 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 persons of the product's users by making the product as safe as technically possible. The legal concept of "producer's liability" has been developed by European courts as case law based on the principles of tortious liability. This development has already taken place before the European Directive 85/374 EEC and its national implementations (e.g. in Germany by the Product Liability Act (PHG)⁵) came into effect. This directive contains the European statutory framework for the legal concept of "product

liability". Product liability and producer's liability coexist independently. The major difference between both legal concepts is that product liability applies regardless of whether the product user's damages were caused by the producer's fault or not.

Neither product liability nor producer's liability covers financial losses. In fact, both concepts only apply with respect to damages to products and with respect to injuries of persons.

2.2.2.1 Product Liability

Product liability applies in cases in which a defect of a product leads to damages, regardless whether the manufacturer is at fault or not. The only exception therefrom is set forth in Art. 7 lit. e of the European Directive 85/374 EEC: Product liability is not applicable if the defect of the product could not have been prevented even by using state-of-the-art technologies at the time the product has been sold. As almost all defects of products are technically avoidable, product liability will apply in almost all cases in which a product contains 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/or development process.

This is one reason why a safety designed development process must be implemented into the organizational structure of any entity dealing with the design and development of products, in particular dealing with the design and development of software which is used in safety critical application areas.

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 in each single exemplar of the series),
- The manufacturing the product (i.e. the defect can only be found in the product 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 the jurisdiction of many European countries (e.g. the jurisdiction of Germany), 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 defence against claims for damages requires the producer and/or distributor to be prepared to prove that he has undertaken anything possible to produce the relevant software 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 software, 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 software 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 software. This implies the application of quality assurance measures which match the current state-of-the-art methods and technologies.

If the software was not distributed by the manufacturer but by a (pre-)supplier, the supplier has to prove that he has taken any 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 software 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 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 such as IEC 61508, the European Directive 2001/95/EG concerning Product Security and its national transpositions (e.g. the German Product Security Act = GPSG⁶) determine only the minimum standard the customer may expect from the products, i.e. compliance with these norms is not sufficient to exclude nor to limit the producer's liability.

In practise, this means that the adherence with all statutory laws and safety standards is only circumstantial evidence that the product complies with the state-of-the-art techniques.⁷ If the technical progress has 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 such new requirements.⁸ In effect, this means that the compliance with all applicable safety norms and/or state-of-the-art-techniques such as IEC 61508 may not be sufficient to prove that the manufacturer has in fact been faultless for a defect 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 defense against contractual and statutory claims relating to product defects is a standardized project management taking into account all necessary organizational and legal requirements to achieve the following 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 carried out all required tests.⁹
- The producer has to monitor its products after the distribution, to be able to detect possible defects which have remained undetected during the development and manufacturing process.
- The development process has to be structured with a clear phase scheme and milestones.
- The application of and the compliance with the organizational measures have to be documented and saved 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 of the general public including the European Directive 2001/95/EG concerning Product Security and its national transpositions;
 - All technical standards and safety standards applicable at the time of the delivery of the products;
 - 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 manufacturer or supplier has indeed complied with all applicable norms, and not only claims to have done so. Since, in the event of occurred damages, some European (e.g. the German) courts oblige the producer to exculpate itself from the allegation of

negligent behavior¹⁰ 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 phase of the development and manufacturing of the software.

- When developing embedded systems, the manufacturer has to fulfil additional requirements, since embedded systems are highly complex systems. Since software cannot be developed without defects,¹¹ the project management must include and take into account all the requirements for hardware and software in parallel environments including all necessary concepts for the design, implementation, testing, integration and simulation processes. Thus, an effective risk management, risk control procedures and a comprehensive configuration management are 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 the contractual management?

- We strongly advise that any manufacturer of products in safety relevant applications shall 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 then 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 it also includes a clear specification of when exactly which version 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 and released version which shall go into production in serial products.
- 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, clear change request procedures, test criteria, acceptance criteria as well as the compliance with all of the above are only some of the essential measures necessary to achieve the

sub-ordinate target of a successful contractual and project management, on the way to the final aim: "non-defective product".

4.3 Implementation of the Organizational and Legal Requirements

For safety related systems IEC 61508 is an international generic standard. For the automotive industry it is a main standard until there is an automotive specific adaptation. The development of an ISO norm based on IEC 61508 is in process but available probably not before 2008¹². Although being vague in some requirements, IEC 61508 is nevertheless a helpful means to fulfil the organizational and legal requirements, because the standard is a comprehensive survey of requirements regarding the development of safety related systems.

Part 1 to 3¹³ define the main requirements addressing document management, (organizational) requirements for the management of functional safety, the institutionalization of a safety life cycle and safety assessments. In addition, there is a catalogue (part 7) with well known methods and techniques that are recommended to be applied to ensure the safety integrity of systems.

On the other hand, a direct implementation of the requirements of IEC 61508 is very difficult because it is a hefty and complex tome without any hints how to implement its requirements. Although defining a safety life cycle comparable to the V-Model¹⁴ the structure of IEC 61508 is not process oriented. It is rather a bundle of requirements assigned to the phases of the safety life cycle. When trying to implement these bundles of requirements there will be the risk to take only single measures which are not coordinated and therefore may be of little efficiency from an overall process point of view.

The recommended way for implementing IEC 61508 is applying a process management approach based on maturity models like CMMI or ISO 15504 (SPICE)¹⁵. Maturity models incorporate accepted best practices and provide a structured process framework that supports an efficient way for improving process maturity step-by-step and therefore to improve the transparency of processes, the traceability of any product changes and the integrity of the work products. All of the above support the development of non-defective software.

Comparing the requirements of IEC 61508 with the Process Areas and Specific Practices of CMMI goes to show that the Process Areas representing a Maturity Level 3 are a very good basis for implementing a development process that conforms to IEC 61508¹⁶. Some safety specific requirements of IEC 61508 like e.g. performing hazard analysis can be considered as safety specific adaptations of

Specific Practices of CMMI, in this case a specific application of the Risk Management Process Area.

Increasing the Safety Integrity Level (SIL) for a product also increases the requirements for the development process regarding the methods and techniques to be applied. According to IEC 61508-2 e.g. statistical testing should be applied for SIL3 products. In addition, with increasing the Safety Integrity Level of a product the requirements regarding the efficiency of applied methods and techniques will also increase, from low, medium to high efficiency.

Both SIL dependent requirements can be fulfilled with increasing the process maturity by applying maturity models based on CMMI or ISO 15504.

Maturity models like CMMI or ISO 15504 are therefore a smart and efficient approach for implementing requirements of IEC 61508 and to fulfil the organizational and legal requirements.

5. Summary

The implementation and application of procedures described in applicable safety standards such as IEC 61508 are core pre-conditions in order to prevent liability risks applicable under European law with respect to defective software.

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 Bodewig, *Der Rückruf fehlerhafter Produkte*, p. 106, Mohr-Siebeck 1999

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. 2.3.

¹¹ Cf. Amsler/Fetzer/Lederer/Erben, „Sicherheitsgerechte Entwicklungsprozesse (Safety-Designed Developing Processes)“, in Automotive Engineering Partners, 5/2004, p. 60-63.

¹² Amsler/Erben/Günther/Lederer, *Über Prozessreife zur Sicherheitsintegrität (Safety Integrity Based on Process Maturity)*, in Elektronik im Kraftfahrzeug (Electronic Systems for Vehicles), VDI-Berichte 1907, p. 199, 207, VDI Verlag GmbH, 2005.

¹³ Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508).

¹⁴ V-Modell 97: www.v-modell.iabg.de

¹⁵ 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.

¹⁶ Amsler/Erben/Günther/Lederer, „Über Prozessreife zur Sicherheitsintegrität (Safety Integrity Based on Process Maturity)“, in Elektronik im Kraftfahrzeug (Electronic Systems for Vehicles), VDI-Berichte 1907, p. 199, 207, VDI Verlag GmbH, 2005.

Glossary

Bürgerliches Gesetzbuch, (BGB)

German Civil Code

CMMI®

Capability Maturity Model Integration

DIN (Deutsche Industrie Norm)

German Industrial Standard

EN

European Norm

Geräte- und Produktsicherheitsgesetz (GPSG):

German Product Security Act

IEC

International Electrotechnical Commission

ISO

International Organization for Standardization

MMI®

Maturity Model Integration

Produkthaftungsgesetz (PHG)

German Product Liability Act

SPICE

Software Process Improvement and Capability Determination