Hans-Leo Ross

# Functional Safety for Road Vehicles

## New Challenges and Solutions for E-mobility and Automated Driving

Springer

Functional Safety for Road Vehicles

Hans-Leo Ross

# Functional Safety for Road Vehicles

## New Challenges and Solutions for E-mobility and Automated Driving

Springer

Hans-Leo Ross
Lorsch
Germany

ISBN 978-3-319-33360-1 ISBN 978-3-319-33361-8 (eBook)
DOI 10.1007/978-3-319-33361-8

Library of Congress Control Number: 2016944354

Translation from the German language edition: *Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen* by Hans-Leo Ross, © Carl Hanser Verlag GmbH & Co. KG. All Rights Reserved.


Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

# Foreword of the Author

The German automobile industry took notice of the topic as IEC 61508 got published as DIN EN 61508 (VDE 0803) "Functional safety-related electric/electronic/programmable electronic systems" in 2001. Official correspondence between the VDA and the VDTÜVs led to the foundation of AK16 in FAKRA (Facharbeitskreis Automobil—German expert group from vehicle manufacturers and equipment suppliers), a group I became part of when I joined Continental Teves in 2004. In the same year, the first structures for the later ISO 26262 were designed and contact was established to further automobile standardization committees in other countries. Especially with France, concrete parameters for the standard were developed. The first meeting of the standardization group of ISO/TC22/SC03/WG16 took place from October 31 to November 2, 2015 in Berlin. The biggest delegate groups were from France and Germany besides representatives from other countries such as Japan, the USA, Sweden, Great Britain et cetera. Up to this point, ISO 26262 was still called 'FAKRA-Norm' (FAKRA-Standard). SafeTronic 2005 (Safety Event from Hanser-Verlag) already addressed the first ideas for future automobile standards and the presentations held included 'Best Practices' and methods. Until today, SafeTronic supported the development of ISO 26262, which got published as "International Standard" in November 2011. This book tries to compile all the background information that has been collected over the years. Moreover, it aims to give a better understanding of safety architecture as a basis for the development of safety-related products.

# Preface

The following book is the result of over 20 years of professional experience in the field of functional safety. When I started my career after graduating as an engineer in 1992, plant engineering and construction was highly influenced by catastrophic events such as 'Bhopal' and 'Seveso'. The first set of rules and regulation which led later to IEC 61508 and ISO 26262 that addressed the issue of functional safety was the VDI/VDE guideline 2180 "Sicherung von Anlagen der Verfahrenstechnik; Safeguarding of industrial process plants by means of process control engineering" from 1966. However, it only covered the mere process of how to establish a safe environment in such facilities. In 1984 the differentiation between operational safety and safety equipment as well as monitoring and safeguarding equipment were added to the guideline. Thereafter, DIN VDE 31000—"General guide for designing of technical equipment to satisfy safety requirements" got published, which elaborated on the correlation between risk, safety and danger and introduced tolerable risk. At this time machinery standards, which prohibited the use of micro-controller for safety applications, were still common. However, an established market for safety-related control systems already existed. Different rules and standards defined the base of requirements for examinations, certifications and design of such systems. Those requirements were scaled in requirement classes (AK 1-8) according to DIN V 19250, independently from application or technology and explained a qualitative risk assessment procedure with the help of a risk graph.

In 1990 DIN V VDE 0801 "Principles for computers in safety-related systems" was released and in its revision of 1994 terms such as 'well-proven design principles' and the usage of 'consideration item' were added. By then, 'redundancy' was the only known answer to the various risk and requirement classes. However, various measuring principles were already used in measurement and control system engineering in order to detect hazardous situations early.

The technical rules for steam or the regulations for pressure vessels already required the redundant measurement of steam and temperature due to safety issues. Even the German Water Ecology Act mentioned the filling quantity limit from tanks according to regulations as well as the independent overfill safety device as a

safety measure. A lot of those safety principals emerged from the safety standards of plant operators and even served as a foundation for official permits or releases. Even before in the early sixties DGAC (Direction General de L´Aviation Civil in France), CAA (Civil Aviation Authority) in Great Britain or FAA (Federal Aviation Administration) in USA and the military and space industry defined regulations about "Functional Safety", but those were not in the focus of the development of standards like IEC 61508 and ISO 26262. Due to today's discussion about 'autonomous' or 'automated' driving, those standards become more and more in the focus of the automotive industry. Especially topics such as safety-in-use, fail-operational, security, operational safety are becoming important for future revisions of ISO 26262.

In 1998, at the time I started my job as a sales manager of safety-related control systems, discussions over the early drafts of IEC 61508 took place, especially in countries such as England, the Netherlands and Norway. The scalable redundancy was a known concept so the discussion focused on the distinction between redundancy for safety and availability. Micro-controllers were coupled according to the lockstep principle and could change the program sequence or control logistics during runtime of a plant. Programming software was available, which allowed configuring the safety logic within a defined runtime environment.

The publication of IEC 61508 introduced a lifecycle approach for safety systems. Additionally, it formulated a process approach for product development and the relations to quality management systems were formulated.

During my graduate studies at the Faculty of Business and Economy at the University of Basel, I was able to hear a lecture of Prof. Dr. Walter Masing, who had a huge impact on quality management systems in Germany. The introduction of implemented diagnostics for the safety of functions and the electric carrier systems of these functions, respectively, broadened the view of safety architecture. In 1998, I introduced the first passive electronic system in Birmingham, which until SIL 4 was certified according to IEC 61508. I witnessed when the first certificate for a single-channel control system got signed after SafeTronic in 1999, which took place in the facilities of TÜV-Süd. This system was completely developed according to IEC 61508.

During VDMA-events (Verein Deutscher Machinen und Anlagenbauer; German machinery and plant engineering association) I reported on my experiences with IEC 61508 regarding plant engineering and its influence on the development of safety-related control systems. In these days, the machinery engineering industry was still heavily influenced by relay technology. Nobody wanted to believe that software-based safety technology would change the industry so drastically and in such a short time by providing new solutions and change existing systems. In 2001 I became the head of product management; the main task was to find new applications for new safety systems. Another main topic was 'safe network technology', which was so far based on serial link data busses. The challenge was to realize distributed and decentralized safety systems based on dynamic, or situation-, or condition-dependent safety algorithm. The only possible solution turned out to be 'Ethernet'. It was important to make the existing computer or data technology for

safety technology easily manageable. In Norway, in the context of diploma theses, safety control systems got distributed, which exchanged safety-relevant data within the data network of the Norwegian mineral oil association “Statoil”. The experiences with the data transfer over satellites between oil platforms and plants ashore or between Norway and Germany as well as various solutions to the pipeline monitoring via radio systems proved that the safety technical data systems were also able to be realized based on Ethernet.

Hans-Leo Ross

# Acknowledgments

The plentiful discussions with experts of international standardizations, colleagues, within the working groups, universities and presentations as well as the insights of diploma theses and public funding projects have contributed to this book. I would like to thank all the people involved for their shared passion for functional safety. Besides all the experts I especially want to thank my wife, who showed a lot of understanding and gave me the freedom and space to write this book.

# Contents

# Chapter 1
# Introduction

ISO 26262 [1] changes vehicle development in a way, nobody would have expected 10 years ago, when functional safety became a relevant topic in the automobile industry. During the early 21st century the first German (VDA) working group already started dealing with functional safety and when the first international working groups got founded in 2005 everybody was looking for a lean standard for product safety. In the following 10 years before the final publication of the ISO 26262, those working groups compiled 10 parts with about 1000 requirements. Even though a lot of pertinent knowledge, methodologies and approaches have been discussed throughout the years, only a fracture of it has been incorporated in ISO 26262. Some information has only been added as footnotes, some disappeared completely until the final release of the standard.

In order to translate ISO 26262 there are currently various standardization projects in progress in different countries worldwide. The aim is to translate ISO 26262, provide further guidelines and develop additional methodologies for functional safety based on ISO 26262.

ISO 26262 is not intended to serve as a guideline it simply provides requirements for activities and methods, which should be taken into account in the respective functional safety activities. There is no description included as to how the requirements are supposed to be met. The underlying assumption is that such a state-of-the-art safety standard is considered to be a current up-to-date knowhow and will only be valid within a certain period of time. Recommendations on which designs are considered to be safe or which methodologies are adequate for certain activities are only valid and satisfactory until new or better methods are found. Also, safety design and methodology should be continuously improved and never limited to safety standards. There is an enormous need for guidelines and this book aims to provide further insights and background information on the respective topic but it does not offer guidelines on the correct application of ISO 26262. It focuses on methods and methodologies but none of those mentioned could fulfill the requirements of ISO 26262. Standards can only be fulfilled in the context of developing a real product in a given environment.



H.-L. Ross, *Functional Safety for Road Vehicles*,
DOI 10.1007/978-3-319-33361-8_1

Requirements, hints and notes in ISO 26262 are often described in a very complex way. The choice of words is a compromise experts who developed those safety standards had to agree upon. This is why all translations in this book may already be seen as interpretations, which could be interpreted or translated in other ways in the light of a different context. The strong recommendation to all readers is to reference to the text of ISO 26262 when trying to interpret and apply those standards in the field.

## 1.1 Definitions and Translations from the ISO 26262

ISO 26262 was only written in English. Even the usually common translation to French was not implemented due to the different use and interpretation of certain terms. This is why ISO 26262 is one of the only standards for which the original English text is also used in France. Asian countries are the only countries that have published a translation in their native language, a necessary requirement considering that the average developer in Japan would face difficulties in reading, understanding and interpreting the English language. After Japanese, Korean and Chinese translations followed afterwards during last years. For example, there is only one word in Japanese for verification, analysis, investigation and validation, thus the English text could have caused too many interpretation issues. Japanese translators assured that the content would not be falsified.

Finding the right and accurate words proved to be difficult even for the translation to the German language. Terms such as verification, analysis and validation were used in accordance with ISO 26262. However, some terms from the ISO 26262 glossary, highlighted in the blue boxes found throughout the book are citations from ISO 26262, but all explanations before or after are interpretations from the understanding of the author. Free interpretations, opinions or even recommendations of the author are written in the standard font chosen throughout the book; direct quotes are written in italics.

Throughout this book, the terminology "assessment of functional safety" is used to refer to the activity involved in "Functional Safety Assessment" as described in ISO 26262. In considering this concept of "assessment," it should be noted that "examination" is the basis for assessment and results in "judgment" of a property of the vehicle system or element.

*ISO2626, Part 1, Clause 1.4*:

> 1.4 (Assessment)
> Examination of a property of a vehicle system (1.69) or element (1.32)
> Note: A certain degree of independence (1.61) of a certain party or parties who perform an assessment should be ensured for each assessment.

The English word ‘assessment’ is translated as the German word used for ‘judgment’ and examination is seen as the basis for an assessment. The term “Assessment of Functional Safety” is used regarding the activity “Functional Safety Assessment” described in ISO 26262.

*ISO2626, Part 1, Clause 1.6*:

> 1.6 ASIL (Automotive Safety Integrity Level)
> One of four levels to specify the item’s (1.69) or element’s (1.32) necessary requirements of ISO 26262 and safety measures (1.110) to apply for avoiding an unreasonable residual risk (1.97), with D representing the most stringent and A the least stringent level.

For ‘Automotive Safety Integrity Level’, this book only uses the abbreviation ASIL.

ISO 26262 already provides a description of the elements of a vehicle system in part 10. An ‘element’ could be a system, a subsystem (logical or technical element and thus also a functional group), a component, a hardware device or a SW unit.

Part 1 of ISO 26262 is described under 1.69 Vehicle System (item) as follows:

*ISO2626, Part 1, Clause 1.69*:

> 1.69 (vehicle system, item)
> system (1.129) or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied.

The word ‘item’ in English is often considered as ‘vehicle system’ in the context of this book, if it refers to the concrete word ‘item’ as used in ISO 26262 the word “ITEM” is used.

Historically, the German term for “Betrachtungseinheit” could be translated as “unit or item under consideration”. The English word ‘item’ and its definition as a system better applies to the idea of a vehicle system. Whenever this is relevant in the text, the term ‘item’ is added in brackets. The term ‘array of systems’ will be questioned in Chap. 4 of this book. A systematic hierarchical structured systems and associated subsystems are required in the technical parts from ISO 26262.

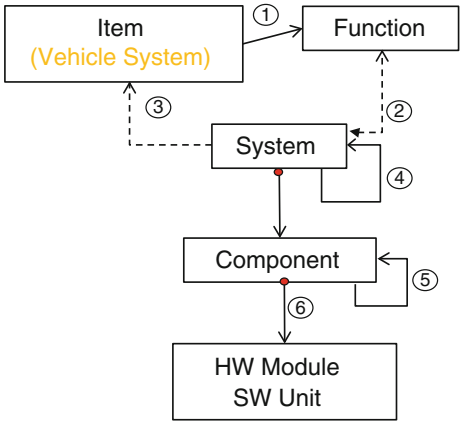


**Fig. 1.1** Elements of a vehicle system (*Source* ISO 26262, Part 10, Fig. 3)

Figure 3 (here Fig. 1.1) from part 10 can be described as follows according to this definition:

*ISO2626, Part 10, Fig. 3*:

1. A system (1.129) or more systems, which realize one (or more) function(s) on the vehicle level for which ISO 26262 can be used.
2. A system may implement one or more functions, but also one function can be implemented in several systems.
3. A vehicle system is comprised of one or more systems, where one system is composed of at least one sensor, a processing unit and an actuator. ISO 26262 draws the conclusion that a system should have at least three elements but it could be possible for example that an actuator is integrated in the processing unit.
4. A system can be divided into any subsystems but according to ISO 26262 the systems have to be hierarchically structured. In regards to systems, which together should realize functions with a higher ASIL, a clear hierarchical structure of systems has to be defined due to multiple fault control.
5. A system (or subsystem) is comprised of one or more components.
6. Components consist of (electrical) hardware components (hardware parts) or of SW units.

Terms such as module, SW-files et cetera are not defined in ISO 26262. In regards to embedded semiconductors the term ‘Sub-Parts’ is used. Sub-Parts are logical functional elements, which implement specific functions and safety mechanisms within an integrated semiconductor.

## 1.2 Error Terms of the ISO 26262

ISO 26262 specifies terms in Volume 1 as follows:
*ISO2626, Part 1, Clause 1.36, 39, 42*:

> 1:36 (error)
> discrepancy between a computed, observed or measured value or condition, and the true, specified, or theoretically correct value or condition
> NOTE 1 An error can arise as a result of unforeseen operating conditions or due to a fault (1.42) within the system (1.129), subsystem or component (1.15) being considered.
> NOTE 2 A fault can manifest itself as an error within the considered element (1.32) and the error can cause a failure (1.39) ultimately.
>
> 1:39 (failure)
> termination of the ability of an element (1.32), to perform a function as required
> NOTE Incorrect specification is a source of failure.
>
> 1:42 (fault)
> abnormal condition that can cause an element (1.32) or an item (1.69) to fail
> NOTE 1 Permanent, intermittent and transient faults (1.134) (especially soft-errors) are considered.
> NOTE 2 An intermittent fault occurs time and time again—and disappears. These faults can happen when a component (1.15) is on the verge of breaking down or, for example, due to a glitch in a switch. Some systematic faults (1.131) (e.g. timing marginalities) could lead to intermittent faults.

The following assumptions were made due to different usages of the terms "Fault", "failure" and "error" in their context:

- Fault: Deviation, anomaly, defect, defect, non-conformity
- Error: mistake, fault or error
- Failure: Failure or malfunction.

The relationships of these three terms and also their model of error propagation are described in Sect. 4.4.2. Here only needs to be noted that the term "error" in German more generally and is thus used in this book primarily as a collective term for all three terms. If error purely regarded as "error", this is explained in the context.

In the safety analysis the following aspects can be distinguished:

- Single point fault (or single failure) and
- Multiple-point faults.

If a single fault or a deviation of an observable behavior or property alone leads to a failure of a system, this is referred to as a single point fault. Perform only a combination of several faults, deviations to unintentional changes, observable behavior or changed properties; this is regarded as a multiple-point faults. At least combinations of minimum two faults are necessary to propagate to a multiple-point failure. In ISO 26262 this naming is not based on a system's behavior, but on a safety goal. For example single point faults are considered only if a single fault leads to a violation of the safety goal within the specified Item, boundary or the specified environment or specified space. Faults which lead only to failure outside the "Item" are not considered as a single point fault, unless the "Item Definition" not changed due to systematic failures.

## References

1. [ISO 26262]. ISO 26262 (2011): Road vehicles – Functional safety. International Organization for Standardization, Geneva, Switzerland.

# Chapter 2
# Why Functional Safety in Road Vehicles?

It took a while until functional safety started to play a significant role in the automotive industry in comparison to other industries. Customers, producers and dealers networks demanded more functionality and complexity of the products and market. One of the major reasons was that mechanical engineers primarily dominated the entire automobile engineering industry. The same industry developed the safety mechanism in the related field, without relying on electronics or even software. Therefore, these safety mechanisms were first and foremost based on a robust design as well as hydraulic or pneumatic safety mechanisms. With the increased amount of automation and electrification of essential vehicle functions and the desire to make these systems applicable for higher speeds and dynamics, electrification was the only way to go. Also the earlier concepts steer-by-wire and brake-by-wire, right up until today's autonomous or highly automated driving systems, make the usage of software based safety mechanisms unavoidable. If you look at one of today's common mid-range cars such as the 'Volkswagen Golf', you will find about 40 control units, which are still mainly networked by a CAN-Bus. It is "State-of-Science and Technology" that no complex vehicle systems could be realized without a systems approach. One of the main challenges of ISO 26262 [1] was that various methods, methodology, principles, best practices had been established but there was no consistent system development approach.

The main task in the development of ISO 26262 was to agree upon one basic understanding of system engineering. Therefore, it is not a surprise that the word 'system engineering' appears quite often in the introduction.

## 2.1 Risk, Safety and Functional Safety in Automobiles

In general, risk is described as a possible event with a negative impact. The Greek origin of the word risk had been also used for hazard or danger. In regards to product safety it is referred to as the cross product of probability of occurrence and



H.-L. Ross, *Functional Safety for Road Vehicles*,
DOI 10.1007/978-3-319-33361-8_2

hazard/danger. There are different opinions on the term and definition of risk in the economic literature. Definitions vary from 'danger of a variance of error' to the mathematical definition 'risk = probability × severity'.

The general definition is as follows: The probability of damage or loss as consequence of a distinct behavior or events; this refers to hazardous/dangerous situations in which unfavorable consequences may occur but do not necessarily have to.

On the one hand, risk can be traced back etymologically to 'riza' (Greek = root, basis); see also 'risc' (Arabic = destiny). On the other hand, risk can be referred to 'ris(i)co' (Italian); "The cliff, which has to be circumnavigated". 'Safety' derives from Latin and could be translated as 'free from worry' (se cura = without worry). Today, the topic of safety is viewed in various different contexts for example, in regards to economic safety, environmental safety, admittance and access security but also in terms of work safety, plant and machinery safety and vehicle safety. The term safety varies significantly from just only functional safety.

In relation to technical systems or products, safety is described as the freedom of unacceptable risks. 'Damage' is generally seen as harm or impairment of people as well as the environment.

There are various distinctions of hazard:

- Chemical reactions of substances, materials etc. lead to fire, explosions, injuries, health impairments, poisoning, environmental damage etc.
- Toxic substances lead to poisoning (also carbon monoxide), injuries (consequence of for example degassing of batteries, error reactions of the driver or mistakes of the auto repair shop staff), other damages etc.
- High currents and especially high voltages lead to damages (in particular personal protection).
- Radiations (nuclear, but also radiations like alpha particle semiconductor).
- Thermic (damages due to overheating, singe, fire, smoke etc.).
- Kinetics (deformation, movement, accelerated mass can lead to injuries).

The potential reasons for hazard cannot be easily defined, since chemical reactions can also lead to poisoning and overheating, to fire and thus also to smoke intoxication. Similar correlations appear in high currents or excessive voltages. High voltages lead to burns when touching but can also cause fires. Overvoltage is often seen as a non-functional risk or hazard. This is why most of the standards encounter such hazards with design constraints. A contact safety device or touch guard on a safety plug connector is a typical example. This leads us to the following point of view and distinction of functional safety.

Functional safety is generally described as the correct technical reaction of a technical system in a defined environment, with a given defined stimulation as an input of the technical system. ISO 26262 defines functional safety as absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems. Also, the error or failure reactions of mechanic or hydraulic safety components are

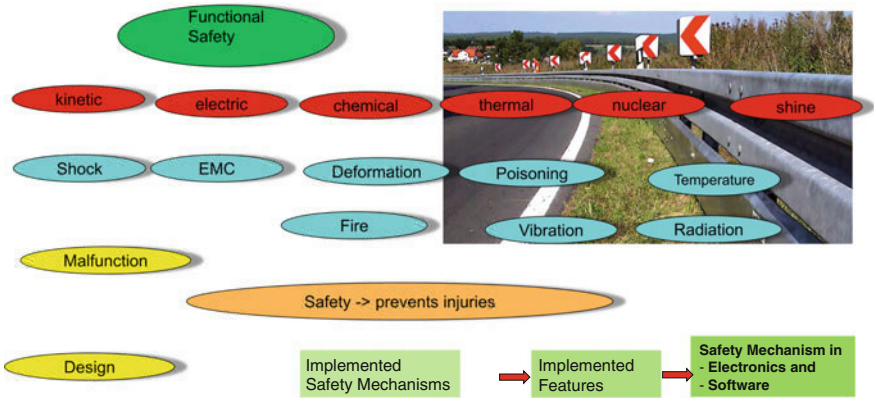


**Fig. 2.1** Functional safety—safety design, control of forces and energies

controlled by electronic safety mechanisms in mechatronic systems. This distinction will be discussed later in reference to ISO 26262 (Fig. 2.1).

Functional safeguarding with hydraulic systems has always been used for automobiles. A typical example would be the dual-circuit braking system or the hydraulic steering system. Electronic and software based functional safety mechanisms were introduced as for example the ABS (Anti-Wheel-Blocking-System) for brake systems 30 years ago. Prior to that the necessary safety was only established by sufficient robust system and safe component characteristics (meaning through design).

The following definitions of risk, hazard/danger and integrity have been added to *DIN EN 61508-1:2002–11:*

*Citation from IEC 61508* [2], *Part 5, A5:*
*A.5 Risk and Safety Integrity*

*It is important that the distinction between risk and safety integrity be fully appreciated. Risk is a measure of the probability and consequence of a specified hazardous event occurring. This can be evaluated for different situations [EUC risk, risk required to meet the tolerable risk, actual risk (see Fig. A.1)]. The tolerable risk is determined on a societal basis and involves consideration of societal and political factors. Safety integrity applies solely to the E/E/PE safety-related systems, other technology safety related-systems and external risk reduction facilities and is a measure of the likelihood of those systems/facilities satisfactorily achieving the necessary risk reduction in respect of the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the safety-related systems can be allocated. (see 7.4, 7.5 and 7.6 of IEC 61508-1)* (Fig. 2.2).

Furthermore, IEC 61508 shows the following figure to explain coherences (Fig. 2.3):

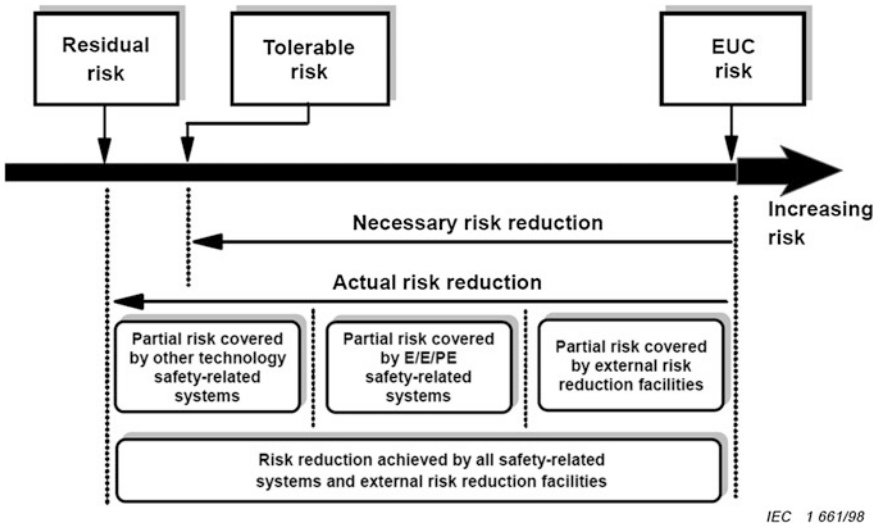


**Fig. 2.2** Risk reduction according to IEC 61508 (*Source* IEC 61508-1:2011)

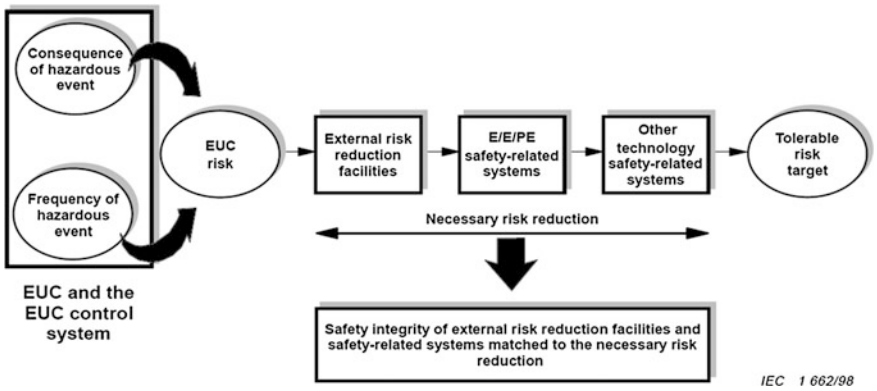


**Fig. 2.3** Risk- and safety integrity according to IED 61508 (*Source* IEC 61508-1:2011)

ISO 26262 defines the relation of risk, danger and safety integrity differently. The term safety integrity is not directly used in ISO 26262. In particular the term EUC (Equipment under Control) is not used at all. EUC could be explained as "device or system, which should be controlled by means of functional safety measures". Under certain limiting conditions ISO 26262 admits to develop a desired vehicle function that is safety-related on its own. In this case, the system does not receive safety through EUC itself. Technically, according to IEC 61508, EUC and the safety functions have to cause an error at the same time in order to create a hazardous situation. If for example a hydraulic braking system was the

EUC, which in its function can be monitored by an EE-system, errors of the hydraulic systems could be avoided by the EE-system. The automobile industry relies here on other technology and engineering of the electronic safety system will be considered as a fail-safe-system.

As mentioned previously, ISO 26262 defines functional safety as freedom of unacceptable risks based on hazards, which are caused by malfunctional behavior of E/E-systems. However, interactions of systems with E/E-functions are included as well and therefore also mechatronic systems. Whether pure mechanical systems really show not any interactions with E/E is doubtful. Furthermore, the introduction chapter of ISO 26262, which describes the scope of the norm, excludes hazards such as electric shock, fire, smoke, heat, radiation, poisoning, inflammation, (chemical) reactions, corrosion, release of energy or comparable hazards, as long as the failure was not caused by electrical components. Such hazards are caused more by the battery as well as the poisonous electrolytes in the capacitors. Whether a motor winding is an electrical device or a mechanical component is also questionable.

In general, it will be difficult to assign the ASIL with non-functional hazards. Such components have so far been construed sturdily in order to avoid any danger. In the context of the hazard and risk analysis it is difficult to allocate a specific ASIL to a weakness in design or construction.

ISO 26262 also excludes functional performances. Therefore, safety-in-use or functional inadequacy means functions, which already lead to a hazard, even if they functioning correctly are generally excluded in advance.

All explain the correlation of risk and damage as follows:

*ISO 26262, part 3, appendix B1:*

*For this analytical approach a risk (R) can be described as a function (F), with the frequency of occurrence (f) of a hazardous event, the ability of the avoidance of specific harm or damage through timely reactions of the persons involved (controllability: C), and the potential severity (S) of the resulting harm or damage:*

$$R = F(f, C, S)$$

*The frequency of occurrence f is, in turn, influenced by several factors. One factor to consider is how frequently and for how long individuals find themselves in a situation where the aforementioned hazardous event can occur. In ISO 26262 this is simplified to be a measure of the probability of the driving scenario taking place in which the hazardous event can occur (Exposure: E). Another factor is the failure rate of the item that could lead to the hazardous event (Failure rate: λ). The failure rate is characterized by*

*hazardous hardware random failures and systematic faults that remained in the system:*

$$f = E \times C$$

*Hazard analysis and risk assessment is concerned with setting requirements for the item such that unreasonable risk is avoided.*

ISO 26262 mentions normative methods that describe a systematic derivation of the potential risk, which may originate from the investigated of the considered Item (vehicle system), based on a hazard analysis and risk assessment. Hazard or risk analyses are not normatively defined in other safety standards. Either the requirements for these methods are listed or the method itself is exemplarily described (Fig. 2.4).

The reduction of risk cannot be achieved with the activities and methods mentioned in ISO 26262 if a function is not suitable, inadequate suitable, inadequate or falsely indicated for certain safety related functions. This represents a special challenge, considering that ISO 26262 does not directly addresses a EUC (Equipment under Control, e.g. a system, machinery or vehicle, which should be controlled safety-related systems) or the distinction between safety functions of designated safety requirements for on-demand (low demand) or continuous mode (high demand) safety systems. How is it possible to find out whether or not reactions of a vehicle system or certain measurements are sufficient, tolerable or safety-related appropriate?

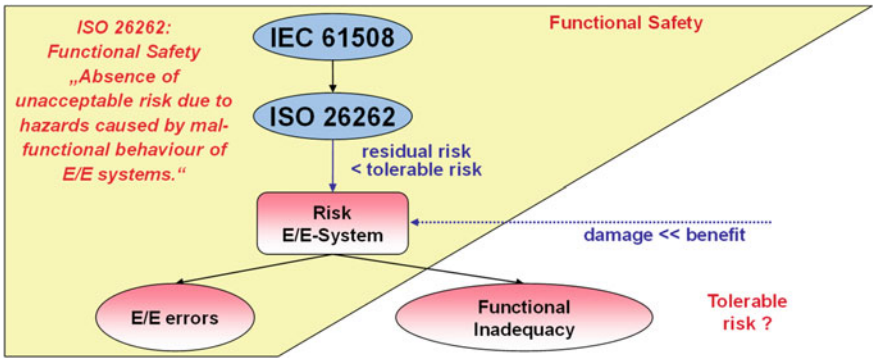


**Fig. 2.4** Distinction of hazards, based on correctly functioning systems (*Reference* unpublished research project [7])

## 2.2 Quality Management System

Prof. Dr. rer. nat. Dr. oec. h. c. Dr.-Ing. E. h. Walter Masing, is also called the father of quality management systems, at least in Germany. His standard reference "Masing Handbook Quality Management" had a substantial influence on the standardization and interpretation of quality management systems.

A lot of methods and principles of management systems are explained already in ISO 9000. However, in 2005, statistics and trial methods became less relevant as the process approach became more and more important.

In the automotive industry an addition to ISO 9001 exists, called ISO TS 16949 [3]. It describes additions especially to the product development and production, which developed into standards in this industry. Today, in order for a distributor to be able to supply automotive manufacturers, the certification of ISO TS 16949 is an essential basic. Manufacturers from Asia still refer to different standards, based on historical reasons. Especially in Japan, quality requirements focus more on the ideals of the six-sigma-philosophy (for example DFSS, Design for Six Sigma). In particular the static analysis and trial methods mentioned in Masing's book, in DSFF as well as in functional safety are often based on comparable principles. ISO TS 16949 asks in the following chapters for essential basics for functional safety according to ISO 26262:

*ISO TS 16949, 4.2.3.1: Engineering specifications*

*The organization shall have a process to assure the timely review, distribution and implementation of all customer engineering standards/specifications and changes based on customer-required schedule. Timely review should be as soon as possible, and shall not exceed two working weeks.*

*The organization shall maintain a record of the date on which each change is implemented in production. Implementation shall include updated documents.*

*NOTE A change in these standards/specifications requires an updated record of customer production part approval when these specifications are referenced on the design record or if they affect documents of production part approval process, such as control plan, FMEAs,* etc.

Here, the norm refers to document and change management, application of necessary norms and standards, methods, output/work results and the regulation of responsibility (clearance), which is mentioned in ISO 26262 as QM-methods.

*ISO TS 16949, 5.6.1.1 Quality management system performance*

*These reviews shall include all requirements of the quality management system and its performance trends as an essential part of the continual improvement process.*

*Part of the management review shall be the monitoring of quality objectives, and the regular reporting and evaluation of the cost of poor quality (see 8.4.1 and 8.5.1).*

*These results shall be recorded to provide, as a minimum, evidence of the achievement of*

- *the quality objectives specified in the business plan, and*
- *customer satisfaction with product supplied.*

This explains the fact that product development as well as the satisfaction of the products delivered has to be documented and proven. If it concerns safety related features this may affect the customer substantially.

*ISO TS 16949, 5.6.2: Review input*
*ISO 9001:2000, Quality management systems—Requirements*

5.6.2 Review input
*The input to management review shall include information on*

*a) results of audits,*
*b) customer feedback,*
*c) process performance and product conformity,*
*d) status of preventive and corrective actions,*
*e) follow-up actions from previous management reviews,*
*f) changes that could affect the quality management system, and*
*g) recommendations for improvement.*

This list can also be seen as a "safety culture" in infrastructure requirements and essential for functional safety.

*ISO TS 16949, 5.6.2.1: Review input*

*Input to management review shall include an analysis of actual and potential field-failures and their impact on quality, safety or the environment.*

This chapter refers directly to the essential field observations, which are also required by the government in the context of product liability laws. It also directly refers to safety defects.

*ISO TS 16949, 5.6.3: Review output*
*ISO 9001:2000, Quality management systems—Requirements*

*5.6.3 Review output*
*The output from the management review shall include any decisions and actions related to*

*a) improvement of the effectiveness of the quality management system and its processes,*
*b) improvement of product related to customer requirements, and*
*c) resource needs.*

There are further additions mentioned to this topic in particular in ISO 26262.

*ISO TS 16949, 6: Resource management*

*6.1 Provision of resources*

*ISO 9001:2000, Quality management systems—Requirements 6 Resource management 6.1 Provision of resources The organization shall determine and provide the resources needed (a) to implement and maintain the quality management system and continually improve its effectiveness, and (b) to enhance customer satisfaction by meeting customer requirements.*

*6.2 Human resources*

*6.2.1 General*

*ISO 9001:2000, Quality management systems—Requirements 6.2 Human resources 6.2.1 General*

*Personnel performing work affecting product quality shall be competent on the basis of appropriate education, training, skills and experience.*

Sections 6.1 and 6.2 show, that also in the development stage essential requirements of people, their qualifications and the organization of product creation are well defined according to quality management systems.

*ISO TS 16949, 7.3.1.1: Multidisciplinary approach*

*The organization shall use a multidisciplinary approach to prepare for product realization, including*

- *development/finalization and monitoring of special characteristics,*
- *development and review of FMEAs, including actions to reduce potential risks, and*
- *development and review of control plans.*

*NOTE A multidisciplinary approach typically includes the organization's design, manufacturing, engineering, quality, production and other appropriate personnel.*

This cross-functional approach of ISO TS 16949 defines the basis for a necessary safety culture as the foundation of functional safety and address directly FMEAs as a mayor quality analysis method.

*ISO TS 16949, 7.3.2.3: Special characteristics*

*The organization shall identify special characteristics [see 7.3.3 d] and*

- *include all special characteristics in the control plan,*
- *comply with customer-specified definitions and symbols, and*
- *identify process control documents including drawings, FMEAs, control plans, and operator instructions with the customer's special characteristic symbol or the organization's equivalent symbol or notation to include those process steps that affect special characteristics.*

*NOTE Special characteristics can include product characteristics and process parameters.*

This chapter defines the way safety requirements were handled previously in the automobile industry. In particular "special characteristics" are still used for a safety-related design parameter of mechanic parts. The paragraph also defines the basics for the production of safety related components.

*ISO TS 16949, 7.3.3.1: Product design output—Supplemental*

*The product design output shall be expressed in terms that can be verified and validated against product design input requirements. The product design output shall include*

- *Design FMEA, reliability results,*
- *product special characteristics and specifications,*
- *product error-proofing, as appropriate,*
- *product definition including drawings or mathematically based data,*
- *product design reviews results, and*
- *diagnostic guidelines where applicable.*

This is a list of the output of product development, which had to be extended in ISO 26262 for the relevant safety related work-products and components. This output would for example be part of the safety case in a safety related product development.

*ISO TS 16949, 7.3.3.2: Manufacturing process design output*

*The manufacturing process design output shall be expressed in terms that can be verified against manufacturing process design input requirements and validated. The manufacturing process design output shall include*

- *specifications and drawings,*
- *manufacturing process flow chart/layout,*
- *manufacturing process FMEAs,*
- *control plan (see 7.5.1.1),*
- *work instructions,*
- *process approval acceptance criteria,*
- *data for quality, reliability, maintainability and measurability,*
- *results of error-proofing activities, as appropriate, and*
- *methods of rapid detection and feedback of product/manufacturing process nonconformities.*

This list adds to the necessary output/work-products during production. ISO 26262 rarely mentions any further requirements since this area is well regulated by quality management systems.

*ISO TS 16949, 7.5.1.1: Control plan*

*The organization shall*